PASS4SURES.COM

A Composite Solution With Just One Click

Microsoft

70-346 PRACTICE EXAM

Microsoft Managing Office 365 Identities and Requirements Exam

Product Questions: 296/3Case Study

Version: 23.0

Case Study: 1

Fabrikam, Inc (Case Study)

OverView

Fabrikam, inc is a financial services organization.

Fabrikam recently purchased another financial services organization named Contoso, Ltd.

Fabrikam has 2000 users. Contoso has 500 users.

Windows 10 and office 2016 are deployed to all computers.

Physical Location:

Fabrikam has an office in the United States. Contoso has an office in the United Kingdom.

The offices connect to each other by using a WAN link. Each office also connects directly to the internet.

Existing Environment:

Active Directory:

The network Fabrikam contains an Active Directory forest.

The Active Directory environment of Contoso was migrated to the Active Directory forest of Fabrikam. The forest contains three domains named fabrikam.com , contractor.fabrikam.com, and contoso.com.

All domain controllers run Windows Server 2008 R2.

All contractors outsourced by fabrikam use the user principal name (UPN) suffix of contractor.fabrikam.com. If fabrikam hires the contractor as a permanenet employee, the UPN suffix changes to fabrikam.com.

Network

The network has the following configurations:

* External IP address for the United States office: 192.168.1.100

* External IP address for the United Kingdom office: 192.168.2.100

* Internal IP address range for the United States office: 10.0.1.0/24

* Internal IP address range for the United Kingdom office : 10.0.2.0/24

Active Directory Federation Services (ADFS)

AD FS and web Application Proxies are deployed to support an app for the sales department. The app is accessed from the Microsoft Azure Portal.

Office 365 Tenant

You have an Office 365 subscription that has the following configurations:

* Organization name: Fabrikam Financial Services.

* Vanity domain: Fabrikamfinancialservices.onmicrosoft.com

* Microsoft SharePoint domain: Fabrikamfinancialservices .sharepoint.com

* Additional domain added to the subscription: Contoso.com and fabrikam.com

Requirements:

Planned Changes:

* Deploy Azure AD connect.

* Move mailboxes from Microsoft Exchange 2016 to Exchange Online.

* Deploy Azure multi-factor authentication for devices that connect from untrusted networks only.

* Customize the AD FS sign-in webpage to include the Fabrikam logo, a helpdesk phone number, and a sign=in description.

* Once all of the Fabrikam users are replicated to Azure Active Directory (Azure AD), assign an E3 license to all of the users in the United States office.

Technical Requirements:

Contoso identifies the following technical requirements:

* When a device connects from an untrusted network to https://outlook.office.com, ensure that users must type a verification code generated from a mobile app.

* Ensure that all users can access office 365 services from a web browser by using either a UPN or their primary SMTP email address.

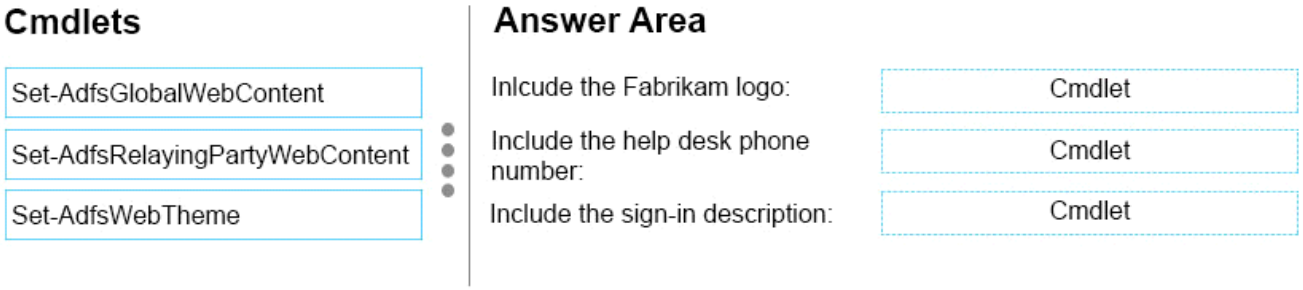
* After Azure AD connect is deployed, change the UPN suffix if all the users in the Contoso sales department to fabrikam.com.

* Ensure that administrator are notified when the health information of Exchange Online changes.

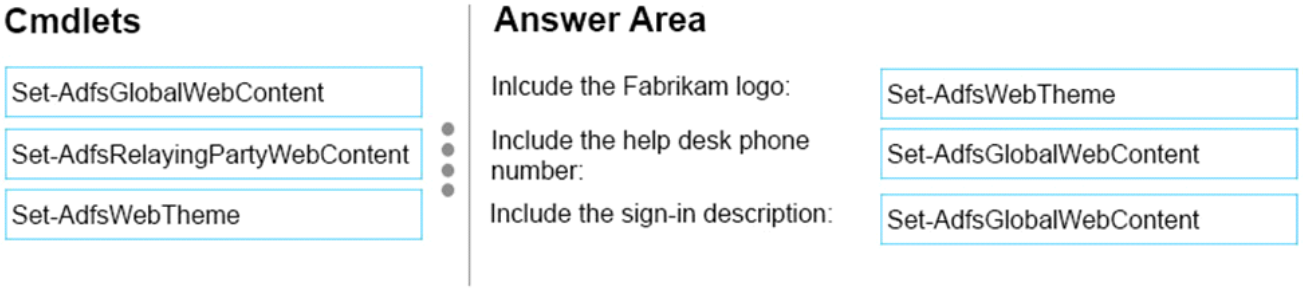
* User Office 365 reports to review previous tasks performed in Office 365.

Question: 1

DRAG DROP
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to ensure that all of the planned changes for the AD FS sign-in webpage are performed successfully.
Which cmdlet should you use to perform each change? To answer, drag the appropriate cmdlets to the correct types of change. Each cmdlet may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:



References:
https://technet.microsoft.com/en-us/library/dn280950(v=ws.11).aspx

Question: 2

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to ensure that a user named User1 can create mailboxes in Exchange Online and sites in SharePoint Online.
Solution: You add User1 to the Exchange administrator admin role.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The Exchange administrator admin role does not have the necessary privileges to create mailboxes in Exchange Online

and sites in SharePoint Online.
References:

https://support.office.com/en-us/article/About-Office-365-admin-roles-da585eea-f576-4f55-a1e0-87090b6aaa9d

Question: 3

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to ensure that a user named User1 can create mailboxes in Exchange Online and sites in SharePoint Online.
Solution: You add User1 to the Service administrator admin role.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The Service administrator admin role does not have the necessary privileges to create mailboxes in Exchange Online and sites in SharePoint Online.
References:

https://support.office.com/en-us/article/About-Office-365-admin-roles-da585eea-f576-4f55-a1e0-87090b6aaa9d

Question: 4

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to recommend a solution to meet the technical requirement for monitoring the heath information.
What should you recommend?

A. Use the Office 365 Admin app to receive push notifications.
B. From the Office 365 admin center, modify the Services and &add-ins settings.
C. From the Office 365 admin center, modify the Organization Profile settings.
D. Use the Company Portal app to receive push notifications.

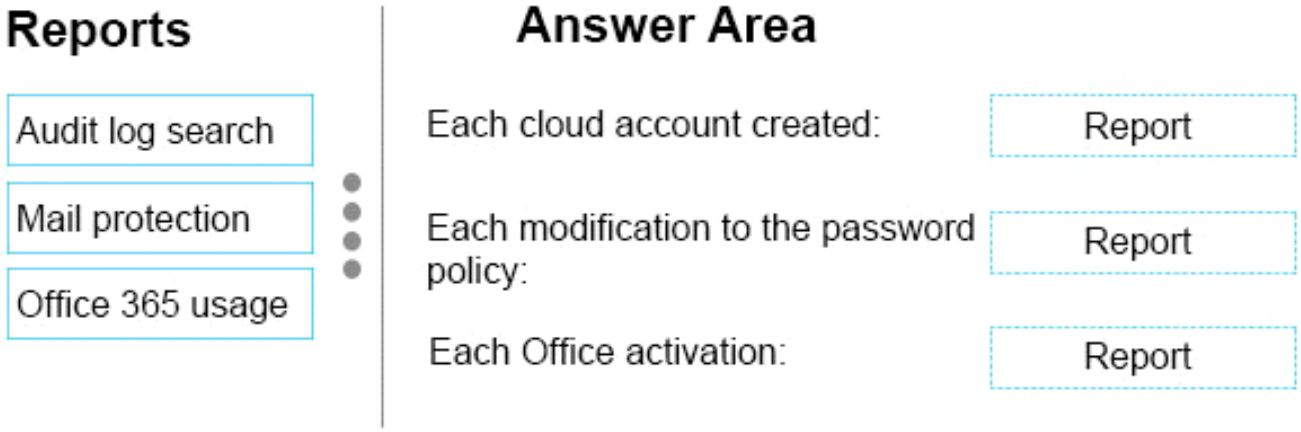
Answer: A

Explanation:
You can use the Office 365 Admin app on your mobile device to view Service health, which is a great way to stay current with push notifications.
References:
https://support.office.com/en-gb/article/How-to-check-Office-365-service-health-932ad3ad-533c-418a-b938-

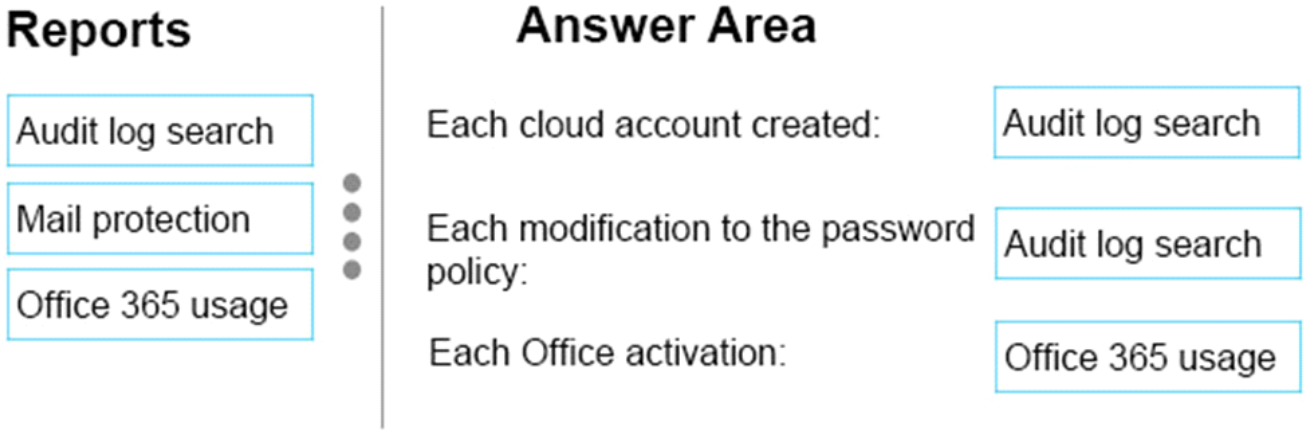
6e44e8bc33b0?ui=en-US&rs=en-GB&ad=GB

Question: 5

DRAG DROP
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to identify which report must be used to view previous tasks performed in Office 365.
Which type of report should you use for each task? To answer, drag the appropriate reports to the correct tasks. Each report may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:



Account creation falls under the user administration activities that are logged by the audit log.
Password policy modification falls under the Azure AD directory and domain related activities that are logged by the audit log.
The Office activations report is available in the Office 365 admin center.
References:
https://support.office.com/en-us/article/Search-the-audit-log-in-the-Office-365-Security-Compliance-Center-0d4d0f35-390b-4518-800e-0c7ec95e946c?ui=en-US&rs=en-US&ad=US#PickTab=Activities
https://support.office.com/en-us/article/Activity-Reports-in-the-Office-365-Admin-Center-0d6dfb17-8582-4172-a9a9-aed798150263

Question: 6

HOTSPOT

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You deploy Azure AD Connect.

You modify the UPN suffix of each sales department user to fabrikam.com.

You need to ensure that the Active Directory changes are updated in Office 365.

What command should you run? To answer, select the appropriate options in the answer area.

Answer Area

```
Set-MsolUserPrincipalName -UserPrincipalName username@
```

[▼]
- Contoso.com
- Fabrikam.com
- Fabrikamfinancialservices.onmicrosoft.com

```
-NewUserPrincipalName username@
```

[▼]
- Contoso.com
- Fabrikam.com
- Fabrikamfinancialservices.onmicrosoft.com

Answer:

Answer Area

```
Set-MsolUserPrincipalName -UserPrincipalName username@
```

[▼]
- Contoso.com
- Fabrikam.com
- Fabrikamfinancialservices.onmicrosoft.com

```
-NewUserPrincipalName username@
```

[▼]
- Contoso.com
- Fabrikam.com
- Fabrikamfinancialservices.onmicrosoft.com

The Set-MsolUserPrincipalName cmdlet is used to change the User Principal Name, or user ID, of a user. It can be used to move a user between a federated and standard domain, which results in their authentication type changing to that of the target domain.

References:

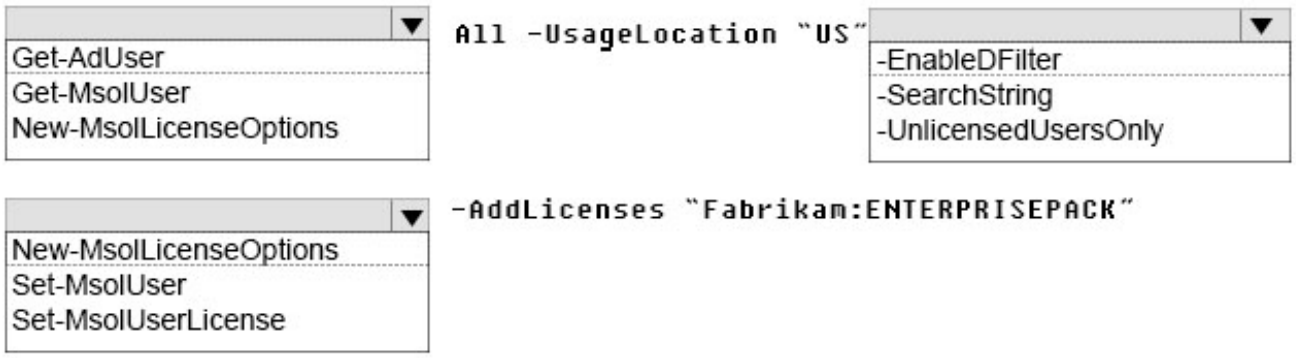
https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserprincipalname?view=azureadps-1.0

Question: 7

HOTSPOT

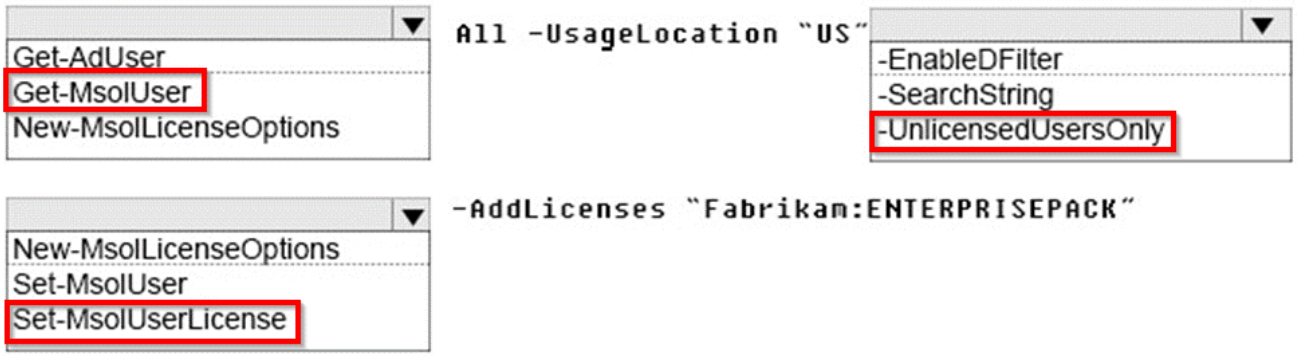
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You synchronize all of the fabrikam.com users to Azure AD.
You need to implement the planned changes for the users in the United States office.
Which command should you run? To answer, select the appropriate options in the answer area.

Answer Area



Answer:

Answer Area



The Get-MsolUser cmdlet gets an individual user or list of users from Azure Active Directory.
The –UnlicensedUsersOnly parameter indicates that only users who are not assigned a license are returned.
The Set-MsolUser cmdlet modifies a user object in Azure Active Directory.
References:
https://docs.microsoft.com/en-us/powershell/module/msonline/get-msoluser?view=azureadps-1.0
https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluser?view=azureadps-1.0

Question: 8

HOTSPOT
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to configure the AD FS servers to meet the technical requirement for accessing Office 365 from a web browser.
What command should you run? To answer, select the appropriate options in the answer area.

Answer Area

Set-AdfsAdditionalAuthenticationRule Set-AdfsClaimsProviderTrust Set-MsolAdfsContext	-TargetIdentifier "AD AUTHORITY"
-AdditionalAuthenticationRules -AdfsUserCredentials -AlternateLoginID	mail -LookupForests fabrikam.com

Answer:

Answer Area

Set-AdfsAdditionalAuthenticationRule **Set-AdfsClaimsProviderTrust** Set-MsolAdfsContext	-TargetIdentifier "AD AUTHORITY"
-AdditionalAuthenticationRules -AdfsUserCredentials **-AlternateLoginID**	mail -LookupForests fabrikam.com

The Set-AdfsClaimsProviderTrust cmdlet is used to configure the trust relationship with a claims provider. The –AlternateLoginID parameter identifies the LDAP name of the attribute that you want to use for login.
References:
https://technet.microsoft.com/en-us/library/dn479371(v=wps.630).aspx

Question: 9

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to configure the Office 365 subscription to ensure that Active Directory users can connect to Office 365 resources by using single sign-on (SSO).
Solution: You run Convert-MsolFederatedUser for all users.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The Convert-MsolFederatedUser cmdlet updates a user in a domain that was recently converted from single sign-on to standard authentication type. This option will not meet the objective of the question.
References:
https://docs.microsoft.com/en-us/powershell/module/msonline/convert-msolfederateduser?view=azureadps-1.0

Question: 10

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to configure the Office 365 subscription to ensure that Active Directory users can connect to Office 365 resources by using single sign-on (SSO).
Solution: You run Convert-MsolDomainToFederated for the fabrikam.com domain and the contoso.com domain.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
The Convert-MSOLDomainToFederated cmdlet converts the specified domain from standard authentication to single sign-on. This includes configuring the relying party trust settings between the Active Directory Federation Services 2.0 server and Microsoft Online. As part of converting a domain from standard authentication to single sign-on, each user must also be converted. This conversion happens automatically the next time a user signs in. No action is required by the administrator.
References:
https://docs.microsoft.com/en-us/powershell/module/msonline/convert-msoldomaintofederated?view=azureadps-1.0

Question: 11

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to configure the Office 365 subscription to ensure that Active Directory users can connect to Office 365 resources by using single sign-on (SSO).
Solution: You run Convert-MsolDomainToFederated for the contractor.fabrikam.com domain and the fabrkamfinancialservices.onmicrosoft.com domain.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The Contoso.com and fabrikam.com domains are being added to the Office 365 subscription, not the contractor.fabrikam.com domain. Fabrikamfinancialservices.onmicrosoft.com is the vanity domain for the Office 365 subscription.

Question: 12

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to configure the Office 365 subscription to ensure that Active Directory users can connect to Office 365 resources by using single sign-on (SSO).
Solution: You run Convert-MsolDomainToStandard for the fabrikam.com domain and the contoso.com domain.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

Question: 13

You need to modify the Office 365 subscription to support the planned changes for the devices that connect from untrusted networks.
You enable Azure multi-factor authentication for all of the users in the subscription.
What should you do next from the Office 365 portal?

A. Add a trusted domain.
B. Set the Trusted IPs to 10.0.1.0/24 and 10.0.2.0/24.
C. Set the Trusted IPs to 192.168.1.100/32 and 192.168.2.100/32
D. Convert the fabrikam.com domain to a federated domain.

Answer: C

Explanation:

Adding trusted IP's is excluding a set of addresses from MFA. MFA is hosted outside your LAN so you communicate with the service using your public IP's.
The case tells us that the external IP's are 192.168.1.100 and 192.168.2.100 so these should be added as trusted IP's in MFA.
References:
https://docs.microsoft.com/nl-nl/azure/multi-factor-authentication/multi-factor-authenticationwhats-next#trusted-ips

Question: 14

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to ensure that a user named User1 can create mailboxes in Exchange Online and sites in SharePoint Online.
Solution: You add User1 to the SharePoint administrator admin role.
Does this meet the goal?

A. Yes
B. No

Answer: B

Case Study: 2

Contoso, Ltd (Case Study)

Background

Contoso, Ltd. is a global manufacturing company with headquarters in Dallas. All sales users are located at the headquarters. Currently all Contoso, Ltd. users use the following on-premises services:

- Microsoft Exchange Server 2016
- Microsoft Skype for Business Server 2015
- Active Directory Domain Services (AD DS) domain for contoso.com

Many temporary workers are hired and terminated on a regular basis at the Dallas location, Contoso, Ltd. purchases two other manufacturing companies, Fabrikam, Inc. and ADatum Corporation. Fabrikam, Inc. is based in London. Fabrikam, Inc. has an on-premises third-party email system that uses @fabrikam.com for all email addresses. Fabrikam, Inc. does not have an Active Directory domain.

ADatum Corporation is based in Paris. The company is in the process of migrating users to Exchange Online. They plan to migrate users to Microsoft OneDrive for Business for file storage and sharing. All ADatum Corporation account identities will be cloud based.

You deploy Microsoft Office 2016 client apps to all corporate devices.

In preparation for the deployment of Office 365 services, you set up the latest version of Azure Active Directory (Azure AD) Connect for the contoso.com domain. The application runs on Server1.contoso.com

and uses a Microsoft SQL Server database instance that runs on Server2.contoso.com. The sync schedule is configured to synchronize every two hours.

You purchase the following four servers for future needs: Server3, Server4, Server5, and Server6. All new servers for the contoso.com domain must run Windows Server 2012 R2.

Business Requirements

Contoso, Ltd. users must be able to store and share personal documents that are accessible from any web browser or mobile device. Fabrikam, Inc. users must be able to send individual instant messages as well as use group chat workspaces.

Office 365

New services should be implemented in Office 365 when possible. There is also a strong push to move existing services to Office 365, but there is currently no money in the budget for data migration. The least expensive Office 365 plan must be used whenever possible.

Password policies

You must implement the following password policies for ADatum Corporation users.

Policy	Value
Set user passwords to never expire	No
Days before passwords expire	180
Days before user is notified about expiration	14

Contoso Sync

You receive reports that new users are not granted access to Office 365 resources fast enough. You must ensure that new accounts are provisioned as quickly as possible.

You observe that the accounts for many temporary workers have not been deprovisioned correctly. You need to ensure terminated users have their access and accounts removed. You must ensure that up to 1,000 accounts can be deleted correctly during each Azure AD Connect sync cycle. You must ensure that deletions of over 1,000 accounts at a time cannot occur.

Single Sign-On

Contoso.com users need to start using sign-on (SSO) for Office 365 resources so they can authenticate against the on-premises Active Directory. Any solution needs to be redundant. Any Internet-facing servers need to reside in the perimeter network.

Problem Statements

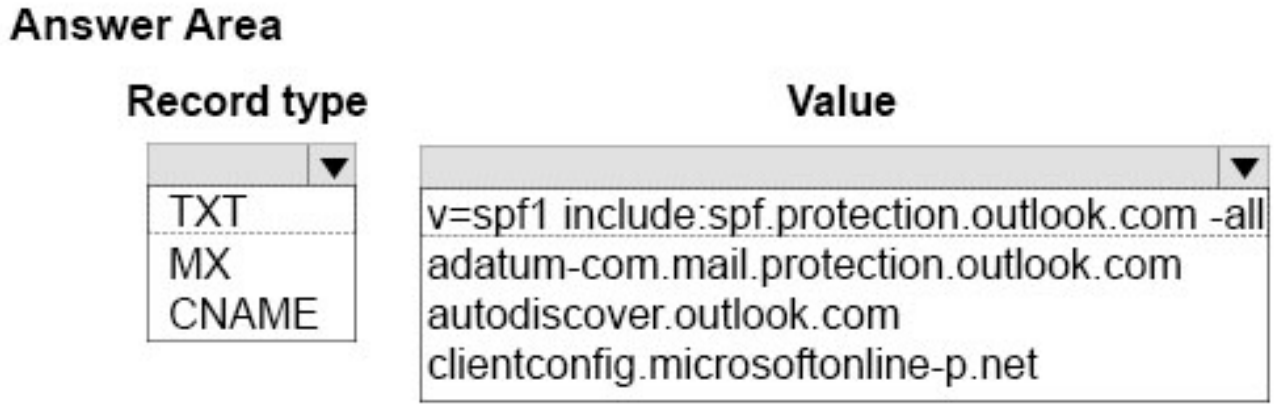
Authentication Fallback

Sales users report that they were not able to access any Office 365 resources. Contoso.com users must be able to access Office 365 resources if the on-premises authentication resources are down or unavailable. You also need to quickly resume SSO authentication when on-premises servers are available again.

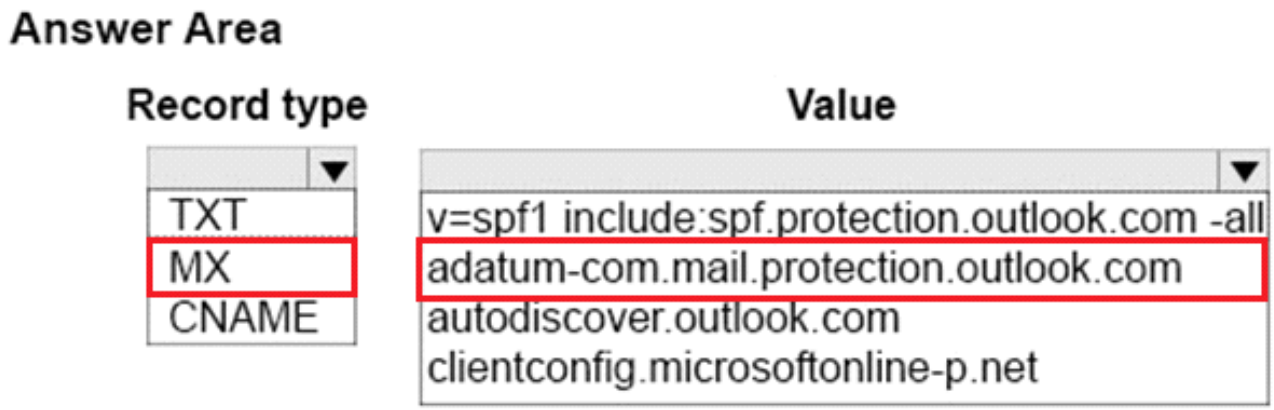
ADatum Corporation users report issues sending and receiving emails. Some business partners report that emails from ADatum Corporation are rejected because the receiving server cannot validate that emails come from an authorized messaging server.

Question: 1

HOTSPOT
You need to create a DNS record to resolve the email issues for ADatum Corporation users.
How should you configure the DNS record? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



MX (mail exchanger) records offer an simple way for mail servers to know where to send email. If you want Office 365 to receive all email addressed to anyone@contoso.com, the MX record for contoso.com should point to Office 365, and it will look like the following example:
Hostname: contoso-com.mail.protection.outlook.com
Priority: 0
TTL: 1 hour
References:
https://support.office.com/en-us/article/Create-DNS-records-at-Register365-for-Office-365-004030b4-10ad-4026-96e7-011b6afc7e73#bkmk_add_mx
https://technet.microsoft.com/en-us/library/jj937232(v=exchg.150).aspx

Question: 2

HOTSPOT
You need to configure the single sign-on environment for Contoso.
Which certificate type and DNS entry should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Action	Option
Certificate to install:	trusted 3rd party SSL self-signed SSL Active Directory Certificate Services issued SSL
DNS entry:	sts.contoso.com sts.fabrikam.com sts.contoso.onmicrosoft.com sts.fabrikam.onmicrosoft.com

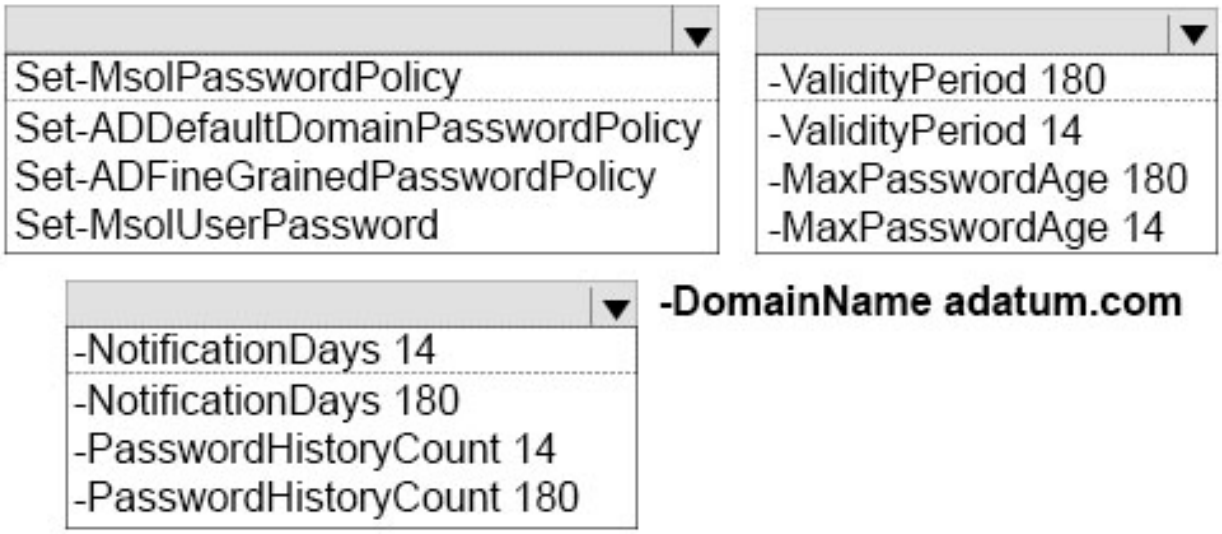
Answer:

Box 1: self-signed SSL
Box 2: sts.contoso.com
The token-signing certificate must contain a private key that chains to a trusted root in the FS. AD FS creates a self-signed certificate by default.
It is recommend that the self-signed token-signing certificate generated by AD FS is used.
Microsoft best practices recommends that you use the host name, STS (secure token service). ie. sts.domain.com.
References:
https://www.digicert.com/csr-creation-microsoft-office-365.htm
https://support.office.com/en-us/article/Plan-for-third-party-SSL-certificates-for-Office-365-b48cdf63-07e0-4cda-8c12-4871590f59ce?ui=en-US&rs=en-US&ad=US

Question: 3

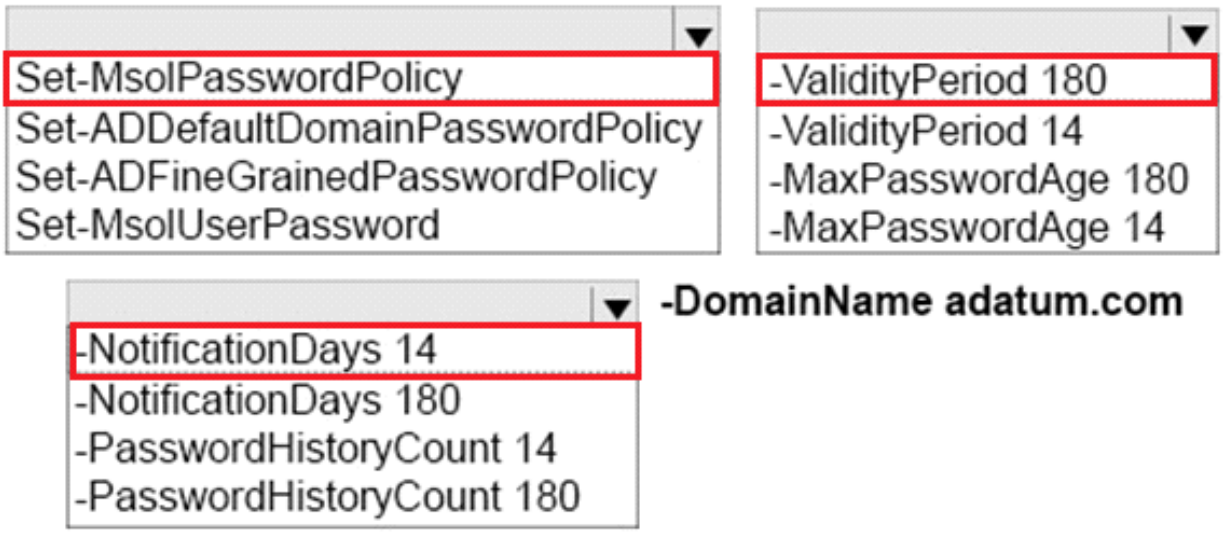
HOTSPOT
You need to implement the password policy for ADatum Corporation users.
How should you complete the Windows PowerShell command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Set-MsolPasswordPolicy -ValidityPeriod 180 -NotificationDays 14 -DomainName adatum.com
The Set-MsolPasswordPolicy cmdlet is used to update the password policy of a specified domain or tenant.
The –ValidityPeriod parameter stipulates the length of time that a password is valid before it must be changed.
The –NotificationDays parameter stipulates the number of days before the password expiration date that triggers when users receive their first notification that their password will soon expire.
References:
https://docs.microsoft.com/en-us/powershell/module/msonline/set-msolpasswordpolicy?view=azureadps-1.0

Question: 4

You enable password synchronization for Contoso, Ltd.
You need to implement the authentication requirements for users in the sales team.
Which Windows PowerShell command should you run?

A. Set-MsolDomainAuthentication -DomainName fabricam.com -Authentication Managed
B. Convert-MsolDomainToStandard -DomainName contoso.com
C. Set-MsolDomainAuthentication -DomainNAme contoso.com -Authentication Managed
D. Convert-MsolDomainToStandard -DomainNAme fabricam.com

Answer: C

Explanation:
The domain being associated with Office 365 must be managed by Office 365 before single sign-on and provisioning can be enabled for your users.
References:
https://support.onelogin.com/hc/en-us/articles/203748160-Disabling-ADFS-federation-to-enable-OneLogin-SSO-with-Office-365

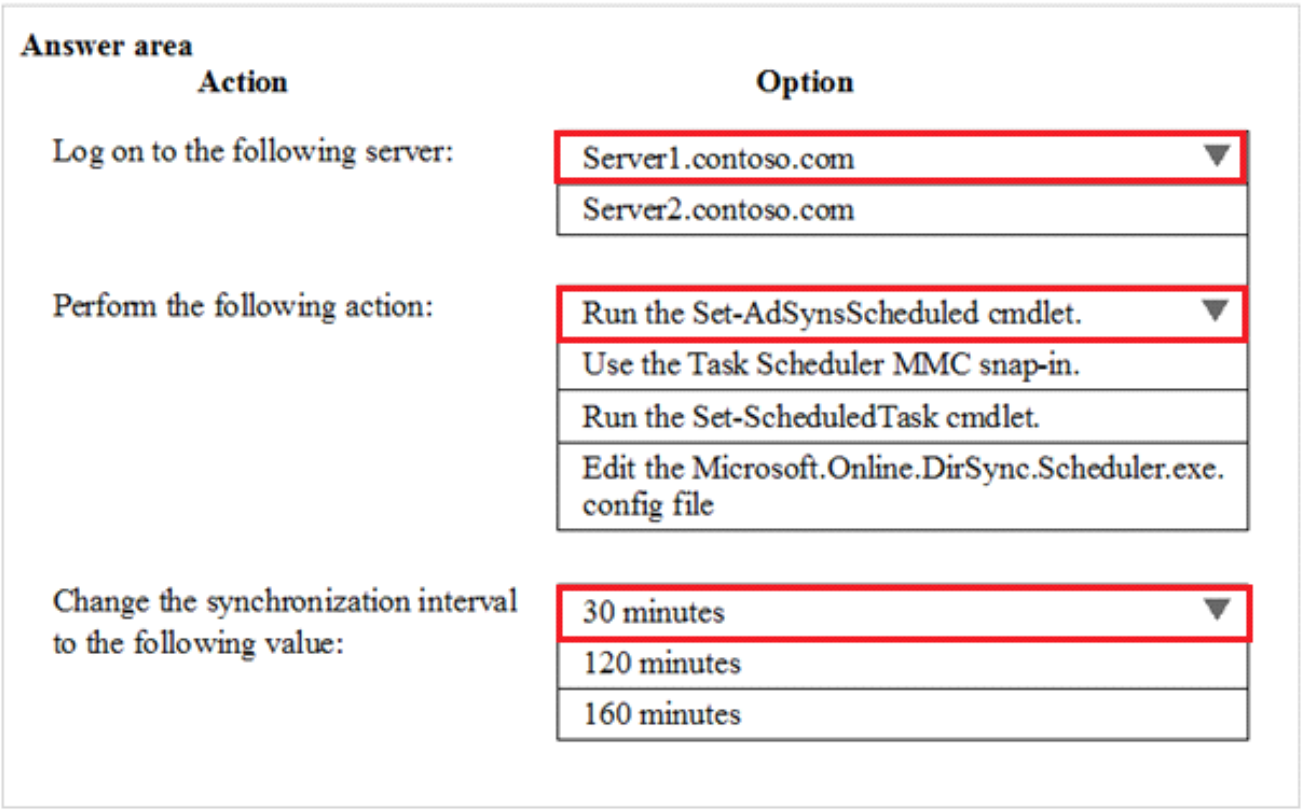
Question: 5

HOTSPOT
You need to ensure that new accounts are provisioned correctly.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each selection is worth one point.

Answer area

Action	Option
Log on to the following server:	Server1.contoso.com Server2.contoso.com
Perform the following action:	Run the Set-AdSynsScheduled cmdlet. Use the Task Scheduler MMC snap-in. Run the Set-ScheduledTask cmdlet. Edit the Microsoft.Online.DirSync.Scheduler.exe. config file
Change the synchronization interval to the following value:	30 minutes 120 minutes 160 minutes

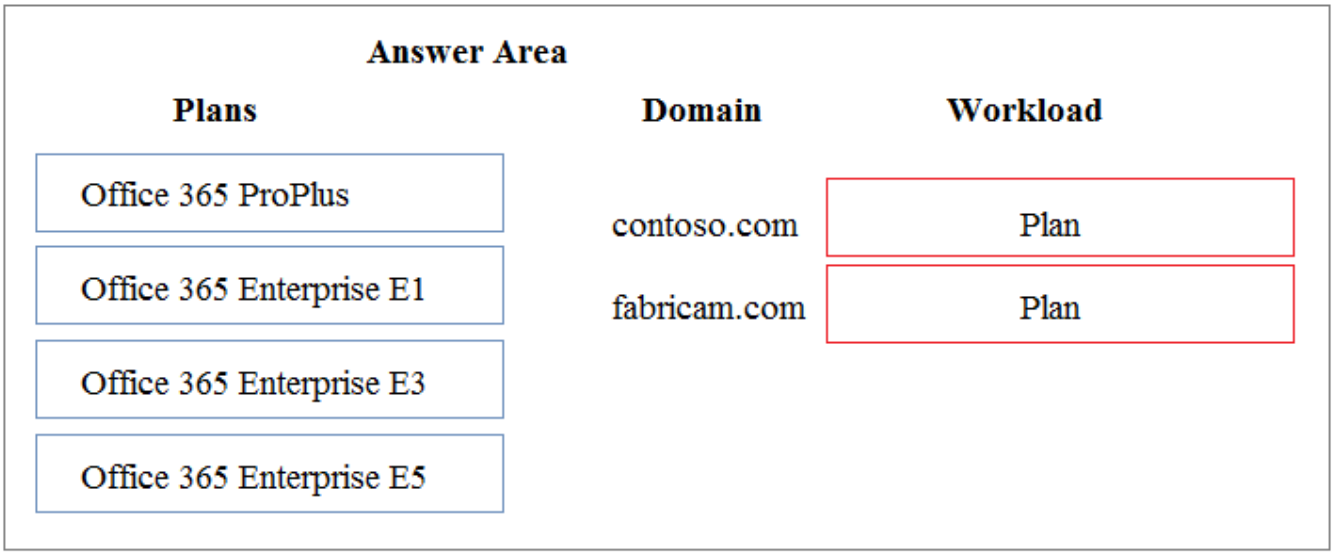
Answer:



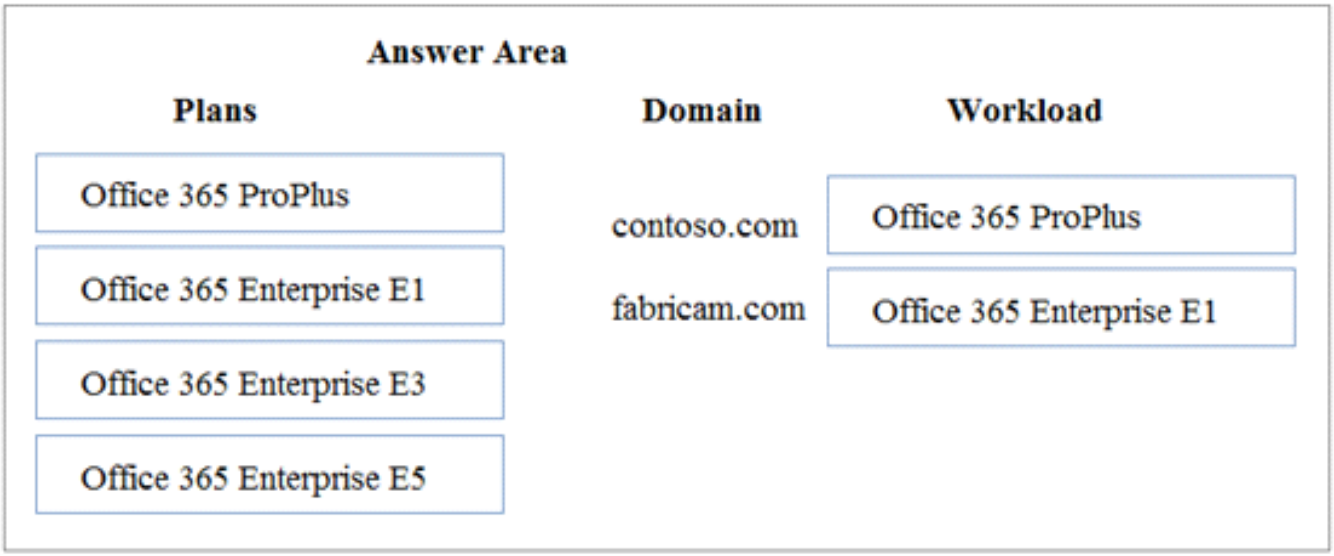
The Azure Active Directory (Azure AD) Connect application for the contoso.com domain runs on Server1.contoso.com.
The Set-ADSyncScheduler cmdlet allows you to modify the CustomizedSyncCycleInterval parameter.
The question states: "You receive reports that new users are not granted access to Office 365 resources fast enough. You must ensure that new accounts are provisioned as quickly as possible." Since the scheduler is already configured to sync every 2 hours (120 min.), 30 minutes should be configured.
References:
https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-feature-scheduler

Question: 6

DRAG DROP
You need to enable the new features in Office 365 for contoso.com and fabricam.com users.
Which plans should you implement? To answer, drag the appropriate plans to the correct domains. Each plan may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:



The scenario states: "Contoso, Ltd. users must be able to store and share personal documents that are accessible from any web browser or mobile device. Fabrikam, Inc. users must be able to send individual instant messages as well as use group chat workspaces." The scenario also states: "The least expensive Office 365 plan must be used whenever possible."

Office 365 ProPlus offers Office applications plus cloud file-storage and sharing.

Office 365 Enterprise E1 offers email, file storage and sharing, Office Online, meetings and IM, and more.

References:

https://products.office.com/en-za/business/compare-more-office-365-for-business-plans

Question: 7

HOTSPOT

You need to provision an account for a new sales executive at Contoso, Ltd.

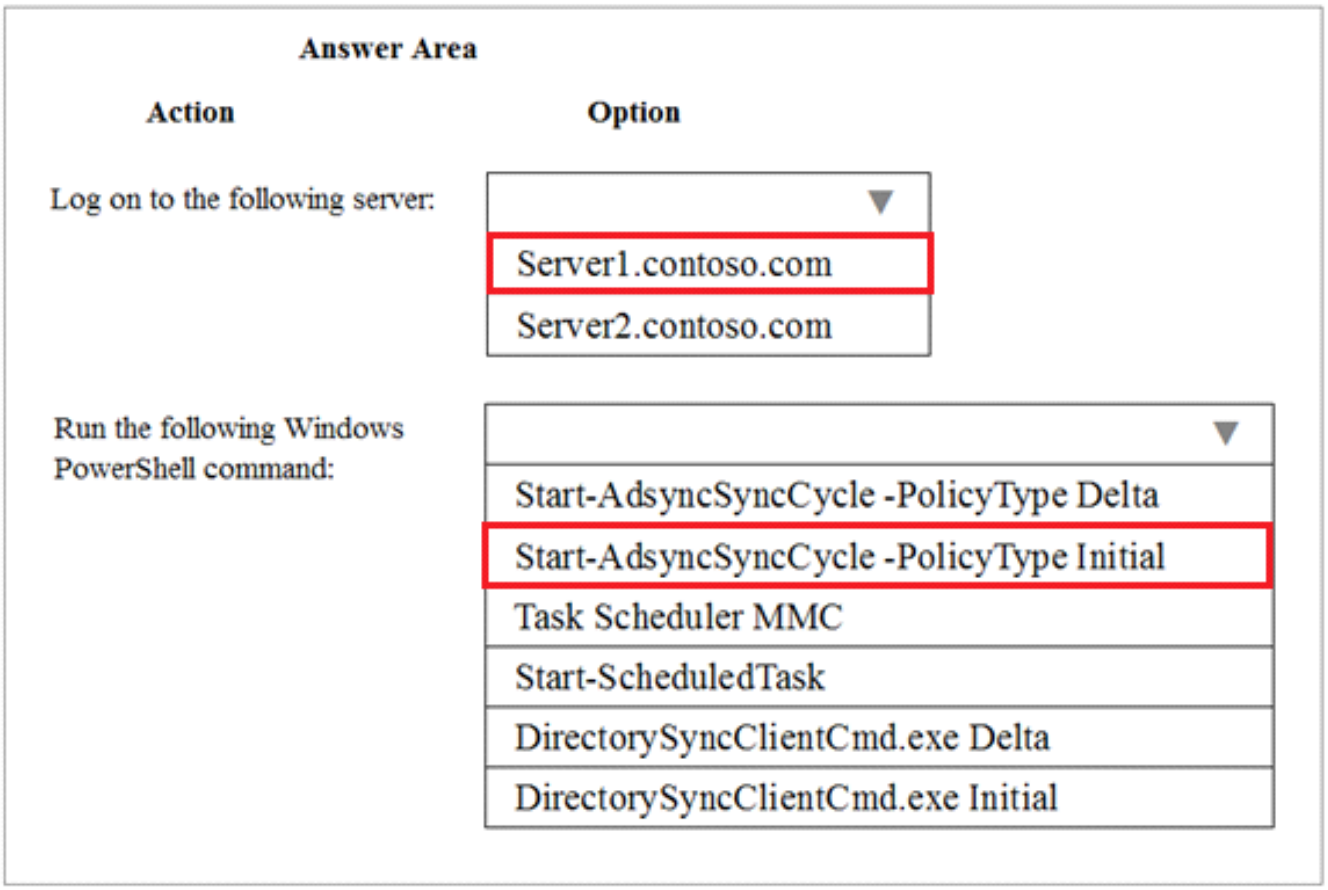
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Action	Option
Log on to the following server:	Server1.contoso.com Server2.contoso.com
Run the following Windows PowerShell command:	Start-AdsyncSyncCycle -PolicyType Delta Start-AdsyncSyncCycle -PolicyType Initial Task Scheduler MMC Start-ScheduledTask DirectorySyncClientCmd.exe Delta DirectorySyncClientCmd.exe Initial

Answer:



The Azure Active Directory (Azure AD) Connect application for the contoso.com domain runs on Server1.contoso.com. The Start-ADSyncSyncCycle -PolicyType Initial command initiates a full sync cycle. A full sync cycle is required when you have made one of the following configuration changes:
An account falls under objects.
References:
https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-feature-scheduler#start-the-scheduler

Question: 8

You need to implement an authentication solution for contoso.com users.
What should you do?

A. Install two Active Directory Federation Services (AD FS) servers and two AD FS Proxy servers.
B. Install a second Azure AD Connect server. Add a second SQL Server instance in an Always On Failover Cluster and implement password sync.
C. Install two Active Directory Federation Services (AD FS) servers and two Web Application Proxy (WAP) servers.
D. Install a single Active Directory Federation Services (AD FS) server and a single Web Application Proxy (WAP) server.

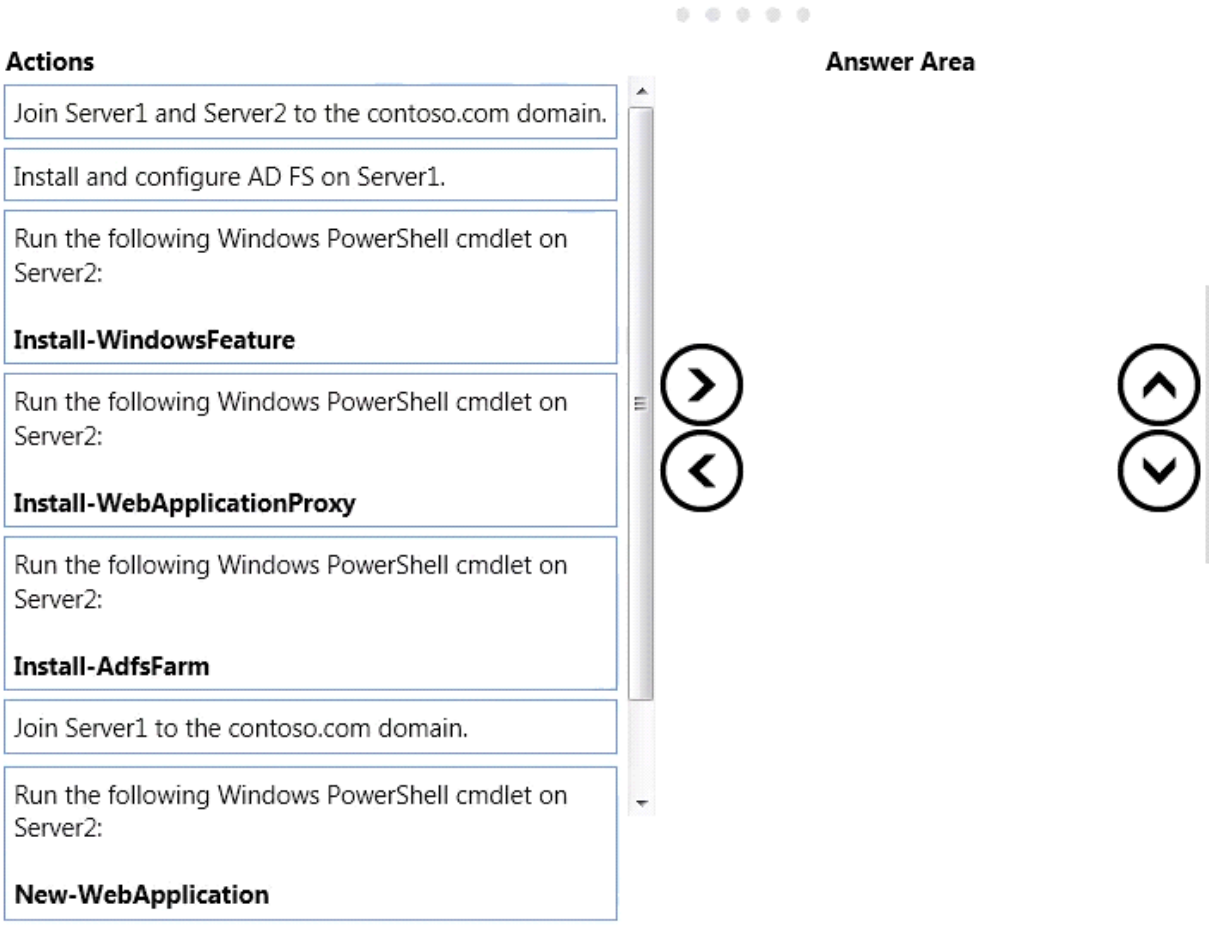
Answer: A

Case Study: 3

Mix Questions

Question: 1

DRAG DROP
Contoso, Ltd. has an Office 365 tenant. The company has two servers named Server1 and Server2 that run Windows 2012 R2 Server. The servers are not joined to the contoso.com domain. Server2 is deployed to the perimeter network.
You install Secure Sockets Layer (SSL) certificates on both servers.
You must use Integrated Windows authentication
You need to install and configure all AD FS components in the environment.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Box 1: Install and Configure AD FS on Server1.
Box 2: Join Server1 to the contoso.com domain
Box 3: Run the following Windows PowerShell cmdlet on Server2:
Install-WindowsFeature
Box 4: Run the following Windows PowerShell cmdlet on Server2:
Install-WebApplicationproxy
Note:
Prepare the Base Servers
Box 1, Box 2: AD FS Server

Box 3, Box 4: AD FS Proxy Server
Once the necessary WAP role services are installed, we are then able to launch the Web Application Proxy Wizard to configure WAP.
Note:

Question: 2

A company has an Office 365 tenant and uses Exchange Online and Skype for Business Online.
User1 is scheduling a Skype meeting with User2. User 1 is not able to see availability information for User2.
You need to troubleshoot the issue.
What should you use?

A. Microsoft Skype for Business Connectivity Analyzer Tool
B. OCSLogger
C. ClsController
D. Remote Connectivity Analyzer

Answer: C

Explanation:
Centralized Logging Service (CLS) is a new feature in Lync Server 2013. It provides a mechanism to enable/disable logging across all Skype for Business servers in a deployment from a single interface and to search the resulting logs from the same interface.
You specify what should be logged based on the scenario you want to investigate. The scenarios supported are AlwaysOn, MediaConnectivity, ApplicationSharing, AudioVideoConferencingIssue, HybridVoice, IncomingAndOutgoingCall, VoiceMail, IMAndPresence, AddressBook,DeviceUpdate, LYSSAndUCS, CLS, SP, WAC, UserReplicator, HostedMigration, MonitoringAndArchiving, LILRLegacy, LILRLYSS, MeetingJoin, RGS, CPS, XMPP and CAA.

Question: 3

You have an Exchange Online tenant. User1 reports that they are not able to check their email. Other users can check their email.
You remotely connect to User1's session.
You need to troubleshoot why the user cannot check his email.
What should you use?

A. POP Email test
B. Outlook Connectivity test
C. Microsoft Remote Connectivity Analyzer
D. Microsoft Connectivity Analyzer
E. Outlook Autodiscover test
F. IMAP Email test

Answer: C

Explanation:
Microsoft Remote Connectivity Analyzer (https://testconnectivity.microsoft.com/) can test incoming and outgoing e-mail.
References:
https://testconnectivity.microsoft.com/

Question: 4

You have an Exchange Online tenant.
You must identify mailboxes that are no longer in use.
You need to locate the inactive mailboxes.
Which Windows PowerShell command should you run?

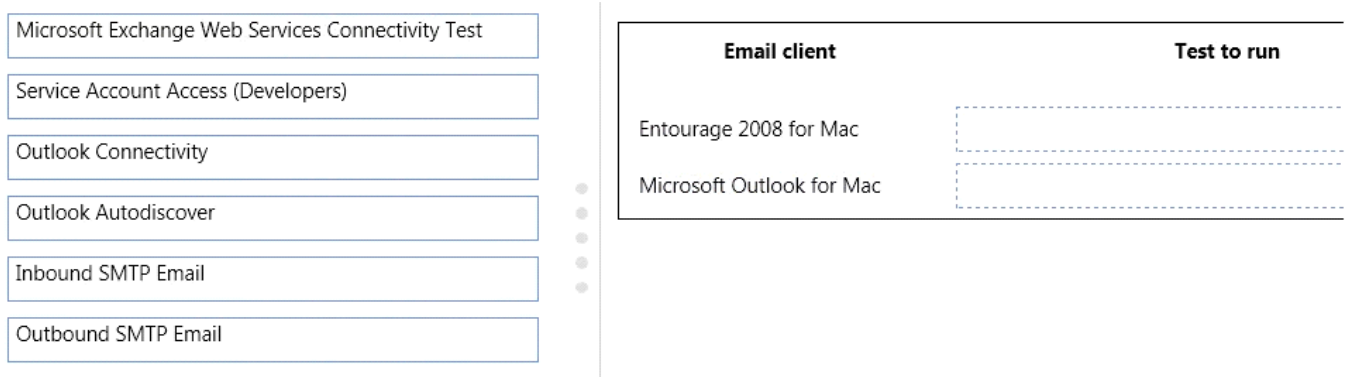
A. Get-StaleMailboxReport-StartDate
B. Get-MailboxActivityReport-StartDate
C. Get-MailboxActivityReport-Expression
D. Get-MailboxActivityReport-EndDate

Answer: A

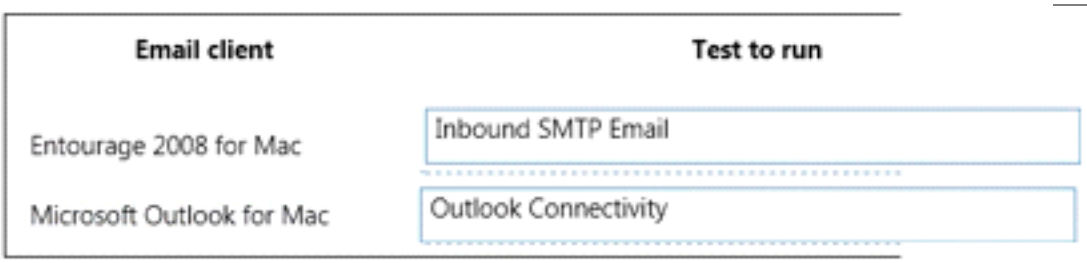
Explanation:
Use the Get-StaleMailboxDetailReport cmdlet to view mailboxes that haven't been accessed for at least 30days.
The StartDate parameter specifies the start date of the date range.

Question: 5

DRAG DROP
A graphic design agency has an Office 365 tenant. The agency uses only computers that run the Apple Macintosh operating system. Some users have Microsoft Entourage 2008 for Mac, and some have Microsoft Outlook for Mac.
All users report that they cannot access Exchange Online to check their email.
You need to run test connectivity for all users to identify the problem. You need to use the Microsoft Remote Connectivity Analyzer and the credentials of the users.
What should you do? To answer, drag the appropriate test to run to the correct email client. Each test may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:



Question: 6

A company has an Office 365 tenant. You implement two-factor authentication for all users. You hire an employee named User1 to track service usage and status.
User1 must be able to monitor the status of the services over a period of time by using a report. User1 does not have administrator access.
You need to provide a report for User1.
Which report solution should you choose?

A. downloadable spreadsheet
B. REST reporting web service
C. reporting Windows PowerShell cmdlets
D. Office 365 admin center

Answer: B

Explanation:
The Office 365 Reporting web service enables developers to integrate information on email and spam, antivirus activity, compliance status, and Skype for Business Online activities into their custom service reporting applications and web portals.
All the reports available in the admin portal, within the downloadable Microsoft Excel spreadsheets, and those accessed through Windows PowerShell cmdlets, are accessible using the Reporting web service.

Question: 7

A company has an Office 365 tenant that has an Enterprise E1 subscription.
You use single sign-on for all user accounts. You plan to migrate all services to Office 365.
You need to ensure that all accounts use standard authentication.
Which Windows PowerShell cmdlet should you run?

A. Set-MsolUser
B. Redo-MsolProvisionUser
C. Set-MsolUserLicense
D. Set-MsolUserPrincipalName
E. Convert-MsolFederatedUser
F. Set-MailUser
G. Set-LinkedUser
H. New-MsolUser

Answer: E

Explanation:
The Convert-MsolFederatedUser cmdlet is used to update a user in a domain that was recently converted from single sign-on (also known as identity federation) to standard authentication type.

Question: 8

A company has an Office 365 tenant that has an Enterprise E1 subscription. You configure the policies required for self-service password reset.
You need to ensure that all existing users can perform self-service password resets.
Which Windows PowerShell cmdlet should you run?

A. Set-MsolUser
B. Redo-MsolProvisionUser
C. Set-MsolUserLicense
D. Set-MsolUserPrincipalName
E. Convert-MsolFederatedUser
F. Set-MailUser
G. Set-LinkedUser
H. New-MsolUser

Answer: C

Explanation:
Self-service password reset with on-premises write-back is a Premium-only feature.
Example:
The following command adds the Office 365 for enterprises license to the user.
Set-MsolUserLicense -UserPrincipalName user@contoso.com -AddLicenses "Contoso:ENTERPRISEPACK"
Note: The Set-MsolUserLicense cmdlet can be used to adjust the licenses for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.
References:
https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0

Question: 9

A company has an Office 365 tenant that has an Enterprise E1 subscription. The company has offices in several different countries.
You need to restrict Office 365 services for existing users by location.
Which Windows PowerShell cmdlet should you run?

A. Set-MsolUser
B. Redo-MsolProvisionUser
C. Set-MsolUserLicense
D. Set-MsolUserPrincipalName
E. Convert-MsolFederatedUser
F. Set-MailUser
G. Set-LinkedUser
H. New-MsolUser

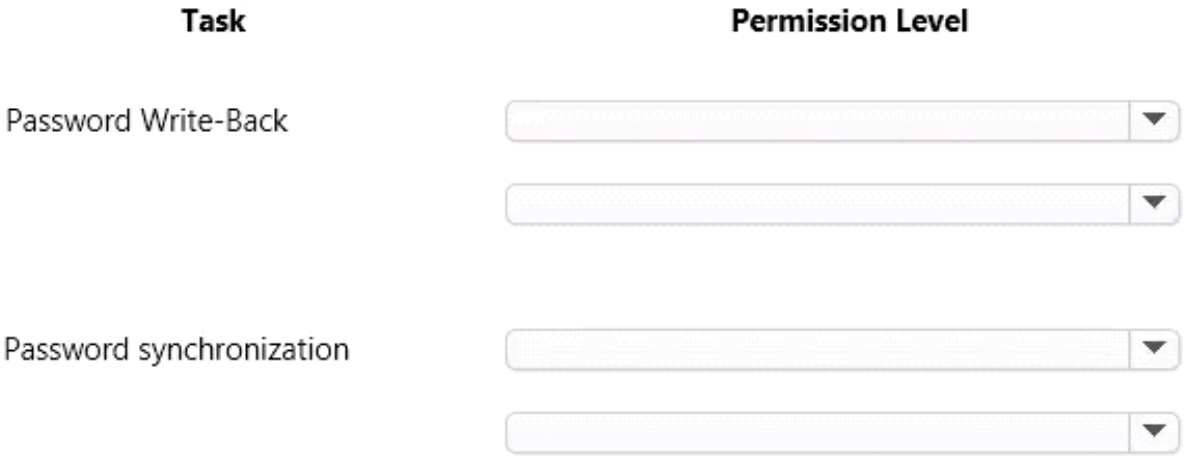
Answer: A

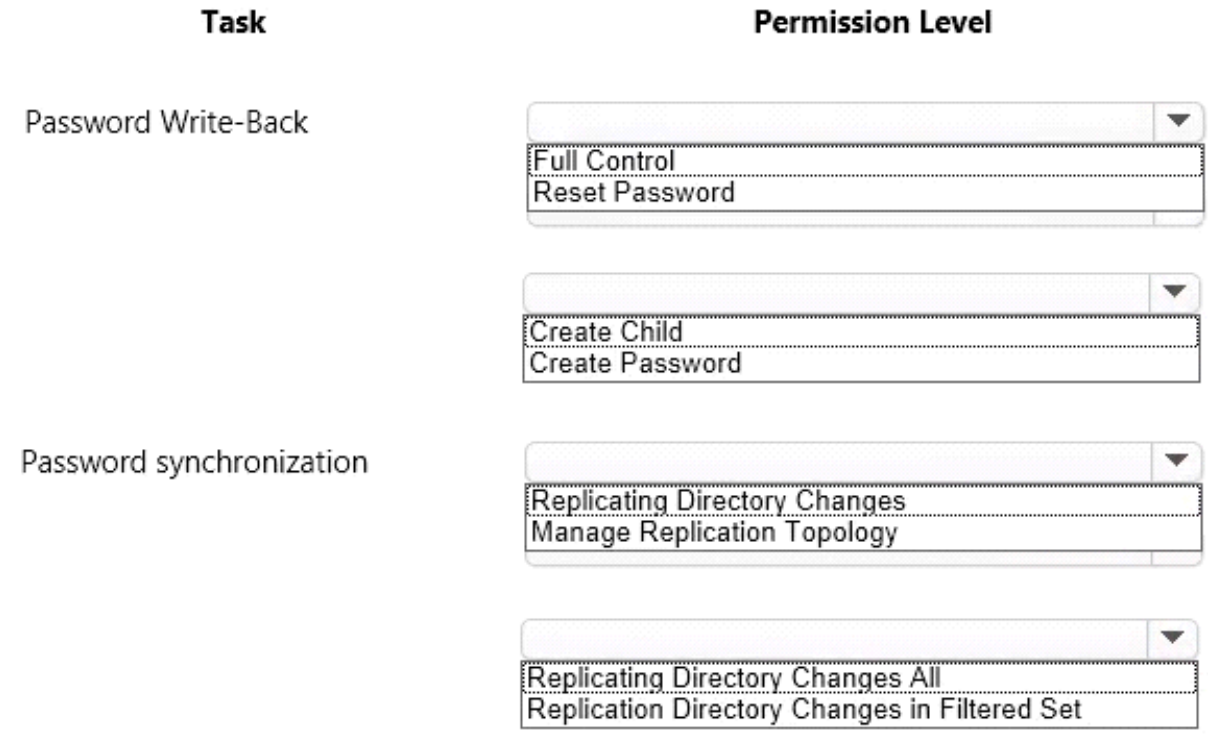
Explanation:
The Set-MsolUser cmdlet is used to update a user object.
Example: The following command sets the location (country) of this user. The country must be a two-letter ISO code. This can be set for synced users as well as managed users.
Set-MsolUser -UserPrincipalName user@contoso.com -UsageLocation "CA"
Note:
Some organizations may want to create policies that limit access to Microsoft Office 365 services, depending on where the client resides.
Active Directory Federation Services (AD FS) 2.0 provides a way for organizations to configure these types of policies. Office 365 customers using Single Sign-On (SSO) who require these policies can now use client access policy rules to restrict access based on the location of the computer or device that is making the request. Customers using Microsoft

Online Services cloud User IDs cannot implement these restrictions at this time.

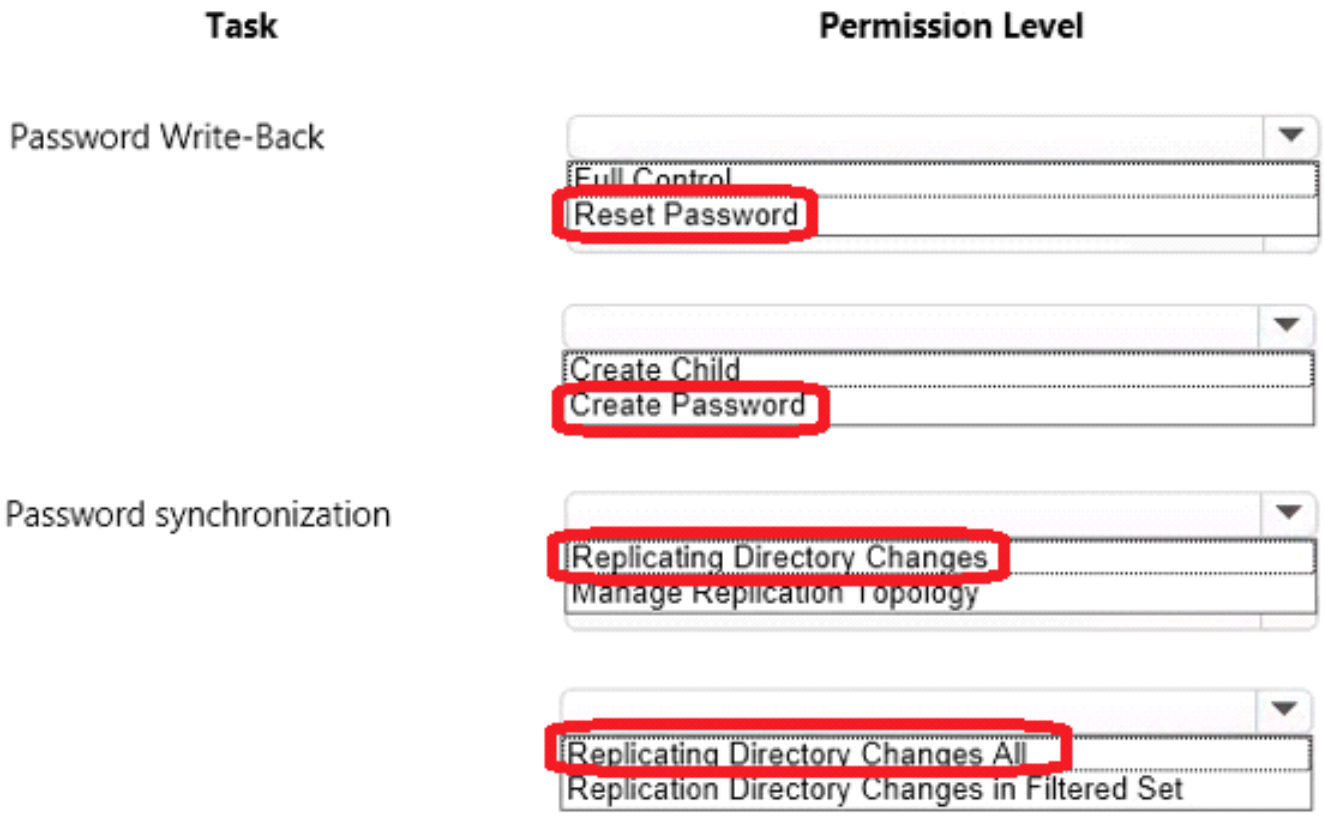
Question: 10

HOTSPOT
A company plans to synchronize users in an existing Active Directory organizational unit with Office 365.
You must configure the Azure Active Directory Connect with password sync
You need to ensure that the service account has the minimum level of permissions required.
Which two permission levels should you assign to the account for each task? To answer, select the appropriate permission level from each list in the answer area.





Answer:



Password Write-Back
For each forest you have configured in Azure AD Sync, the account you have specified for a forest in the wizard must be given the "Reset-Password" and "Change Password" extended rights on the root object of each domain in the forest.
Permissions for password synchronization
If you want to enable password synchronization between your on-premises AD DS and your Azure Active Directory for your users, you need to grant the following permissions to the account that is used by Azure AD Sync to connect to your AD DS:

Question: 11

You have an Office 365 tenant that uses an Enterprise E3 subscription. You activate Azure Rights Management for the tenant.
You must test the service with the Development security group before you deploy Azure Rights Management for all users.
You need to enable Azure Rights Management for only the Development security group.
Which Windows PowerShell cmdlet should you run?

A. Enable-Aadrm
B. New-AadrmRightsDefinition
C. Enable-AadrmSuperUserFeature
D. Add-AadrmSuperUser
E. Set-AadrmOnboardingControlPolicy

Answer: E

Explanation:
The Set-AadrmOnboardingControlPolicy cmdlet sets the policy that controls user on-boarding for Azure Rights

Management. This cmdlet supports a gradual deployment by controlling which users in your organization can protect content by using Azure Rights Management.
Example:
Restrict Azure RMS to users who are members of a specified group
This command allows only users that are members of the security group withthe specified object ID to protect content by using Azure Rights Management. The command applies to Windows clients and mobile devices.
Windows PowerShell
PS C:\> Set-AadrmOnboardingControlPolicy -UseRmsUserLicense $False-SecurityGroupObjectId "f
References:
https://docs.microsoft.com/en-us/powershell/module/aadrm/set-aadrmonboardingcontrolpolicy?view=azureipps

Question: 12

You have a legacy application that needs to send email to employees. The legacy application runs on a client computer.
The legacy application must send email by using IMAP through Exchange Online.
You need to identify the correct host name and port information.
Which settings should you use?

A. Imap.office365.com and port 993
B. Imap.office365.com and port 143
C. Outlook.office365.com and port 993
D. Outlook.office365.com and port 143

Answer: C

Explanation:
For Office 365for business, use the following settings.
IMAP4
outlook.office365.com
993 implicit

Question: 13

A company has an Office 365 tenant. You plan to distribute the Office 365 ProPlus client to users.
The client machines do not normally have Internet access.
You need to activate the Office 365 ProPlus installations and ensure that the licenses remain active.
What should you do?

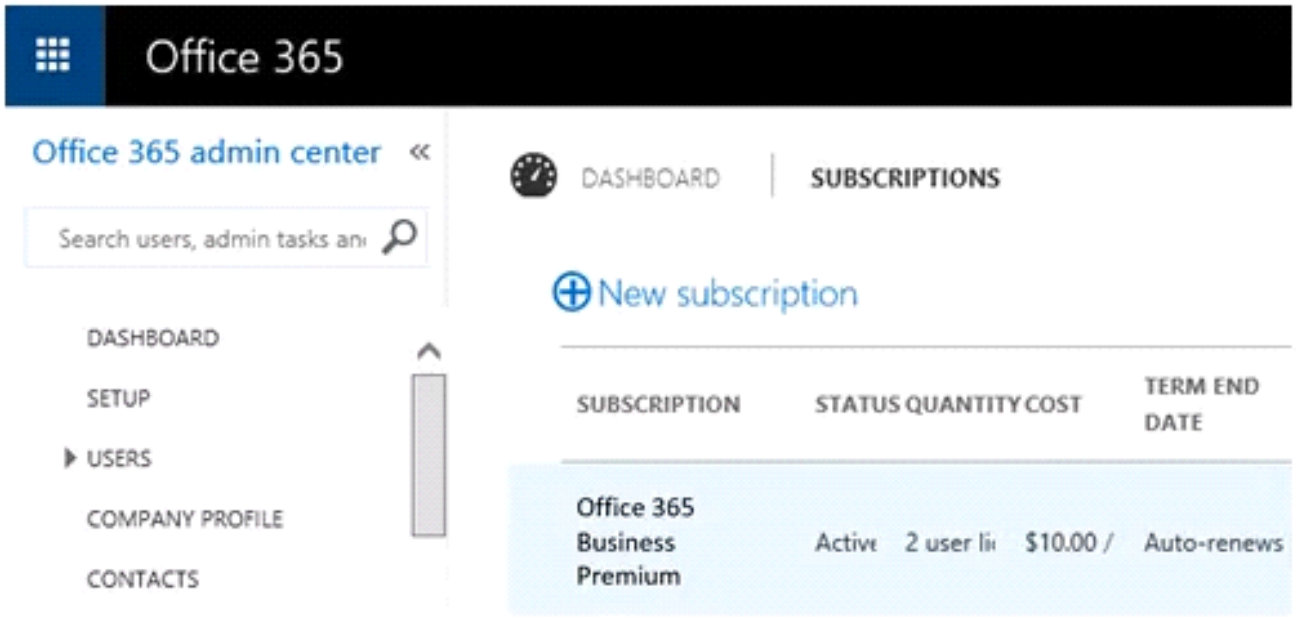
A. Connect the client computer to the Internet once to activate the Office 365 ProPlus client, and once every 90days after that.
B. Connect the client computer to the Internet once to activate the Office 365 ProPlus client, and once every 30 days after that.
C. Connect the client computer to the Internet only once to activate the Office 365 ProPlus client.
D. Connect the client computer to the Internet once to activate the Office 365 ProPlus client, and once every 180 days after that.
E. Connect the client computer to the Internet once to activate the Office 365 ProPlus client, and once every 365 days after that.

Answer: B

Explanation:
After you've verified the user is assigned a license, you should check that Office 365 ProPlus is activated. Activation usually occurs during initial installation. The computer has to connect to the Internet at least once every 30 days for Office 365 ProPlus to remain activated.
References:
https://technet.microsoft.com/en-us/library/gg702620.aspx

Question: 14

HOTSPOT
You manage an Office 365 tenant. The subscription details for the tenant are displayed in the following screenshot.



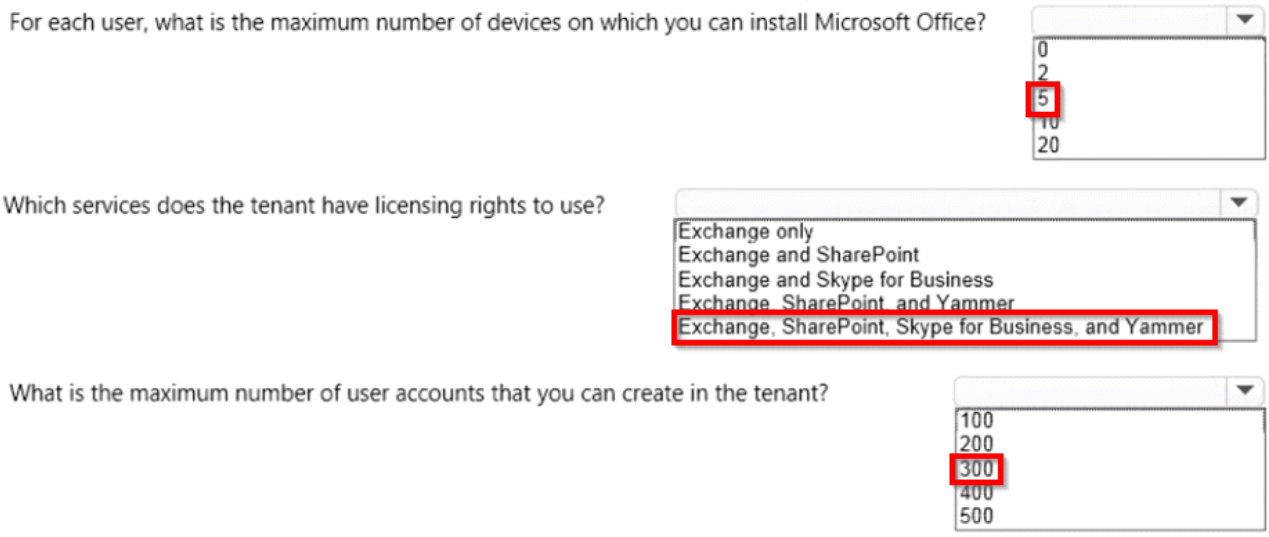
Use the drop-down menus to select the answer choice that answers each question.
NOTE: Each correct answer is worth one point.

For each user, what is the maximum number of devices on which you can install Microsoft Office?
0
2
5
10
20

Which services does the tenant have licensing rights to use?
Exchange only
Exchange and SharePoint
Exchange and Skype for Business
Exchange, SharePoint, and Yammer
Exchange, SharePoint, Skype for Business, and Yammer

What is the maximum number of user accounts that you can create in the tenant?
100
200
300
400
500

Answer:



Each user can install Office on 5 PCs or Macs, 5 tablets (Windows, iPad, and Android), and 5 phones.
Online Services include:Exchange, Sharepoint, Yammer, Skype for Business, etc.
Office 365Small Business Premium supports a maximum of 300 users

Question: 15

A company has an Office 365 tenant. The company uses a third-party DNS provider that does not allow TXT records.
You need to verify domain ownership.
What should you do?

A. Create an MX record.
B. Create a CNAME record.
C. Create an A record.
D. Create an SRV record.

Answer: A

Explanation:
Add a TXT or MX record for DNS verification.
References:
https://support.office.com/en-us/article/Change-nameservers-to-set-up-Office-365-with-any-domain-registrar-a8b487a9-2a45-4581-9dc4-5d28a47010a2

Question: 16

A company has an Office 365 tenant.
You must reset the password for an account named User1.
You need to ensure that the new password for the account meets complexity rules.
Which two passwords can you use? Each correct answer presents a complete solution.

A. Summer2015
B. May2015
C. User1User1
D. summer2015

E. May 2015
F. summer!@#$
G. M1crosoft

Answer: A,G

Explanation:
If the user is set to require a strong password, then all of the following rules must be met:
The password must contain at least one lowercase letter.
The password must contain at least one uppercase letter.
The password must contain at least one non-alphanumeric character.
The password cannot contain any spaces, tabs, or line breaks.
The length of the password must be 8-16 characters.
The user name cannot be contained in the password.
References:
https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-policy

Question: 17

Your company deploys an Office 365 tenant.
You need to ensure that you can view service health and maintenance reports for the past seven days.
What are two possible ways to achieve this goal? Each correct answer presents a complete solution.

A. View the service health current status page of the Office 365 admin center.
B. Subscribe to the Office 365 Service Health RSS Notifications feed.
C. View the service settings page of the Office 365 admin center.
D. Run the Microsoft OnRamp Readiness Tool.

Answer: A,B

Explanation:
As an Office 365 admin, you can see whether there has been a service interruption or outage in your service on the Office 365 service health page. The Service health page shows status information for today, the past six days, and 30 days of history.

Question: 18

You are the Office 365 administrator for your company.
Users report that they have received significantly more spam messages over the past month than they normally receive.
You need to analyze trends for the email messages received over the past 60 days.
From the Office 365 admin center, what should you view?

A. the Mail protection reports
B. the Office 365 Malware detections in received mail report
C. messages on the Message center page
D. the Mailbox access by non-owners report

Answer: A

Explanation:
Use mail protection reports in Office 365 to view data about malware, spam, and rule detections.
If you're an Exchange Online or Exchange Online Protection (EOP) admin, there's a good chance you'd like to monitor how much spam and malware is being detected, or how often your transport rules are being matched. With the interactive mail protection reports in the Office 365 admin center, you can quickly get a visual report of summary data, and drill-down into details about individual messages, for as far back as 90 days.

Question: 19

An organization plans to migrate to Office 365.
You need to estimate the post-migration network traffic.
Which tool should you use?

A. Skype for Business Bandwidth Calculator
B. Process Monitor
C. Microsoft Network Monitor
D. Microsoft OnRamp Readiness tool

Answer: A

Explanation:
Office 365 includes Skype for Business.
With this latest version of the Microsoft Skype for Business Server Bandwidth Calculator, you can enter information about your users and the Skype for Business Server features that you want to deploy, and the Bandwidth Calculator will determine bandwidth requirements for the WAN that connects sites in your deployment. The accompanying Bandwidth Calculator User Guide describes the recommended process for estimating your WAN bandwidth needs for Skype for Business client real-time traffic.

Question: 20

HOTSPOT
You have an Office 365 tenant. A user named User1 has a mailbox. The user creates documents and saves the documents in a shared document library.
User1 leaves the company. You must delete the account for User1.
In the table below, identify when each type of data will be deleted.
NOTE: Make only one selection in each column. Each correct selection is worth one point.

Answer Area

Timeframe	User1 Exchange Online mailbox	Documents Created by User1 on SharePoint Online
Never removed	○	○
Removed immediately	○	○
Removed after 30-day grace period	○	○
Removed after 90-day grace period	○	○

Answer:

Answer Area

Timeframe	User1 Exchange Online mailbox	Documents Created by User1 on SharePoint Online
Never removed	○	○
Removed immediately	○	○
Removed after 30-day grace period	○	○
Removed after 90-day grace period	○	○

When you delete an Office 365 user account, the corresponding Exchange Online mailbox is deleted and removed from the list of mailboxes in the EAC. After the user account is deleted, it's listed on the Deleted Users page in the Office 365 admin center. It can be recovered within 30 days after being deleted. After 30 days, the user account and mailbox are permanently deleted and not recoverable.
View, restore, or delete items in the Recycle Bin of a SharePoint site
The Recycle Bin provides a safety net when deleting documents, list items, lists, folders and files. When you or site visitors delete any of these items from a Web site, the items are placed in the Recycle Bin. Items in the Recycle Bin remain there until you decide to permanently delete them from your Web site, or until the items are permanently deleted after a set number of days, which is based on a schedule defined in Central Administration.
References:
https://technet.microsoft.com/en-us/library/dn186233(v=exchg.150).aspx
https://support.office.com/en-sg/article/View-restore-or-delete-items-in-the-Recycle-Bin-of-a-SharePoint-site-6df466b6-55f2-4898-8d6e-c0dff851a0be

Question: 21

Contoso, Ltd., has an Office 365 tenant. You configure Office 365 to use the domain contoso.com, and you verify the domain. You deploy and configure Active Directory Federation Services (AD FS) and Azure Active Directory Connect with password synchronization. You connect to Azure Active Directory by using a Remote PowerShell session.
You need to switch from using password-synced passwords to using AD FS on the Office 365 verified domain.
Which Windows PowerShell command should you run?

A. Convert-MsolDomainToFederated –DomainName contoso.com
B. Convert-MsolDomainToStandard –DomainName contoso.com
C. Convert-MsolFederatedUser
D. Set-MsolDomainAuthentication –DomainName contoso.com

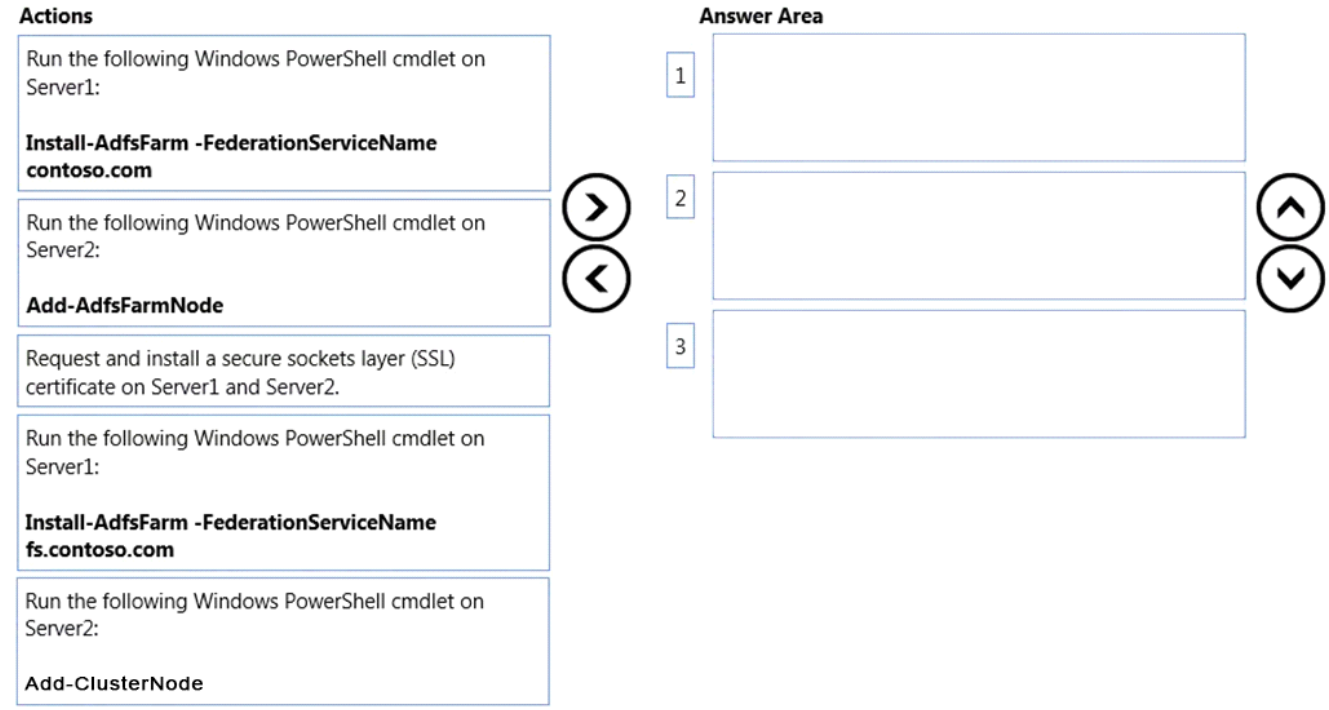
Answer: A

Explanation:
The Convert-MSOLDomainToFederated cmdlet converts the specified domain from standard authentication to single sign-on (also known as identity federation), including configuring the relying party trust settings between the Active Directory Federation Services (AD FS) server and the Microsoft Online Services. As part of converting a domain from standard authentication to single sign-on, each user must also be converted. This conversion happens automatically the next time a user signs in; no action is required by the administrator.
References:
https://docs.microsoft.com/en-us/powershell/module/msonline/convert-msoldomaintofederated?view=azureadps-1.0

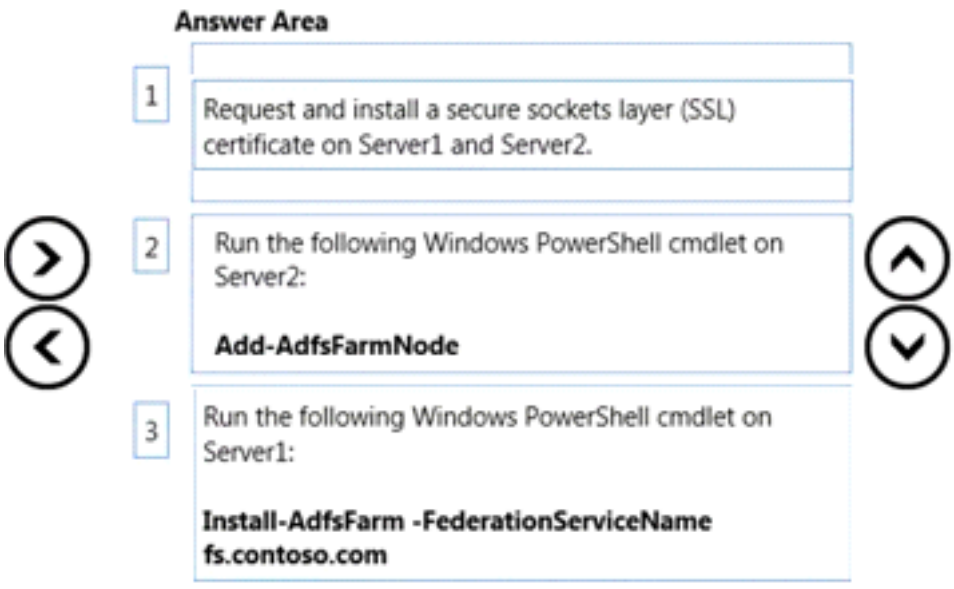
Question: 22

DRAG DROP

Contoso, Ltd., uses SharePoint Online and plans a new single sign-on (SSO) implementation that uses Active Directory Federation Services (AD FS).
Your environment contains the following configurations:
two servers named Server1 and Server2
a partner collaboration website for the domain contoso.com that points to a SharePoint Online team site
a hardware load balancer to use with Server1 and Server2
You need to install AD FS to support the environment.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Example: Creates the first node in a federation server farm that uses the Windows Internal Database(WID) on the local server computer.
In this example, a certificate thumbprint value is supplied for the CertificateThumbprint parameter. This certificate

will be used as the SSL certificate and the service communications certificate.
PS C:\> $fscredential= Get-Credential
PS C:\> Install-AdfsFarm -CertificateThumbprint 8169c52b4ec6e77eb2ae17f028fe5da4e35c0bed -FederationServiceName fs.corp.contoso.com -ServiceAccountCredential $fscredential
Install-AdFsFarm command creates the first node of a new federation serverfarm.
/ The parameter -CertificateThumbprint<String>
Specifies the value of the certificate thumbprint of the certificate that should be used in the Secure Sockets Layer (SSL) binding of the Default Web Site in Internet Information Services (IIS). This value should match the thumbprint of a valid certificate in the Local Computer certificate store.
/ The parameter -FederationServiceName<String>
Specifies the DNSname of the federation service. This value must match the subject name of the certificate configured on the SSL binding in IIS.
The Add-AdfsFarmNode command adds this computer to an existing federation server farm.
References:
https://technet.microsoft.com/en-us/library/dn479416(v=wps.630).aspx

Question: 23

You have an Office 365 tenant that uses an Enterprise E3 subscription. You have two servers in a perimeter network that have the Active Directory Federation Services (AD FS) proxy role service installed. A federation server farm is located behind a firewall.
You need to ensure that the AD FS proxies can communicate with the federation server farm.
Which two name resolution strategies can you use? Each correct answer presents a complete solution.

A. HOSTS file on the proxy servers
B. DNS server in the perimeter network
C. LMHOSTS file on the proxy servers
D. LMHOSTS file on the federation servers
E. HOSTS file on the federation servers

Answer: A,B

Explanation:
Configure Name Resolution for a Federation Server Proxy in a DNS Zone That Serves Only the PerimeterNetwork
So that name resolution can work successfully for a federation server in an Active Directory Federation Services (AD FS) scenario in which one or more Domain Name System (DNS) zones serve only the perimeter network, the following tasks must be completed:
The hosts file on the federation server proxy must be updated to add the IP address of a federation server.
DNS in the perimeter network must be configured to resolve all client requests for the AD FS host name to the federation server proxy. To do this, you add a host (A) resource record to perimeter DNS for the federation server proxy.
References:
https://technet.microsoft.com/en-us/library/dd807045.aspx

Question: 24

A company has an Office 365 tenant.
You must retrieve mailbox diagnostic data.
You need to provide a report with this data for all users.
Which report solution should you choose?

A. Office 365 admin center
B. downloadable spreadsheet
C. reporting Windows PowerShell cmdlets
D. REST reporting web service

Answer: D

Explanation:
The Office 365 Reporting web service enables developers to integrate information on email and spam, antivirus activity, compliance status, and Skype for Business Online activities into their custom service reporting applications and web portals.
References:
https://msdn.microsoft.com/en-us/library/office/jj984325.aspx

Question: 25

You have an Exchange Online tenant.
You must identify mailboxes that are no longer in use.
You need to locate the inactive mailboxes.
Which Windows PowerShell command should you run?

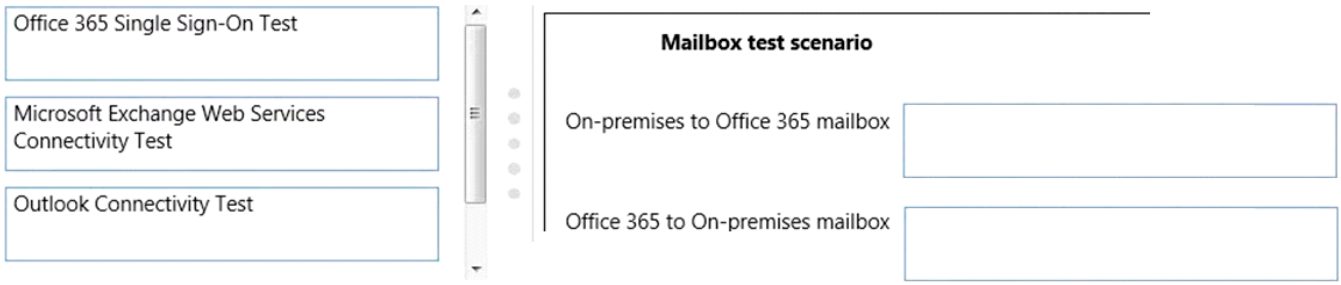
A. Get-StaleMailboxReport -Expression
B. Get-StaleMailboxReport -Organization
C. Get-MailboxActivityReport -Organization
D. Get-StaleMailboxReport -EndDate

Answer: D

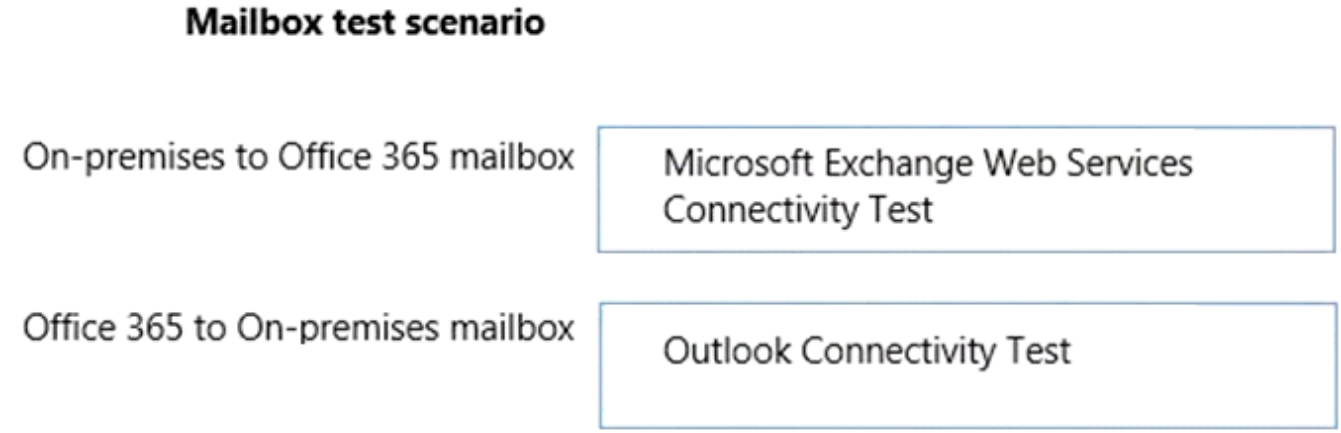
Explanation:
Use the Get-StaleMailboxReport cmdlet to view the number of mailboxes that haven't been accessed for at least 30 days.
The EndDate parameter specifies the end date of the date range.

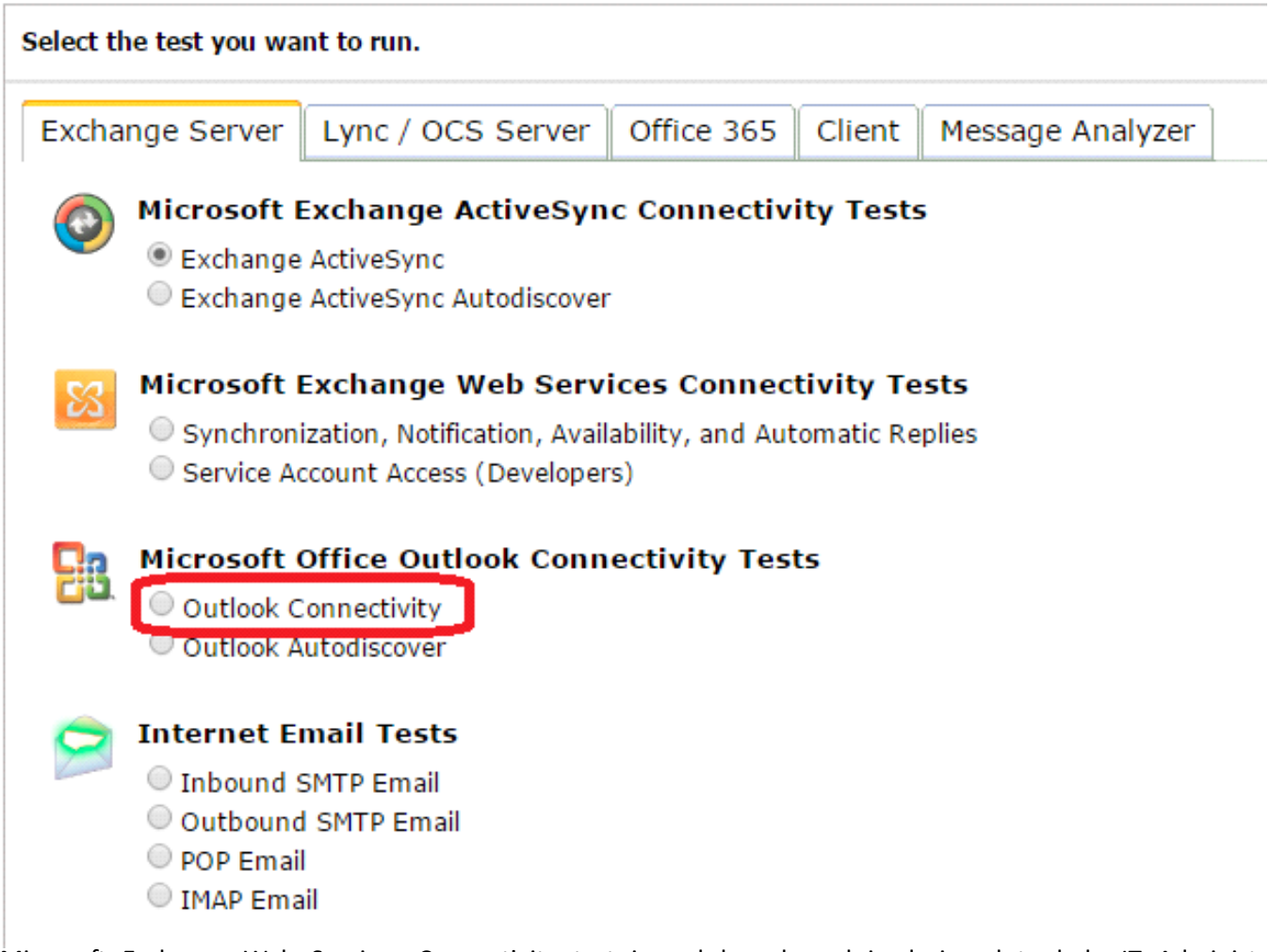
Question: 26

DRAG DROP
You have an Office 365 tenant. An organization is migrating from an Exchange organization to Office 365.
Users report that Outlook does not display the availability of other users for meetings. You must determine whether an Office 365 mailbox can access the scheduling availability of a user with an on-premises mailbox. You must also run a test to verify that an on-premises mailbox can access the scheduling availability of a user that has an Office 365 mailbox.
You need to conduct the tests.
What should you do? To answer, drag the appropriate test to run to the correct mailbox test scenario. Each test may be used once, more than once or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:





Microsoft Exchange Web Services Connectivity test is web-based, and is designed to help IT Administrators

troubleshoot connectivity issues that affect their Exchange Server deployments. The tool simulates several client logon and mail flow scenarios. When a test fails, many of the errors have troubleshooting tips to assist the IT Administrator to correct the problem.
The Outlook Connectivity Test is available with the Microsoft Office 365 Support and Recovery Assistant.

Question: 27

A company with 75,000 employees has an Office 365 tenant.
You need to install the Azure Active Directory Synchronization (AAD Sync) tool by using the least amount of administrative effort.
Which versions of each product should you implement? (Select three)
Select three.

A. .Net 3.5
B. Net 4.0
C. .Net 4.5
D. .Net 4.5.1
E. PowerShell(PS1)
F. PowerShell (PS2)
G. PowerShell (PS3)
H. PowerShell (PS4)
I. SQL Server Express
J. SQL Server 2008
K. SQL Server 2012
L. SQL Server 2014

Answer: D,F,L

Explanation:
The following components need to be installed:
Net 4.5.1
PowerShell (PS3 or better is required)
Azure AD Sync requires a SQL Server database to store identity data. By default a SQL Express LocalDB (a light version of SQL Server Express) is installed and the service account for the service is created on the local machine.
SQL Server Express has a 10GB size limit that enables you to manage approximately 100.000objects. This is fine for the scenario in this question.
If you need to manager a higher volume of directory objects, you need to point the installation process to a different version of SQL Server. AAD Sync supports all flavors of Microsoft SQL Server from SQL Server 2008 to SQL Server 2014.

Question: 28

A company has an Office 365 tenant that has an Enterprise E1 subscription. Users currently sign in with credentials that include the contoso.com domain suffix.
The company is acquired by Fabrikam. Users must now sign in with credentials that include the fabrikam.com domain suffix.
You need to ensure that all users sign in with the new domain name.
Which Windows PowerShell cmdlet should you run?

A. Set-MsolUser
B. Redo-MsolProvisionUser
C. Set-MsolUserLicense

D. Set-MsolUserPrincipalName
E. Convert-MsolFederatedUser
F. Set-MailUser
G. Set-LinkedUser
H. New-MsolUser

Answer: D

Explanation:
The Set-MsolUserPrincipalName cmdlet is used to change the User Principal Name (user ID) of a user. This cmdlet can be used to move a user between a federated and standard domain, which will result in their authentication type changing to that of the target domain.
The following command renames user1@contoso.com to CCole@contoso.com.
Set-MsolUserPrincipalName -UserPrincipalName User1@contoso.com -NewUserPrincipalName CCole@contoso.com
References:
https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserprincipalname?view=azureadps-1.0

Question: 29

You have an Office 365 tenant that uses an Enterprise E1 subscription.
You need to convert the users in the tenant to an Enterprise E3 subscription.
Which Windows PowerShell cmdlet should you run?

A. Set-MsolUser
B. Redo-MsolProvisionUser
C. Set-MsolUserLicense
D. Set-MsolUserPrincipalName
E. Convert-MsolFederatedUser
F. Set-MailUser
G. Set-LinkedUser
H. New-MsolUser

Answer: C

Explanation:
The Set-MsolUserLicense cmdlet can be used to adjust the licenses for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.
Note: Switching plans manually means that you're completing the following separate procedures instead of using the switch plans wizard. The procedures are:
Buy licenses for the subscription you're switching users to.
Verify the subscription is ready to switch users to.
Reassign user licenses
Remove unneeded licenses from the subscription you're switching from.
Cancel the original subscription (if switching all users).
Switching only some users isn't supported by the switch
References:
https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0

Question: 30

A company has an Office 365 tenant that has an Enterprise E1 subscription.
You plan to test a new deployment by using 50 tenant user accounts.
You need to ensure that the passwords for the test user accounts do not expire.
Which Windows PowerShell cmdlet should you run?

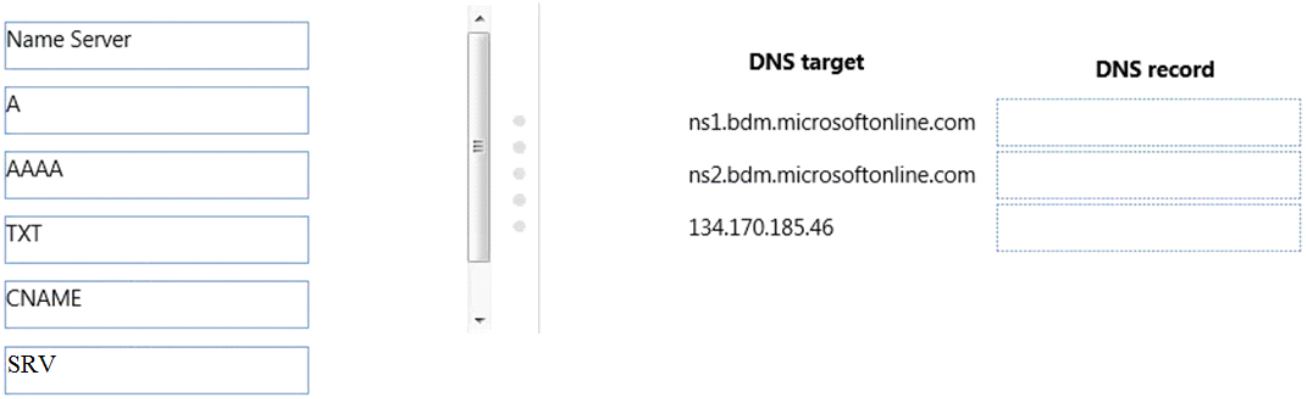
A. Set-MsolUser
B. Redo-MsolProvisionUser
C. Set-MsolUserLicense
D. Set-MsolUserPrincipalName
E. Convert-MsolFederatedUser
F. Set-MailUser
G. Set-LinkedUser
H. New-MsolUser

Answer: A

Explanation:
The Set-MsolUser cmdlet is used to update a user object. This cmdlet should be used for basic properties only.
Parameter -PasswordNeverExpires <Boolean>
Sets whether or not the user's password will expire periodically.
References:
https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluser?view=azureadps-1.0

Question: 31

DRAG DROP
A company has an Office 365 tenant. You plan to use Office 365 to manage the DNS settings for a custom domain. You purchase the domain through a third-party provider.
You create a custom website. You must host the website through a third-party provider at the IP address 134.170.185.46. You need to configure the correct DNS settings.
What should you do? To answer, drag the appropriate DNS record to the correct DNS target. Each record may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:

Change your domain's name server (NS) records
When you get to the last step of the domains setup wizard in Office 365, you have one task remaining. To set up your domain with Office 365 services, like email, you change your domain's name server (or NS) records at your domain registrar to point to the Office 365 primary and secondary name servers.
Use (A) DNS record for the web site.

Question: 32

A company has an Office 365 tenant.
You need to monitor active Directory synchronization.
Which tool should you run?

A. IdFix
B. Office 365 Health, Readiness, and Connectivity Check
C. Microsoft Remote Connectivity Analyzer Tool
D. Synchronization Service (MIISClient)

Answer: A

Explanation:
One of the first steps you should take before installing DirSync is to look at the directory that you have on-premises and make sure it's healthy and ready to synchronize to Azure Active Directory.
You need to check Active Directory remediation.
DirSync has certain requirements on attributes in the directory, and aligning the attribute values with the DirSync requirements is commonly known as Active Directory remediation. To help with Active Directory remediation, you should use the IdFix tool, which reviews the directory and performs interactive Active Directory remediation. This tool checks for and helps you correct any invalid data and duplicate data in directory attributes, including user PrincipalName (UPN), mailNickName, proxyAddress, sAMAccountName, targetAddress, and others. The IDFix tool also provides assistance for migrating from a non-routable UPN (such as "domain.local," for example) to an Internet routable domain name, because using an Internet-routable domain is one of the requirements for Azure Active Directory. Be sure to run the IdFix tool from within your network, so that it has access to the domain controllers.
References:
https://blogs.office.com/2014/04/15/synchronizing-your-directory-with-office-365-is-easy/

Question: 33

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution. Determine whether the solution meets the stated goals.
You have an on-premises Active Directory forest.
You deploy Active Directory Federation Services (AD FS) and purchase an Office 365 subscription.

You need to create a trust between the AD FS servers and the Office 365 subscription.
Solution: You run the Convert-MsolDomainToFederated cmdlet.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Each domain that you want to federate must either be added as a single sign-on domain or converted to be a single sign-on domain from a standard domain. Adding or converting a domain sets up a trust between AD FS and Microsoft Azure Active Directory (Microsoft Azure AD).
The Convert-MSOLDomainToFederated cmdlet converts the specified domain from standard authentication to single sign-on (also known as identity federation), including configuring the relying party trust settings between the Active Directory Federation Services (AD FS) server as part of converting a domain from standard authentication to single sign-on, each user must also be converted. This conversion happens automatically the next time a user signs in; no action is required by the administrator.
References:
https://msdn.microsoft.com/en-us/library/azure/dn194092(v=azure.98).aspx
https://msdn.microsoft.com/en-us/library/azure/jj205461.aspx

Question: 34

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution. Determine whether the solution meets the stated goals.
You have an on-premises Active Directory forest.
You deploy Active Directory Federation Services (AD FS) and purchase an Office 365 subscription.
You need to create a trust between the AD FS servers and the Office 365 subscription.
Solution: You run the New-MsolFederatedDomain cmdlet.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Each domain that you want to federate must either be added as a single sign-on domain or converted to be a single sign-on domain from a standard domain. Adding or converting a domain sets up a trust between AD FS and Microsoft Azure Active Directory (Microsoft Azure AD).
Note: The New-MSOLFederatedDomain cmdlet adds a new single sign-on domain (also known as identity-federated domain) to and configures the relying party trust settings between the on-premises AD FS server. Due to domain verification requirements, you may need to run this cmdlet several times in order to complete the process of adding the new single sign-on domain.
References:
https://msdn.microsoft.com/en-us/library/azure/dn194105(v=azure.98).aspx
https://msdn.microsoft.com/en-us/library/azure/jj205461.aspx

Question: 35

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution. Determine whether the solution meets the stated goals.
You have an on-premises Active Directory forest.
You deploy Active Directory Federation Services (AD FS) and purchase an Office 365 subscription.
You need to create a trust between the AD FS servers and the Office 365 subscription.
Solution: You run the netdom.com command.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Each domain that you want to federate must either be added as a single sign-on domain or converted to be a single sign-on domain from a standard domain. Adding or converting a domain sets up a trust between AD FS and Microsoft Azure Active Directory (Microsoft Azure AD).
References:
https://msdn.microsoft.com/en-us/library/azure/jj205461.aspx

Question: 36

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains a single Active Directory forest. The forest contains a domain controller and Active Directory Federation Services (AD FS) servers that are deployed to virtual machines. The virtual machines run either on-premises or on Microsoft Azure.
You have Azure AD Connect deployed on-premises. The Azure AD Connect database is installed on an on-premises instance of Microsoft SQL Server 2014.
Last month, an Azure AD Connect server experienced a hardware failure that caused an Azure AD Connect server to go offline for several days.
You need to recommend a solution to reduce the outage window when hardware failure occurs on the Azure AD Connect server.
Solution: You deploy a new Azure AD Connect server to an Azure virtual machine that uses a new SQL Server instance. You set the Azure AD Connect server to staging mode.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Azure AD Connect sync Staging mode can be used for several scenarios, including:
High availability.
Test and deploy new configuration changes.

Introduce a new server and decommission the old.
If you have a more complex environment, then having one or more standby servers is recommended. During installation, you can enable a server to be in staging mode.
Use virtual machines
A common and supported method is to run the sync engine in a virtual machine. In case the host has an issue, the image with the sync engine server can be migrated to another server.
References:
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-operations/

Question: 37

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution. Determine whether the solution meets the stated goals.
Your network contains a single Active Directory forest. The forest contains a domain controller and Active Directory Federation Services (AD FS) servers that are deployed to virtual machines. The virtual machines run either on-premises or on Microsoft Azure.
You have Azure AD Connect deployed on-premises. The Azure AD Connect database is installed on an on-premises instance of Microsoft SQL Server 2014.
Last month, an Azure AD Connect server experienced a hardware failure that caused an Azure AD Connect server to go offline for several days.
You need to recommend a solution to reduce the outage window when hardware failure occurs on the Azure AD Connect server.
Solution: You deploy a new on-premises Azure AD Connect server that uses a new SQL Server instance. You set the Azure AD Connect server to staging mode.
Does this meet the goal?

A. Yes
B. No

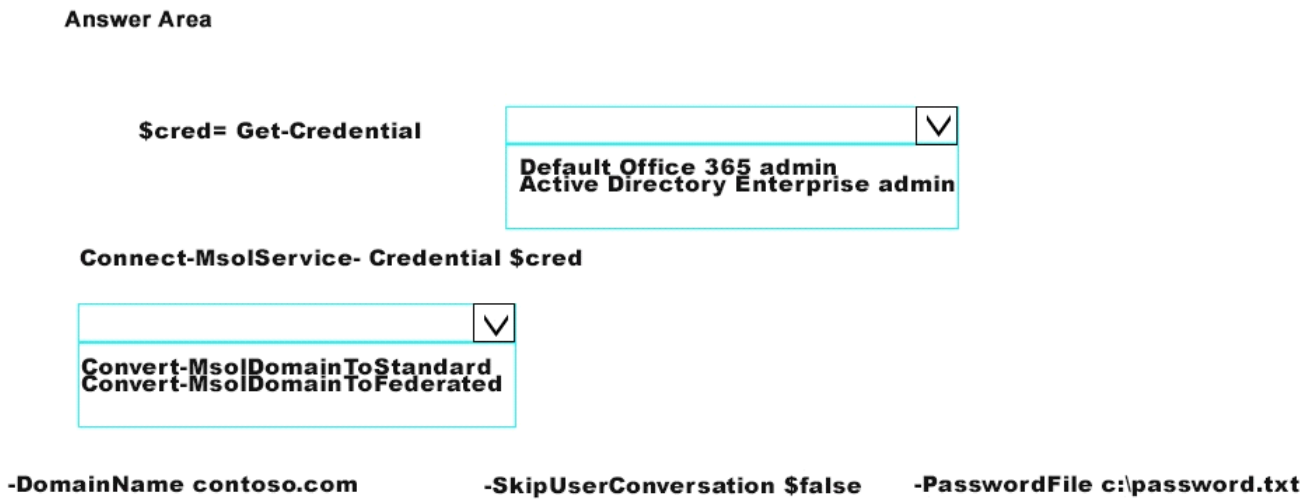
Answer: B

Explanation:
Azure AD Connect sync Staging mode can be used for several scenarios, including:
High availability.
Test and deploy new configuration changes.
Introduce a new server and decommission the old.
Have a spare standby server - staging mode
If you have a more complex environment, then having one or more standby servers is recommended. During installation, you can enable a server to be in staging mode.
SQL Clustering would be needed for high availability.
Note: SQL High Availability
If you are not using the SQL Server Express that comes with Azure AD Connect, then high availability for SQL Server should also be considered. The only high availability solution supported is SQL clustering. Unsupported solutions include mirroring and Always On.
References:
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-operations/

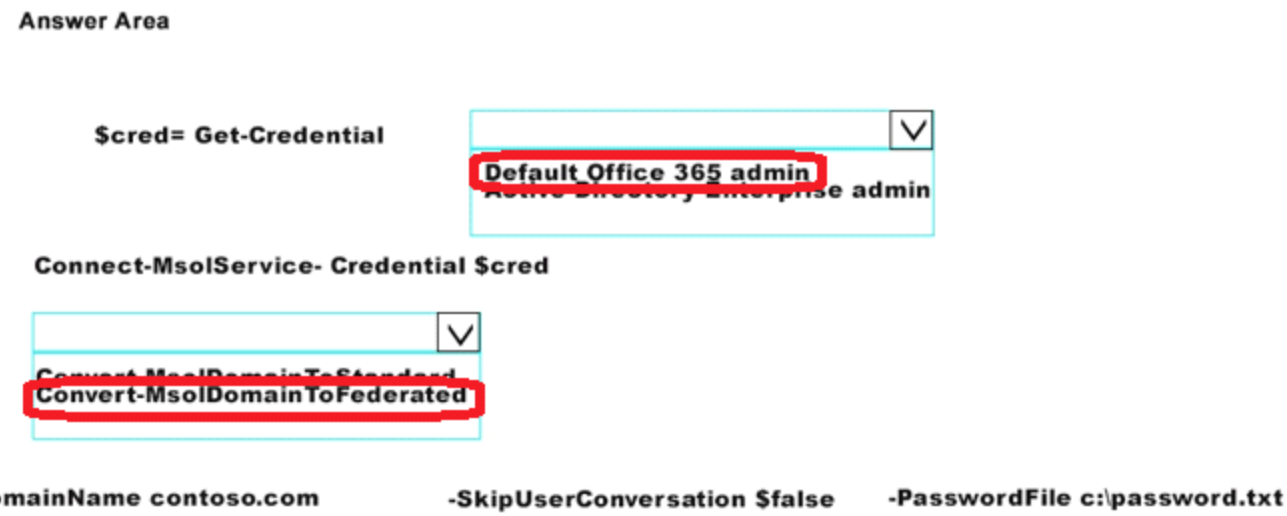
Question: 38

HOTSPOT

Contoso, Ltd. has an Office 365 Tenant. The company plans to implement single sign-on (SSO). You install Active Directory Federation Services.
You need to enable the use of SSO.
How should you complete the relevant Windows PowerShell commands? To answer, select the appropriate Windows PowerShell segment from each list in the answer area.



Answer:

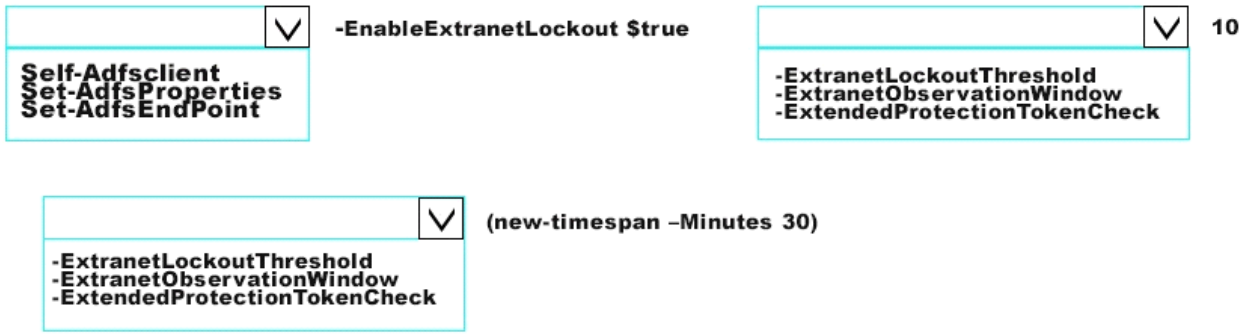


See step 2) and step 5) below.
To convert an existing domain to a single sign-on domain, follow these steps.
References:
https://msdn.microsoft.com/en-us/library/azure/jj205461.aspx

Question: 39

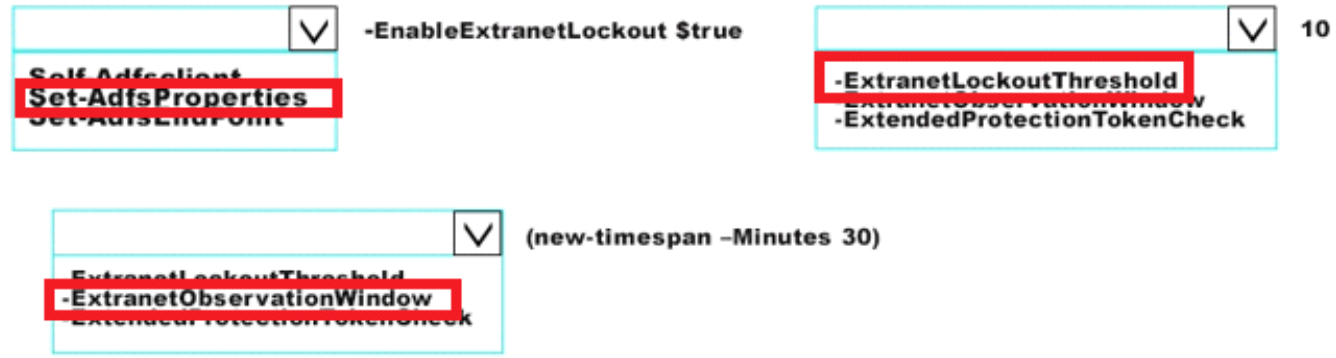
HOTSPOT
You implement single sign-on (SSO) between Office 365 and an on-premises deployment of Active Directory.
You need to configure Active Directory Federation Services (AD FS) to prevent users from being able to log on for 30 minutes after they attempt to log on by using a bad password 10 consecutive times.
What command should you run? To answer, select the appropriate options in the answer area.

Answer Area



Answer:

Answer Area



An example of enabling ExtranetLockout feature with maximum of 10 number of bad password attempts and 30 mins soft-lockout duration is as follows:
Set-AdfsProperties-EnableExtranetLockout $true -ExtranetLockoutThreshold 10 -ExtranetObservationWindow (new-timespan -Minutes 30)
References:
https://blogs.msdn.microsoft.com/luzhao1/2015/06/24/demystify-extranet-lockout-feature-in-ad-fs-3-0/

Question: 40

An organization plans to migrate to Office 365. You use Azure AD Connect.
Several users will not migrate to Office 365. You must exclude these users from synchronization. All users must continue to authenticate against the on-premises Active Directory.
You need to synchronize the remaining users.
Which three actions should you perform to ensure users excluded from migration are not synchronized? Each correct answer presents part of the solution.

A. Run the Windows PowerShell command Set-MsolDirSyncEnabled -EnableDirSync $false.
B. Perform a full synchronization.
C. Populate an attribute for each user account.
D. Configure the connection filter.
E. Disable the user accounts in Active Directory.

Answer: B,C,D

Explanation:
D: With filtering, you can control which objects should appear in Azure AD from your on-premises directory. For example, you run a pilot for Azure or Office 365 and you only want a subset of users in Azure AD.
C: Attribute–based filtering: This option allows you to filter objects based on attribute values on the objects. You can also have different filters for different object types.
B: After you have made your configuration changes, these must be applied to the objects already present in the system. It could also be that objects not currently in the sync engine should be processed and the sync engine needs to read the source system again to verify its content.
If you changed configuration using attribute filtering, then you need to do Full synchronization.
References:
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-configure-filtering/

Question: 41

You use a centralized identity management system as a source of authority for user account information. You export a list of new user accounts to a file on a daily basis. Your company uses a local Active Directory for storing user accounts for on-premises solutions. You are also using Azure AD Connect.
New user accounts must be created in both the local Active Directory and Office 365. You must import user account data into Office 365 daily.
You need to import the new users.
What should you do?

A. Create a Windows PowerShell script to import account data from the file into Active Directory.
B. Create a Windows PowerShell script that uses the MSOnline module to import account data from the file.
C. Use the Azure Management Portal to import the file.
D. Use the Office 365 admin center to import the file.

Answer: A

Explanation:
To force a full sync with the Azure AD Connect tool from Windows PowerShell run Import-Module ADSync followed by Start-ADSyncSyncCycle -PolicyType Initial
Note: The DirSync tool, which you can use to synchronize your on-premises Active Directory Domain Services (AD DS) with an instance of Azure Active Directory (AD), has been updated with the new Azure AD Connect tool. You typically use the DirSync or Azure AD Connect tools to configure either password synchronization or single sign-on so that your users can use their on-premises AD DS credentials to authenticate to Office 365.
The new Azure AD Connect tool provides a richer feature set than the DirSync tool and is now the recommended tool to use.

Question: 42

You have an on-premises Exchange organization. The organization plans to migrate to Exchange Online.
Users report that after their mailboxes are migrated to Exchange Online they are no longer able to send email to a specific dynamic distribution list. All other distribution lists work as expected.
You need to resolve the issue.
What should you do?

A. In the Active Directory Synchronization Services console, change the connector filter to include dynamic distribution lists.
B. In Office 365, re-create the dynamic distribution list.

C. Run the following Windows PowerShell cmdlet: Set-DynamicDistributionGroup
D. Reduce the number of members in the distribution list to fewer than 1,500 contacts.

Answer: C

Explanation:
PROBLEM
You have a hybrid deployment of Exchange Online in Office 365 and on-premises Exchange Server. In this environment, certain members of a dynamic distribution group do not receive email messages.
CAUSE
This problem occurs if the dynamic distribution group was set up before the environment became a hybrid deployment and if the dynamic distribution group uses filters to include only mailboxes. Mailboxes that are migrated to Office 365 become mail-enabled users in the on-premises directory.
SOLUTION
Use the Set-DynamicDistributionGroup cmdlet to update the filters for the dynamic distribution group to include mail-enabled users.
References:
https://support.microsoft.com/en-us/kb/3061396

Question: 43

Contoso, Ltd. has an on-premises SharePoint environment. The company plans to deploy SharePoint Online.
You must use Active Directory Federation Services (AD FS). The global administrator account must be able to access the Office 365 tenant even if AD FS is unavailable.
You need to set up the global administrator account.
What should you do?

A. In the Office 365 admin center, create a user named sp_admin@contoso.onmicrosoft.com
B. In the Office 365 admin center, create a user named sp_admin@contoso.com
C. In Active Directory Domain Services Users and Computers, create a user named sp_admin@contoso.onmicrosoft.com
D. In Active Directory Domain Services Users and Computers, create a user named sp_admin@contoso.com

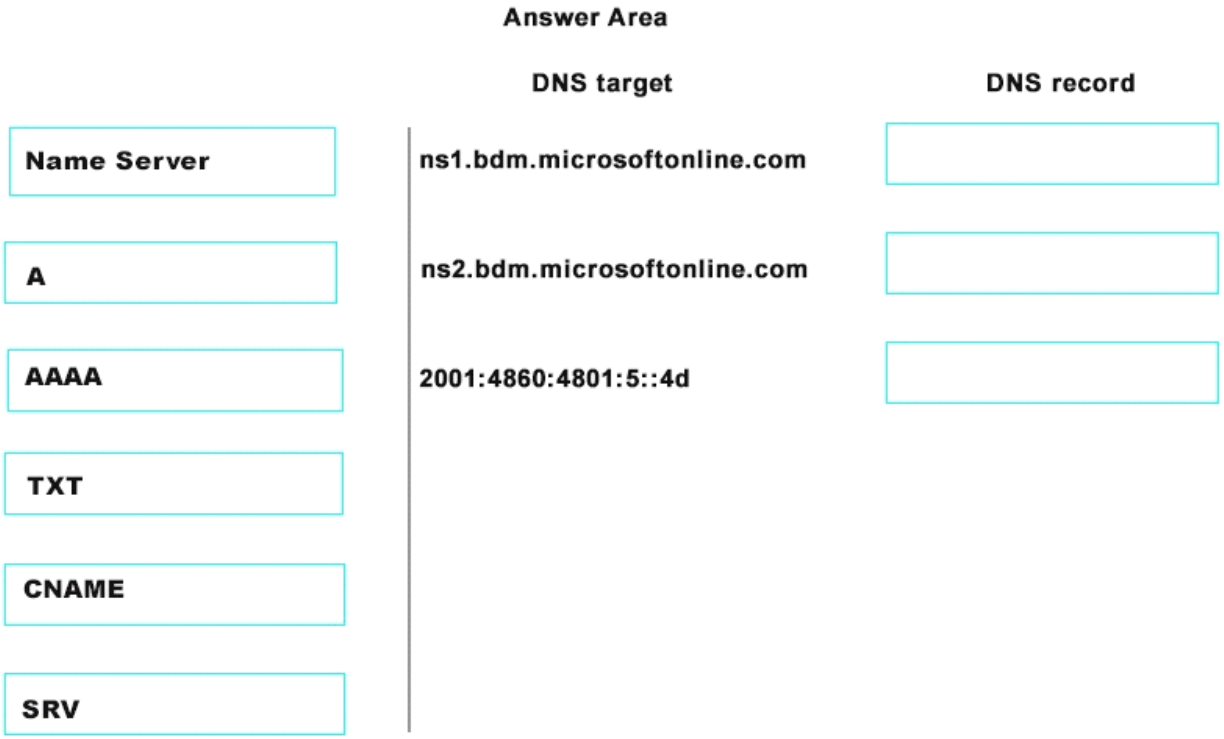
Answer: A

Explanation:
One of the first steps is to create SPO administrative account. You should always plan to create this account as Cloud ID, E.g. sp_admin@yourdomain.onmicrosoft.com. Having this as Cloud ID, it allows you to access your tenant even if On-Premises ADFS environment is unavailable. You can provision new Cloud Account from the Office 365 Administration site.
References:
https://nikpatel.net/2014/06/03/best-practices-for-configuring-sharepoint-online-tenant-part-ii-configuring-sharepoint-administrative-accounts-for-sharepoint-online/

Question: 44

DRAG DROP
A company has an Office 365 tenant. You plan to use Office 365 to manage the DNS settings for a custom domain. You purchase the domain through a third-party provider.
You create a custom website. You must host the website through a third-party provider at the IP v6 address

2001:4860:4801:5::4d.
You need to configure the correct DNS settings.
What should you do? To answer, drag the appropriate DNS record to the correct DNS target. Each record may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



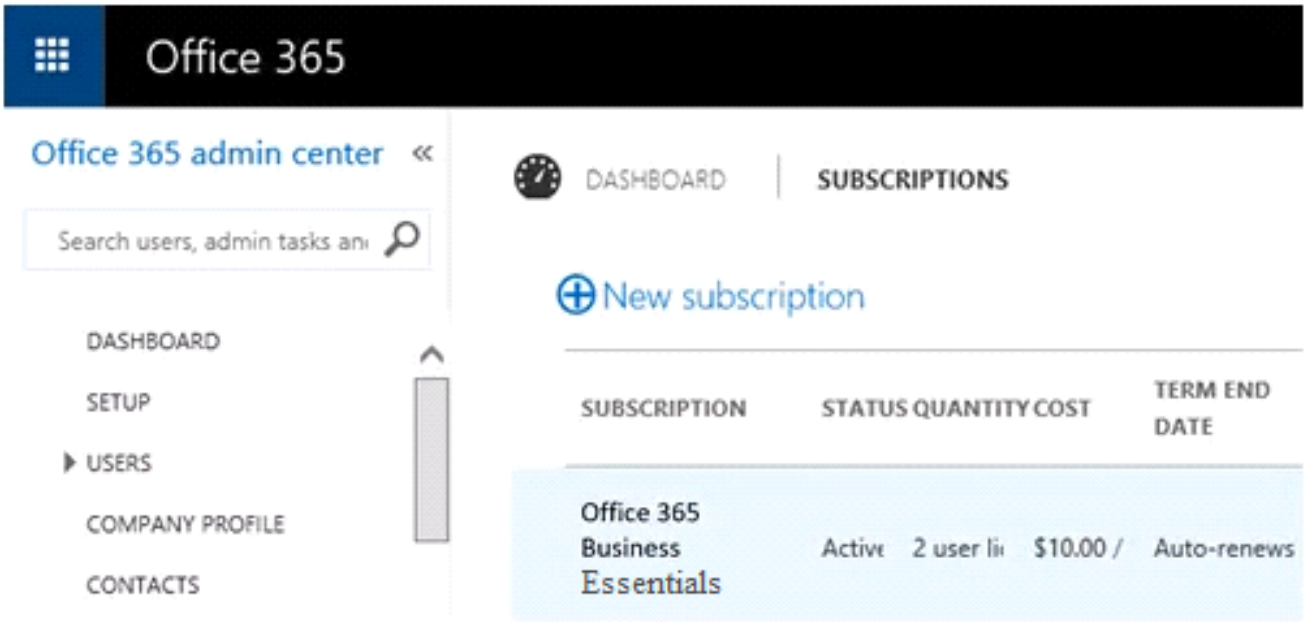
Answer:

Change your domain's name server (NS) records
When you get to the last step of the domains setup wizard in Office 365, you have one task remaining. To setup your domain with Office 365 services, like email, you change your domain's name server (or NS) record sat your domain registrar to point to the Office 365 primary and secondary name servers.
Use (AAAA) DNS record for the website. We must use an (AAAA) and not an (A) record since an Ipv6 address is used.

Question: 45

HOTSPOT

You manage an Office 365 tenant. The subscription details for the tenant are displayed in the following screenshot.



Use the drop-down menus to select the answer choice that answers each question.
NOTE: Each correct answer is worth one point.

Answer Area

Which services does the tenant have licensing rights to use?

- Exchange only
- Exchange and SharePoint
- Exchange and Skype for Business
- Exchange, SharePoint, and Yammer
- Exchange, SharePoint, Skype for Business, and Yammer

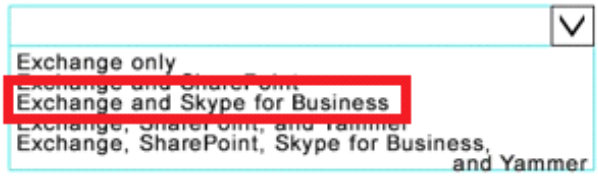
What is the maximum number of user accounts that you can create in the tenant?

- 100
- 200
- 300
- 400
- 500

Answer:

Answer Area

Which services does the tenant have licensing rights to use?



What is the maximum number of user accounts that you can create in the tenant?

Box1:
Skype for Business is included in Office 365 Business Essentials.
SharePoint is not included in Office 365 Business Essentials.
Box 2: Office 365 Business Essentials user maximum is 300 users.
References:
https://products.office.com/en/business/compare-office-365-for-business-plans

Question: 46

Your company deploys an Office 365 tenant.
You need to ensure that you can view service health and maintenance reports for the past seven days.
What are two possible ways to achieve this goal? Each correct answer presents a complete solution.

A. Subscribe to the Office 365 Service Health RSS Notifications feed.
B. View the service settings page of the Office 365 admin center.
C. Run the Microsoft Fast Track Tool.
D. View the service health current status page of the Office 365 admin center.

Answer: A,D

Explanation:
D: See the status of all your services and their components in the Office 365 admin center
Sign in to Office 365 with your work or school account.
Go to the Office 365 admin center.
Go to Health > Service health.
On the Service health page, view the current status of your services. Do any of the following:a) For details, select a service.b) To see status history, select View history, and then select a day on the calendar.
A: In the top right corner of the Service Health page, there is an RSS icon. You can click on the RSS icon to sign up for the service health RSSfeed, which will email you when a new event is added or an existing event is updated.
References:
https://support.office.com/en-us/article/View-the-status-of-your-services-932ad3ad-533c-418a-b938-6e44e8bc33b0

Question: 47

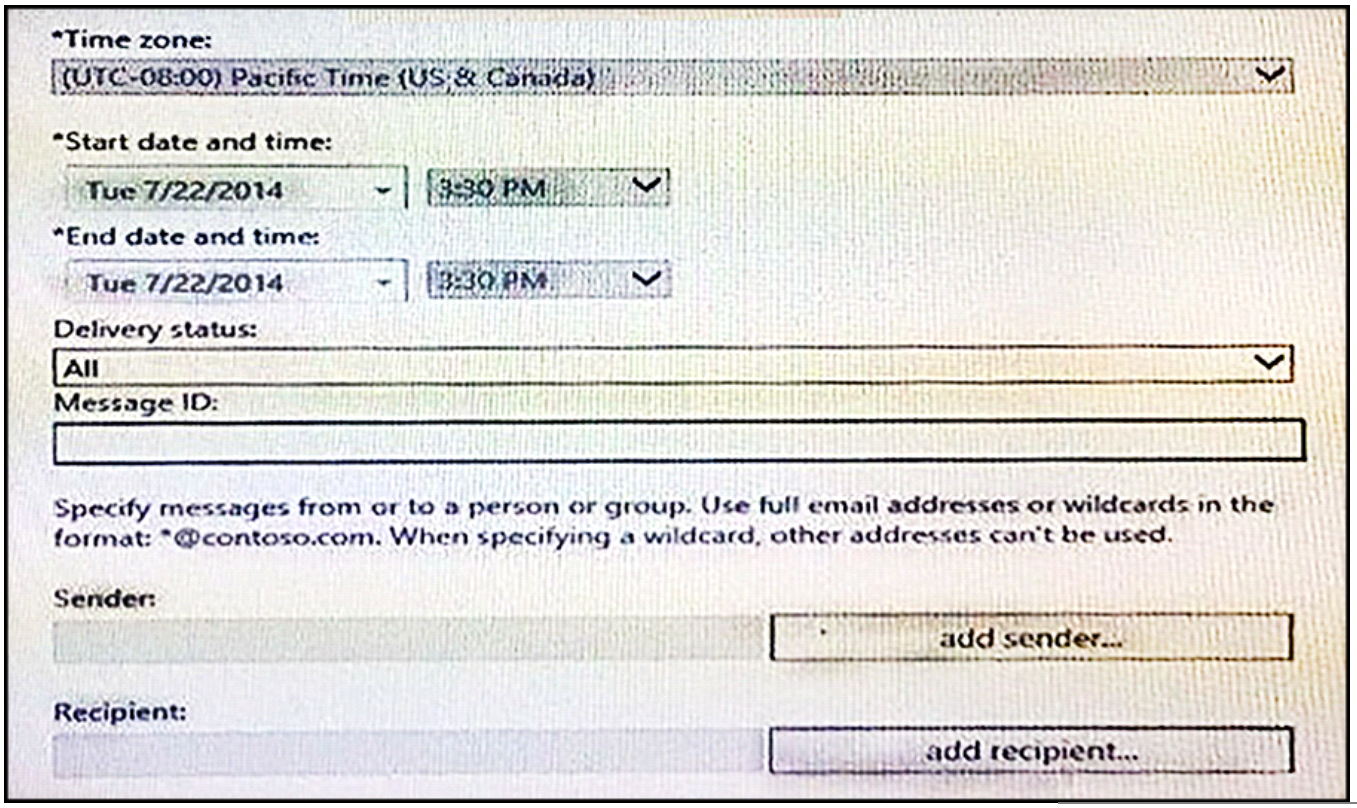
HOTSPOT

You are the Exchange Online administrator for an organization. The organization migrates all users to Exchange Online. An employee works for a partner organization named Contoso, Ltd. The employee uses the email alias employeel@contoso.com.

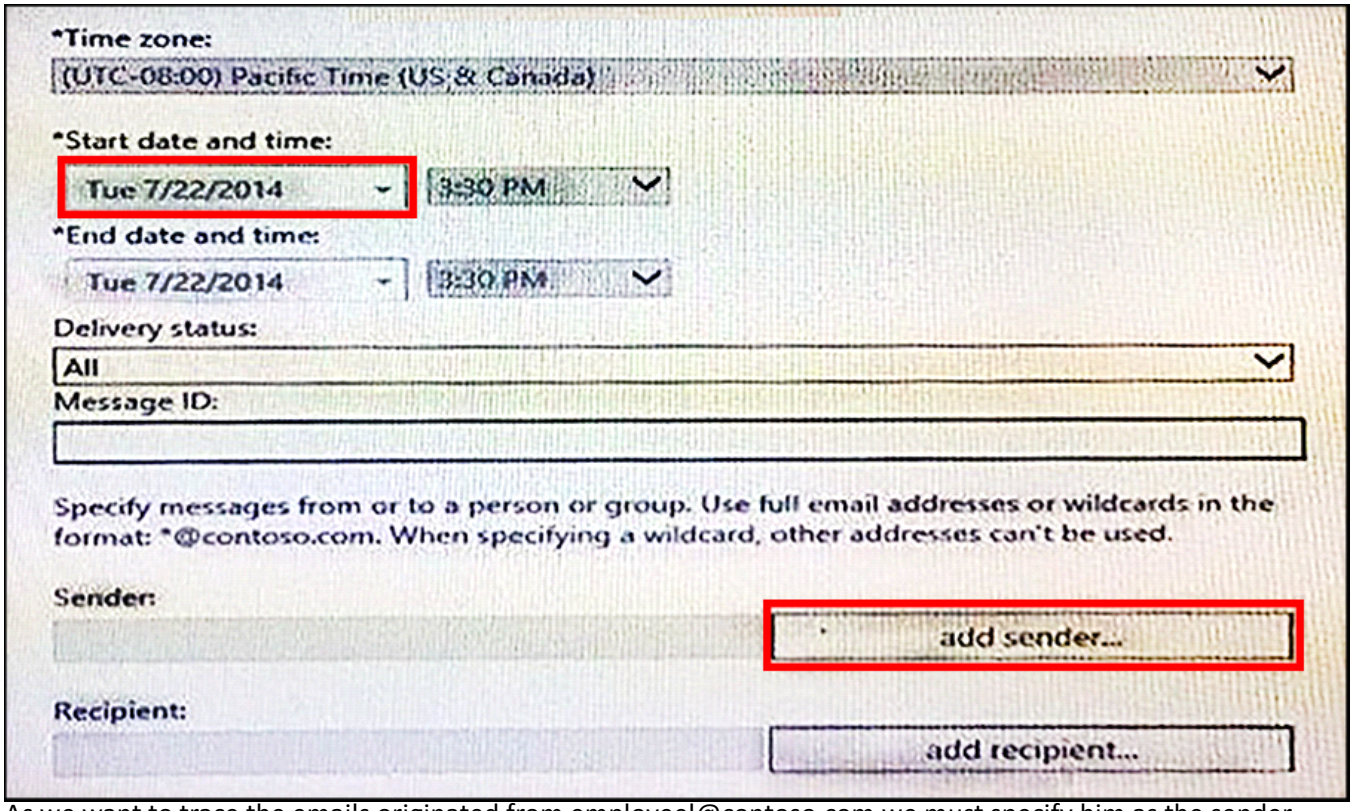
Users report that over the past week, they have not received email messages from employee1@contoso.com.

You need to trace email messages that originate from employeel@contoso.com to users inside your organization.

In the message trace window, which two settings should you configure? To answer, select the appropriate objects in the answer area.



Answer:



As we want to trace the emails originated from employeel@contoso.com we must specify him as the sender.
We also know that email messages from this user has not been received for the last 7 days. We should therefore change the start date and put it back 7 days.
References:
https://support.office.com/en-au/article/Troubleshoot-email-delivery-using-the-Exchange-Online-message-trace-tool-e7758b99-1896-41db-bf39-51e2dba21de6

Question: 48

You have an Office 365 subscription.
All users have mailboxes hosted in Microsoft Exchange Online.
The network administrators in your organization are updating the network infrastructure, including making changes to the DNS providers and updating the SSL certificates.
You need to perform the following test in the Exchange Online environment:
Verify that the mail exchanger (MX) records for Exchange Online are published correctly.
Send a test message from an external recipient to an Exchange Online recipient.
Verify that the SMTP service is accessible from the Internet.
Which tool should you use?

A. Microsoft Connectivity Analyzer Tool
B. Microsoft Remote Connectivity Analyzer
C. Microsoft Office 365 Client Performance Analyzer
D. Office 365 health, readiness, and connectivity checks
E. Microsoft Support and Recovery Assistant for Office 365

Answer: B

Explanation:
The Microsoft Connectivity Analyzer Tool includes multiple different tests that can be run online.

Question: 49

You have an Office 365 subscription that has several thousand mailboxes.
The users in the Office 365 organization are located in different regions.
You need to view the path of the email messages sent from a user to an external recipient.
Which cmdlet should you use?

A. Get-MailDetailTransportRuleReport
B. Get-MailTrafficReport
C. Get-MailboxActivityReport
D. Get-ServiceDeliveryReport

Answer: D

Explanation:
Use the Get-ServiceDeliveryReport cmdlet to view information about the message delivery path for a specified recipient.
Example:
This example shows the delivery path information for the recipient john@contoso.com.
Get-ServiceDeliveryReport -Recipientjohn@contoso.com

Question: 50

An organization is migrating from an on-premises Exchange organization to Office 365 tenant.
Users report that they cannot see the free/busy information for other users.
You need to determine why free/busy information does not display.
Which two Windows PowerShell cmdlets should you run? Each correct answer presents a complete solution.

A. Get-OrganizationRelationship
B. Get-SharingPolicy
C. Get-CsMeetingConfiguration
D. Get-CsClientPolicy
E. Get-IntraOrganizationConnector

Answer: A,D

Explanation:
A: Problem: Free/busy information can't be retrieved from one environment
Users can't access free/busy information through Exchange federation in one direction only.
To display the trust information that is currently set up for the default Office 365 domain, run the following command:
Get-OrganizationRelationship | FL
B: If the free/busy problem persists, make sure that the sharing policies in the on-premises Exchange Server environment and in Exchange Online match. To determine this, run the following command in the Exchange ManagementShell, and then note the value in the Domains field in the results:
Get-SharingPolicy | FL
References:
https://support.microsoft.com/en-us/kb/2555008

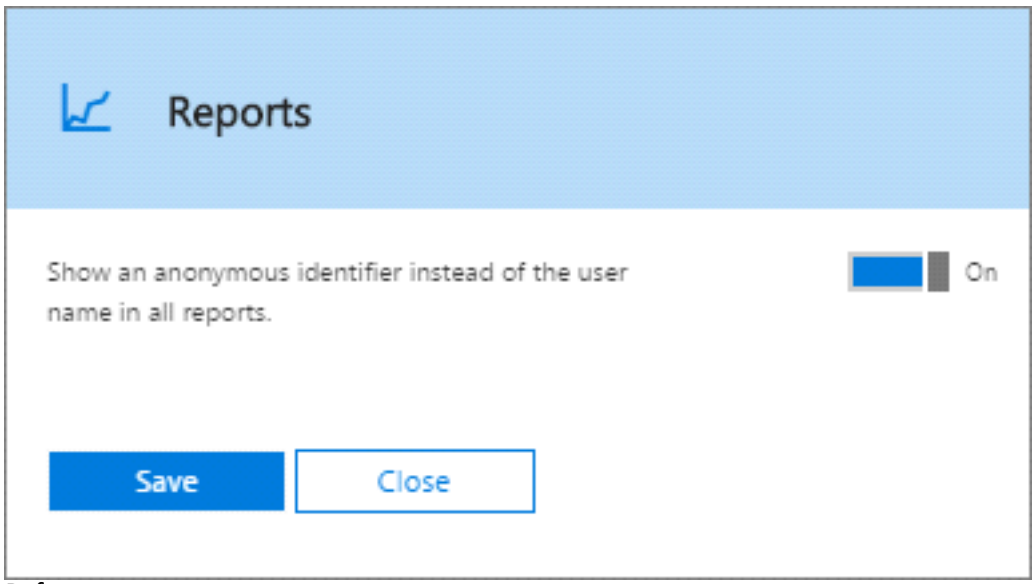
Question: 51

You have an Office 365 subscription.
You plan to create a report about Microsoft OneDrive for Business usage that will be given to a third party.
You need to ensure that the OneDrive for Business report shows anonymous identifiers instead of user names.
What should you configure from Settings in the Office 365 admin center?

A. Organization Profile
B. Services & add-ins
C. Security & privacy
D. Domains

Answer: B

Explanation:
If your organization's policies prevent you from viewing reports where user information is identifiable, you can change the privacy setting for all these reports.
If you want to hide user level information when you're generating your reports, you can quickly make that change in the Office 365 admin center.
Go to the Office 365 admin center > Services & add-ins
Select Reports
Set the toggle to On and Save.



References:
https://support.office.com/en-us/article/Activity-Reports-in-the-Office-365-admin-center-0d6dfb17-8582-4172-a9a9-aed798150263?ui=en-US&rs=en-US&ad=US

Question: 52

An Organization uses Exchange Online. You enable mailbox audit logging for all mailboxes.
User1 reports that her mailbox has been accessed by someone else.
You need to determine whether someone other than the mailbox owner has accessed the mailbox.
What should you do?

A. Run the following Windows PowerShell command: Search-MailboxAuditLog-Identity User1-LogonTypes Admin, Delegate, External-ShowDetails
B. In the Exchange Admin Center, navigate to the In-place eDiscovery & Hold section of the Protection page. Run a non-owner mailbox access report.

C. In the Exchange Admin Center, navigate to the In-place eDiscovery & Hold section of the Compliance Management page. Run a non-owner mailbox access report.
D. Run the following Windows PowerShell command: New-AdminAuditLogSearch-Identity User1-LogonTypes Admin, Delegate, External-ShowDetails

Answer: C

Explanation:
The Non-Owner Mailbox Access Report in the Exchange Administration Center (EAC) lists the mailboxes that have been accessed by someone other than the person who owns the mailbox.
Run a non-owner mailbox access report
Note: When a mailbox is accessed by anon-owner, Microsoft Exchange logs information about this action in a mailbox audit log that's stored as an email message in a hidden folder in the mailbox being audited. Entries from this log are displayed as search results and include a list of mailboxes accessed by a non-owner, who accessed the mailbox and when, the actions performed by the non-owner, and whether the action was successful.
In the EAC, navigate to Compliance Management > Auditing.
Click Run a non-owner mailbox access report.
By default, Microsoft Exchange runs the report for non-owner access to any mailboxes in the organization over the past two weeks. The mailboxes listed in the search results have been enabled for mailbox audit logging.
To view non-owner access for a specific mailbox, select the mailbox from the list of mailboxes. View the search results in the details pane
References:
https://technet.microsoft.com/en-us/library/jj150575(v=exchg.150).aspx

Question: 53

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in the question apply only to that question.
A company has an Office 365 tenant that has an Enterprise E1 subscription. You synchronize disabled user accounts from an Active Directory Domain Services environment.
You need to enable the user accounts in Office 365.
Which Windows PowerShell cmdlet should you run?

A. Set-MsolUser
B. Redo-MsolProvisionUser
C. Set-MsolUserLicense
D. Set-MsolUserPrincipalName
E. Convert-MsolFederatedUser
F. Set-MailUser
G. Set-LinkedUser
H. New-MsolUser

Answer: A

Explanation:
The Set-MsolUser cmdlet is used to update a user object. This cmdlet should be used for basic properties only.
Example: The following command sets the multi-factor authentication on this user.
Enable a user:
$st = New-Object -TypeNameMicrosoft.Online.Administration.StrongAuthenticationRequirement

$st.RelyingParty = "*"
$st.State = “Enabled”
$sta = @($st)
Set-MsolUser -UserPrincipalName user@contoso.com -StrongAuthenticationRequirements $sta

Question: 54

DRAG DROP
You have an Office 365 tenant that has an Enterprise E3 subscription. You enable Azure Rights Management for users in the tenant.
You need to define the methods that you can implement to encrypt and decrypt email messages.
What should you do? To answer, drag the appropriate method to the correct action. Each method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Answer Area

Action	Method
Send encrypted email	
Receive encrypted replies	
View encrypted email	

Transport rule
Organization account
One-time password
Text message
Connector

Answer:

Answer Area

Action	Method
Send encrypted email	Transport rule
Receive encrypted replies	Transport rule
View encrypted email	One-time password

As an Office 365 global administrator, you can create mail flow rules, also known as transport rules, to help protect email messages you send and receive. You can set up rules to encrypt any outgoing email messages and remove encryption from encrypted messages coming from inside your organization or from replies to encrypted messages sent from your organization.

To view encrypted messages, recipients can either get a one-time password, sign in with a Microsoft account, or sign in with a work or school account associated with Office 365. Recipients can also send encrypted replies. They don't need an Office 365 subscription to view encrypted messages or send encrypted replies.
References:
https://technet.microsoft.com/en-us/library/dn569289.aspx
https://technet.microsoft.com/en-us/library/dn569287.aspx

Question: 55

You are the Office 365 administrator for a company. You plan to implement rights management.
You need to activate Microsoft Azure Rights Management.
What should you use?

A. the Windows PowerShell Enable-AadrmSuperUserFeature cmdlet
B. the Office 365 Admin Center portal
C. the Windows PowerShell Set-OrganizationConfig cmdlet
D. the Microsoft Exchange Online Admin Center

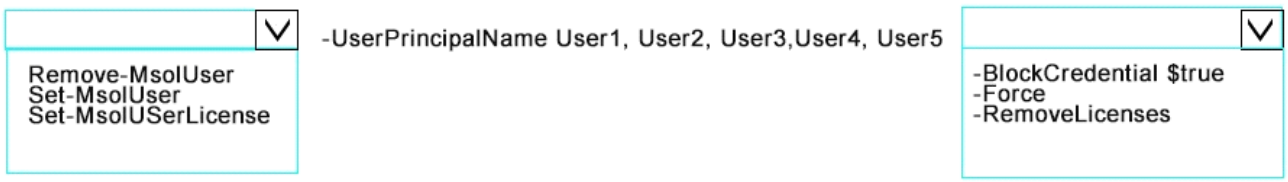
Answer: B

Explanation:
Once you have signed up for an Office 365 plan that includes Rights Management, sign in to Office 365 with a work or school account that has the global administrator role for your Office 365 deployment. You should then navigate to the rights management page via Settings > Services & add-ins > Microsoft Azure Information Protection > Manage Microsoft Azure Information Protection settings. On the rights management page, click activate.
References:
https://docs.microsoft.com/en-us/information-protection/deploy-use/activate-office365

Question: 56

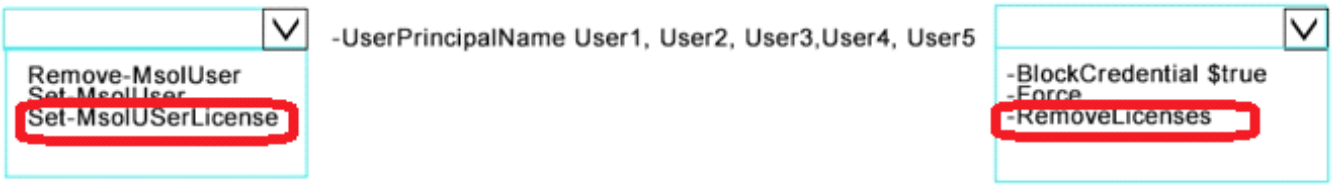
HOTSPOT
You have an Office 365 subscription.
The Office 365 organization contains five temporary administrators. The administrators are members of multiple role groups.
You need to create a script that prevents the temporary administrators from performing administrative tasks from the Office 365 admin center. The solution must meet the following requirements:
Provide the ability to reestablish administrative access to the temporary administrators within 14 days.
Release the Office 365 licenses assigned to the temporary administrators.
Which cmdlet should you run? To answer, select the appropriate options in the answer area.

Answer Area



Answer:

Answer Area



The Set-MsolUserLicense cmdlet can be used to adjust the licenses for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.
Example:
The following command removes the for enterprises license from the user. This may result in the user's data being removed from each service.
Set-MsolUserLicense -UserPrincipalName user@contoso.com -RemoveLicenses "contoso:ENTERPRISEPACK"
References:
https://msdn.microsoft.com/en-us/library/azure/dn194094(v=azure.98).aspx

Question: 57

DRAG DROP
A company deploys an Office 365 tenant. All employees use Skype for Business Online.
You need to configure the network firewall to support Skype for Business Online.
Which ports must you open? To answer, drag the appropriate port number to the correct feature or features. Each port number may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Answer Area

Port Number

443

3478

5223

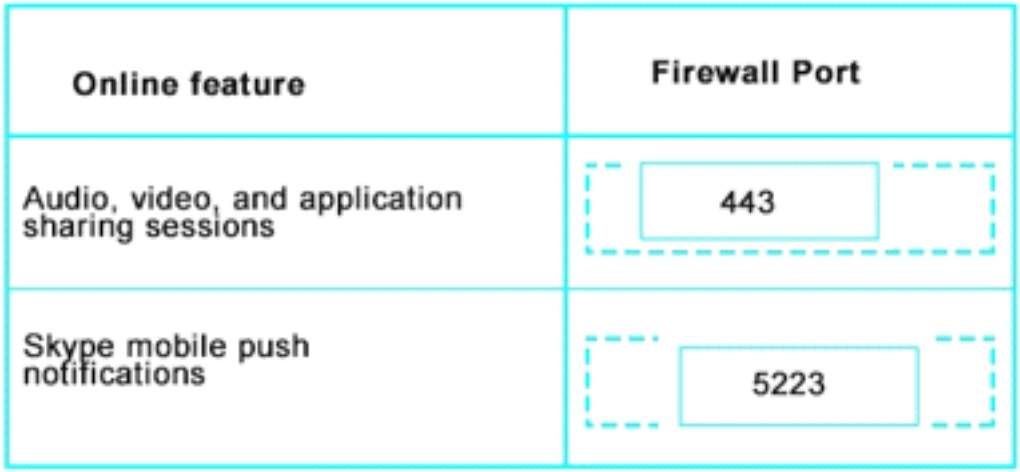
80

389

Online feature	Firewall Port
Audio, video, and application sharing sessions	*Port number*
Skype mobile push notifications	*Port number*

Answer:

Answer Area



Transport Control Protocol (TCP), User Datagram Protocol (UDP) ports, and Protocol Numbers are important to TCP/IP networking, intranets, and the Internet. Ports and protocol numbers provide access to a host computer. However, they also create a security hazard by allowing uninvited access. Therefore, knowing which port to allow or disable increases a network's security. If the wrong ports or protocol numbers are disabled on a firewall, router, or proxy server as a security measure, essential services might become unavailable.
Port 443 is used for Audio, video and application sharing sessions as well as data sharing sessions - For HTTPS.
Port 5223 is used for mobile push notifications - Extensible Messaging and Presence Protocol (XMPP) client connection over SSL.

Question: 58

You have a legacy application that needs to send email to employees.
The legacy application runs on a client computer that must send email by using SMTP through Exchange Online.
You need to identify the correct host name and port information.
Which settings should you use?

A. Outlook.office365.com and port 25
B. Outlook.office365.com and port 587
C. Smtp.office365.com and port 587
D. Smtp.office365.com and port 25

Answer: D

Explanation:
The legacy applications would use port 25 for smtp. The host name should be Smtp.office365.com.

Question: 59

An organization plans to migrate to Office 365.
You need to estimate the post-migration network traffic.
Which two tools will achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Exchange Client Network Bandwidth Calculator
B. Microsoft Remote Connectivity Analyzer
C. Skype for Business Bandwidth Calculator
D. Windows Assessment and Deployment Kit (ADK)
E. Process Monitor

Answer: A,C

Explanation:
There are calculators available to assist you with estimating network bandwidth requirements. These calculators work for on-premises as well as Office 365 deployments. You can use the Exchange client network bandwidth calculator to estimate the bandwidth required for a specific set of Outlook, Outlook Web App, and mobile device users in your Office 365 deployment. With the Skype for Business bandwidth calculator, you enter information about users and the Skype for Business features you want to deploy, and the calculator helps you determine bandwidth requirements.
Skype for Business Bandwidth Calculator - A Microsoft Excel spreadsheet that calculates WAN bandwidth requirements for a Skype for Business Server deployment based on administrator-specified user profiles and network information.

Question: 60

DRAG DROP
You have an Office 365 subscription and an on-premises deployment of Active Directory. The environment also contains a deployment of Active Directory Federation Services (AD FS).
The AD FS deployment contains an AD FS server named ADFS1 and a Web Application Proxy server named WAPSERVER1.
The service communications certificate expires in one day.
You need to replace the certificate on the servers in the AD FS deployment. The solution must maintain client encryption.

Actions		Answer Area
On ADFS1, run the **Set-AdfsSslCertificate** cmdlet and the **Set-AdfsCertificate** cmdlet.	1	
Install a new self-signed certificate on each server.	2	
Install a new certificate from a trusted third-party certification authority (CA) on each server.	3	
On WAPSERVER1, run the **Set-WebApplicationProxySslCertificate** cmdlet.		
On ADFS1, run the **Update-AdfsCertificate** cmdlet		

Answer:

Actions		Answer Area
On ADFS1, run the **Set-AdfsSslCertificate** cmdlet and the **Set-AdfsCertificate** cmdlet.	1	Install a new certificate from a trusted third-party certification authority (CA) on each server.
Install a new self-signed certificate on each server.	2	On ADFS1, run the **Set-AdfsSslCertificate** cmdlet and the **Set-AdfsCertificate** cmdlet.
Install a new certificate from a trusted third-party certification authority (CA) on each server.	3	On WAPSERVER1, run the **Set-WebApplicationProxySslCertificate** cmdlet.
On WAPSERVER1, run the **Set-WebApplicationProxySslCertificate** cmdlet.		
On ADFS1, run the **Update-AdfsCertificate** cmdlet		

Question: 61

An organization migrates to Office 365.
The Office 365 administrator must be notified when Office 365 maintenance activities are planned.
You need to configure the administrator's computer to receive the notifications.
What should you configure?

A. Office 365 Business Connectivity Service
B. Service requests
C. Service health page
D. Office 365 Service Health RSS Notifications feed

Answer: D

Explanation:
You can log in to Office 365 as an Office 365 Administrator and view the Service Health Page to view the status of your Office 365 services. You can use the Service Health Page to view information on the status of your services for the current day or you can select the last 6 days or 30 days for a historical view.
In the top right corner of the Service Health page, there is an RSS icon. You can click on the RSS icon to sign up for the service health RSS feed, which will email you when a new event is added or an existing event is updated.

Question: 62

An Organization uses Exchange Online. You enable mailbox audit logging for all mailboxes.
User1 reports that her mailbox has been accessed by someone else.
You need to determine whether someone other than the mailbox owner has accessed the mailbox.
What should you do?

A. Run the following Windows PowerShell command: Search-MailboxAuditLog-Identity User1-LogonTypes Admin, Delegate, External-ShowDetails
B. In the Exchange Admin Center, navigate to the Auditing section of the Protection page. Run a non-owner mailbox access report.
C. In the Exchange Admin Center, navigate to the In-place eDiscovery & Hold section of the Compliance Management page. Run a non-owner mailbox access report.

D. Run the following Windows PowerShell command: New-AdminAuditLogSearch-Identity User1-LogonTypes Admin, Delegate, External-ShowDetails

Answer: C

Explanation:
The Non-Owner Mailbox Access Report in the Exchange Administration Center (EAC) lists the mailboxes that have been accessed by someone other than the person who owns the mailbox.
Run a non-owner mailbox access report
Note: When a mailbox is accessed by a non-owner, Microsoft Exchange logs information about this action in a mailbox audit log that's stored as an email message in a hidden folder in the mailbox being audited. Entries from this log are displayed as search results and include a list of mailboxes accessed by a non-owner, who accessed the mailbox and when, the actions performed by the non-owner, and whether the action was successful.
References:
https://technet.microsoft.com/en-us/library/jj150575(v=exchg.150).aspx

Question: 63

Your company purchases an Office 365 plan. The company has an Active Directory Domain Services domain.
User1 must be able to manage Office 365 delegation for the company.
You need to ensure that User1 can assign administrative roles to other users.
What should you do?

A. Create an Office 365 tenant and assign User1 the service administrator role.
B. Use an existing user management administrator account to assign a role with the correct permissions to User1.
C. Create an Office 365 tenant and assign User1 the global administrator role.
D. Create an Office 365 tenant and assign User1 the user management administrator role.

Answer: D

Explanation:
D: The Global Administrator account is similar to the Company administrator. Users in this role have access to everything or the permission to add them to a dedicated role where they do not have permission (such as discovery management and assigning administrative roles to other users).

Question: 64

You are planning an Office 365 pilot.
You need to ensure that the environment is ready for Office 365.
Which tool should you use?

A. Microsoft Connectivity Analyzer
B. Office 365 Best Practices Analyzer
C. Remote Connectivity Analyzer
D. Office 365 Health, Readiness, and Connectivity Checks

Answer: D

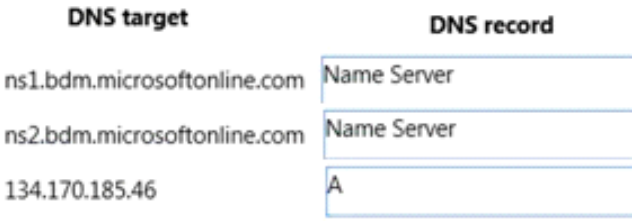
Explanation:
Running Office 365 Health, Readiness, and Connectivity Checks prior to setting up Office 365 allows you to make sure

that your environment is prepared for the Office 365 services. It can find settings in your existing environment that might cause problems when you start to set up or use your services. This will allow you to fix or work around the potential problems to make your deployment path easier to complete.
References:
https://support.office.com/en-us/article/Office-365-readiness-checks-c01571b8-183e-4a61-9ca0-80729a48bbda

Question: 65

DRAG DROP
A company has an Office 365 tenant. You plan to use Office 365 to manage the DNS settings for a custom domain. You purchase the domain through a third-party provider.
You create a custom website. You must host the website through a third-party provider at the IPv6 address 2001:4860:4801:1:5:4d. You need to configure the correct DNS settings.
What should you do? To answer, drag the appropriate DNS record to the correct DNS target. Each record may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Answer:



Change your domain's name server (NS) records
When you get to the last step of the domains setup wizard in Office 365, you have one task remaining. To set up your domain with Office 365 services, like email, you change your domain's name server (or NS) records at your domain registrar to point to the Office 365 primary and secondary name servers.
Use (A) DNS record for the web site.

Question: 66

You are an Office 365 administrator for your company. You enable mailbox auditing for all user mailboxes.
You receive reports that someone is accessing another user's mailbox without authorization.
You need to identify which account was used to access the mailbox in Microsoft Exchange Online.
What should you run?

A. the PowerShell cmdlet Search-AdminAuditLog
B. the PowerShell cmdlet New-AdminAuditLogSearch
C. the non-owners' mailbox access report

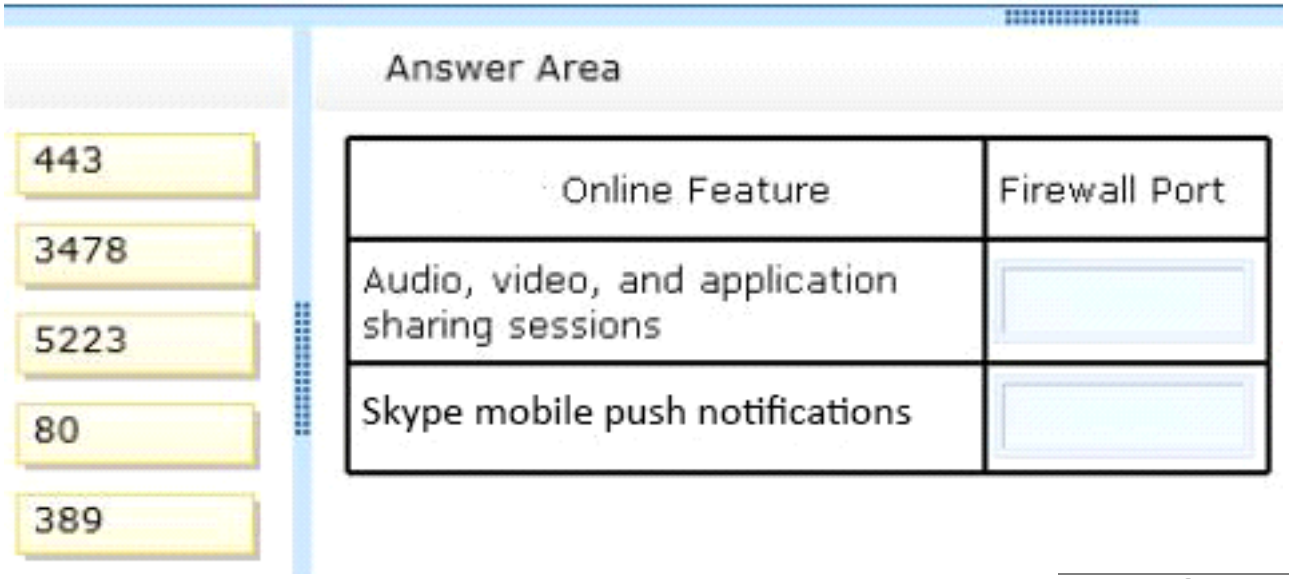
D. the mailbox content search and hold report

Answer: C

Explanation:
The Non-Owner Mailbox Access Report in the Exchange admin center (EAC) lists the mailboxes that have been accessed by persons who do not own the mailbox.
References:
https://technet.microsoft.com/en-us/library/jj150575(v=exchg.160).aspx

Question: 67

DRAG DROP
A company deploys an Office 365 tenant. All employees use Skype for Business Online.
You need to configure the network firewall to support Skype for Business Online.
Which ports must you open? To answer, drag the appropriate port number to the correct feature or features. Each port number may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:

Online Feature	Firewall Port
Audio, video, and application sharing sessions	443
Skype mobile push notifications	5223

Transport Control Protocol(TCP), User Datagram Protocol(UDP) ports, and Protocol Numbers are important to TCP/IP networking, intranets, and the Internet. Ports and protocol numbers provide access to a host computer. However, they also create a security hazard by allowing uninvited access. Therefore, knowing which port to allow or disable increases a network's security. If the wrong ports or protocol numbers are disabled on a firewall, router, or proxy server as a security measure, essential services might become unavailable.
Port 443 is used for Audio, video and application sharing sessions as well as data sharing sessions - For HTTPS.

Port 5223 is used for mobile push notifications - Extensible Messaging and Presence Protocol (XMPP) client connection over SSL.

Question: 68

HOTSPOT

You work for a company named Contoso Ltd. The company deploys Office 365. Only cloud-based identities are used to access Office 365 resources.

Users must be able to log in Office 365 after create new accounts.

You need to reset passwords for all company employees.

What should you do? To answer, select the appropriate Windows PowerShell segment in the dialog box in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
Import-Module MSOnline
$Cred = Get-Credential
$Pass = "!Summer2020"
```

[▼] -Credential $Cred

- Connect-MsolService
- Connect-PSSession
- Select-AzureSubscription

[▼]

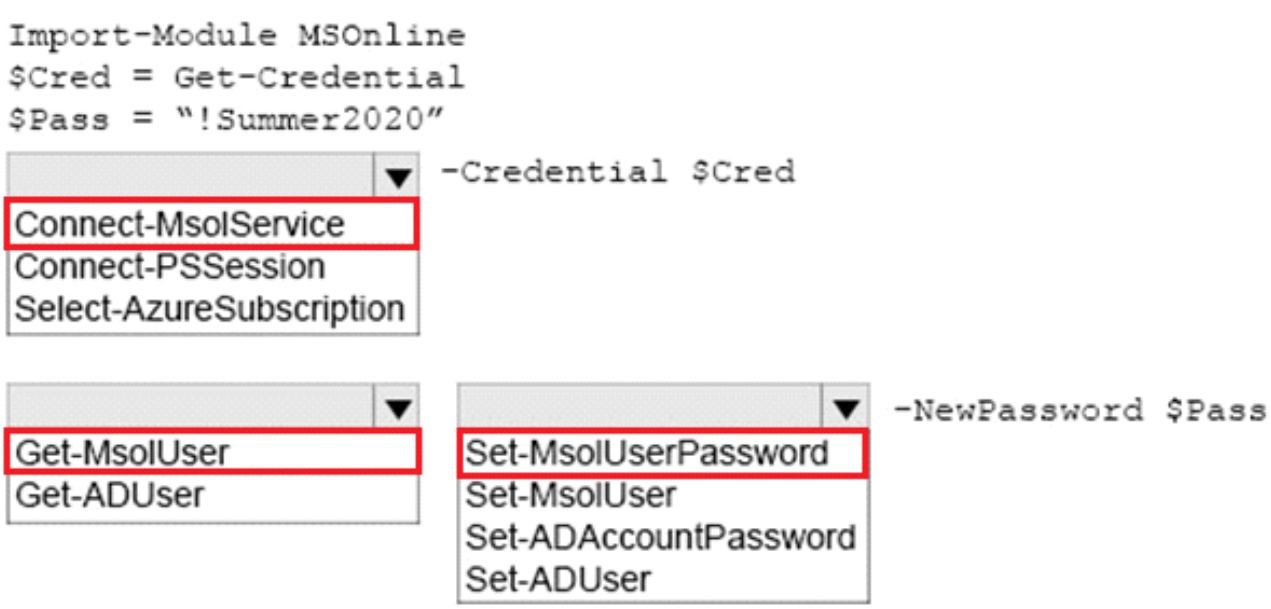
- Get-MsolUser
- Get-ADUser

[▼] -NewPassword $Pass

- Set-MsolUserPassword
- Set-MsolUser
- Set-ADAccountPassword
- Set-ADUser

Answer:

Answer Area



The Connect-MsolService cmdlet attempts to initiate a connection to Azure Active Directory. Running the Get-MsolUser cmdlet without parameters retrieves all users in the company.
The Set-MsolUserPassword cmdlet resets the password for a user.
References:
https://www.lewan.com/blog/2012/01/10/microsoft-office-365-how-to-reset-all-user-passwords
https://docs.microsoft.com/en-us/powershell/module/msonline/connect-msolservice?view=azureadps-1.0
https://docs.microsoft.com/en-us/powershell/module/msonline/get-msoluser?view=azureadps-1.0
https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserpassword?view=azureadps-1.0

Question: 69

Note: This question is part of a series of questions that use the same or similar answer choices. An answer choice may be correct for more than one question in the series. Each question is independent of the other questions in this series. Information and details provided in the question apply only to that question.
A company has an Office 365 tenant that has an Enterprise E1 subscription. You synchronize disabled user accounts from an Active Directory Domain Services environment.
You need to enable the user accounts in Office 365.
Which Windows PowerShell cmdlet should you run?

A. Set-MsolUser
B. Redo-MsolProvisionUser
C. Set-MsolUserLicense
D. Set-MsolUserPrincipalName
E. Convert-MsolFederatedUser
F. Set-MailUser
G. Set-LinkedUser

Answer: A

Explanation:
The Set-MsolUser cmdlet is used to update a user object. This cmdlet should be used for basic properties only.

Example: The following command sets the multi-factor authentication on this user.
Enable a user:
$st = New-Object -TypeName Microsoft.Online.Administration.StrongAuthenticationRequirement
$st.RelyingParty = "*"
$st.State = “Enabled”
$sta = @($st)
Set-MsolUser -UserPrincipalName user@contoso.com -StrongAuthenticationRequirements $sta

Question: 70

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Office 365 subscription.
Several users report that they fail to connect to Microsoft Skype for Business Online by using the Skype for Business 2016 client.
You verify that you can connect to Skype for Business Online successfully from your computer.
You need to identify what prevents the users from connecting to Skype for Business Online.
Solution: You use the Microsoft Support and Recovery Assistant for Office 365.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Use the Microsoft Skype for Business Connectivity Analyzer instead.

Question: 71

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Office 365 subscription.
Several users report that they fail to connect to Microsoft Skype for Business Online by using the Skype for Business 2016 client.
You verify that you can connect to Skype for Business Online successfully from your computer.
You need to identify what prevents the users from connecting to Skype for Business Online.
Solution: You use the Microsoft Skype for Business Connectivity Analyzer.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
The Microsoft Skype for Business Connectivity Analyzer tool has a very specific purpose. It is meant to determine if a Skype for Business environment, either on-prem or Skype for Business Online, meets the necessary requirements for client connectivity from mobile clients and the Skype for Business Windows Store App.
The tool, in the course of its analysis, tests several components. Among them, it checks public DNS records to make sure the necessary A records and SRV records are in place. It also checks the proxy configuration for the environment. Lastly, but definitely not least important, it checks on the validity of the SSL certificates that are in place.
References:
http://blog.get-csjosh.com/2015/05/microsoft-remote-connectivity-analyzer-and-associated-tools.html

Question: 72

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an on-premises Active Directory forest.
You deploy Active Directory Federation Services (AD FS) and purchase an Office 365 subscription.
You need to create a trust between the AD FS servers and the Office 365 subscription.
Solution: You run the New-MsolDomain cmdlet.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The New-MsolDomain cmdlet adds a domain to Azure Active Directory.
The New-MsolFederatedDomain command should be used instead.
Note: The New-MsolFederatedDomain cmdlet adds a new single sign-on domain to Microsoft Online Services and configures the relying party trust settings between the on-premises Active Directory Federation Services 2.0 server and Microsoft Online.
References:https://docs.microsoft.com/en-us/powershell/msonline/v1/new-msolfederateddomain

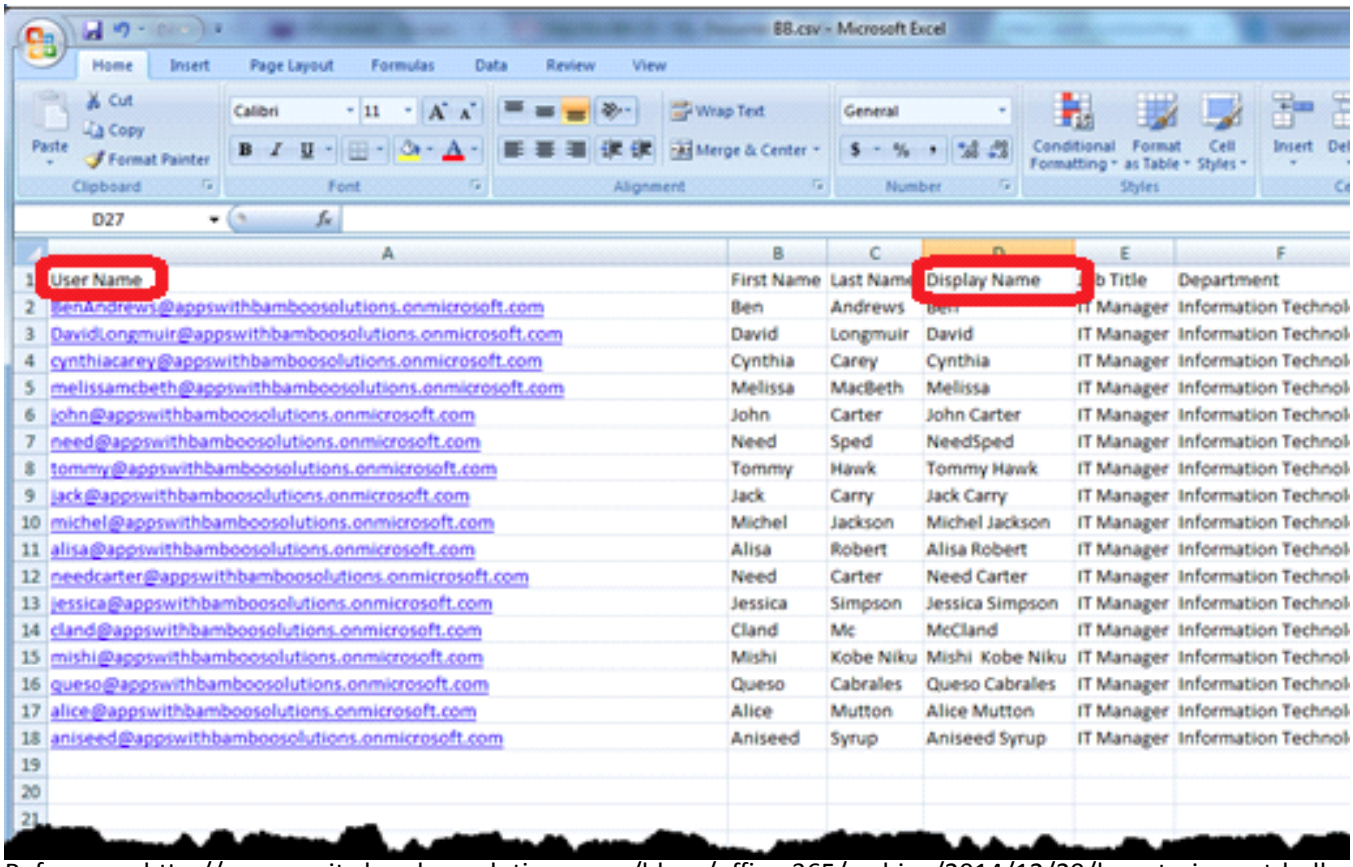
Question: 73

You plan to import several user accounts to an Office 365 subscription by using a CSV file.
You download a sample CSV file from the Office 365 admin center.
You need to prepare the file for the planned import.
What should you do?

A. Add a column named Managed By.
B. Add values to the UserName and Country columns.
C. Add values to the UserName and DisplayName columns.
D. Add a column named Password.

Answer: C

Explanation:
Example of CSV file content:



References:http://community.bamboosolutions.com/blogs/office-365/archive/2014/12/29/how-to-import-bulk-user-accounts-to-office-365-from-a-csv-file.aspx

Question: 74

You are the Office 365 administrator for your company.
You must use Windows PowerShell to manage cloud identities in Office 365. You must use a computer that runs Windows 8 to perform the management tasks.
You need to ensure that the Windows 8 computer has the necessary software installed.
What should you install first?

A. Microsoft Office 365 Best Practices Analyzer for Windows PowerShell
B. Windows PowerShell 4.0
C. Azure Active Directory Module for Windows PowerShell
D. Windows Management Framework

Answer: C

Explanation:
Cloud identities in Office 365 are user accounts in Azure Active Directory.
You can use Windows PowerShell to administer Office 365 and Azure Active Directory. However, the default installation of Windows PowerShell on Windows 8 (or any other version of Windows) does not include the PowerShell cmdlets required to manage Office 365 or Azure Active Directory.
You need to install the PowerShell module that includes the necessary cmdlets for managing Azure Active Directory.

This module is the Windows Azure Active Directory Module for Windows PowerShell module. This module also requires that Microsoft .NET Framework 3.5 is installed and enabled.
Before the Windows Azure Active Directory Module for Windows PowerShell, can be installed, the Microsoft Online Services Sign-in Assistant must be installed. This will allow you to connect to your Office 365/Azure subscription from a PowerShell session on a remote computer.

Question: 75

You have an Office 365 subscription that contains 500 user accounts.
None of the Office 365 users are forced to use a strong password.
You need to force all of the users to use a strong password.
Which cmdlet should you use?

A. Set-ADUser
B. Set-MsolUser
C. Set-MsolUserPassword
D. Set-MsolPasswordPolicy

Answer: B

Explanation:
Force the users to use a strong password with the Set-MSOlUser cmdlet.
References:https://blogs.technet.microsoft.com/heyscriptingguy/2014/08/05/use-powershell-to-force-office-365-online-users-to-change-passwords/

Question: 76

You have an Office 365 tenant that has an Enterprise E3 subscription. You configure multi-factor authentication for all users in the tenant. Remote users configure Outlook 2016 to use their Office 365 credentials.
You need to ensure that users only authenticate with Office 365 by using two-step verification.
What should you do?

A. Disable app passwords for the user accounts.
B. Remove the rights management license from the user accounts.
C. Modify the license type of the user accounts to an Enterprise E1 subscription.
D. Add the user accounts to a new security group.

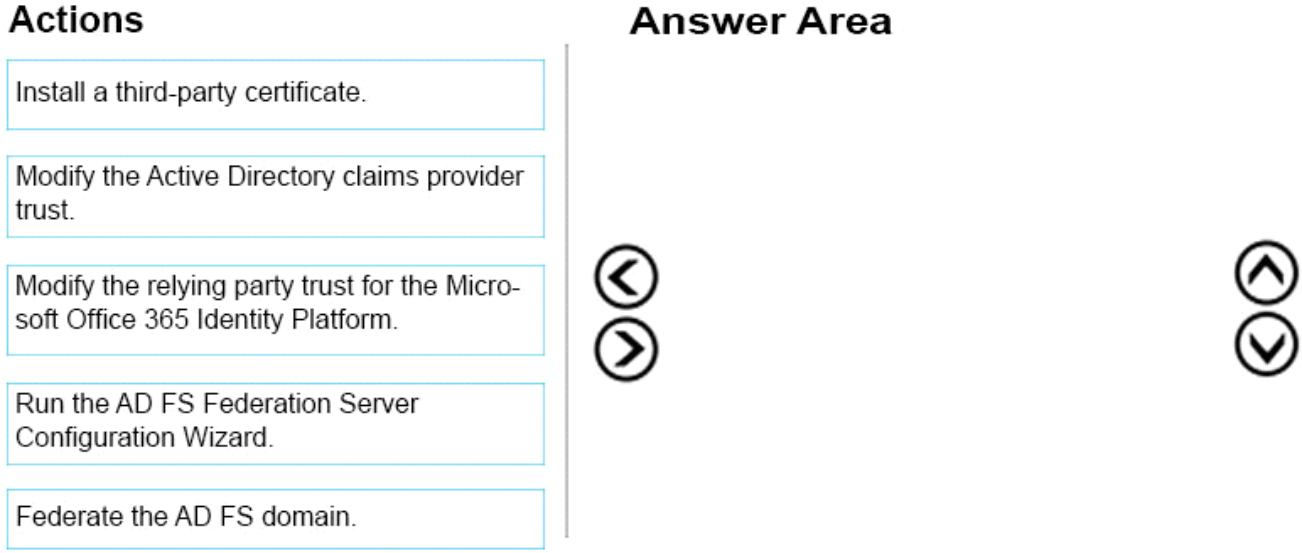
Answer: A

Explanation:
All the Office 2016 client applications support multi-factor authentication through the use of the Active Directory Authentication Library (ADAL). This means that app passwords are not required for Office 2016 clients.
References:https://support.office.com/en-us/article/Set-up-multi-factor-authentication-for-Office-365-users-8f0454b2-f51a-4d9c-bcde-2c48e41621c6

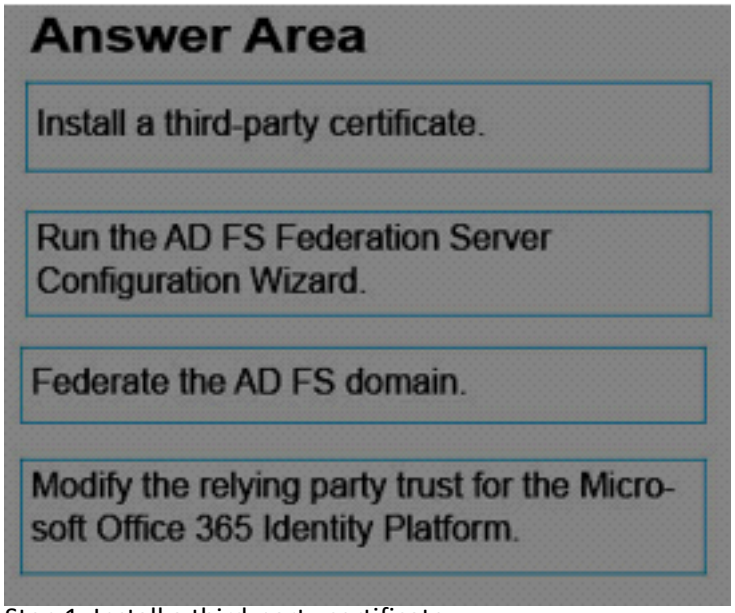
Question: 77

DRAG DROP
Your organization has an Office 365 subscription. Microsoft Azure AD Connect is deployed to the organization.
You need to deploy Active Directory Federation Services (AD FS) to meet the following requirements:

Use an AD FS namespace of sts.fabrikam.com.
Allow mobile devices to connect from untrusted networks and prevent all other devices from connecting from untrusted networks.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Step 1: Install a third-party certificate.
Since AD FS leverages SSL, we need to have a SSL certificate.
Before starting the AD FS configuration wizard install a third-party certificate.
Step 2: Run the AD FS Federation Server Configuration Wizard.
Step 3: Federate the AD FS Domain
We must change the Office 365 domain to be a federated domain.
Step 4: Modify the relying party trust for the Microsoft Office 365Identity Platform
After enabling claims-based authentication, the next step is to add and configure the claims provider and relying party trusts in AD FS.
After you enable claims-based authentication, you must configure Microsoft Dynamics 365 Server as are lying party to consume claims from AD FS for authenticating internal claims access.

References:
https://blogs.technet.microsoft.com/rmilne/2014/04/28/how-to-install-adfs-2012-r2-for-office-365/
https://technet.microsoft.com/en-us/library/gg188595.aspx

Question: 78

Your company has an Office 365 subscription that is configured for single sign-on (SSO) to an on-premises deployment of Active Directory.
Office 2016 is deployed to all workstations. Microsoft OneDrive for Business is used to replicate My Documents to OneDrive for Business.
You need to ensure that when clients connect to Office 365 from an untrusted network, they can access Office 365 resources by using a web browser.
Which two actions should you perform? Each correct answer presents part of the solution.

A. Modify the Sharing settings for SharePoint Online.
B. Disable modern authentication.
C. Add a claims provider trust.
D. Add a relying party trust.
E. Add a new rule.

Answer: B,C

Explanation:
B: In Skype for Business Server 2015, Modern Authentication is used between on-premises clients and on-premises servers in order to give users a proper level of authorization to resources.
C: A Claims Provider trust is one where ADFS gets claims from the Claim Provider, which could be the local AD as Claims Provider or an external Claims Provider.

Question: 79

A company has an Office 365 tenant.
You need to verify domain ownership.
What two options can you use? Each correct answer presents a complete solution.

A. Create an MX record.
B. Create a CNAME record.
C. Create an A record.
D. Create an SRV record.
E. Create an TXT record.

Answer: A,E

Explanation:
Add a TXT or MX record for DNS verification.
References:

Question: 80

You plan to migrate from a third-party IMAP email system to an Office 365 tenant.
You must ensure that the tenant passes the health, readiness, and connectivity steps. The solution must also provide step-by-step assistance to migrate email account.

You need to plan the migration.
What should you do?

A. Run the Domains setup wizard.
B. Use the Remote Connectivity Analyzer.
C. Run the Office 365 advanced setup wizard.
D. Use the Office 365 Service Health Dashboard.

Answer: C

Explanation:
Use the Office 365 Setup wizard to perform an IMAP migration.
The advance setup wizard can run automated checks to discover how your current environment is set up and then, based on what is found, recommend a path to Office 365. If you tell Office 365 Setup wizard that your source email system uses IMAP, and you have fewer than 151 mailboxes, it recommends that you use the Office 365 Setup wizard to copy your users email to Office 365 by using IMAP migration.
References:https://support.office.com/en-us/article/Use-the-Office-365-Setup-wizard-to-perform-an-IMAP-migration-d0800530-22fa-4ec5-9a29-efe900f2e3d0

Question: 81

A company has offices in New York and London. The current on-premises Exchange 2013 organization has servers in both sites. Mailboxes for users located in New York are on an Exchange server in the New York office. Mailboxes for users located in London are on an Exchange server in the London office.
You must migrate all mailboxes to Exchange Online. You create an Office 365 tenant and specify the company's New York address.
You need to determine where the user's mailboxes will be created.
Where are the mailboxes created in Exchange Online?

A. Mailboxes for users in London are created in European datacenters. Mailboxes for users in New York are created in North American datacenters.
B. All user mailboxes are created in North American datacenters.
C. All user mailboxes are created in a random datacenter anywhere in the world.
D. During the migration process, an administrator must specify the region where each mailbox is created.

Answer: B

Explanation:

Question: 82

You have a SharePoint Online tenant. A user named User1 manages several site collections.
User1 must be able to view the following information for the site collections:
a list of side administrators
the number of subsites in a site collection
storage and usage quotas
You need to ensure that User1 can view the requested reports while minimizing the privileges that you grant to User1.
Which two permission levels can you assign to User1? Each correct answer presents a complete solution.

A. Global admin

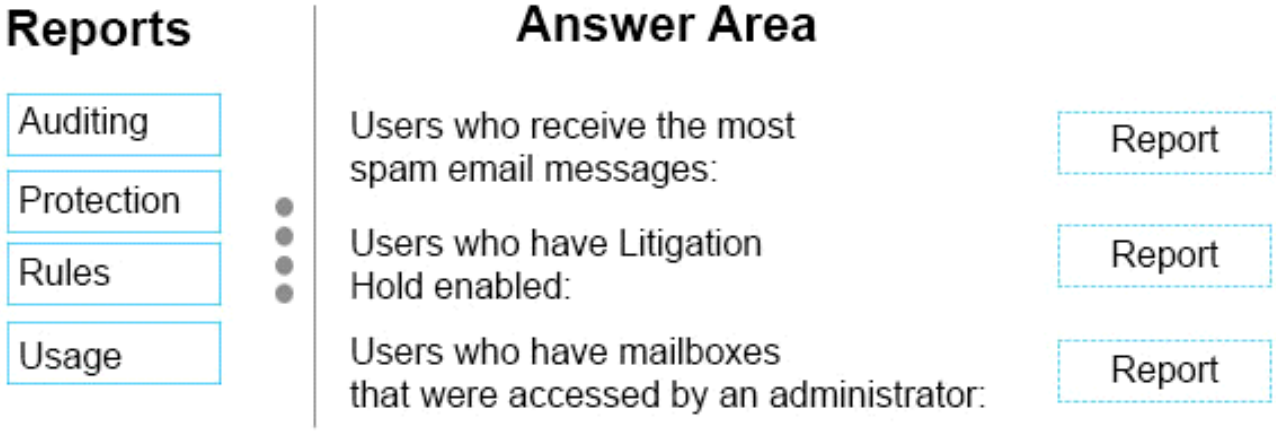
B. SharePoint Online admin
C. Site Collection admin
D. Site admin
E. User management admin
F. Service admin

Answer: B,C

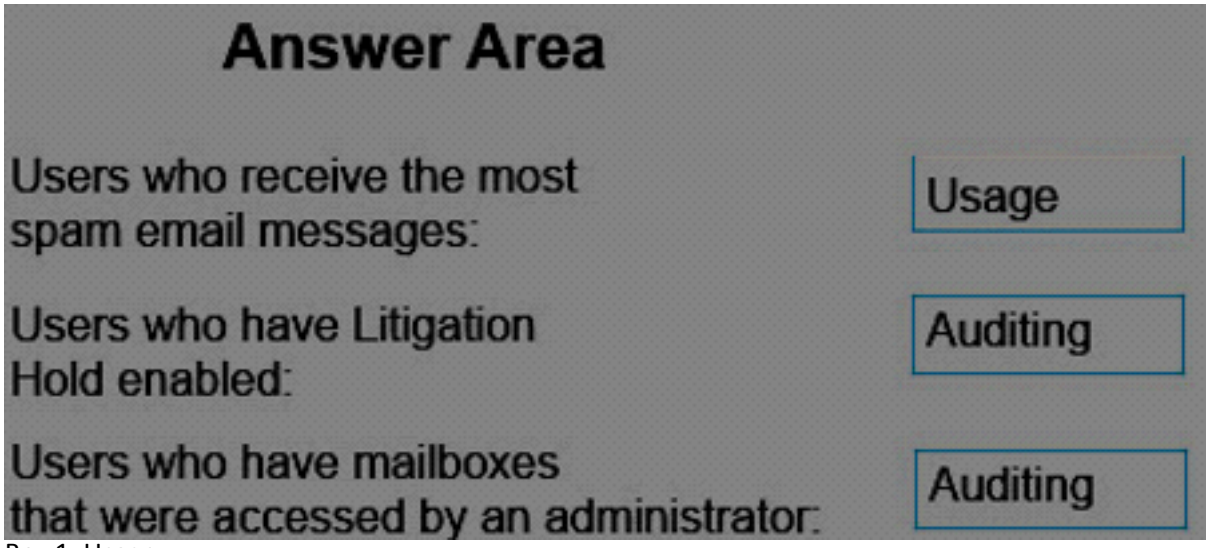
Explanation:
C: The Site collection administrator has permissions to manage a site collection.
B: Here are some of the key tasks users can do when they are assigned to the SharePoint Online admin role:
Create site collections
Manage site collections and global settings
Assign site collection administrators to manage site collections
Manage site collection storage limits
Manage SharePoint Online user profiles
References:
https://support.office.com/en-us/article/About-the-SharePoint-Online-admin-role-f08144d5-9d50-4922-8e77-4e1a27b40705#bk_keytasks

Question: 83

DRAG DROP
You have an Office 365 subscription.
The Office 365 organization contains 500 users.
You need to identify the following users in the organization:
users who have Litigation Hold enabled
users who receive the most spam email messages
users who have mailboxes that were accesses by an administrator
Which type of report should you review to identify each type of user? To answer, drag the appropriate reports to the correct types of users. Each report may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



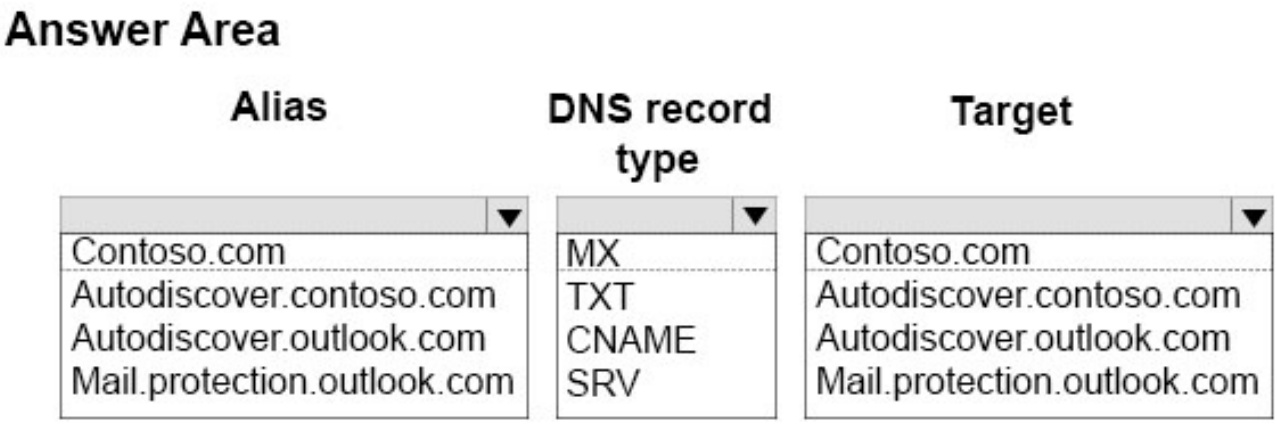
Answer:



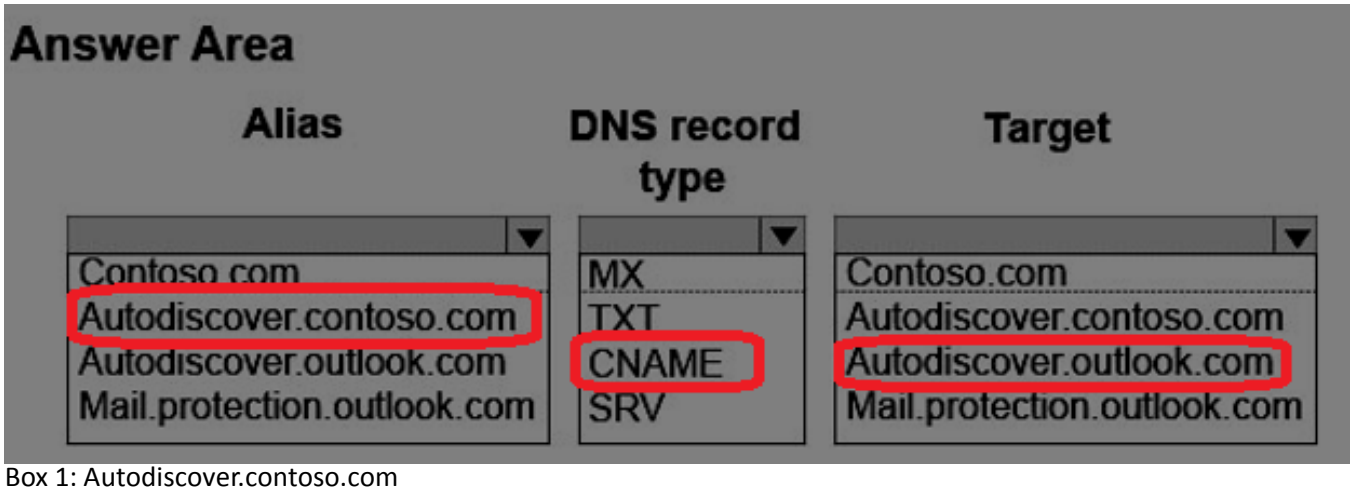
Box 1: Usage
Box 2: Auditing
To run a litigation hold report
Select Manage My Organization > Roles & Auditing > Auditing.
Click Run a litigation hold report
Box 3: Auditing
References:https://mshiyas.wordpress.com/tag/run-a-litigation-hold-report-in-office-365/

Question: 84

HOTSPOT
A company uses Exchange Online. You plan to use the email domain contoso.com for all employees.
You must configure Exchange Online to support Outlook 2016 client connectivity.
You need to configure the appropriate DNS entries.
Which record should you create? To answer, select the appropriate entries from each list in the answer area.



Answer:



Box 1: Autodiscover.contoso.com
You can define an alias in one domain to point to a target server in a completely different domain.
Box 2: CNAME
The cloud-based service uses a CNAME record to implement the Autodiscover service for Outlook clients.
Box 3: Autodiscover.outlook.com
The Autodiscover CNAME record must contain the following information:
Alias autodiscover
Target autodiscover.outlook.com
References:https://msdn.microsoft.com/en-us/library/cc950655(v=exchsrvcs.149).aspx

Question: 85

You have an Office 365 tenant that uses an Enterprise E3 subscription. You activate Azure Rights Management for the tenant.
You need to deploy Azure Rights Management for all users.
Which Windows PowerShell cmdlet should you run?

A. Enable-Aadrm
B. New-AadrmRightsDefinition
C. Enable-AadrmSuperUserFeature
D. Add-AadrmSuperUser
E. Set-AadrmOnboardingControlPolicy

Answer: A

Explanation:
The Enable-Aadrm cmdlet enables your organization to use Azure Rights Management when you have a subscription that includes this service.

Question: 86

You have an Office 365 subscription and an on-premises deployment of Active Directory.
You deploy Microsoft Azure AD Connect.
Currently, the synchronization process is running.
You need to modify the synchronization schedule.
Which task should you perform first?

A. Enable staging mode.
B. Invoke an Azure Active Directory (Azure AD) sync cycle profile.

C. Create an Azure Active Directory (Azure AD) sync connector.
D. Start the Azure AD Connect installation wizard.

Answer: C

Explanation:
The sync engine processes identity information from different data repositories, such as Active Directory or a SQL Server database. The sync engine encapsulates interaction with a connected data source within a module called a Connector. Each type of connected data source has a specific Connector. The Connector translates a required operation into the format that the connected data source understands.
References:
https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-understanding-architecture

Question: 87

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to ensure that a user named User1 can create mailboxes in Exchange Online and sites in SharePoint Online.
Solution: You add User1 to the Global administrator admin role.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
The Global administrator admin role has access to all administrative features in the Office 365 suite of services in your plan.
References:
https://support.office.com/en-us/article/About-Office-365-admin-roles-da585eea-f576-4f55-a1e0-87090b6aaa9d

Question: 88

HOTSPOT
A company has an Office 365 tenant. You install the Microsoft Azure Active Directory module for Windows PowerShell.
An employee leaves the company. The employee's account is named user1@contoso.com.
You need to hard delete the user's account.
How should you complete the relevant Windows PowerShell commands? To answer, select the appropriate Windows PowerShell segments from each list in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

$Credential = Get-Credential

[▼] -Credential $Credential

- New-PSSession
- Enter-PSSession
- Connect-PSSession
- Connect-MsolService

[▼] -UserPrincipalName user1@contoso.com [▼]

- Remove-ADUser
- Remove-MsolUser
- Remove-ADObject

- Force
- IncludeDeletedObjects
- RemoveFromRecycleBin

Answer:

Answer Area

$Credential = Get-Credential

[▼] -Credential $Credential

- New-PSSession
- Enter-PSSession
- Connect-PSSession
- **Connect-MsolService**

[▼] -UserPrincipalName user1@contoso.com [▼]

- Remove-ADUser
- **Remove-MsolUser**
- Remove-ADObject

- Force
- IncludeDeletedObjects
- **RemoveFromRecycleBin**

The Connect-MsolService cmdlet attempts to establish a connection to Azure Active Directory. Running the Remove-MsolUser cmdlet with the -UserPrincipalName <String>-RemoveFromRecycleBin parameters will remove a specific user from Azure Active Directory permanently.
References:
https://docs.microsoft.com/en-us/powershell/module/msonline/remove-msoluser?view=azureadps-1.0

Question: 89

You deploy Office 365.
You must implement Microsoft Skype for Business Online for all users. including audio and video for all desktop clients. All company desktop machines reside behind a company firewall.
You need configure the firewall to allow clients to use Skype for Business Online.
Which three outbound ports or port ranges should you open? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. TCP 80
B. TCP 5061
C. UDP 3478

D. TCP 443
E. TCP and UDP 50000-59999

Answer: C,D,E

Explanation:

Purpose	Source IP	Destination IP	Source Port	Destination Port
Session Initiation Protocol (SIP) Signaling	Client	Office 365	Ephemeral ports TCP	443 TCP
Persistent Shared Object Model (PSOM) Web Conferencing	Client	Office 365	Ephemeral ports TCP	443 TCP
HTTPS downloads	Client	Office 365	Ephemeral ports TCP	443 TCP
Audio	Client	Office 365	50000 - 50019 UDP and TCP	443 TCP, 3478 & 3479 UDP, 50000 - 59999 UDP and TCP (optional)
Video	Client	Office 365	50020 - 50039 UDP and TCP	443 TCP, 3478 & 3480 UDP, 50000 - 59999 UDP and TCP (optional)
Desktop Sharing	Client	Office 365	50040 - 50059 UDP and TCP	443 TCP, 3478 & 3481 UDP, 50000 - 59999 UDP and TCP (optional)

References:
https://support.microsoft.com/en-za/help/2409256/you-can-t-connect-to-skype-for-business-online--or-certain-features-do

Question: 90

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Office 365 subscription.
All of the users in your tenant are assigned an E5 license.
You need to view the list of planned updates for Microsoft Skype for Business Online.
Solution: You open the Skype for Business admin center and you review the contents of the dashboard.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Office 365 admin center allows you to view the health of the Skype for Business Online service, change and release

notifications, and usage reports.
References:
https://support.office.com/en-us/article/About-the-Skype-for-Business-admin-role-aeb35bda-93fc-49b1-ac2c-c74fbeb737b5

Question: 91

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Office 365 subscription.
All of the users in your tenant are assigned an E5 license.
You need to view the list of planned updates for Microsoft Skype for Business Online.
Solution: You open the Office 365 admin center and you review the contents of the Security & Compliance reports.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The Office 365 Security & Compliance Center will help you manage compliance features across Office 365 for your organization. It will not, however, allow you to view the list of planned updates for Microsoft Skype for Business Online.
References:
https://technet.microsoft.com/en-us/library/dn933793.aspx

Question: 92

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Office 365 subscription.
All of the users in your tenant are assigned an E5 license.
You need to view the list of planned updates for Microsoft Skype for Business Online.
Solution: You open the Office 365 admin center and you review the contents of service health dashboard.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
The Service health section of Office 365 allows you to view the current status of the service and details about service

disruptions and outages. Information regarding planned maintenance is can be found on the Message Center.
References:
https://support.office.com/en-us/article/How-to-check-Office-365-service-health-932ad3ad-533c-418a-b938-6e44e8bc33b0
https://technet.microsoft.com/en-us/library/office-365-service-health.aspx

Question: 93

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains a single Active Directory forest. The forest contains a domain controller and Active Directory Federation Services (AD FS) servers that are deployed to virtual machines. The virtual machines run either on-premises or on Microsoft Azure.
You have Azure AD Connect deployed on-premises. The Azure AD Connect database is installed on an on-premises instance of Microsoft SQL Server 2014.
Last month, an Azure AD Connect server experienced a hardware failure that caused an Azure AD Connect server to go offline for several days.
You need to recommend a solution to reduce the outage window when hardware failure occurs on the Azure AD Connect server.
Solution: You deploy a new on-premises Azure AD Connect server that uses the same SQL Server instance. You start Azure AD Connect sync.
Does this meet the goal?

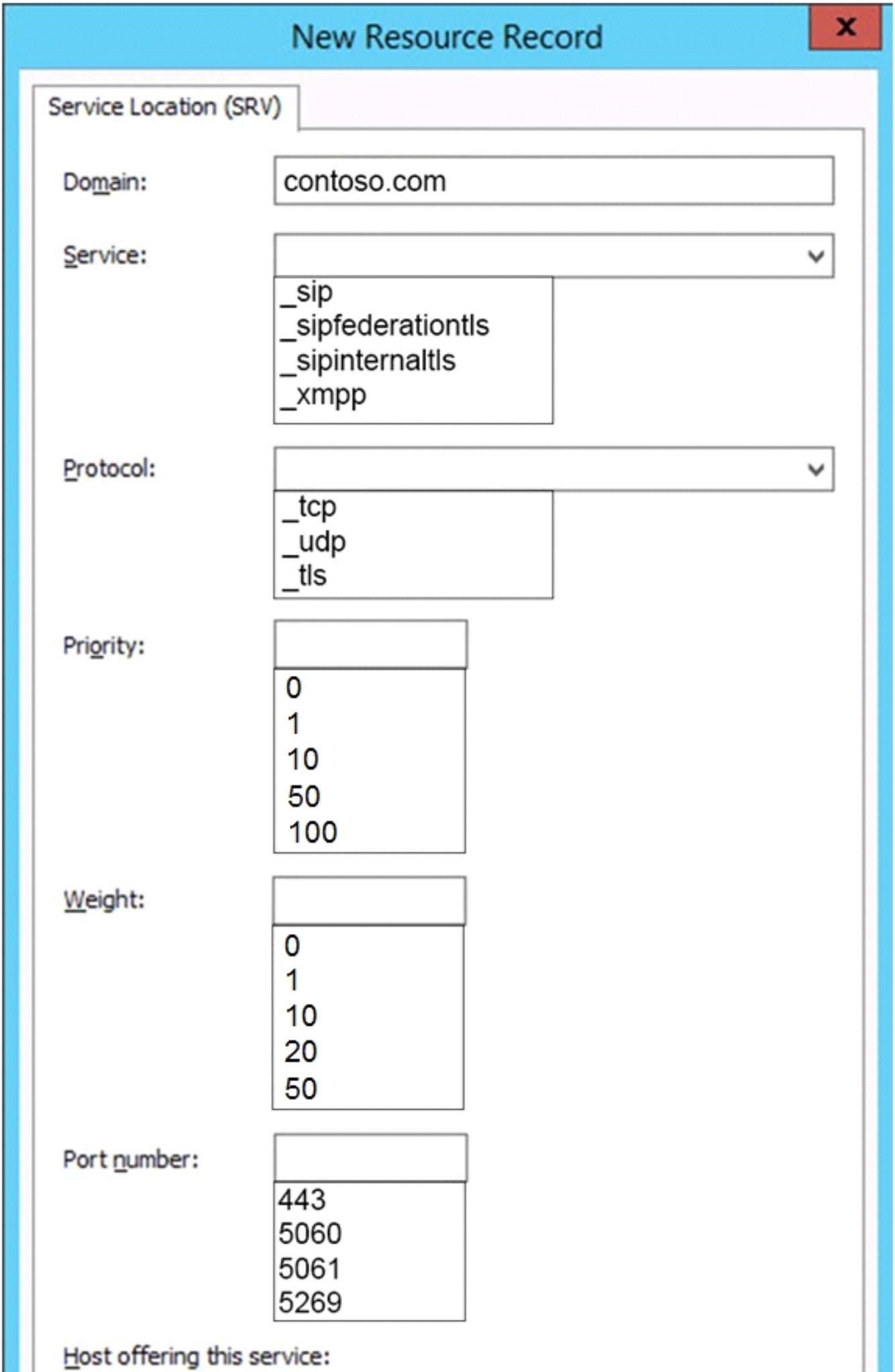
A. Yes
B. No

Answer: B

Explanation:
An on-premises Azure AD Connect server already exists. A server in staging mode is required to provide High Availability.
References:
https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-operations/

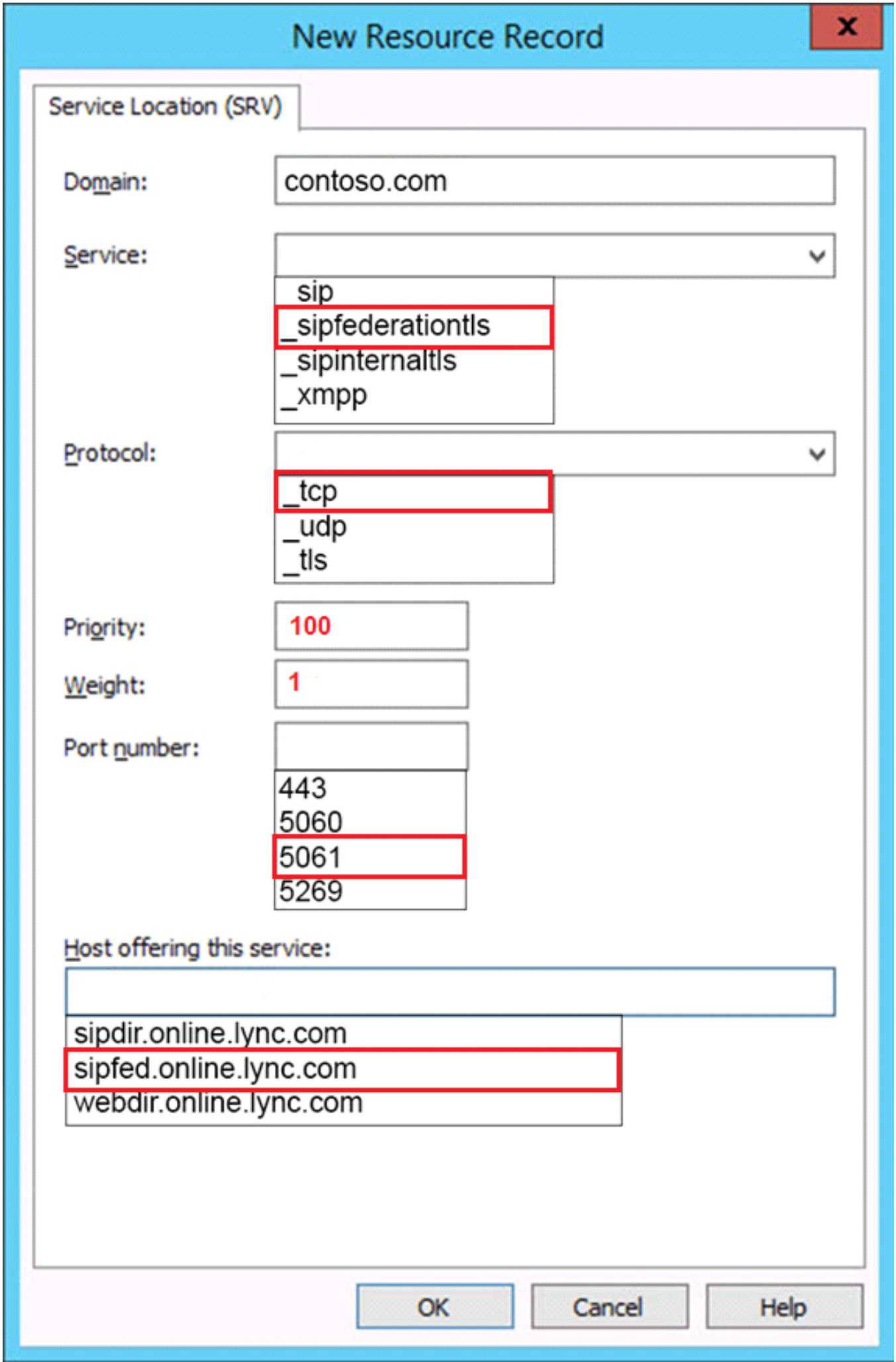
Question: 94

HOTSPOT
A company has an Office 365 tenant. You use the domain contoso.com for both email and session initiation protocol (SIP) addresses. You plan to deploy Skype for Business Online and enable federation for all Skype users.
You need to create a DNS record to support Skype for Business Online federation.
How should you configure the record? To answer, select the appropriate option from each list in the answer area.
NOTE: Each correct selection is worth one point.


New Resource Record
Service Location (SRV)
Domain:
contoso.com
Service:
_sip
_sipfederationtls
_sipinternaltls
_xmpp
Protocol:
_tcp
_udp
_tls
Priority:
0
1
10
50
100
Weight:
0
1
10
20
50
Port number:
443
5060
5061
5269
Host offering this service:

Priority: 0, 1, 10, 50, 100
Weight: 0, 1, 10, 20, 50

Answer:


New Resource Record
Service Location (SRV)
Domain:
contoso.com
Service:
_sip
_sipfederationtls
_sipinternaltls
_xmpp
Protocol:
_tcp
_udp
_tls
Priority:
100
Weight:
1
Port number:
443
5060
5061
5269
Host offering this service:
sipdir.online.lync.com
sipfed.online.lync.com
webdir.online.lync.com
OK
Cancel
Help

Add the SIP SRV record for Skype for Business Online federation.

1. On the DNS Manager page for your domain, go to **Action** > **Other New Records**.

   To find this page for your domain, see Find your DNS records in Windows-based DNS.

2. In the **Resource Record Type** window, choose **Service Location (SRV)**, and then click **Create Record**.

3. In the **New Resource Record** dialog box, make sure that the fields are set to precisely the following values:

   - **Service**: _sipfederationtls
   - **Protocol**: _tcp
   - **Priority**: 100
   - **Weight**: 1
   - **Port**: 5061
   - **Target (Hostname)**: sipfed.online.lync.com

References:
https://support.office.com/en-us/article/Create-DNS-records-for-Office-365-using-Windows-based-DNS-9eec911d-5773-422c-9593-40e1147ffbde

Question: 95

You plan to deploy an Office 365 tenant to multiple offices around the country.
You need to modify the accounts that are authorized to administer the Rights Management service.
Which Windows PowerShell cmdlet should you run?

A. Enable-AadrmSuperUserFeature
B. Add-MsolGroupMember
C. Add-AadrmRoleBasedAdministrator
D. Get-AadrmRoleBasedAdministrator

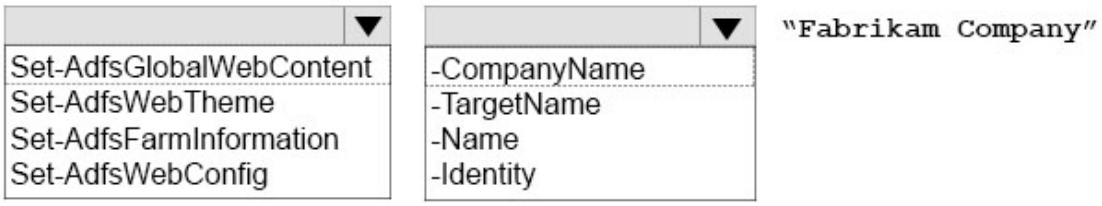
Answer: D

Explanation:
The Get-AadrmRoleBasedAdministrator cmdlet lists the role-based administrators for Azure Rights Management.

Question: 96

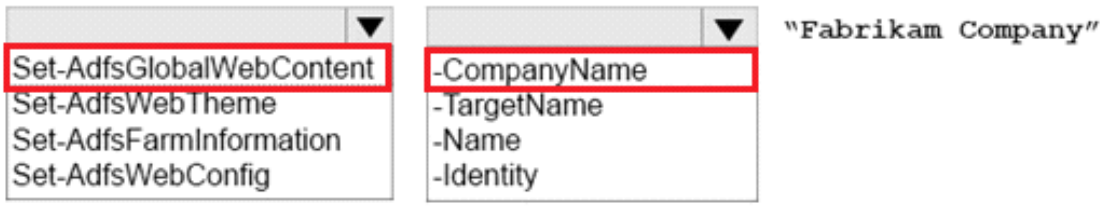
HOTSPOT
You administer an Office 365 tenant for a company named Fabrikam, Inc. You deploy Active Directory Federation Services (AD FS) including Web Application Proxy servers.
You need to customize the AD FS logon screen to display your company name.
How should you complete the Windows PowerShell command? To answer, select the appropriate Windows PowerShell segments in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Set-AdfsGlobalWebContent -CompanyName " Fabrikam Company"
Running the Set-AdfsGlobalWebContent cmdlet with the –CompanyName parameter specifies the company name for AD FS to display in the sign-in pages when you have not set a logo on the active web theme.

Question: 97

A company has an Office 365 tenant.
You need to ensure that Active Directory is ready for synchronization.
Which tool should you run?

A. IdFix
B. Office 365 Health, Readiness, and Connectivity Check
C. Microsoft Remote Connectivity Analyzer Tool
D. Synchronization Service (MIISClient)

Answer: A

Explanation:
DirSync has certain requirements on attributes in the directory, and aligning the attribute values with the DirSync requirements is commonly known as Active Directory remediation. The IdFix tool reviews the directory and performs interactive Active Directory remediation. It also checks for and helps you correct any invalid data and duplicate data in directory attributes, including userPrincipalName (UPN), mailNickName, proxyAddress, sAMAccountName, targetAddress, and others. Furthermore, it provides assistance for migrating from a non-routable to an Internet

routable domain name, because using an Internet-routable domain is one of the requirements for Azure Active Directory.

Question: 98

You manage an Active Directory Domain Services (AD DS) domain. Your company plans to move all of its resources to Office 365.
You must implement Active Directory Federation Services (AD FS). You place all internet-facing servers on a perimeter network.
You need to ensure that intranet and extranet users are authenticated before they access network resources.
Which three authentication methods should you provide for extranet users? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Windows Integrated Authentication using Negotiate for NTLM
B. Windows Integrated Authentication using Negotiate for Kerberos
C. Authentication with RADIUS
D. Forms Authentication using username and passwords
E. Certificate Authentication using certificates mapped to user accounts in AD DS

Answer: B,D,E

Explanation:
Windows Integrated Authentication makes use of Negotiate/Kerberos or NTLM to authenticate users based on an encrypted ticket/message passed between a browser and a server.
With Azure AD you need Forms-based authentication in ADFS for Azure AD/MSOnline PowerShell Module and Azure AD Self-Service Password Reset.
In Active Directory mapping, when the IIS server receives a certificate from the user, it passes it on to Active Directory, which maps it to a Windows user account. The IIS server then logs this account on.
Active directory mapping is most useful when the account mappings are the same on all IIS servers. Administration is simplified because the mapping is done in only one place.

Question: 99

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are the administrator for a company. You plan to use Office 365 for email and file sharing. You plan to implement a hybrid deployment with your current on-premises Active Directory Domain Services (AD DS) environment and Microsoft Azure Active Directory (Azure AD) Connect.
You must deploy Microsoft Exchange Online and OneDrive for Business for all employees. You have the following security requirements:
All employees must use complex passwords.
Passwords must be changed every six months.
Employees must use multi-factor authentication (MFA) when possible.
You need to implement MFA verification options to use with the employee's password.
Solution: Have the employee use a virtual smart card.
Does the solution meet the goal?

A. Yes
B. No

Answer: B

Explanation:
MFA for Office 365 requires users to acknowledge a phone call, text message, or app notification on their smart phones after correctly entering their passwords. Virtual smartcards are not required.
References:
https://support.office.com/en-us/article/Set-up-multi-factor-authentication-for-Office-365-users-8f0454b2-f51a-4d9c-bcde-2c48e41621c6

Question: 100

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are the administrator for a company. You plan to use Office 365 for email and file sharing. You plan to implement a hybrid deployment with your current on-premises Active Directory Domain Services (AD DS) environment and Microsoft Azure Active Directory (Azure AD) Connect.
You must deploy Microsoft Exchange Online and OneDrive for Business for all employees. You have the following security requirements:
All employees must use complex passwords.
Passwords must be changed every six months.
Employees must use multi-factor authentication (MFA) when possible.
You need to implement MFA verification options to use with the employee's password.
Solution: Have the employee receive an SMS text.
Does the solution meet the goal?

A. Yes
B. No

Answer: A

Explanation:
MFA for Office 365 requires users to acknowledge a phone call, text message, or app notification on their smart phones after correctly entering their passwords.
References:
https://support.office.com/en-us/article/Set-up-multi-factor-authentication-for-Office-365-users-8f0454b2-f51a-4d9c-bcde-2c48e41621c6

Question: 101

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not

appear in the review screen.
You are the administrator for a company. You plan to use Office 365 for email and file sharing. You plan to implement a hybrid deployment with your current on-premises Active Directory Domain Services (AD DS) environment and Microsoft Azure Active Directory (Azure AD) Connect.
You must deploy Microsoft Exchange Online and OneDrive for Business for all employees. You have the following security requirements:
All employees must use complex passwords.
Passwords must be changed every six months.
Employees must use multi-factor authentication (MFA) when possible.
You need to implement MFA verification options to use with the employee's password.
Solution: Have the employee receive a phone call.
Does the solution meet the goal?

A. Yes
B. No

Answer: A

Explanation:
MFA for Office 365 requires users to acknowledge a phone call, text message, or app notification on their smart phones after correctly entering their passwords.
References:
https://support.office.com/en-us/article/Set-up-multi-factor-authentication-for-Office-365-users-8f0454b2-f51a-4d9c-bcde-2c48e41621c6

Question: 102

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Office 365 subscription.
Several users report that they fail to connect to Microsoft Skype for Business Online by using the Skype for Business 2016 client.
You verify that you can connect to Skype for Business Online successfully from your computer.
You need to identify what prevents the users from connecting to Skype for Business Online.
Solution: You use the Microsoft Remote Connectivity Analyzer.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The Microsoft Remote Connectivity Analyzer has the capability to help troubleshoot, diagnose, and verify settings for various public-facing applications. However, in this scenario, the Microsoft Skype for Business Connectivity Analyzer should be used instead.
http://blog.get-csjosh.com/2015/05/microsoft-remote-connectivity-analyzer-and-associated-tools.html

Question: 103

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Office 365 subscription.
Several users report that they fail to connect to Microsoft Skype for Business Online by using the Skype for Business 2016 client.
You verify that you can connect to Skype for Business Online successfully from your computer.
You need to identify what prevents the users from connecting to Skype for Business Online.
Solution: You use the Microsoft Connectivity Analyzer Tool.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
The main purpose of the Microsoft Connectivity Analyzer is to test connectivity between email clients and servers running Exchange server. However, in this scenario, the Microsoft Skype for Business Connectivity Analyzer should be used instead.
References:
http://blog.get-csjosh.com/2015/05/microsoft-remote-connectivity-analyzer-and-associated-tools.html

Question: 104

You have an Office 365 subscription.
You deploy Microsoft Azure multi-Factor authentication for all users.
Which three methods can the users use to verify their identity? Each correct answer presents a complete solution.

A. Use a verification code from an email message sent to your primary SMTP address.
B. Use a verification code from a mobile app.
C. Make a verification phone call to your authenticated phone number.
D. Use a verification code from an instant message sent to your registered SIP address.
E. Make a verification phone call to your office phone number.

Answer: A,B,C

Explanation:
MFA for Office 365 requires users to acknowledge a phone call, text message, or app notification on their smart phones after correctly entering their passwords.
References:
https://support.office.com/en-us/article/Set-up-multi-factor-authentication-for-Office-365-users-8f0454b2-f51a-4d9c-bcde-2c48e41621c6

Question: 105

You have an on-premises Exchange organization. The organization plans to migrate to Office 365.
You need to identify a group of users to designate as the pilot group.
Which factor makes a user a poor choice to be included in the pilot group?

A. users who use Android devices
B. users who are delegates for multiple mailboxes
C. users who need access to public folders on Exchange 2007 servers
D. users who receive fewer than 25 email messages per day

Answer: C

Explanation:
Users who have a dependency on resources that are still on-premises are not considered good candidates a pilot as they require send-as and receive as permissions on those resources.
References:
https://books.google.co.za/books?id=aaU2DwAAQBAJ&pg=PA84&lpg=PA84&dq=exchange+online+pilot+group&source=bl&ots=I7kKLHpYLR&sig=7zrAVKi44oZa5n1Hz8JxLBwA5JU&hl=en&sa=X&ved=0ahUKEwi5j5HQxMDXAhXmJ8AKHfTGChkQ6AEIZDAJ#v=onepage&q=pilot&f=false

Question: 106

DRAG DROP
You deploy Active Directory Federation Services (AD FS) for a company's Office 365 environment. You have a server named Server1 that runs Windows Server 2016. You allocate Server1 for the AD FS deployment.
You have the following requirements:
Use Integrated Windows Authentication.
Deploy a proxy server for AD FS.
Ensure the proxy server is secure.
You need to install the proxy server.
Which three steps should you perform in sequence? To answer, move the appropriate steps from the list of step to the answer area and arrange them in the correct order.

Steps	Answer area
Install AD FS Proxy and configure the proxy.	
Join Server1 to the Active Directory Domain Services (AD DS) domain.	
Configure Kerberos constrained delegation.	
Leave Server1 as a standalone server.	
Install the Web Application Proxy (WAP) role service and configure the service.	

Answer:

Steps	Answer area
Install AD FS Proxy and configure the proxy.	Leave Server1 as a standalone server.
Join Server1 to the Active Directory Domain Services (AD DS) domain.	Install the Web Application Proxy (WAP) role service and configure the service.
	Configure Kerberos constrained delegation.

Box1
Leave Server1 as a standalone server.
Box2
Install the Web Application Proxy (WAP) role service and configure the service.
Box3
Configure Kerberos constrained delegation.
Web Application Proxy can be deployed without joining the server to an AD DS domain or by joining the Web Application Proxy server to a standalone domain in a perimeter network.
The Web Application Proxy role service is a replacement for the AD FS proxy role.
When publishing applications that use Integrated Windows authentication, the Web Application Proxy server uses Kerberos constrained delegation to authenticate users to the published application.
References:
https://technet.microsoft.com/en-us/library/dn584113(v=ws.11).aspx
https://technet.microsoft.com/en-us/library/dn383648(v=ws.11).aspx

Question: 107

DRAG DROP
You are the Office 365 administrator for a company. You have an on-premises Active Directory Domain Services (AD DS) environment.
You configure Active Directory Federation Services (AD FS) and directory synchronization. You use Windows Server 2016 for AD FS. You deploy the Web Application Proxy (WAP) role.
You need to deploy a custom web theme for the WAP server.
In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer area
Customize the theme files	
Run the Set-AdfsWebTheme cmdlet	
Run the New-AdfsWebTheme cmdlet	
Run the Set-AdfsRelyingPartyWebTheme cmdlet	
Run the Export-AdfsWebTheme cmdlet	

Answer:

Actions	Answer area
	Run the New-AdfsWebTheme cmdlet
	Customize the theme files
	Run the Export-AdfsWebTheme cmdlet
	Run the Set-AdfsWebTheme cmdlet
	Run the Set-AdfsRelyingPartyWebTheme cmdlet

Box1
Run the New-AdfsWebTheme cmdlet.
Box2
Customiize the theme files.
Box3
Run the Export-AdfsWebTheme cmdlet.
Box4
Run the Set-AdfsWebTheme cmdlet.
Box5
Run the Set-AdfsRelyingPartyWebTheme cmdlet.
The New-AdfsWebTheme cmdlet creates a custom web theme.
You can modify the .css file and configure the new web theme by using the new .css file.
The Export-AdfsWebTheme cmdlet exports the web theme to the required directory.
The Set-AdfsWebTheme cmdlet applies the .css file to the new theme.
The Set-AdfsRelyingPartyWebTheme cmdlet applies a web theme to a relying party.
References:
https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/custom-web-themes-in-ad-fs
https://docs.microsoft.com/en-us/powershell/module/adfs/set-adfsrelyingpartywebtheme?view=win10-ps

Question: 108

You are the Office 365 administrator for a company.

You hire a third-party company to provide Office 365 support.
You need to ensure that the third-party company can access the following data:
current status for each service
historical data for service health
outage message and other Office 365 communications for the tenant
programmatic access to the service health data
What should you do?

A. Connect to the Office 365 Security and Compliance Center by using Windows PowerShell commands.
B. Grant the third-party company access to the Office 365 Service Communications API.
C. Add the users from the third-party company to the Office 365 Service administrator role.
D. Grant the third-party company access to the Office 365 Management Activity API.

Answer: C

Explanation:
The service administrator role gives a user rights to open and handle support requests with Microsoft related to Office 365 services. Service administrators have very limited permissions other than opening and reading support tickets. This role is often coupled with other administrative roles such as Exchange, SharePoint and others to let those administrators follow key details such as service health and new release notices.
References:
http://searchexchange.techtarget.com/definition/Microsoft-Office-365-admin-roles

Question: 109

HOTSPOT
You are deploying a new Office 365 tenant for a company. You plan to use the default domain Fabricam.onmicrosoft.com. Employees currently use Fabricam.com for their email address in the on-premises email system.
You have the following requirements:
All users need to be migrated to Microsoft Exchange Online.
Fabricam.com must be used for the email domain and Office 365 user principal name.
You need to start the new domain process and generate a CSV import file for your on-premises DNS servers.
How should you complete the Windows PowerShell commands? To answer, configure the appropriate options in the dialog box in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

$domain = " [ ] "

- Fabricam.com
- Fabricam.onmicrosoft.com
- Fabricam.microsoft.com

[ ] -Name $domain

- New-MsolDomain
- New-RemoteDomain

[ ] -DomainName $domain -Mode DnsTxtRecord

- Get-MsolDomain
- Get-MsolDomainVerificationDns
- Get-RemoteDomain

| select Label, Text, Ttl | export -csv -Path c:\DNS.csv -NoTypeInformation

Answer:

Answer Area

$domain = " [Fabricam.onmicrosoft.com] "

- Fabricam.com
- **Fabricam.onmicrosoft.com**
- Fabricam.microsoft.com

[New-MsolDomain] -Name $domain

- **New-MsolDomain**
- New-RemoteDomain

[Get-MsolDomainVerificationDns] -DomainName $domain -Mode DnsTxtRecord

- Get-MsolDomain
- **Get-MsolDomainVerificationDns**
- Get-RemoteDomain

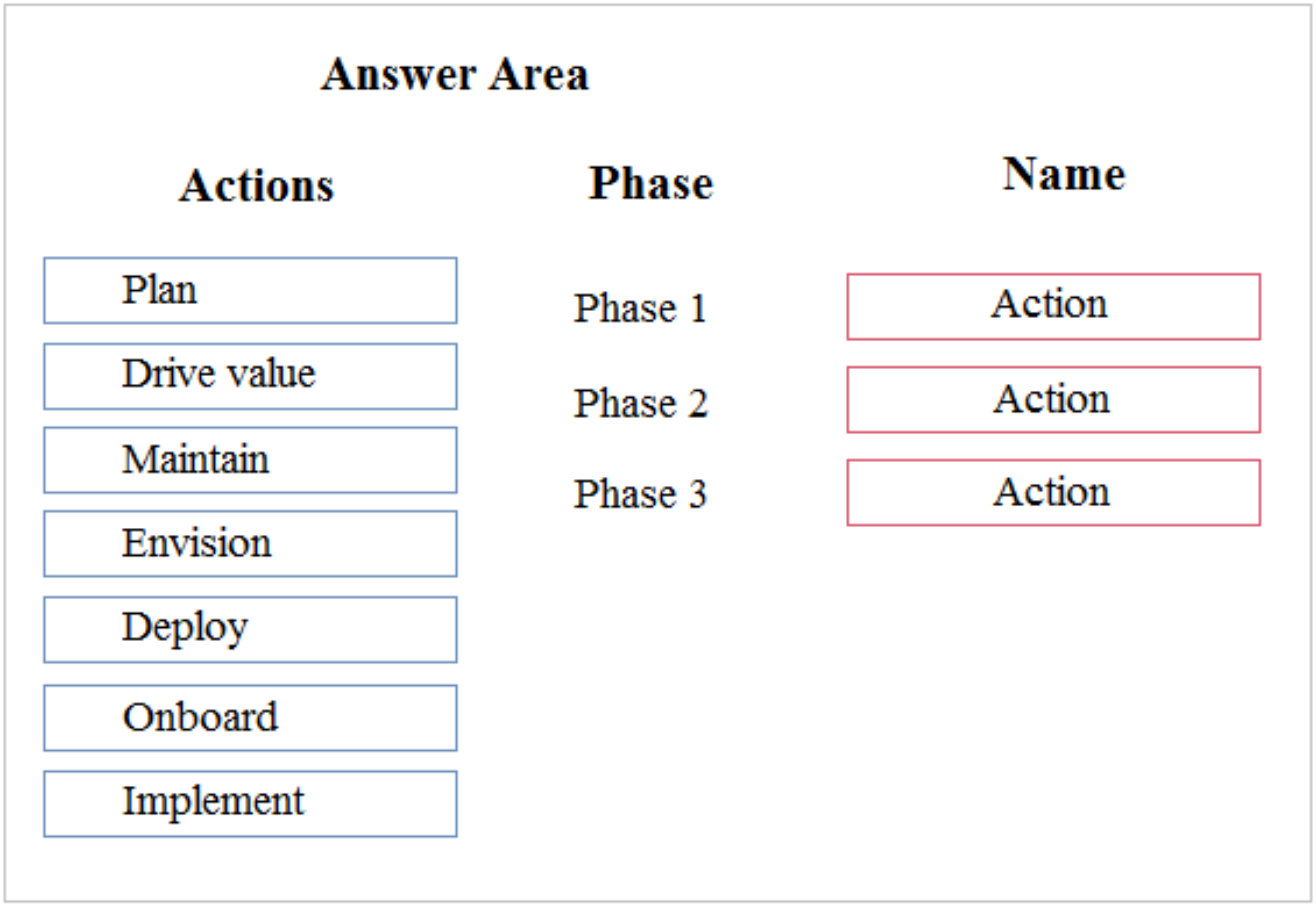
| select Label, Text, Ttl | export -csv -Path c:\DNS.csv -NoTypeInformation

Box1
Fabricam.onmicrosoft.com
Box2

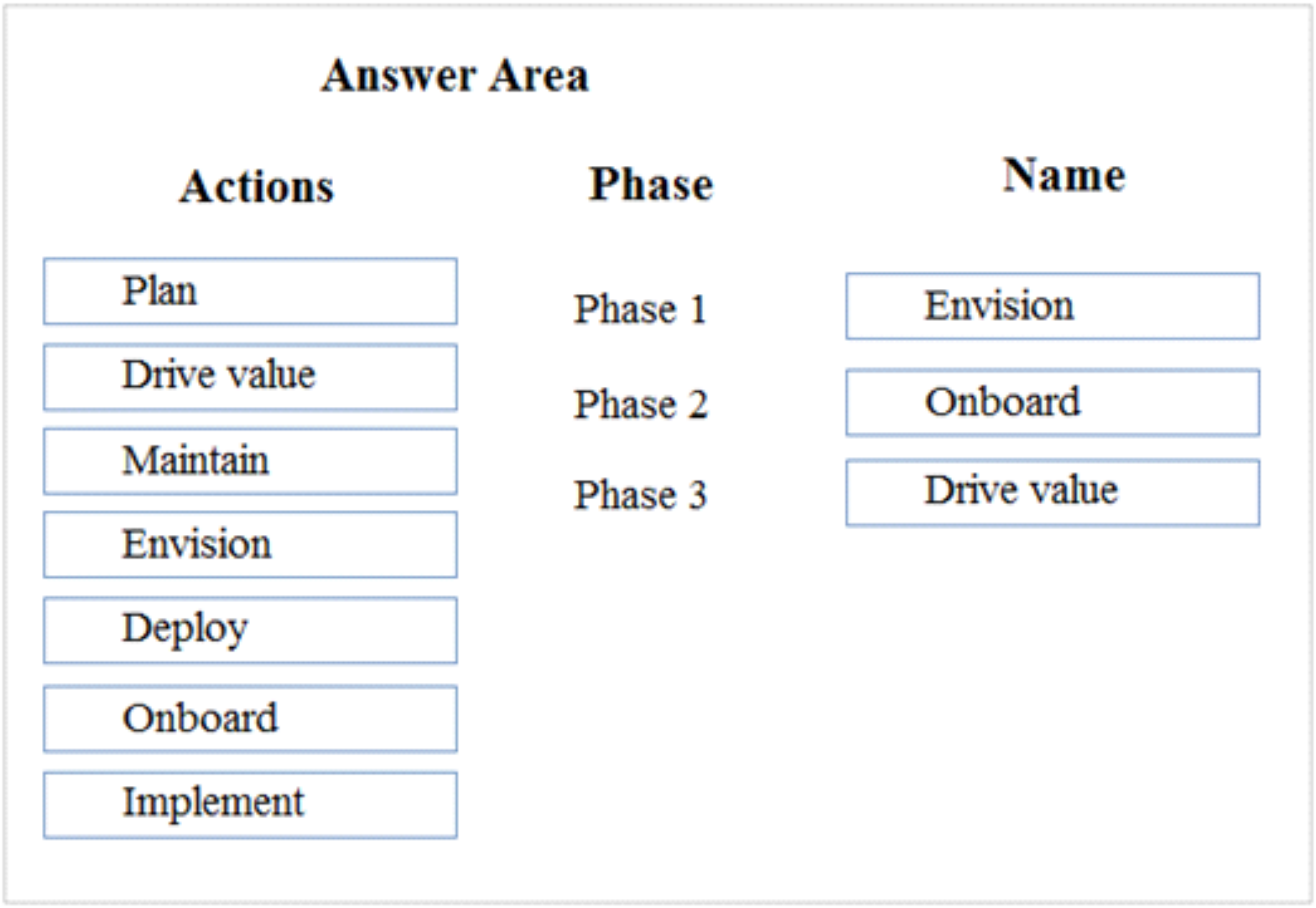
New-MsolDomain
Box3
Get-MsolDomainVerificationDns
The questions states: “You plan to use the default domain Fabricam.onmicrosoft.com.”
The New-MsolDomain cmdlet adds a domain to Azure Active Directory.
The Get-MsolDomainVerificationDns cmdlet retrieves the necessary DNS records to verify a domain.
References:
https://docs.microsoft.com/en-us/powershell/module/msonline/new-msoldomain?view=azureadps-1.0
https://docs.microsoft.com/en-us/powershell/module/msonline/get-msoldomainverificationdns?view=azureadps-1.0

Question: 110

DRAG DROP
You plan to use Office 365 FastTrack to deploy an Office 365 tenant.
Which action should you perform for each phase? To answer, drag the appropriate actions to the correct phases. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



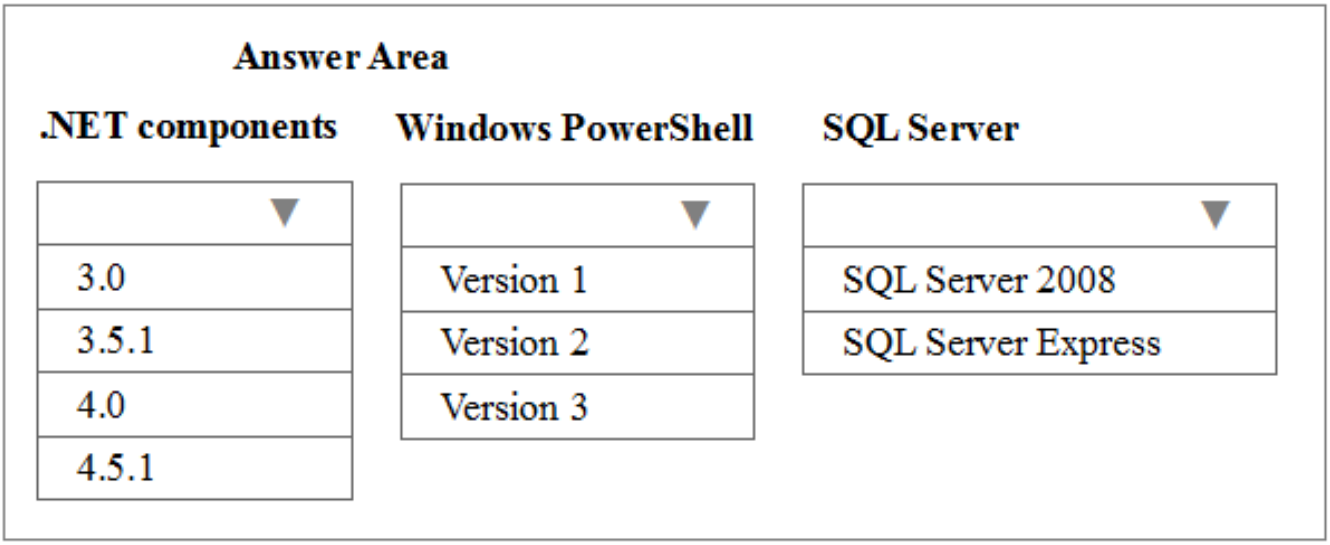
Answer:



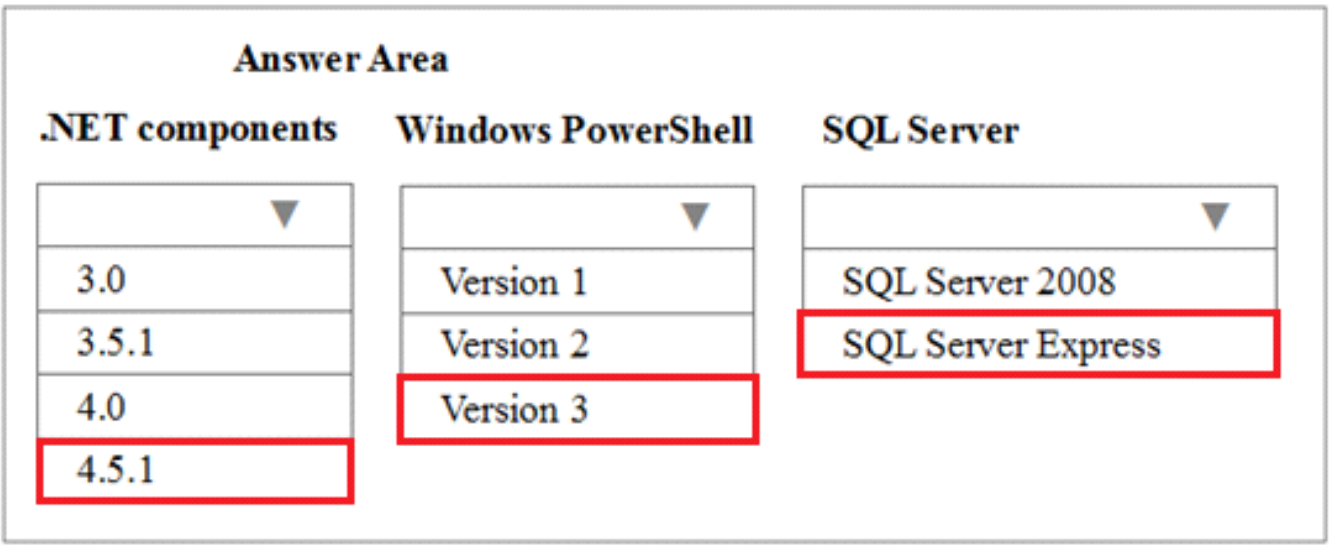
References:
https://fasttrack.microsoft.com/about

Question: 111

HOTSPOT
A company with 75,000 employees has an Office 365 tenant.
You need to install the Azure Active Directory Connect by using the least amount of administrative effort.
Which versions of each product should you implement? To answer, select the appropriate version from each list in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



The Azure AD Connect server must have .NET Framework 4.5.1 or later and Microsoft PowerShell 3.0 or later installed.
Azure AD Connect requires a SQL Server database to store identity dat
a. SQL Server Express has a 10 GB size limit that enables you to manage approximately 100,000 objects.
References:
https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-prerequisites

Question: 112

Your company has an Office 365 subscription that is configured for single sign-on (SSO) to an on-premises deployment of Active Directory.
After a security breach, management at the company decides that only clients from the internal corporate network can be authenticated by using Active Directory Federation Services (AD FS).
You need to configure AD FS to prevent external clients from being authenticated by using AD FS.
What should you add in AD FS?
A. a claims provider trust
B. a relying party trust
C. a claim rule
D. a non-claims-aware relying party trust

Answer: B

Explanation:
Access control in AD FS is implemented with issuance authorization claim rules that are used to issue a permit or deny claims that will determine whether a user or a group of users will be allowed to access AD FS-secured resources or not. Authorization rules can only be set on relying party trusts. So you need to add a relying party trust to AD FS.
References:
https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/manage-risk-with-conditional-access-control

Question: 113

Contoso, Ltd, has an Office 365 tenant. You configure Office 365 to use the domain contoso.com, and you verify the domain. You deploy and configure Active Directory Federation Services (AD FS) and Azure Active Directory Connect with password synchronization. You connect to Azure Active Directory by using a Remote Windows PowerShell session.
You need to switch from using AD FS to using password-synced passwords on the Office 365 verified domain.
Which Windows PowerShell command should you run?

A. Convert-MsolDomainToFederated -DomainName contoso.com
B. Convert-MsolDomainToStandard -DomainName contoso.com
C. Convert-MsolFederatedUser
D. Set-MsolDomainAuthentication -DomainName contoso.com

Answer: B

Explanation:
To switch large sets of users from federated authentication to managed authentication with password sync you can use the Entire namespace conversion approach. To convert the desired namespace from Federated to Managed, you have to use the Convert-MsolDomainToStandard cmdlet.
References:
https://social.technet.microsoft.com/wiki/contents/articles/17857.dirsync-how-to-switch-from-single-sign-on-to-password-sync.aspx

Question: 114

You are the Office 365 administrator for your company. You have a server that runs Windows Server 2012. You plan to install an Active Directory Federation Services (AD FS) web app proxy server.
You need to install and configure the required roles.
What role should you install and configure?

A. Web Server (IIS)
B. Network Policy and Access Service
C. Application Server
D. Active Directory Certificate Services (AD CS)
E. Remote Access

Answer: E

Explanation:

In Windows Server 2012, a Web Application Proxy, a new role service of the Remote Access server role, is used to enable your AD FS for accessibility from outside of the corporate network.
References:
https://msdn.microsoft.com/en-us/library/azure/dn151311.aspx

Question: 115

A company has an Office 365 tenant and uses Exchange Online and Skype for Business Online.
User1 is scheduling a Skype meeting with User2. User 1 is not able to see availability information for User2.
You need to troubleshoot the issue.
What should you use?

A. Microsoft Connectivity Analyzer Tool
B. Microsoft Skype for Business Connectivity Analyzer Tool
C. Message Header Analyzer
D. IdFix

Answer: A

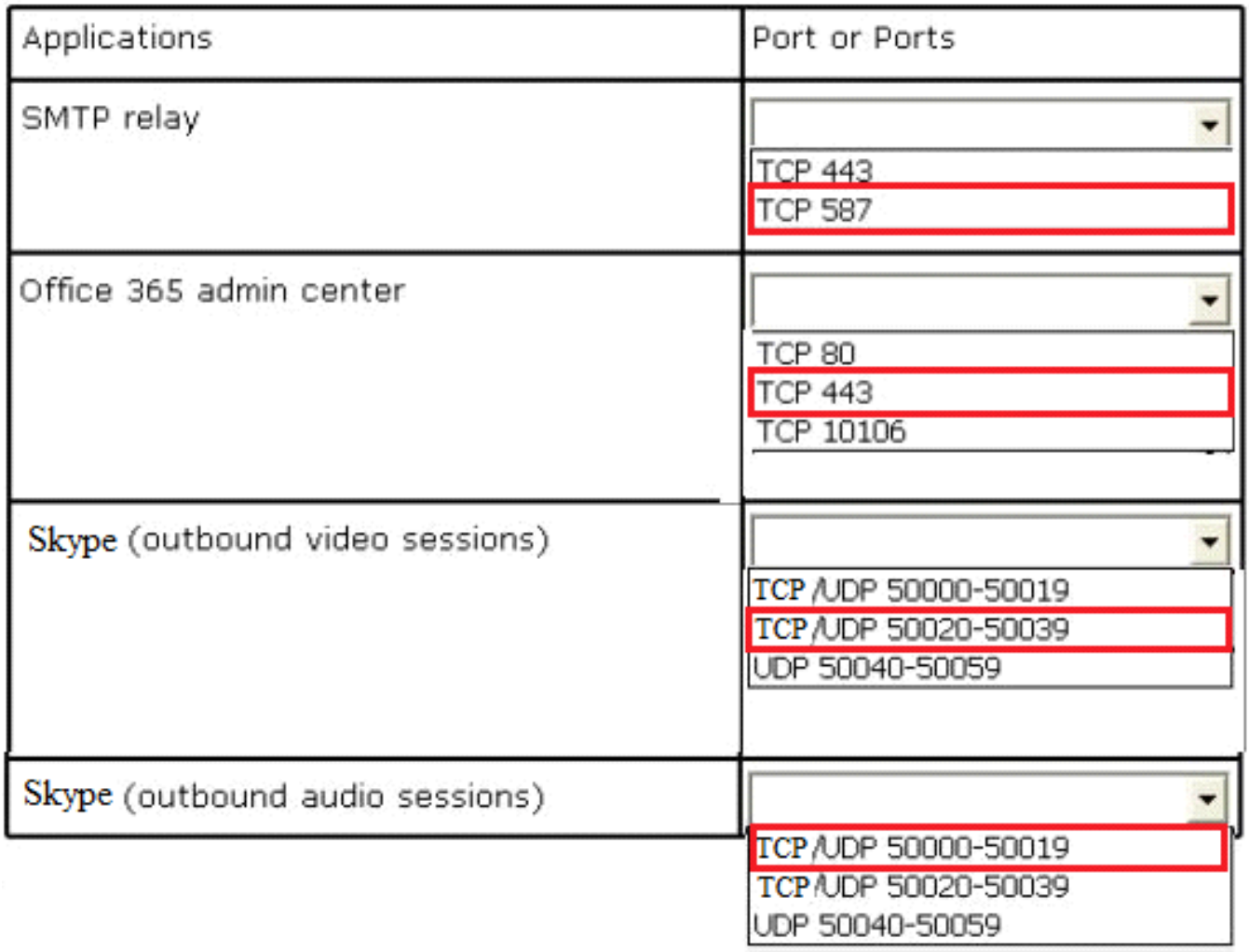
Explanation:
The Microsoft Connectivity Analyzer Tool verifies that an Office 365 mailbox can access the free/busy information of an on-premises mailbox, and vice versa
References:
https://blogs.technet.microsoft.com/exchange/2013/03/11/announcing-microsoft-connectivity-analyzer-mca-1-0-and-microsoft-remote-connectivity-analyzer-rca-2-1/

Question: 116

HOTSPOT
A company plans to deploy an Office 365 tenant.
You have the following requirements:
Administrators must be able to access the Office 365 admin center.
Microsoft Exchange Online must be used as a Simple Mail Transfer Protocol (SMTP) relay for a line-of-business application that sends email messages to remote domains.
All users must be able to use the audio and video capabilities in Microsoft Skype for Business.
You need to configure the ports for the firewall.
Which port should you use for each application? Select the correct answer from each list in the answer area.
NOTE: Each correct selection is worth one point.

Applications	Port or Ports
SMTP relay	TCP 443 TCP 587
Office 365 admin center	TCP 80 TCP 443 TCP 10106
Skype (outbound video sessions)	TCP/UDP 50000-50019 TCP/UDP 50020-50039 UDP 50040-50059
Skype (outbound audio sessions)	TCP/UDP 50000-50019 TCP/UDP 50020-50039 UDP 50040-50059

Answer:



Transport Control Protocol(TCP), User Datagram Protocol (UDP) ports, and Protocol Numbers are important to TCP/IP networking, intranets, and the Internet. Ports and protocol numbers provide access to a host computer. However, they also create a security hazard by allowing uninvited access. Therefore, knowing which port to allow or disable increases a network's security. If the wrong ports or protocol numbers are disabled on a firewall, router, or proxy server as a security measure, essential services might become unavailable.
TCP port 587 is an outgoing SMTP Mail port (TLS/Start TLS Port). Used by various outgoing mail servers as an alternative to port 25.
TCP port 443 is used for Audio, video and application sharing sessions as well as data sharing sessions.
RTP/UDP port 50020-50039 must be used for outbound video sessions.
RTP/UDP port 50000-50019 must be used for outbound audio sessions.
References:
https://support.office.com/en-us/article/Office-365-URLs-and-IP-address-ranges-8548a211-3fe7-47cb-abb1-355ea5aa88a2?ui=en-US&rs=en-US&ad=US
https://www.speedguide.net/port.php?port=587

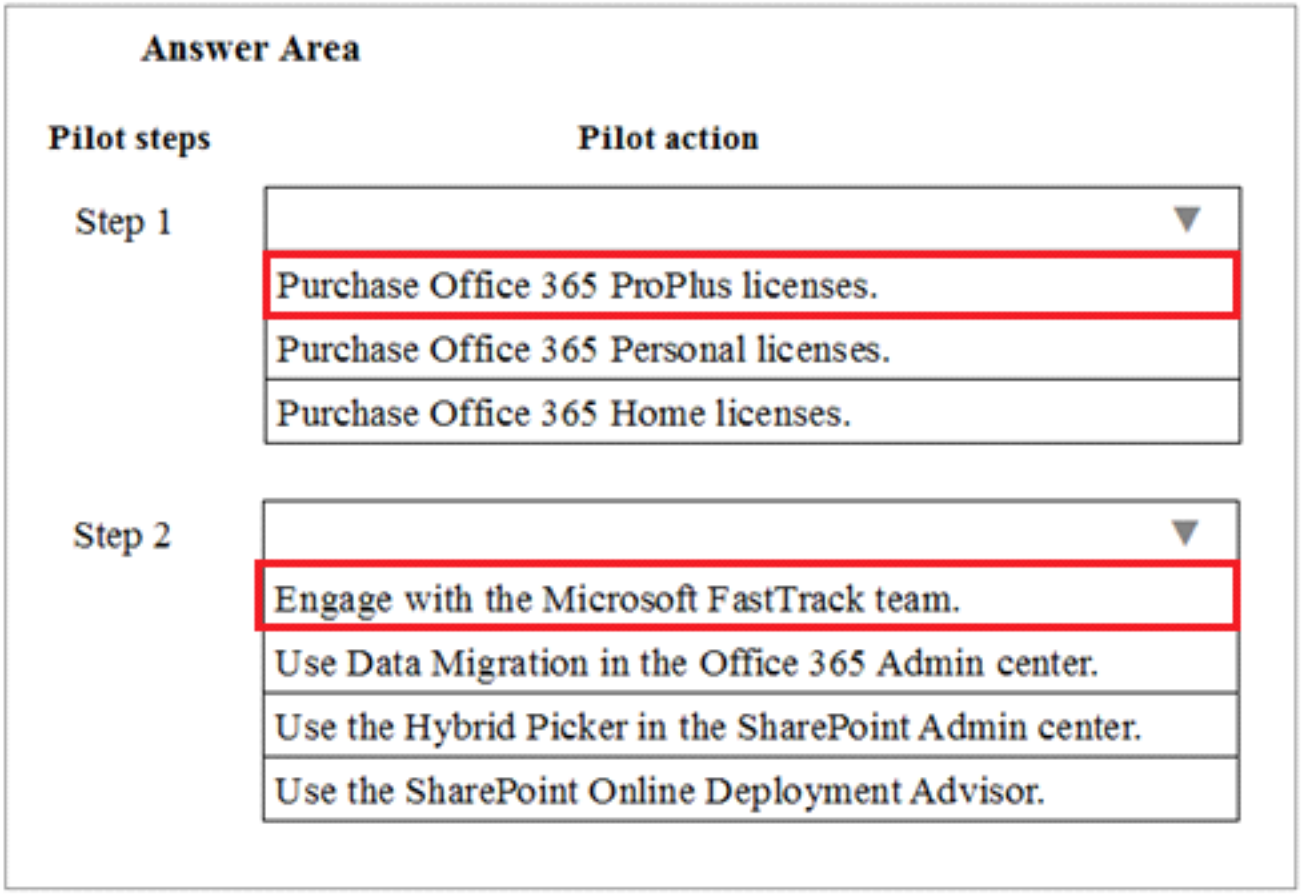
Question: 117

HOTSPOT
You are the system administrator for a small business. You manage on-premises file shares.
You need to migrate the file shares to Microsoft SharePoint Online document libraries.
Which actions should you perform? To answer, select the appropriate action in the dialog box in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Pilot steps	Pilot action
Step 1	▼
	Purchase Office 365 ProPlus licenses.
	Purchase Office 365 Personal licenses.
	Purchase Office 365 Home licenses.
Step 2	▼
	Engage with the Microsoft FastTrack team.
	Use Data Migration in the Office 365 Admin center.
	Use the Hybrid Picker in the SharePoint Admin center.
	Use the SharePoint Online Deployment Advisor.

Answer:



You can use Office 365 ProPlus with supported versions of Exchange Server or SharePoint Server that are installed on-premises in your organization. Or, if they're part of your Office 365 plan, you can use Office 365 ProPlus with Exchange Online and SharePoint Online.
Users can store the files they create with Office 365 ProPlus on their local computers or elsewhere on your network, such as a SharePoint site. Office 365 also provides cloud-based file storage options.
FastTrack Specialists provide guidance on steps for data migration to Office 365. We provide guidance for you by using a combination of tools and documentation and by performing configuration tasks where applicable and feasible. This is available for all eligible customers with Office 365 services for Exchange Online, OneDrive for Business, and SharePoint Online.
References:
https://support.office.com/en-us/article/About-Office-365-ProPlus-in-the-enterprise-9f11214c-911d-4e3c-9993-a566f12b1a68
https://technet.microsoft.com/en-us/library/mt651702.aspx

Question: 118

DRAG DROP
You manage an on-premises Active Directory environment. You implement an Office 365 tenant for a company. Password requirements for the environments are listed in the table below.

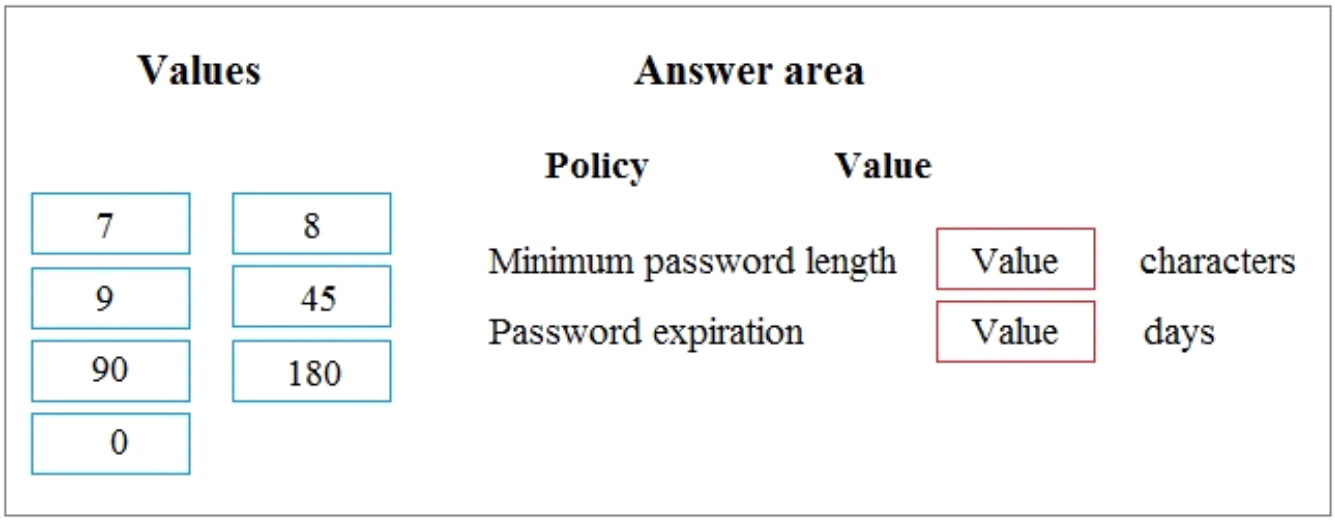
Environment	Password requirements
On-premises Active Directory	Passwords must be at least seven characters. Passwords expire after 45 days.
Office 365	Passwords must be at least nine characters. Passwords expire after 180 days.

You deploy Microsoft Azure Active Directory (Azure AD) Connect and configure synchronization between Office 365 and the on-premises Active Directory.

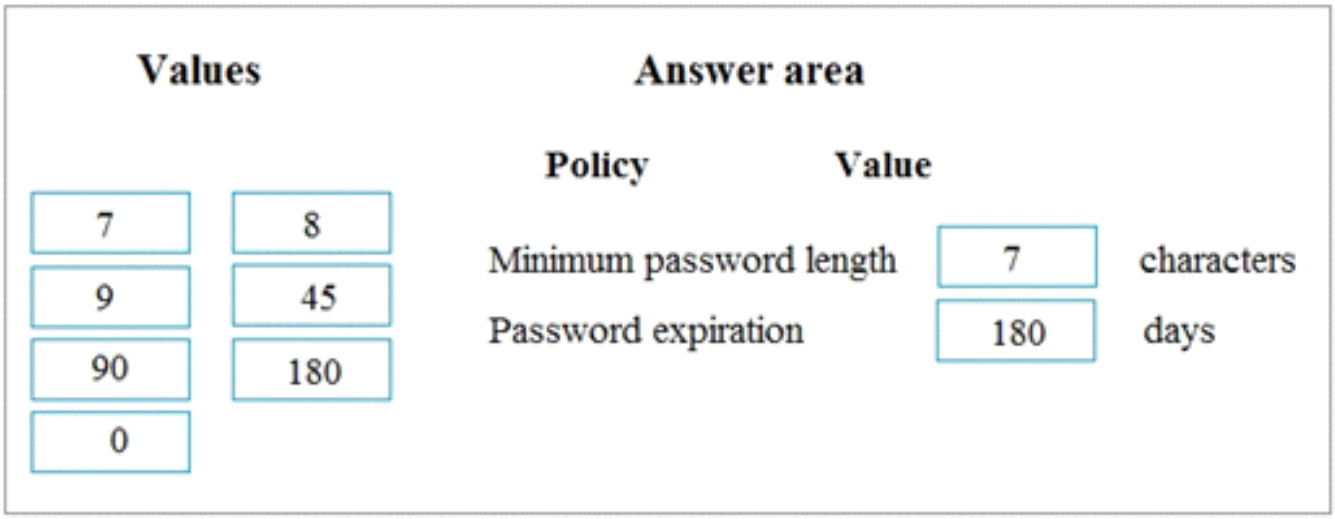
You need to determine the resulting password policies for Office 365 users.

Which password policies will take effect? To answer, drag the appropriate values to the correct policies. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:



When password synchronization is enabled, the password complexity policies in your on-premises Active Directory instance override complexity policies in the cloud for synchronized users. You can use all of the valid passwords from your on-premises Active Directory instance to access Azure AD services.

You can continue to sign in to your cloud services by using a synchronized password that is expired in your on-premises environment.

References:

https://scottcroucher.com/2017/08/11/implement-password-synchronization-with-azure-ad-connect-sync/

Question: 119

DRAG DROP

You manage an on-premises Active Directory environment. You implement an Office 365 tenant. Password requirements for the environments are listed in the table below.

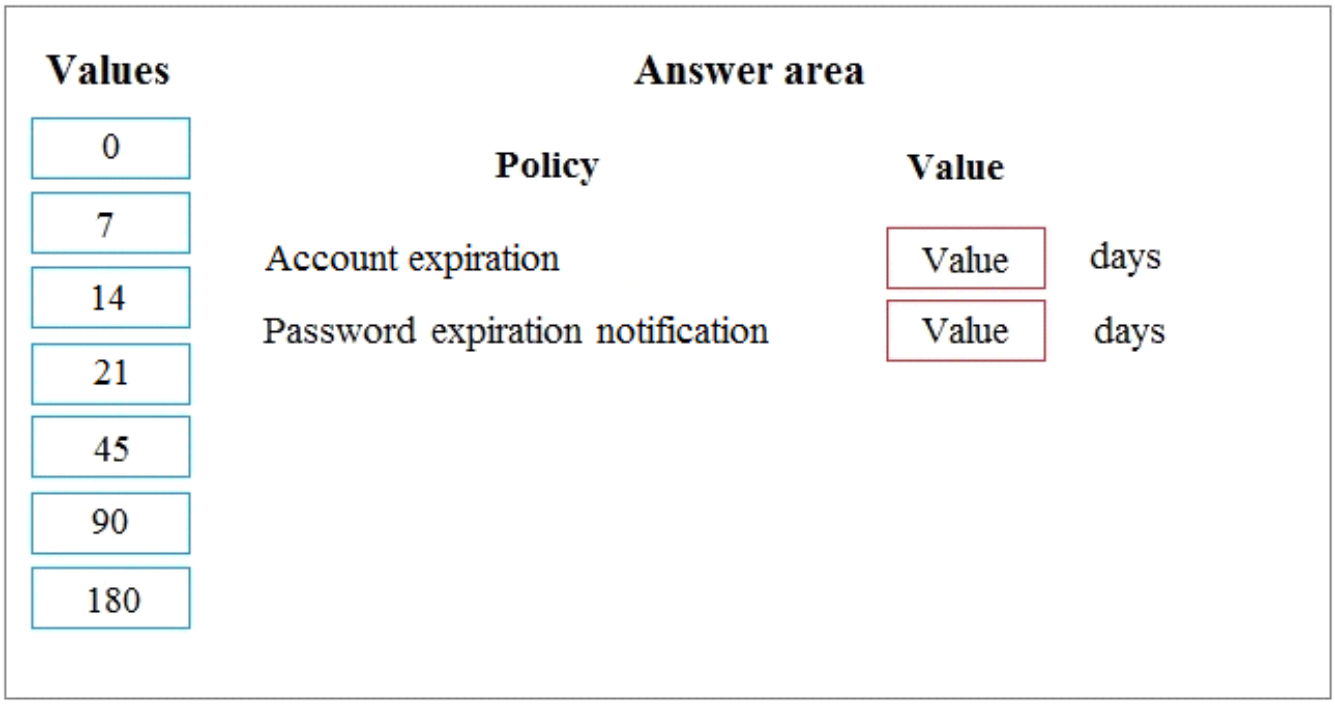
Environment	Password requirements
On-premises Active Directory	Accounts expire after 180 days. Passwords expiration notifications must be sent 7 days before a password expires.
Office 365	Accounts expire after 90 days. Passwords expiration notifications must be sent 21 days before a password expires.

You deploy Microsoft Azure Active Directory (Azure AD) Connect and configure synchronization between Office 365 and the on-premises Active Directory.

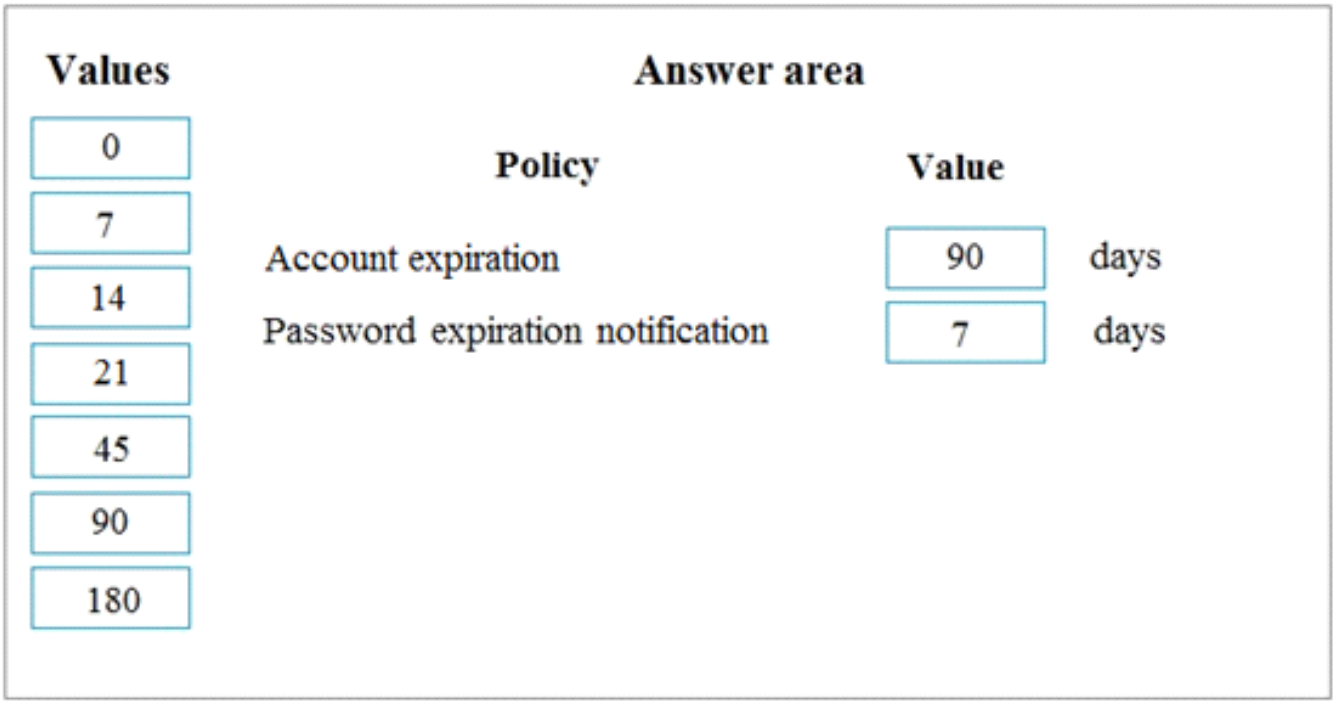
You need to determine the resulting policies for Office 365 users.

Which password policies will take effect? To answer, drag the appropriate values to the correct policies. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer:



If your organization uses the accountExpires attribute as part of user account management, be aware that this attribute is not synchronized to Azure AD. As a result, an expired Active Directory account in an environment configured for password synchronization will still be active in Azure AD.
When password synchronization is enabled, the password complexity policies in your on-premises Active Directory instance override complexity policies in the cloud for synchronized users. You can use all of the valid passwords from your on-premises Active Directory instance to access Azure AD services.
References:
https://scottcroucher.com/2017/08/11/implement-password-synchronization-with-azure-ad-connect-sync/

Question: 120

A company deploys an Office 365 tenant.
You need to configure single sign-on (SSO) for all user accounts. External users are not allowed to connect directly to internal servers.
Which three actions should you perform? Each correct answer presents part of the solution.

A. Run the Windows PowerShell cmdlet Enable-ADFSEndpoint.
B. Deploy a federation server proxy.
C. Run the Windows PowerShell cmdlet Convert-MsolDomainToStandard.
D. Run the Windows PowerShell cmdlet New-ADFSOrganization.
E. Deploy a federation server farm.
F. Run the Windows PowerShell cmdlet Convert-MsolDomainToFederated.

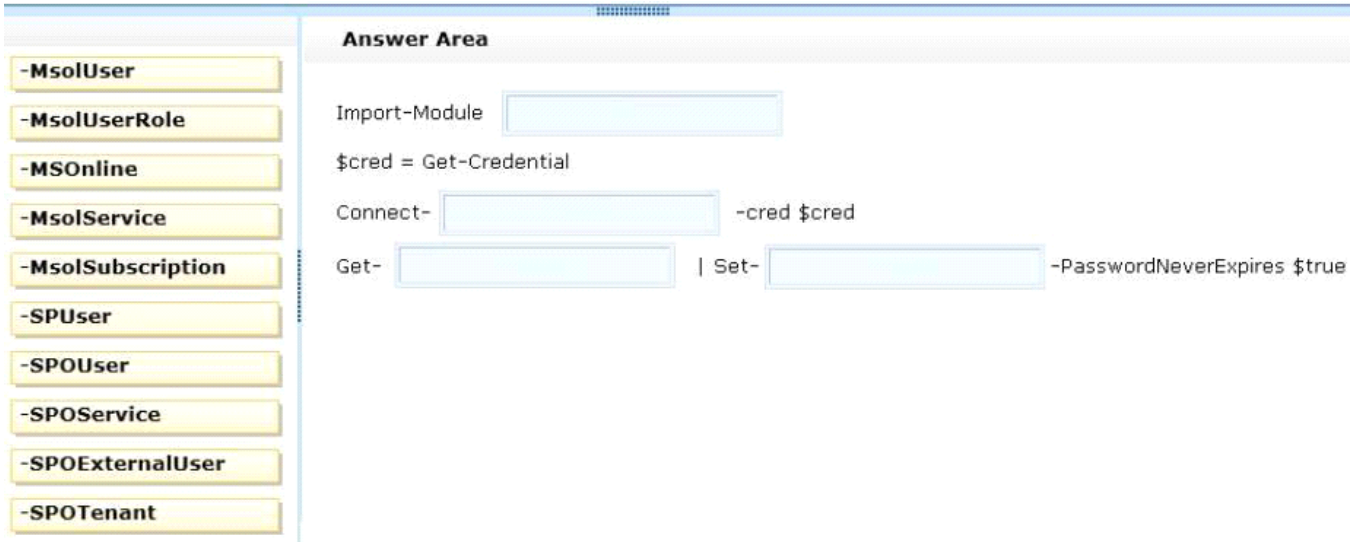
Answer: B,E,F

Explanation:

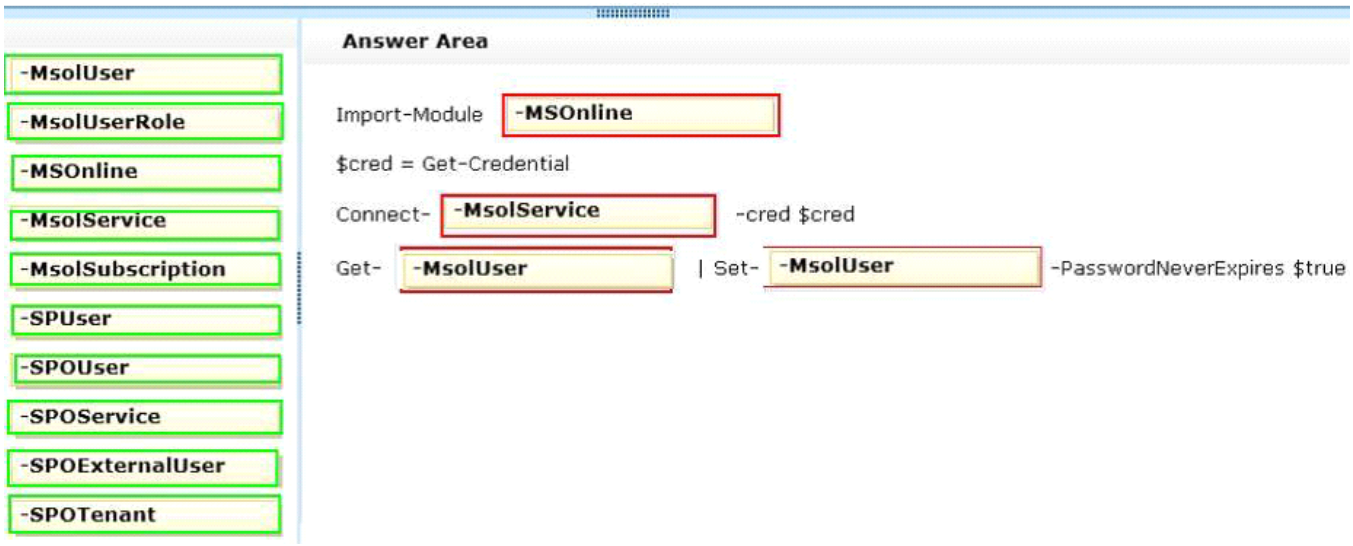
Question: 121

DRAG DROP
A company has 50 employees that use Office 365.

You need to disable password expiration for all accounts.
How should you complete the relevant Windows PowerShell commands? To answer, drag the appropriate Windows PowerShell segment to the correct location in the answer are
a. Each Windows PowerShell segment may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:



Question: 122

You are the administrator for a company named Contoso, Ltd.
The company has an Office 365 subscription.
You need to prevent users from changing their user display name by using Outlook Web App.
What should you do?

A. Run the Set-MsolCompanyContactInformation cmdlet.
B. Modify the default email address policy.
C. Run the Set-MsolUserPrincipalName cmdlet.
D. Modify the default role assignment policy.

Answer: D

Explanation:
References:
http://help.outlook.com/en-us/140/ff852817.aspx

Question: 123

Your company uses Office 365.
You need to prevent users from initiating remote wipes of mobile devices by using the Office 365 portal.
What should you modify?

A. the Outlook Web App mailbox policy
B. the Exchange ActiveSync device policy
C. the default role assignment policy
D. the Exchange ActiveSync Access settings

Answer: B

Explanation:
References:
https://technet.microsoft.com/en-us/library/dn792010.aspx

Question: 124

Your company uses Office 365.
You need to retrieve a list of all the mail-enabled objects in Office 365.
Which Windows PowerShell cmdlet should you use?

A. Get-MSOLUser
B. Get-MSOLContact
C. Get-RoleGroupMember
D. Get-Group
E. Get-Recipient
F. Get-LogonStatistics
G. Get-MailContact
H. Get-RemovedMailbox
I. Get-Mailbox
J. Get-ManagementRoleAssignment
K. Get-MailboxStatistics
L. Get-User

Answer: E

Explanation:
References:
https://technet.microsoft.com/en-us/library/aa996921(v=exchg.160).aspx

Question: 125

Your company has an Office 365 subscription. The network contains an Active Directory domain. You configure single sign-on for all users. Corporate security policy states that all account passwords used by Windows services must be changed every 90 days.
An administrator changes all of the account passwords used by Windows services.
You need to ensure that single sign-on continues to function.
What should you do?

A. From Windows PowerShell, run the Update-MSOLFederatedDomain cmdlet.
B. From Internet Information Services (IIS) Manager, modify the properties of the ADFS virtual directory.
C. From the Services console, modify the properties of the AD FS 2.0 Windows Service.
D. From Windows PowerShell, run the Set-MSOLADFSContext cmdlet.

Answer: C

Explanation:
References:
https://technet.microsoft.com/en-us/library/hh344806(v=ws.10).aspx

Question: 126

You are implementing a hybrid deployment of Office 365.
You discover that users who have migrated to Office 365 cannot view the free/busy information of users who are hosted on the Microsoft Exchange Server on-premises environment. The Exchange on-premises users can view the free/busy information of all users.
You need to ensure that the users who have Office 365 mailboxes can view the free/busy information of users who have Exchange on premises mailboxes.
Which node should you modify from the Exchange Management Console?

A. Microsoft Exchange On-Premises - Organization Configuration
B. Microsoft Exchange On-Premises - Server Configuration
C. Microsoft Exchange On-Premises - Recipient Configuration
D. Office 365 - Organization Configuration
E. Office 365 - Recipient Configuration

Answer: A

Explanation:
References:
https://technet.microsoft.com/en-us/library/aa997669(v=exchg.141).aspx

Question: 127

Your company uses Office 365 for all users. The company has the contoso.com SIP domain.
You need to change the SIP address of a user named User1 from userl@contoso.com to user2@contoso.com.
You must achieve this goal in the minimum amount of time.
What should you do?

A. Modify the PrimarySmtpAddress attribute of User1.
B. Add a proxy address to the properties of User1.

C. Create a service request.
D. Modify the sign-in status of User1.

Answer: A

Explanation:
References:
https://technet.microsoft.com/en-us/library/dd335189(v=exchg.150).aspx

Question: 128

Your company has an Office 365 subscription. A user named Test5 has a mailbox.
You need to ensure that all of the email messages sent and received by Test5 are accessible to members of the audit department for 60 days, even if Test5 permanently deletes the messages.
What should you do?

A. Run the Set-User cmdlet.
B. Run the Set-Mailbox cmdlet.
C. Run the Set-RetentionPolicyTag cmdlet.
D. Run the Set-MailboxDatabase cmdlet.
E. Run the Set-RetentionPolicy cmdlet.

Answer: B

Explanation:
References:
https://technet.microsoft.com/en-us/library/bb123981(v=exchg.160).aspx

Question: 129

You deploy Office 365.
All the members of a team named Sales have full access to a shared mailbox named Sales.
You enable auditing for all shared mailboxes.
From the Sales mailbox, an email message that contains inappropriate content is sent.
You need to identify which user sent the message.
What should you do?

A. From the Exchange Control Panel, run an administrator role group report.
B. From Windows PowerShell, run the Get-SharingPolicy cmdlet.
C. From Windows PowerShell, run the Write-AdminAuditLog cmdlet.
D. From Windows PowerShell, run the New-MailboxAuditLogSearch cmdlet.

Answer: D

Explanation:
By process of elimination:
The Write-AdminAuditLog cmdlet will write a comment to the administrator audit log.
The Get-SharingPolicy cmdlet allows you to view the settings of sharing policies
The administrator role group report in EOP will list changes to the management role groups within a particular time frame.

The New-MailboxAuditLogSearch cmdlet performs an async search of mailbox audit logs for the specified mailboxes and sends the search results by email to the specified recipients.
References:
https://technet.microsoft.com/en-us/library/ff522362%28v=exchg.150%29.aspx

Question: 130

Your company has a Microsoft Exchange Server 2003 organization.
Users access their mailbox by using RPC over HTTP and Exchange ActiveSync.
You purchase an Office 365 subscription. From the Office 365 portal, you create and verify the accepted domain of the company. From the Exchange Control Panel, you attempt to migrate all of the mailboxes to Microsoft Exchange Online and you receive an error message indicating that the remote server is unavailable.
You need to identify what prevents the mailboxes from migrating.
Which tool should you use?

A. the Microsoft Remote Connectivity Analyzer
B. the Exchange Server Deployment Assistant
C. the Office 365 Deployment Readiness Tool
D. the Microsoft Online Services Directory Synchronization Configuration Wizard

Answer: A

Explanation:
References:
http://o365info.com/microsoft-remote-connectivity-analyzer-exrca-autodiscover-troubleshootingtools-part-2-of-4-part-22-of-36/

Question: 131

Your company has a hybrid deployment Office 365.
You create a user in Office 365. The next day, you discover that the new user account fails to appear in the Microsoft Exchange Server on-premises global address list (GAL).
You need to ensure that the user has a mailbox and appears in the Exchange on-premises GAL and the Office 365 GAL.
What should you do?

A. Assign a Microsoft Exchange Online license to the user account.
B. From the Microsoft Online Services Directory Synchronization tool, enable rich coexistence.
C. From the Office 365 portal, modify the sign-in status of the user account.
D. Delete the user account hosted on Office 365.From the Exchange Management Console, create a new remote mailbox.

Answer: D

Explanation:

Question: 132

Your company has a hybrid deployment of Office 365.
You need to set the authentication method of the federation servers to forms-based authentication.
What should you do?

A. Modify the Web.config file in the %systemroot%\inetpub\adfs\ls directory.
B. Modify the Global.asax file in the %systemroot%\inetpub\adfs\ls directory.
C. From the AD FS 2.0 Management console, add a relaying party trust.
D. From the AD FS 2.0 Management console, add a claims provider trust.

Answer: A

Explanation:
References:
http://msdn.microsoft.com/en-us/library/xdt4thhy.aspx

Question: 133

You subscribe to Office 365.
You plan to implement single sign-on.
You need to deploy Active Directory Federation Services (AD FS) to a server for the planned implementation.
Which deployment methods should you use? (Each correct answer presents a complete solution.
(Choose all that apply.)

A. On a server that runs Windows Server 2008 R2, download and install AD FS 2.0.
B. On a server that runs Windows Server 2008, download and install AD FS 2.0.
C. On a server that runs Windows Server 2008, install the AD FS server role.
D. On a server that runs Windows Server 2008 R2, install the AD FS server role.

Answer: A,B

Explanation:
Single sign-on requires AD FS version 2.0. The AD FS server role is version 1.1.

Question: 134

Your company has an Office 365 subscription. A user named User1 has a mailbox.
You need to ensure that all of the email messages sent and received by User1 are accessible to the audit department for 60 days, even if User1 permanently deletes the messages.
What should you do?

A. Run the Set-MailboxDatabase cmdlet and specify the -DeletedItemRetention parameter.
B. Run the Set-Mailbox cmdlet and specify the -LitigationHoldEnabled parameter.
C. Run the Set-Mailbox cmdlet and specify the -SingleItemRecoveryEnabled parameter.
D. Run the Set-MailboxDatabase cmdlet and specify the -EventHistoryRetentionPeriod parameter.

Answer: B

Explanation:
References:
https://technet.microsoft.com/en-us/library/bb123981(v=exchg.160).aspx

Question: 135

Your company has a main office and a branch office. Both offices are directly connected to the Internet. The branch office connection to the Internet has limited bandwidth.
The company deploys Microsoft Skype for Business Online.
You need to ensure that users in the branch office can only use instant messaging (IM) while using Skype for Business Online. The users must be prevented from connecting to audio or video conferences.
What should you do?

A. On the firewall at the branch office, block all of the outbound traffic on port 5061.
B. From the Office 365 portal, modify the user properties of each user in the branch office.
C. From the Office 365 portal, configure the license settings of each user in the branch office.
D. Deploy only the Skype for Business Attendee client to all of the users in the branch office.

Answer: B

Explanation:

Question: 136

You are the administrator for a company named Tailspin Toys. The company uses the tailspintoys.com SMTP domain. All mailboxes are hosted on Office 365. From the Internet, customers send warranty questions to Tailspin Toys by sending an email message to a shared mailbox named Warranty. The Warranty mailbox has the warranty@tailspintoys.com SMTP address. The service manager reports that many email orders sent to warranty@tailspintoys.com are identified as spam.
You need to ensure that all of the messages sent by the customers arrive in the Warranty mailbox.
What should you do?

A. From the Forefront Online Protection Administration Center, enable Directory-Based Edge Blocking.
B. From the Forefront Online Protection Administration Center, create a new policy rule.
C. From Windows PowerShell, run the New Transport Rule cmdlet and specify the - ExceptIfHeaderContainsWords parameter.
D. From Windows PowerShell, run the Set-ContentFilterConfig cmdlet and specify the -BypassedRecipients parameter.

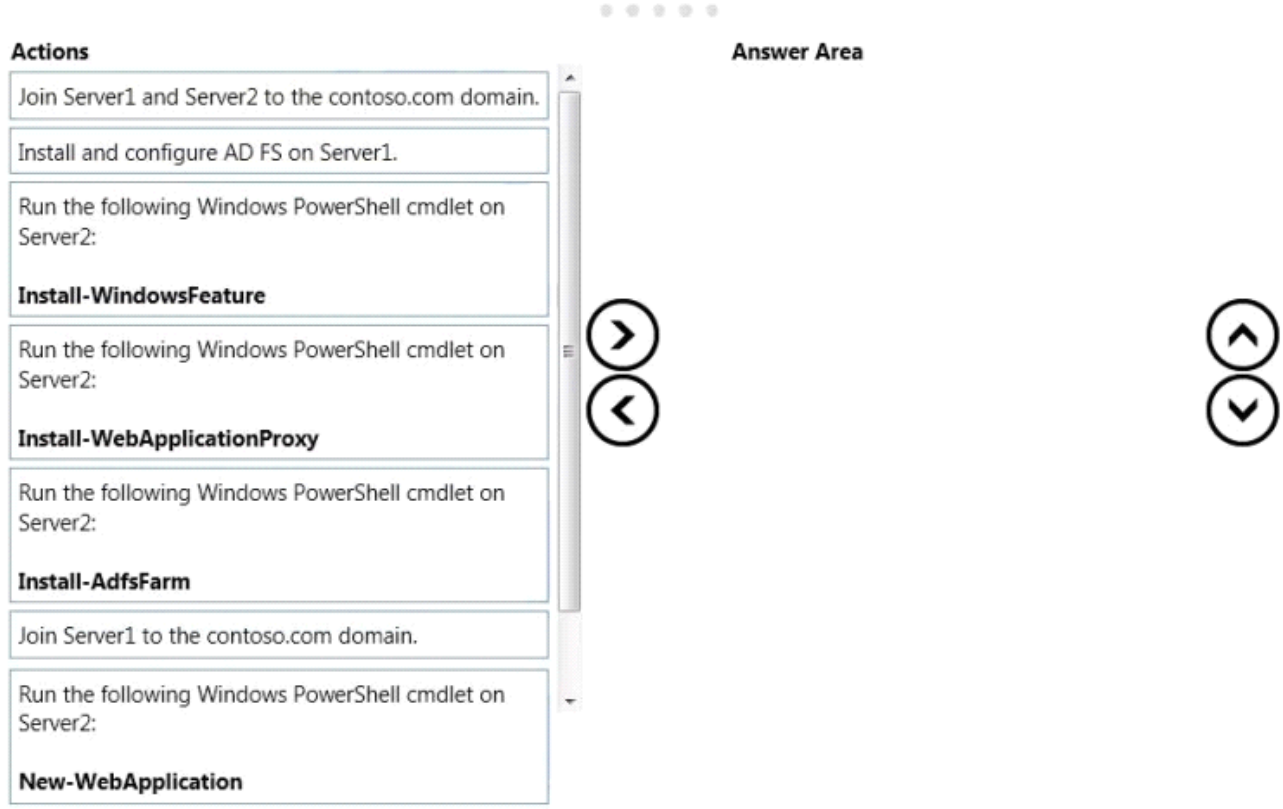
Answer: C

Explanation:
Set-ContentFilterConfig is only available for on-premises Exchange servers.
"….Learn more about this at Configure your spam filter policies. Another option would be create an Exchange transport rule that works like the domain or user-based allow list in the spam filter. You can block messages sent from a particular domain or user in a similar manner too…"
References:

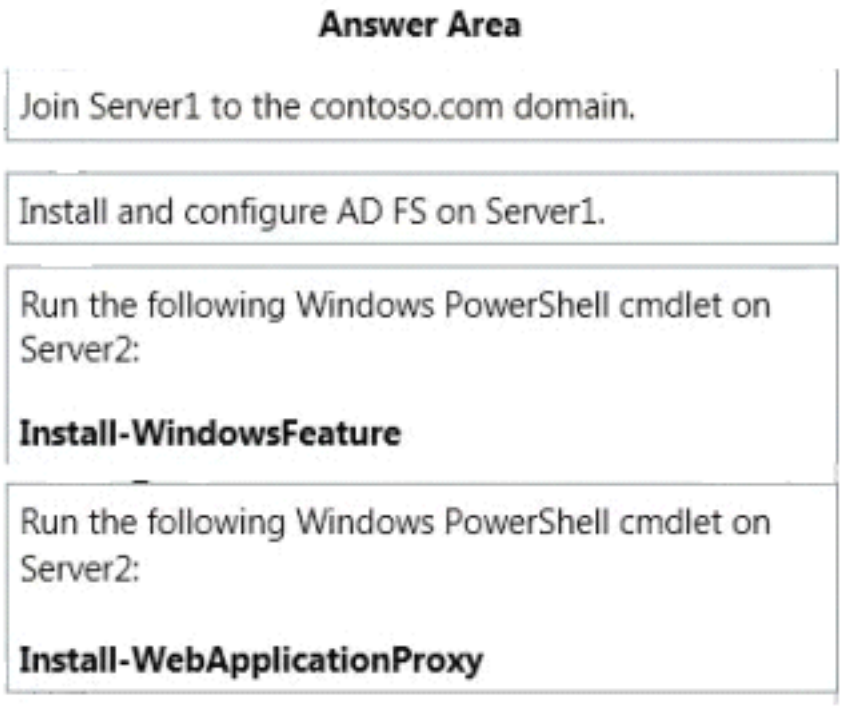
Question: 137

DRAG DROP
Contoso, Ltd. has an Office 365 tenant. The company has two servers named Server1 and Server2 that run Windows 2012 R2 Server. The servers are not joined to the contoso.com domain. Server2 is deployed to the perimeter network.
You install Secure Sockets Layer (SSL) certificates on both servers.
You deploy internal and external firewalls. All firewalls allow HTTPS traffic.
You must deploy single sign-on (SSO) and Active Directory Federation Services (AD FS).

You need to install and configure all AD FS components in the environment.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



All AD FS servers must be domain joined.
References:

https://technet.microsoft.com/en-us/library/dn554247(v=ws.11).aspx#BKMK_4

Question: 138

Your company has a hybrid deployment of Office 365.
You need to identify which certificate is used for token signing between the on-premises environment and Office 365.
Which tool should you use?

A. the Exchange Management Console
B. the AD FS 2.0 Management console
C. the Active Directory Domains and Trusts snap-in
D. the Office 365 portal
E. the Certificates snap-in

Answer: B

Explanation:
References:
http://technet.microsoft.com/en-us/library/gg557729%28v=ws.10%29.aspx

Question: 139

Which role should you assign to staff who you want to be able to create non-privileged Office 365 users without assigning any unnecessary privileges?

A. Global administrator
B. Service administrator
C. Password administrator
D. User management administrator

Answer: D

Explanation:
Assigning the user management administrator role would allow users to create non-privileged Office 365 accounts without assigning unnecessary privileges

Question: 140

DRAG DROP
A company has an Active Directory Domain Services domain.
You plan to implement Active Directory Federation Service (AD FS) with single sign-on.
You have the following requirements:
Servers must a Windows Server 2012 R2.
Internet-facing servers must be placed in the perimeter network.
The solution must support at least 105 AD FS trust relationships.
You need to deploy the appropriate roles.

Answer Area

	Deployment location	Role
Web Application Proxy	Perimeter network	
Federation Service Proxy	Application server	
Active Directory Federation Services	Database server	
Active Directory Domain Services		
SQL Server		

Answer:

Answer Area

	Deployment location	Role
	Perimeter network	Web Application Proxy
Federation Service Proxy	Application server	Active Directory Federation Services
	Database server	SQL Server
Active Directory Domain Services		

Question: 141

HOTSPOT

A company has an Office 365 tenant.

You plan to use Active Directory Federated Services for user authentication.

You create an account named SyscService in Active Directory and in Office 365.

You must configure the permissions for the accounts in both environments by granting the minimum permissions required.

In the table below, identify the role that you must assign to each account.

NOTE: Make only one selection in each column. Each correct answer is worth one point.

Answer Area

Account Location	Active Directory	Office 365
Domain User	○	○
Schema Admin	○	○
Account Operators	○	○
User Management Admin	○	○
Global Administrator	○	○

Answer:

Answer Area

Account Location	Active Directory	Office 365
Domain User	○	○
Schema Admin	○	○
Account Operators	○	○
User Management Admin	●	○
Global Administrator	○	●

References:
https://support.office.com/en-us/article/Assigning-admin-roles-in-Office-365-operated-by21Vianet-D58B8089-CBFD-41EC-B64C-9CFCBEF495AC?ui=en-US&rs=en-US&ad=US

Question: 142

An organization uses Exchange Online.
You enable mailbox audit logging for all mailboxes.
User1 reports that her mailbox has been accessed by someone else.
You need to determine whether someone other than the mailbox owner has accessed the mailbox.
What should you do?

A. Run the following Windows PowerShell command:Search-MailboxAuditLog -Identity User1 -LogonTypes Owner -ShowDetails
B. In the Exchange Admin Center, navigate to the Auditing section of the Protection page.Run a non-owner mailbox access report
C. Run the following Windows PowerShell command:New-AdminAuditLogSearch -Identity User1 -LogonTypes Owner -ShowDetails
D. In the Exchange Admin Center, navigate to the Auditing section of the Compliance Management page. Run a non-owner mailbox access report.

Answer: D

Explanation:
References:
https://technet.microsoft.com/en-us/library/jj150575(v=exchg.150).aspx

Question: 143

You are the Microsoft Skype for Business administrator for a company that uses Skype for Business Online.
The company has mandated that employees may use Skype for Business Online to communicate with contacts from approved external domains.
You need to configure Skype for Business Online to allow Skype for Business federation with only three specific domains.
You must achieve this goal by using the least amount of administrative effort.
Which two actions should you perform? Each correct answer presents part of the solution.

A. In the Skype for Business admin center, set the External Access option to On except for blocked domains.
B. In the Office 365 admin center, add the three domains to the domain list and set the domain intent for each domain to Skype for Business Online.
C. In the Skype for Business admin center, set the External Access option to Off completely.
D. In the Skype for Business admin center, set the External Access option to On only for allowed domains.
E. In the Skype for Business admin center, configure the Presence Privacy Mode option to display presence information only to the users' contacts.
F. In the Skype for Business admin center, add the three domains to the Blocked Or Allowed Domains list.

Answer: D,F

Explanation:
References:
http://technet.microsoft.com/en-us/library/hh852512.aspx
http:// technet.microsoft.com/enus/library/jj205126.aspx

Question: 144

Your company is planning to migrate to Microsoft Exchange Online. The company employs 1,000 people, each with a

mailbox currently located on Exchange 2010 on-premises.
You estimate that it will take a minimum of four weeks to migrate all mailboxes from on-premises Exchange to Exchange Online.
The company has the following migration requirements:
During the migration, do not change the existing Microsoft Outlook profiles and . ost files used by the employees.
Ensure that email messages sent between on-premises mailboxes and online mailboxes during the migration are secure.
Do not send email messages between on-premises mailboxes and online mailboxes over the Internet in plain text.
You need to select the migration strategy that meets the requirements.
Which migration strategy should you use?

A. Cutover migration only
B. IMAP migration only
C. Remote move migration only
D. Staged migration only

Answer: C

Explanation:
References:
http://technet.microsoft.com/en-GB/library/jj863291(v=exchg.150).aspx
http://support.microsoft.com/kb/2798131/en-gb
http://technet.microsoft.com/en-GB/library/dn720476(v=exchg.150).aspx

Question: 145

You are the Office 365 administrator for your company.
The company has established the following new requirements:
Members of the legal team must be able to conduct eDiscovery searches.
Employees must be notified when they send email messages that contain confidential information.
You need to configure the environment.
Which two actions should you perform? Each correct answer presents part of the solution.

A. Configure journaling to a Microsoft Exchange Online mailbox for all mailboxes.
B. Add the members of the legal team to the Discovery Management role group.
C. Create a Data Loss Prevention policy.
D. Place all executive mailboxes on In-Place Hold for 365 days and use In-Place eDiscovery for mailbox searches.
E. Enable Microsoft Exchange Online Archiving for the executive mailboxes.
F. Place all executive mailboxes on Retention Hold.

Answer: B,C

Explanation:
First requirement is "Members of the legal team must be able to conduct eDiscovery searches."
Second requirement employees must be notified when they send email messages that contain confidential information"
B: The Discovery Management role group allows administrators or USERS to perform searches of mailboxes in the Exchange Online organization.
C: Data Loss Prevention Policies can be configured with a Policy Tip to notify the sender when they are sending confidential information.

Existing or custom DLP policy templates can be used to detect the presence of confidential information.

Question: 146

Your company has an Office 365 Enterprise El subscription. The company wants to implement an enterprise document collaboration and social networking platform that allows users to upload documents from their computers and conduct informal polls.
You need to implement a solution that meets the requirements.
Which solution should you implement?

A. Microsoft SharePoint document libraries
B. Microsoft SharePoint surveys
C. Microsoft Yammer
D. Microsoft SharePoint newsfeeds
E. Microsoft SkyDrive Pro

Answer: C

Explanation:
Yammer is Microsoft's private collaboration platform for enterprise social networking.
Unlike public social media platforms such as Twitter, Yammer only allows members to connect with other members who belong to the same email domain. This unique feature provides corporate employees with the ability to communicate privately, using a graphical user interface (GUI) that resembles Facebook.

Question: 147

Your company has an Office 365 Small Business subscription.
You are the Microsoft SharePoint Online administrator.
The company wants to have two separate public websites with different URLs.
What should you do?

A. Upgrade to SharePoint Online for Office 365 Enterprise, Education, and Government.
B. Create one public website and one subsite, and then configure a redirect.
C. Create two public websites and configure the DNS records for each site.
D. Upgrade to SharePoint Online for Office 365 Midsize Business.

Answer: B

Explanation:
References:
http://www.toddklindt.com/blog/Lists/Posts/Post.aspx?ID=48

Question: 148

Your company plans to use Office 365 and Microsoft SharePoint Online. Another employee provisions the company's Office 365 tenant.
You discover that the employee can create and manage SharePoint site collections.
You need to prevent the employee from creating or managing site collections.
From which role should you remove the employee?

A. Service administrator
B. SharePoint Online administrator
C. Global administrator
D. Site collection administrator

Answer: C

Explanation:
The person who provisions the company Office 365 tenant is the first global administrator who in turn is a SharePoint Online Administrator. As long as this person is a global administrator they will be able to create SharePoint sites. Now once the site collection is provisioned you can prevent them from managing the site itself by removing them from the Site Collection Administrator role.
By doing this if they went directly to the site they wouldn't be able to manage it, but they could always add themselves back to that role The way the question is stated you would need to be a global administrator yourself and then remove the person who created the tenant as a global administrator.
"Add an administrator to the Site Collection Administrators list If you are a Global Administrator or a SharePoint Online Administrator in SharePoint Online in Office 365 plans other than Office 365 Small Business, you must add your user name account to the Site Collection Administrator list on the SharePoint admin center page before you can add other site collection administrators via the Team Site. If you are a Global Administrator or SharePoint Online Administrator and you add yourself as a site collection administrator, performing this action is known as taking ownership of a site."
References:
https://support.office.com/en- au/article/Manage-administrators-for-a-site-collection9a7e46f9-3fc4-4297-955a-82cb292a5be0
https:// blogs.office.com/2015/06/11/more-control-overdata-access-with-workload-specific-admin-roles/

Question: 149

Your company uses Microsoft SharePoint Online for collaboration. A document library is configured as shown in the following table.

Configuration Option	Current Selection
Require content approval for submitted items?	Yes
Create a version each time you edit a file in this document library?	Create major versions
Who should see draft items in this document library?	Only users who can edit items
Require documents to be checked out before they can be edited?	Yes

You need to enable the coauthoring of documents in the library.
What should you do?

A. Change the Who should see draft items in this document library? setting to Any user who can read items.
B. Change the Create a version each time you edit a file in this document library? setting to No Versioning.
C. Change the Require documents to be checked out before they can be edited? setting to No.
D. Change the Require content approval for submitted items? setting to No.

Answer: C

Explanation:
From TechNet Article "Overview of co-authoring in SharePoint 2013" Check out When a user checks out a document for editing, the document is locked for editing by that user.
This prevents co-authoring. Do not enable the Require Check Out feature in document libraries in which co- authoring

will be used. By default, Require Check Out is not enabled in SharePoint 2013. Users should not check out documents manually when co-authoring is being used.
References:
https://technet.microsoft.com/en-us/library/ff718249.aspx

Question: 150

Your company uses Office 365 and has an Enterprise E3 plan. The company has a Microsoft SharePoint Online public website that is currently configured to use the onmicrosoft.com domain name.
The company purchases a new domain name.
You need to change the address of the SharePoint Online public website to the new domain name.
What should you do first?

A. In the SharePoint Online Administration Center, add the new domain.
B. In the Office 365 admin center, add the new domain.
C. Create a new site collection and assign it the new domain.
D. Create a new public website and assign it to the new domain.

Answer: B

Explanation:
If you go to the SharePoint Online Administration Center and click the "Add Domain" button it takes you to the same location as if you would have clicked the "Domains" -> "Add domain" option from the Office 365 admin center.
So either A or B is technically correct, but if I had to choose one of the two I would select B.
References:
https://support.office.com/en-us/article/Rename-your-SharePoint-Online-Public-Website-addressto-use-your-custom-domain-3D4BD288-772B-4F88- AF4D-F025B3825ED3
https://support.office.com/en-us/article/Rename-your-SharePoint-Online-Public-Website-addressto-use-your-custom-domain-3403c6d5-aaa6-4775- a1cc-c6bda0a99986?ui=en-US&rs=enUS&ad=US
https://support.office.com/en-us/article/Verify-your-domain-in-Office-365-6383f56d3d09-4dcb-9b41-b5f5a5efd611?ui=en-US&rs=en-US&ad=US

Question: 151

You are the Office 365 administrator for your company. All users have been assigned E3 licenses and use Office Web Apps to create and edit documents.
A user attempts to access documents stored on a USB flash drive. When the user double-clicks a file that is stored on the USB flash drive, an error message states that Windows can't open the file and needs to know what program to use to open it.
You need to ensure that the user can start Office applications and edit Office documents by double-clicking files.
What should you do on the user's computer?

A. Use Office on Demand.
B. Install Office 365 ProPlus from the Office 365 portal.
C. Copy the files from the USB flash drive to the local hard drive.
D. Install and configure Microsoft Word Viewer

Answer: B

Explanation:

The message "can't open the file and needs to know what program to use to open it" Points to Office not being installed/Windows not recognizing Office is installed on the PC, so would need to download Office 365 ProPlus from the Portal.

Question: 152

You are the Office 365 administrator for your company.
The company recently subscribed to Office 365 ProPlus.
When performing a test deployment, you receive the following error message:
"Windows cannot find 'C:\Program Files\Microsoft Office 15 \clientX64
\integratedOffice. exe'. Make sure you typed the name correctly, and then try again."
You need to successfully complete the test deployment.
Which two actions can you perform to achieve this goal? Each correct answer presents a complete solution.

A. Manually remove the registry subkeys associated with Office 2013, and then restart the Office 365 ProPlus installation.
B. Completely uninstall existing versions of Office 2013 and then restart the Office 365 ProPlus installation.
C. Download the Office 365 ProPlus package to a file share, and then deploy Office 365 ProPlus by using Group Policy.
D. Automate the installation of Office 365 ProPlus applications by using Microsoft System Center Configuration Manager

Answer: A,B

Explanation:
The answer is A and B because the issue deals with a conflict between Office 365 ProPlus and an existing Office installation. Both A and B could by themselves be a solution.
Deploying the installation through Group Policy or SCCM wouldn't make a difference and you would still get the same error.

Question: 153

A company is upgrading its 3,000 client computers to Office 365 ProPlus.
The company uses the Telemetry Dashboard to identify document compatibility issues.
The Telemetry Agent is deployed to all client computers.
The telemetry environment is described in the following table.

Item	Configuration
Telemetry database	Microsoft SQL Server 2005
Telemetry Processor	Windows 8

You need to ensure that telemetry data is collected for more than 20 client computers at a time.
What should you do?

A. Migrate the telemetry database to a computer that runs SQL Server 2008.
B. Use the Registry Editor to trigger the data collection.
C. Use Group Policy to set the MaxConnectionsPerServer setting to 100.
D. Migrate the Telemetry Processor to a computer that runs Windows Server 2012.

Answer: D

Explanation:
For test or small production environments You can use computers that run Windows 7, Windows 8, and Windows 8.1 in test environments and in small production environments. There is a limit of 20 concurrent connections for client operating systems, but in small environments, the agent randomization setting should minimize any chances of more than 20 agents connecting at one time.
References:
https://technet.microsoft.com/en-us/library/jj219431(v=office.15).aspx

Question: 154

You are the Office 365 administrator for your company. Employees do not have local administrative privileges on client computers.
The company has the following client computer software:
Windows 7 and Windows 8
32-bit and 64-bit Office 2007, Office 2010, and Office 2013
When accessing the corporate Microsoft SharePoint 2010 site, some users are unable to display SharePoint lists in the Datasheet view.
You need to ensure that all users can display SharePoint lists in the Datasheet view.
What should you do?

A. Upgrade to the latest version of Office 365 ProPlus.
B. Force a reinstallation of Office by using Group Policy and specifying a network location.
C. Uninstall the 64-bit version of Office and then install the 32-bit version of Office.
D. Upgrade all Office 2007 and Office 2010 versions to Office 2013.

Answer: C

Explanation:
A 64-bit version of the Datasheet component is not available for Office 2010.
For SharePoint Server 2010, 64-bit versions install some Office 32-bit client-side controls for supporting solutions in a 32-bit browser (the default browser on current 64-bit Windows systems).
The Edit in Datasheet view functionality in SharePoint Server 2010 isn't supported if you install 64-bit Office 2013 client.
The Edit in Datasheet functionality is available if you install 32-bit Office 2013 client
References:
http://support.microsoft.com/kb/2266203/en-us
http://support.microsoft.com/kb/909506
https://technet.microsoft.com/en-us/library/ee681792.aspx#compat4

Question: 155

Your company uses Office 365 and has an Enterprise E3 license plan. Employees are issued laptop computers that are configured with a standard image.
The image includes an installation of Office 365 ProPlus that must be activated by the employees. An employee recently received a new laptop computer to replace an older laptop.
The older laptop will be reimaged.
When the employee attempts to start Word for the first time, she receives a message saying that she cannot activate

it because she has already activated five devices.
You need to help the employee activate Office on her new laptop computer.
What should you do?

A. Assign a second E3 license to the employee.
B. Remove the employee's E3 license and then assign a new E3 license.
C. Sign in to the Office 365 portal as the employee and deactivate the old laptop.
D. Sign in to the Office 365 portal by using your Global Admin account and then deactivate the old laptop.

Answer: D

Explanation:
Deactivating Office on a particular device for a specific user can be done with either logging in as the employee and deactivating it, or by using your Global Admin account.
Sign into the Office 365 Portal -> Users -> Active Users -> Select User Name -> Edit Office
Installations and pick the device you want to remove.
References:
https://support.office.com/en-us/article/Remove-a-former-employee-from-Office-365-44d96212-4d90-4027-9aa9-a95eddb367d1#bkmk_remove

Question: 156

Your company uses Office 365 and has an Enterprise E3 license plan. Employees are issued laptop computers that are configured with a standard image.
The image includes an installation of Office 365 ProPlus that must be activated by the employees. An employee recently received a new laptop computer to replace an older laptop.
The older laptop will be reimaged.
When the employee attempts to start Word for the first time, she receives a message saying that she cannot activate it because she has already activated five devices.
You need to help the employee to license Office on her new computer.
Which two actions could you perform?

A. Assign a second E3 license to the employee.
B. Remove the employee's E3 license and then assign a new E3 license.
C. Instruct her to Sign in to the Office 365 portal as the employee and deactivate the old laptop.
D. Sign in to the Office 365 portal by using your Global Admin account and then deactivate the old laptop.

Answer: C,D

Explanation:
References:
https://www.bettercloud.com/monitor/the-academy/deactivate-office-365-installation/

Question: 157

You are the Office 365 administrator for your company. The company allows external communications through Microsoft Skype for Business Online for all domains.
The call center manager reports that call center personnel are spending too much time chatting with friends and not enough time taking calls. She requests that the call center personnel be blocked from chatting with anyone external to the company by using Skype for Business Online.

They still must be able to communicate with internal users.
You need to prevent all call center personnel from communicating with external contacts by using Skype for Business Online, while still allowing other employees to communicate with external contacts.
What should you do?

A. In the Skype for Business admin center, select all users, edit their external communications settings, and clear the Skype for Business Users check box.
B. On the External Communications page of the Skype for Business admin center, turn off external access.
C. In the Skype for Business admin center, remove the Skype for Business Online license from each of the call center personnel.
D. In the Skype for Business admin center, select all call center personnel, edit their external communications settings, and clear the People on Public IM Networks check box.

Answer: D

Explanation:
References:
https://theucguy.net/configuring-external-communications-in-Lync-online-wave-1

Question: 158

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You manage the network for a company named Fabrikam, Inc. The network contains a single Active Directory forest named fabrikam.com.
Fabrikam has two separate organizations. Each organization has a child domain in the forest. The two child domains are named org1.fabrikam.com and org2.fabriam.com.
The forest has the following deployed:
Microsoft Exchange Server 2016
Active Directory Federation Services (AD FS) 2.0
You need to synchronize each child domain to a separate Office 365 subscription.
Solution: You deploy an instance of Microsoft Azure AD Connect to org1.fabrikam.com and org2.fabrikam.com.
Does this meet the goal?

A. Yes.
B. No

Answer: B

Explanation:

Question: 159

An organization has an Office 365 tenant. You use multi-factor authentication for all privileged accounts. User1 is on an extended leave of absence.
You must configure the mailbox for User1 to forward to User2.
You need to configure forwarding for User1's mailbox.

What should you do first?

A. Launch Windows PowerShell as an administrator.
B. Launch the Exchange Admin Center.
C. Create an app password for the administrator account.
D. Connect to Exchange Online by using Remote PowerShell.

Answer: C

Explanation:

Question: 160

Contoso, Ltd. has an Office 365 tenant. You configure Azure Active Directory Synchronization for the environment.
You need to identify user objects that will be included from the directory search by using the IDFix tool.
Which account will NOT be marked as a problem account by IDFix?

A. Administrator@contoso.com
B. Guest1@contoso.com
C. msol_User1@contoso.com
D. User1@contoso.com

Answer: D

Explanation:

Question: 161

You company uses Microsoft Exchange Online for all mailboxes.
Users report connectivity issues when they attempt to access their mailbox by using Microsoft Outlook 2016.
You need to identify the following:
Whether port 443 is allowed between the corporate network and Office 365
Whether the number of network hops from the corporate network to Office 365 is less than 25
Whether the network latency between the corporate network and Office 365 is less than 275 milliseconds.
Which tool should you use?

A. Microsoft Connectivity Analyzer Tool
B. Microsoft Office Outlook Connectivity Tests
C. Microsoft Support and Recovery Assistant for Office 365
D. Office 365 health, readiness, and connectivity checks

Answer: B

Explanation:

Question: 162

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution,

while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You deploy Office 365 for all company users. You use Microsoft Exchange Online for company email. You must develop a process to assign licenses to new users in your company.
You need to implement the licensing process.
Solution: Run the Set-Mailbox Windows PowerShell cmdlet.
Does the solution meet the goal?

A. Yes
B. No

Answer: B

Question: 163

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You deploy Office 365 for all company users. You use Microsoft Exchange Online for company email. You must develop a process to assign licenses to new users in your company.
You need to implement the licensing process.
Solution: Use the Office 365 admin center.
Does the solution meet the goal?

A. Yes
B. No

Answer: A

Question: 164

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You deploy Office 365 for all company users. You use Microsoft Exchange Online for company email. You must develop a process to assign licenses to new users in your company.
You need to implement the licensing process.
Solution: Run the Set-MsolUserLicense Windows PowerShell cmdlet.
Does the solution meet the goal?

A. Yes
B. No

Answer: A

Question: 165

You are the office 365 administrator for a company. You deploy Microsoft SharePoint Online.
Many users report that they cannot discover useful content via searches.
You need to run the appropriate SharePoint Online report to help identify the issue.
Which report should you run?

A. SharePoint Site Usage
B. SharePoint Activity
C. Query Rule Usage by Day
D. Abandoned Queues by Day

Answer: D

References:
https://support.office.com/en-us/article/view-search-usage-reports-2cd8f257-c29b-423d-8265-d44e6214d095

Question: 166

You are the Office 365 administrator for a company.
You are starting a new project in the next 15 days. The project is expected to last 30 days.
You need to determine if there are any planned maintenance tasks during the project period.
In the Admin center, which page should you view?

A. the Service Health Dashboard
B. the Service Health Advisories page
C. the Service Health Incidents page
D. the Reports page

Answer: A

Question: 167

DRAG DROP
A company uses Microsoft System Center Operations Manager (SCOM) to monitor their corporate infrastructure. You manage an Office 365 environment.
You need to be able to monitor the Office 365 environment by using SCOM.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
In the Administration workspace, edit the Office 365 Notifications node.	1
Import the Office 365 management pack into SCOM.	2
Extract the Office 365 Management Pack from the SCOM distribution media.	3
Create an Office 365 Management pack for SCOM.	
In the Administration workspace, edit the Office 365 Management Packs node.	
Download the Office 365 Management Pack.	

Answer:

Answer Area

1	Download the Office 365 Management Pack.
2	Import the Office 365 management pack into SCOM.
3	In the Administration workspace, edit the Office 365 Notifications node.

Question: 168

HOTSPOT

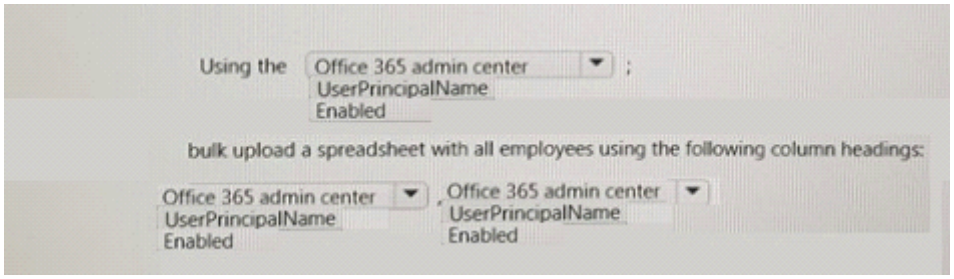
You manage the Office 365 environment for Contoso Ltd. All employees use Microsoft Exchange Online for email.

All employees must use multi-factor authentication (MFA) to access email. You configure MFA for the Office 365 environment.

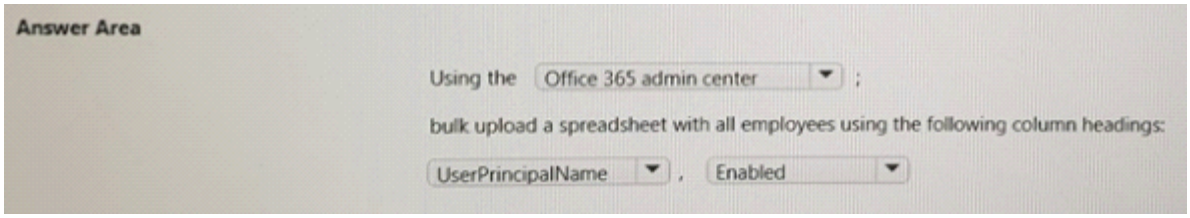
You need to configure MFA for all company employees.

What should you do? To answer, select the appropriate options in the dialog box in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

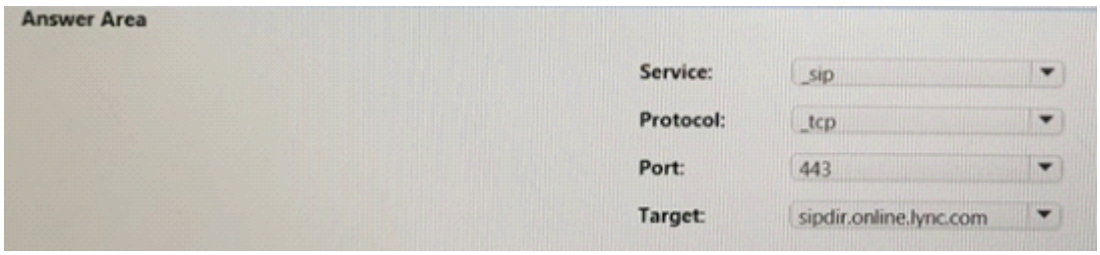


Question: 169

You are the Office 365 administrator for a company.
You deploy Microsoft Skype for Business Online. Users report issues with web conferencing. You determine that a DNS record is missing.
You need to add the required DNS record.
Which settings should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer: Check the explanation part for the answer.

Explanation.
See below.



Question: 170

HOTSPOT
A company uses Exchange Online. You plan to use the email domain contoso.com for all employees.
You must configure Exchange Online to support Outlook 2016 client connectivity.
You need to configure the appropriate DNS entries.
Which record should you create? To answer, select the appropriate entries from each list in the answer area.

Answer Area

Alias	DNS record type	Target
Contoso.com	MX	Contoso.com
Autodiscover.contoso.com	TXT	Autodiscover.contoso.com
Autodiscover.outlook.com	CNAME	Autodiscover.outlook.com
Mail.protection.outlook.com	SRV	Mail.protection.outlook.com

Answer:

Alias	DNS record type	Target
Contoso.com	MX	Contoso.com
Autodiscover.contoso.com	TXT	Autodiscover.contoso.com
Autodiscover.outlook.com	CNAME	Autodiscover.outlook.com
Mail.protection.outlook.com	SRV	Mail.protection.outlook.com

Explanation:
Box 1: Autodiscover.contoso.com
You can define an alias in one domain to point to a target server in a completely different domain.
Box 2: CNAME
The cloud-based service uses a CNAME record to implement the Autodiscover service for Outlook clients.
Box 3: Autodiscover.outlook.com
The Autodiscover CNAME record must contain the following information:
Alias autodiscover
Target autodiscover.outlook.com
References:https://msdn.microsoft.com/en-us/library/cc950655(v=exchsrvcs.149).aspx

Question: 171

DRAG DROP
You are the Office 365 administrator for a company. All employees currently use Microsoft Exchange Online for email.
You must enable message encryption for Exchange Online. The necessary transport rules are in place.
You need to configure and verify the Microsoft Azure Rights Management (Azure RMS) service.
Which four Windows PowerShell cmdlets should you run in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Import-RMSTrustedPublishingDomain	1
Set-AzureRMContext	2
Import-AzureRmContext	3
Set-IRMConfiguration	4
Enable-Aadrm	
Set-AzureRmEnvironment	
Test-IRMConfiguration	

Answer:

Answer Area

1	Enable-Aadrm
2	Set-IRMConfiguration
3	Import-RMSTrustedPublishingDomain
4	Test-IRMConfiguration

Question: 172

A company uses Office 365 services. You implement Azure AD Connect in the local environment.
An employee moves to a new department. All Office 365 services must display the new department information for the employee.
You need to update the employee's user account.
Where should you change the value of the department attribute for the employee?

A. the Active Directory management page in the Azure Management Portal
B. the on-premises Active Directory
C. the Users and groups page in the office 365 admin center
D. the Metaverse Designer

Answer: B

Question: 173

You are the Office 365 administrator Contoso, Ltd. You synchronize Active Directory Domain Services (AD DS) user accounts with an Office 365 environment by using Microsoft Azure Active Directory (Azure AD) Connect. You use a test account named Test1@contoso.com to perform configuration testing. The account currently accesses on-premises resources.
The Test1@contoso.com account experiences issues with Microsoft Exchange Online and SharePoint Online.
You need to quickly recreate the account and prevent interruption in access to the on-premises resources.
What should you do?

A. Run the Remove -SPOUser cmdlet.
B. Run the Remove -MsolUser cmdlet.
C. In the Office 365 admin center, find and delete the account.
D. Run the Remove ADUser cmdlet.
E. In the Azure AD admin center, find and delete the account.

Answer: D

Question: 174

DRAG DROP

You are the system administrator for a company that has an Office 365 tenant. Contoso.onmicrosoft.com is the only configured domain.
You have an on-premises Active Directory Domain Services (AD DS) single forest domain named contoso.local. The user principal name (UPN) for all users includes the suffix @contoso.local.
You also have an on-premises Microsoft Exchange Server 2016 environment that uses @contoso.com as the primary SMTP address suffix domain.
You need to deploy Azure Active Directory (Azure AD) Connect.

Actions	Answer Area
Change UPN for all users to contoso.com and install Azure AD Connect using express settings.	1
Add contoso.local as a custom domain in the Office 365 tenant.	2
Add contoso.com as a custom domain in the Office 365 tenant.	3
Install Azure AD Connect using express settings.	
Verify the contoso.com custom domain.	
Verify the contoso.local custom domain.	

Answer:

Answer Area

1	Add contoso.com as a custom domain in the Office 365 tenant.
2	Verify the contoso.com custom domain.
3	Change UPN for all users to contoso.com and install Azure AD Connect using express settings.

Question: 175

You manage Active Directory Domain Services (AD DS) for a company. You assign Office 365 licenses to all users. You implement Microsoft Azure Active Directory (Azure AD) Connect.
Your company terminates an employee.
You need to ensure that the terminated employee can no longer access any Office 365 rescues.
Which Windows PowerShell cmdlet should you run?

A. Set-AdUser
B. Remove-MsolServicePrincipalCredential
C. Set-MsolUser
D. Remove-MsolServicePrincipal

Answer: D

Question: 176

DRAG DROP
You deploy Office 365. You purchase 50 Office 365 Enterprise E1 licenses and assign the licenses to users.
A sales department user leaves the company and is replaced.
You need to ensure that the new user has a valid license and can access email.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

- Sign in to the Office 365 portal with an account that has the User Management admin role.
- Sign in to the Office 365 portal with an account that has the Service admin role.
- Assign the new sales user an Office 365 ProPlus license.
- Assign the new sales user an Office 365 Enterprise E1 license.
- Delete the old sales user's account.
- Delete the old sales user's mailbox.
- Purchase a new Office 365 ProPlus license.

Answer area

Answer:

Answer area

- Sign in to the Office 365 portal with an account that has the User Management admin role.
- Delete the old sales user's account.
- Assign the new sales user an Office 365 Enterprise E1 license.

Question: 177

You create an Office 365 tenant. You assign administrative roles to other users. You hire a new user named User2.

User2 must be able to assign administrative roles to other users.
You need to assign an administrative role to User2.
Which role should you assign?

A. service administrator
B. global administrator
C. password administrator
D. delegate administrator

Answer: B

Question: 178

You are the system administrator for a manufacturing company. You plan to implement Office 365.
You must create accounts for all employees and implement a password policy that requires strong passwords.
Which two characters can users include in passwords? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. spaces
B. *
C. <
D. Unicode character
E. !

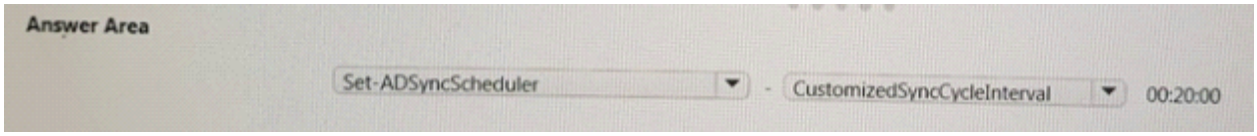
Answer: AE

Question: 179

You are the Office 365 administrator for a company. You deploy Azure Active Directory (Azure AD) Connect.
You need to ensure synchronization occurs every 20 minutes.
How should you complete the Windows PowerShell command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer: Check the explanation part for the answer.

Explanation.
See below.



Question: 180

A company uses Office 365.
You need to permanently delete a user account.
What should you do?

A. Run the Microsoft Azure PowerShell cmdlet Remove-MsolUser.

B. Use the Microsoft Azure portal.
C. Run the Microsoft Azure PowerShell cmdlet Remove-AzureAdUser.
D. Use Office 365 admin center.

Answer: A

Question: 181

You are the system administrator for a small sales company in Chicago.
You must migrate all users to Office 365. You add a domain to the Office 365 tenant.
You need to verify the new domain.
Which type of DNS record should you create?

A. MX
B. PTR
C. CNAME
D. SRV

Answer: C

Question: 182

You are the administrator for Contoso Ltd. The company uses Office 365 and has an on-premises Active Directory Domain Services (AD DS) domain that uses the namespace contoso.com.
You plan to implement Workplace Join. You must implement Active Directory Federation Services (AD FS) and Web Application Proxy (WAP). You take the following actions:
Install the WAP role on a server.
Allocate fs.conroso.com for the AD FS namespace.
Define the server FQDN as server1.contoso.com.
You need to install and configure certificate for the WAP server.

A. a certificate with a subject of fs.contoso.com
B. a certificate with a subject of server1.contoso.com
C. a certificate with a subject alternative name that contains fs.contoso.com and enterpriseregistration.contoso.com
D. a certificate with a subject alternative name that contains server1.contoso.com and fs.contoso.com

Answer: C

Question: 183

You are the Office 365 administrator for a company. You plan to implement Microsoft SharePoint Online, Exchange Online, and Skype for Business Online. End users will only use Outlook on the web for accessing email.
All outbound Internet connections for clients are blocked by default. You create inbound allow rules for the list of IPs that need to be exclude6 for Office 365.
You need to configure the outbound network ports that are required for client devices to connect to Office 365.
Which two ports should you configure? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. 25
B. 80
C. 110
D. 443

Answer: BD

Question: 184

You are the administrator for a company. You plan to use Office 365 for email and file sharing. You plan to implement a hybrid deployment with your current on-premises Active Directory Domain Services (AD DS) environment and Microsoft Azure Active Directory (Azure AD) Connect.
You must deploy Microsoft Exchange Online and OneDrive for Business for all employees. You have the following security requirements:
All employees must use complex passwords.
Passwords must be changed every six months.
Employees must use multi-factor authentication (MFA) when possible.
You need to implement MFA verification options to use with the employee's password.
Solution: Have the employee use a physical smart card.
Does the solution meet the goal?

A. Yes
B. No

Answer: B

Question: 185

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are the Office 365 administrator for a company. You plan to deploy Microsoft Skype for Business Online for all employees.
You need to verify domain ownership.
Solution: Add an SPF record.
Does the solution meet the goal?

A. Yes
B. No

Answer: B

Question: 186

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are the Office 365 administrator for a company. You plan to deploy Microsoft Skype for Business Online for all employees.
You need to verify domain ownership.
Solution: Add an NS record.
Does the solution meet the goal?

A. Yes
B. No

Answer: B

Question: 187

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are the Office 365 administrator for a company. You plan to deploy Microsoft Skype for Business Online for all employees.
You need to verify domain ownership.
Solution: Add an MX record.
Does the solution meet the goal?

A. Yes
B. No

Answer: A

Question: 188

You administer the Office 365 environment for a company that has offices around the world. All of the offices use the same Office 365 tenant.
You need to ensure that all users can access the services that are available in their regions.
Which setting or service should you update?

A. User location settings
B. User licenses
C. Service usage address
D. Rights management

Answer: A

Explanation:
The User Location settings will allow you to set sign-in status and user locations for all the users that are on your network notwithstanding the physical location where they find themselves.
References:
http://blogs.perficient.com/microsoft/2014/11/office-365-assign-licensing-user-location-via-active-directory/

Question: 189

Your company purchases an Office 365 plan. The company has an Active Directory Domain Services domain.
User1 must to manage Office 365 delegation for the company.
You need to ensure that User1 can assign administrative roles to other users.
What should you do?

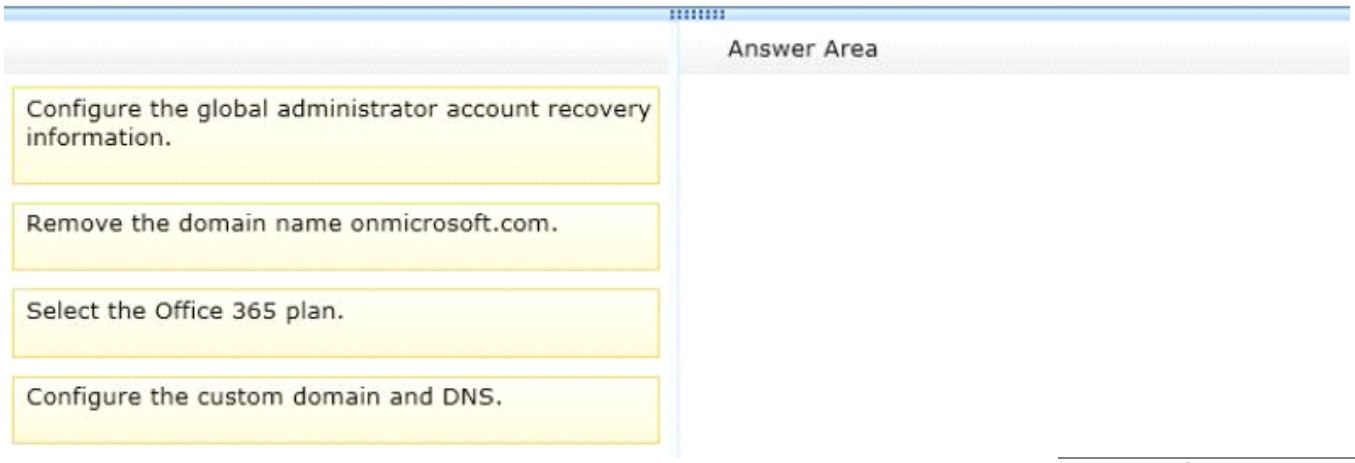
A. Create an Office 365 tenant and assign User1 the password administrator role.
B. Use a password administrator account to assign the role to User1.
C. Use a user management administrator account to assign the role to User1.
D. Create an Office 365 tenant and assign User1 the global administrator role.

Answer: D

Explanation:
The Global Administrator account is similar to the Company administrator. Users in this role have access to everything or the permission to add them to a dedicated role where they do not have permission (such as discovery management and assigning administrative roles to other users).
References:
https://support.office.com/client/Assigning-admin-roles-eac4d046-1afd-4f1a-85fc-8219c79e1504

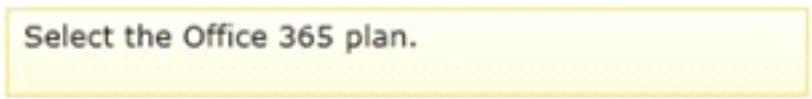
Question: 190

DRAG DROP
A company plans to implement an Office 365 environment to manage email.
All user accounts must be configured to use only a custom domain.
You need to provision an Office 365 tenant for the company.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Box 1:



Box 2:
Configure the global administrator account recovery information
Box 3:

Configure the custom domain and DNS.

The tenant is your Office 365 account, including hosted Exchange, Skype for Business, SharePoint, and your Office 365 Active Directory. The first account that you create when you first purchase Office 365 is the "owner" of your tenant. This account should be an admin account, not a person. This account does not normally require an Office 365 license. Relating to SharePoint, all of your site collections are within your tenant. You can have any number of domains within your tenant (with e-mail accounts), but you will have only one root SharePoint URL:https://xxxx.sharepoint.com.
The Global Administrator account is similar to the Company administrator. Users in this role have access to everything or the permission to add them to a dedicated role where they do not have permission (such as discovery management and assigning administrative roles to other users).
When setting up Office 365 the first step is to purchase your subscription which includes choosing the plan. Step 2 involves the selection of the sign-on method and this is where the global administrator account is of consequence. Step 3 involves the collecting of information such as domain names and DNS, locations, etc…
Step4 is the actual migration plan and schedule, step 5 – the Microsoft account and organizational account, step 6 – the SkyDrive and SkyDrive Pro, and step 7 – the Windows Intune section.
Thus you should perform step 1 through 3 to ensure that all user accounts to make use of a custom domain for their e-mail.
References:
Katzer, Matthew and Don Crawford, Office 365 Migrating and Managing your Business in the Cloud, Apress Media, New York, 2013, pp 87- 93, 373
http://office.microsoft.com/en-gb/office365-suite-help/add-your-domain-to-office-365-HA102818660.aspx

Question: 191

Your company has 100 user mailboxes. The company purchases a subscription to Office 365 for professionals and small businesses. You need to enable the Litigation Hold feature for each mailbox.
What should you do first?

A. Purchase a subscription to Office 365 for midsize business and enterprises.
B. Enable audit logging for all of the mailboxes.
C. Modify the default retention policy.
D. Create a service request.

Answer: A

Explanation:
The first step will always be the purchasing the correct Office 365 plan to suit your needs. There are three plans of Office 365: Professional, Mid-Size Businesses, and Enterprise. The Office 365 Mid-sized businesses and Enterprise plans will allow you to enable Litigation Hold. The Professional plan is not compliant with this setting. User mailboxes that are placed under litigation hold with the external audit enabled meet all compliance requirements, because the data is immutable.

Question: 192

Contoso, Ltd. plans to use Office 365 for email services and Skype for Business Online. Contoso has four unique domain names.
You need to migrate domain names to Office 365.
Which two domain names should you exclude from the migration? Each correct answer presents part of the solution.

A. contoso.us
B. contoso

C. contoso.local
D. contoso.co

Answer: B,C

Explanation:
There are no practical limits on the number of domains that can be verified to Office 365 Enterprise. The rules are simple: you need to verify a domain, and you need to assign the domain based on the needs (or Domain Intent). Domain Intent is what the domain services will be configured as; there are three different types of services for Domain Intent.
A top-level domain (TLD) is the part of the domain name located to the right of the dot (" . "). The most common TLDs are .com, .net, and .org. Some others are .biz, .info, and .ws. These common TLDs all have certain guidelines, but are generally available to any registrant, anywhere in the world.
B: contoso- single labeled domain / or also known as a second-level domain - not valid
C: contoso.local - internal labeled domain - not valid

Question: 193

A company plans to use Office 365 to provide email services for users.
You need to ensure that a custom domain name is used.
What should you do first?

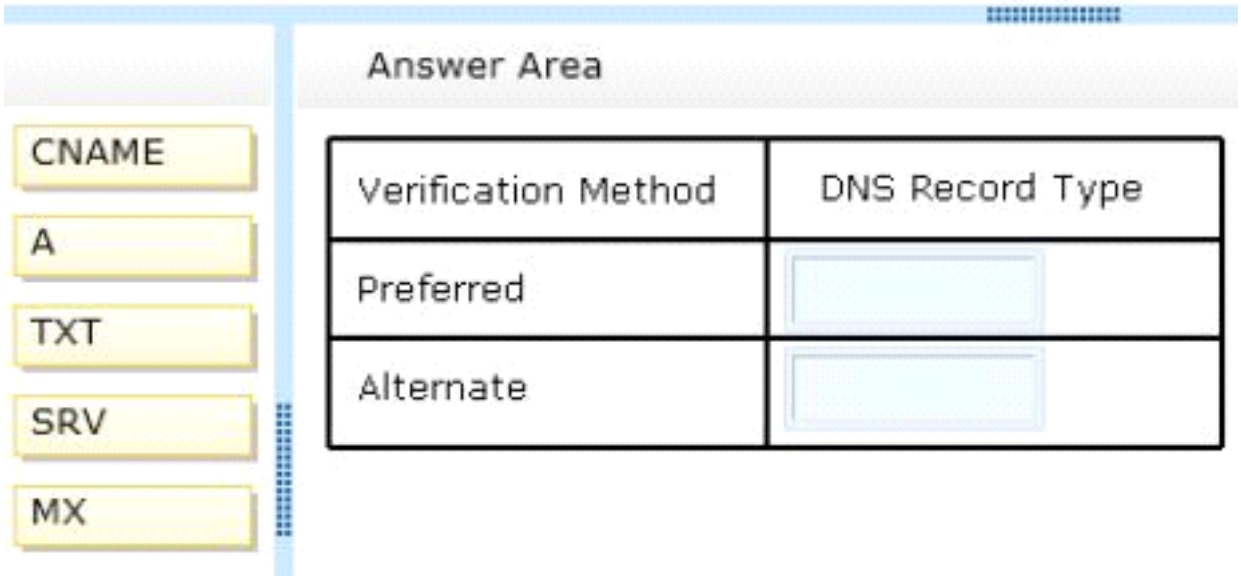
A. Add the custom domain name to Office 365 and then verify it.
B. Verify the existing domain name.
C. Create an MX record in DNS.
D. Create a CNAME record in DNS.

Answer: A

Explanation:
DNS actually tells the Internet where to send email to. Thus you need to make sure that your custom name that you intend using for email is added to Office 365 and verified. When you put the right information into the right DNS records for your domain, the DNS system routes everything correctly so your email, for example, arrives in Office 365 instead of somewhere else.

Question: 194

DRAG DROP
Fabrikam has the Office 365 Enterprise E3 plan.
You must add the domain name fabrikam.com to the Office 365 tenant. You need to confirm ownership of the domain.
Which DNS record types should you use? To answer, drag the appropriate DNS record type to the correct location or locations in the answer are
a. Each DNS record type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Answer:

Verification Method	DNS Record Type
Preferred	TXT
Alternate	MX

TXT record is used for verification. When you have added the record at your domain registrar's site, you'll go back to Office 365 and request Office 365 to look for the record. When Office 365 finds the correct TXT record, your domain is verified.

MX (mail exchanger) record points to where your email should be sent. It also has a priority field so that you can send mail to different servers in a priority order.

Question: 195

HOTSPOT

A company has an Active Directory Domain Service (AD DS) domain. All servers run Windows Server 2008. You have an on-premises Exchange 2010 server.

The company plans to migrate to Office 365.

In the table below, identify the required action for each phase of the pilot. Make only one selection in each column. Each correct selection is worth one point.

Planning Phase	Migration Phase	Project Action
○	○	Assign licenses to users.
○	○	Prepare the on-premises Active Directory for directory synchronization.
○	○	Raise the forest functional level to Windows Server 2008.
○	○	Upgrade the Exchange server to Exchange 2013.

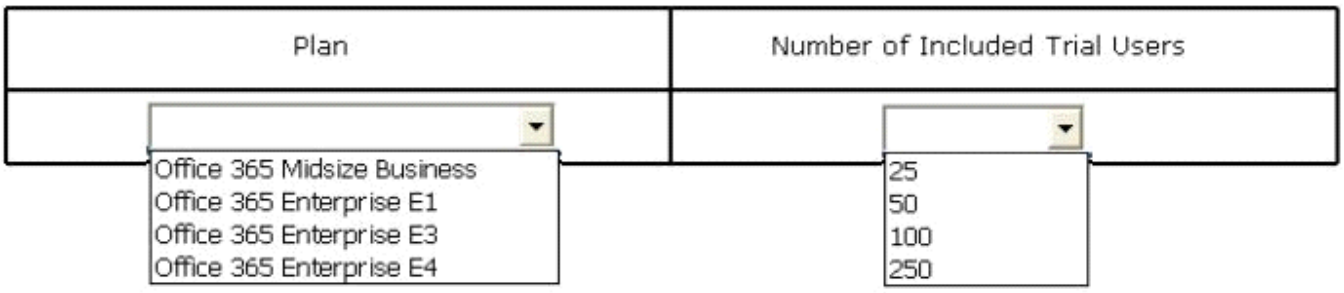
Answer:

Planning Phase	Migration Phase	Project Action
○	●	Assign licenses to users.
●	○	Prepare the on-premises Active Directory for directory synchronization.
○	○	Raise the forest functional level to Windows Server 2008.
○	○	Upgrade the Exchange server to Exchange 2013.

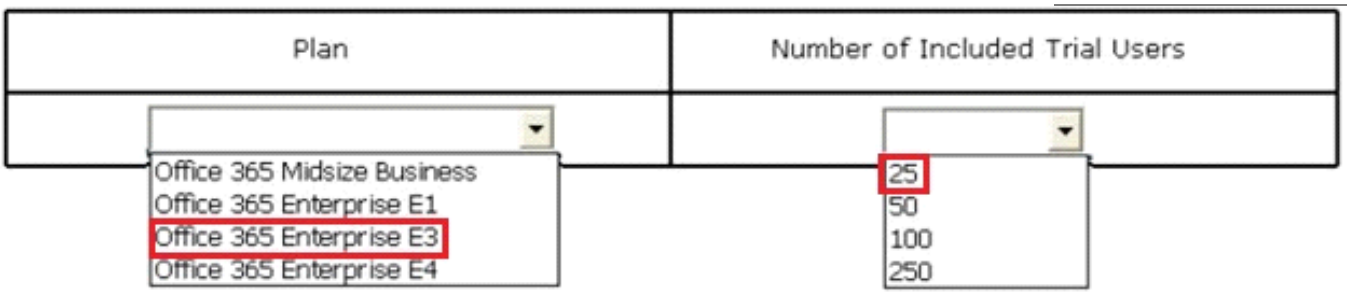
During migration which first step is to have the domain validated, the step that follows is to add users and assign licenses. Microsoft found that it is better to complete the domain configuration (with the exception of changing the MX records) and add users after the domain has been defined when migrating to Office 365.
Planning for the migration involves preparation to synchronize the Active Directory.
References:
https://msdn.microsoft.com/library/azure/jj151831.aspx

Question: 196

HOTSPOT
Fabrikam, Inc. employs 500 users and plans to migrate to Office 365.
You must sign up for a trial plan from the Office 365 website. You have the following requirements:
Create the maximum number of trial users allowed.
Convert the trial plan to a paid plan at the end of the trial that supports all of Fabrikam's users.
You need to create an Office 365 trial plan.
How should you configure the trial plan? Select the correct answer from each list in the answer area.



Answer:



Office 365 Enterprise E 3 offers include unlimited number of users and since you are signing up for a trail to develop into a paid plan. Making use of 25 users in the trial will suffice.
Office 365 Business can accommodate a maximum of 300 users only.
References:
https://technet.microsoft.com/en-us/office/dn788955
https://technet.microsoft.com/en-us/library/office-365-plan-options.aspx
https://technet.microsoft.com/en-us/library/office-365-platform-service-description.aspx
Katzer, Matthew and DonCrawford, Office 365 Migrating and Managing your Business in the Cloud, Apress Media, New York, 2013, pp 84-87

Question: 197

An organization prepares to implement Office 365.
You have the following requirements:
Gather information about the requirements for the Office365 implementation.
Use a supported tool that provides the most comprehensive information about the current environment.
You need to determine the organization's readiness for the Office 365 implementation.
What should you do?

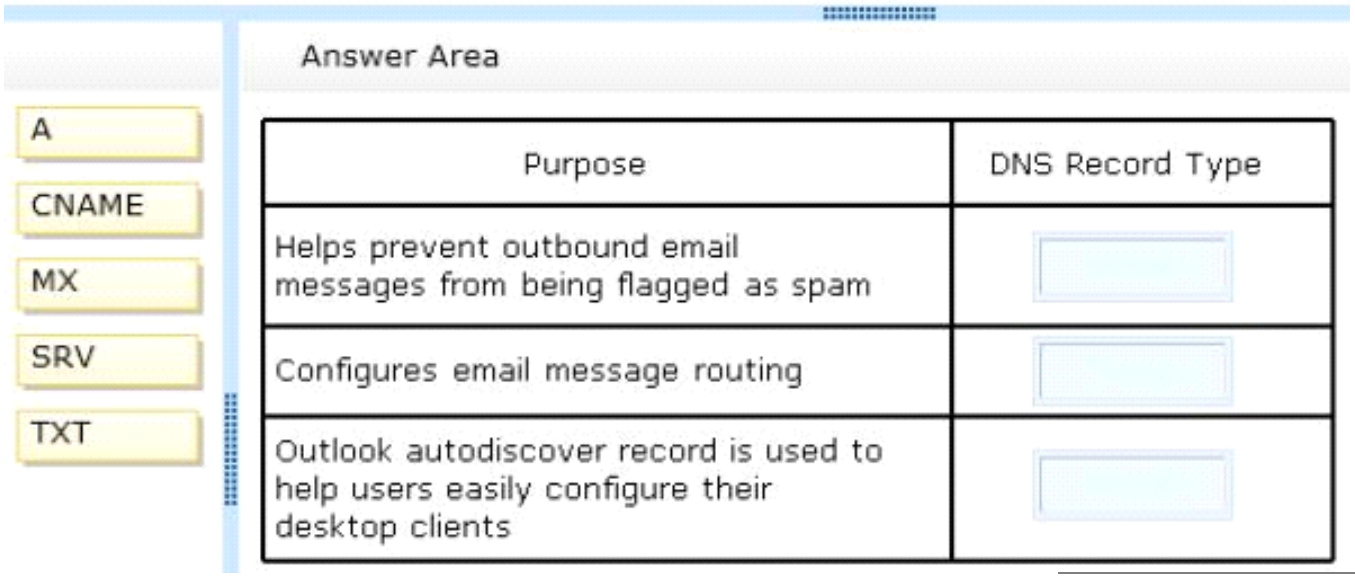
A. Run the Windows PowerShell cmdlet: Get-MsolCompanyInformation.
B. Run the OnRamp for Office 365 tool.
C. Install the Windows Azure Active Directory Sync tool.
D. Run the Office 365 Deployment Readiness Tool.

Answer: B

Explanation:
OnRamp for Office 365 is available to assist you with discovery activities related to Office 365deployments. The tool can be used to check and provide important information about your on-premises environment.

Question: 198

DRAG DROP
You implement Office 365 for an organization.
You must create the correct DNS entries needed to configure Exchange Online.
Which DNS entries should you create? To answer, drag the appropriate DNS record type to the correct purpose. Each DNS record type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:

Purpose	DNS Record Type
Helps prevent outbound email messages from being flagged as spam	TXT
Configures email message routing	MX
Outlook autodiscover record is used to help users easily configure their desktop clients	CNAME

TXT record is used for verification. When you have added the record at your domain registrar's site, you'll go back to Office 365 and request Office 365 to look for the record. When Office 365 finds the correct TXT record, your domain is verified.
MX (mail exchanger) record points to where your email should be sent. It also has a priority field so that you can send mail to different servers in a priority order.
CNAME (alias or canonical) record redirects one domain to another in the DNS system. When a name server looks up a domain and finds that it has a CNAME record, the server replaces the first domain name with the CNAME, and then looks up the new name.

Question: 199

An organization plans to deploy Exchange Online.
You must support all Exchange Online features.
You need to create the required DNS entries.
Which two DNS entries should you create? Each correct answer presents part of the solution.

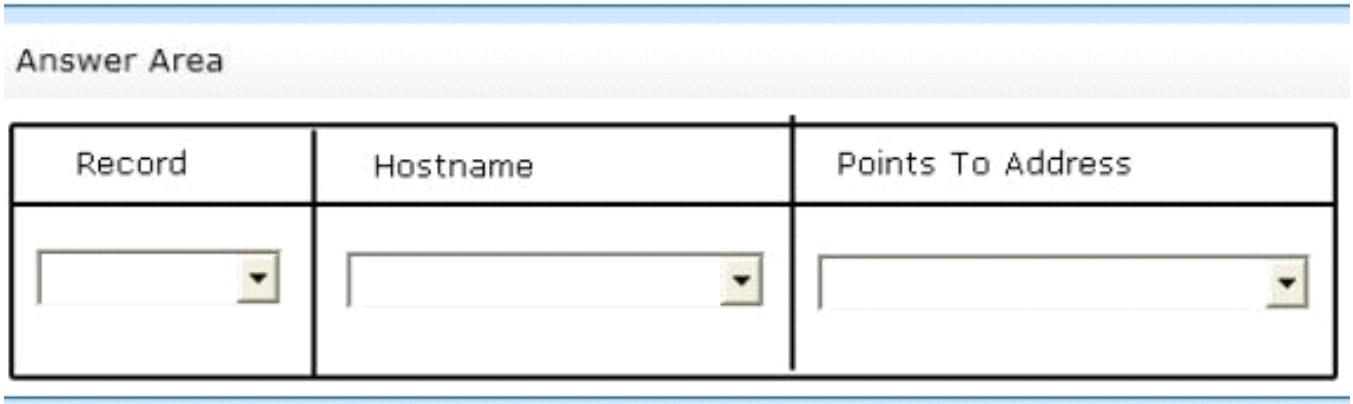
A. A
B. SRV
C. MX
D. CNAME

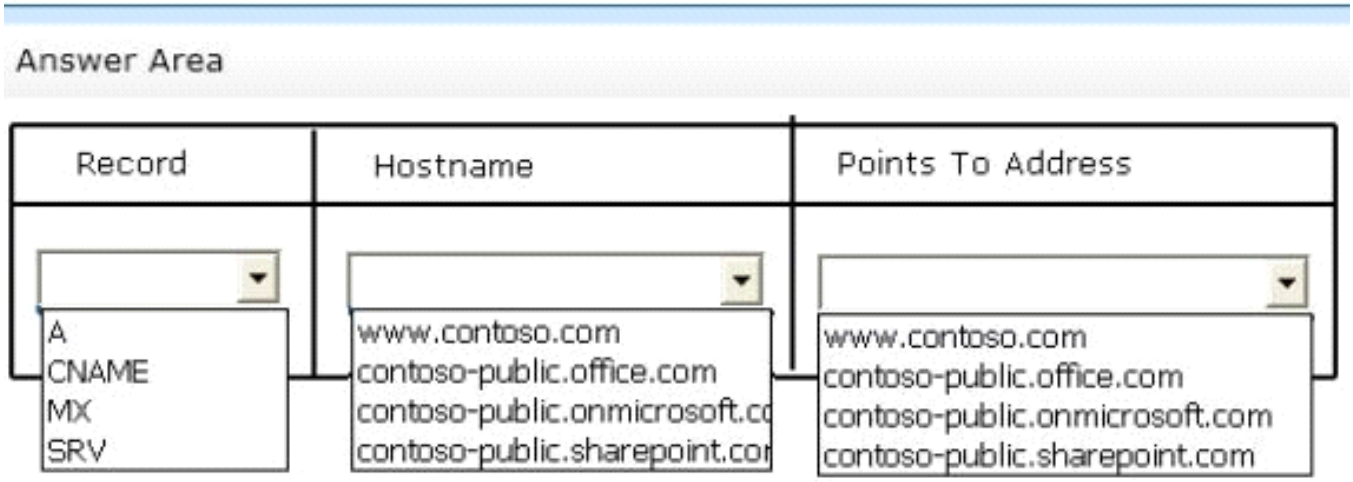
Answer: C,D

Explanation:
C: The MX record is used to send incoming mail for your domain to the Exchange Online service in Office 365.
D: The CNAME record is used to help Outlook clients to easily connect to the Exchange Online service by using the Autodiscover service. Autodiscover automatically finds the correct Exchange Server host and configures Outlook for users.

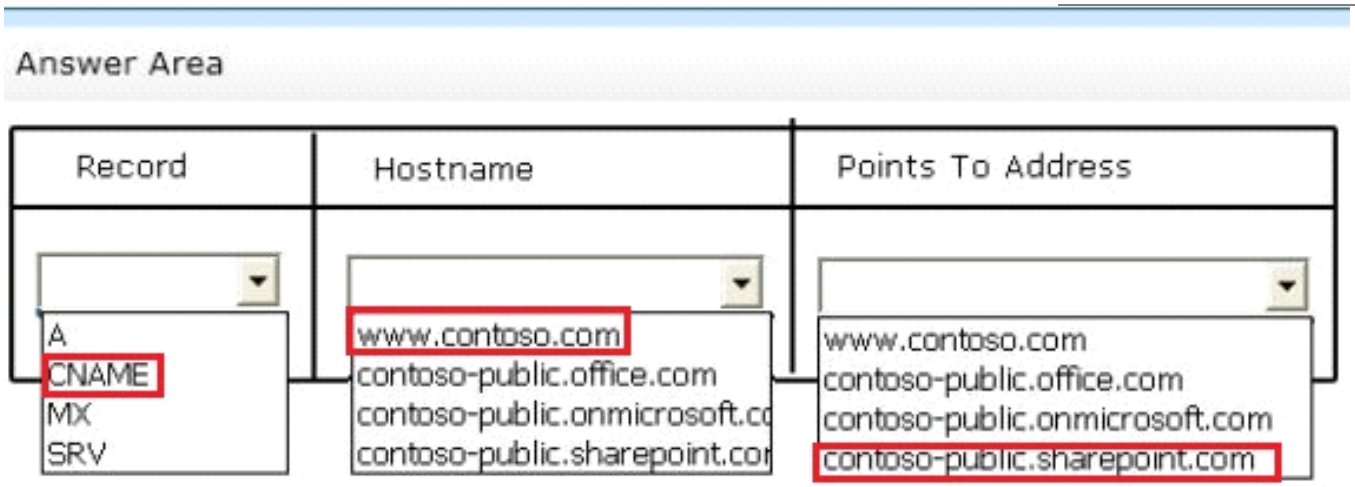
Question: 200

HOTSPOT
You are the SharePoint Online administrator for Contoso, Ltd. The company purchases an Office 365 Enterprise El plan.
The public-facing website must use SharePoint Online and the custom domain contoso.com.
You need to configure the DNS settings for the public-facing SharePoint site.
How should you configure the DNS settings? Select the appropriate options from each list in the answer area.





Answer:



The CNAME record is used to redirect one domain to another in the DNS system. When a name server looks up a domain and finds that it has a CNAME record, the server replaces thefirst domain name with the CNAME, and then looks up the new name.

Question: 201

You deploy Skype for Business Online for a company that has offices in San Francisco and New York. The two offices both connect to the Internet. There is no private network link between the offices.

Users in the New York office report that they cannot transfer files to the users in the San Francisco office by using Skype for Business Online.

You need to ensure that users in both offices can transfer files by using Skype for Business Online.

What should you do?

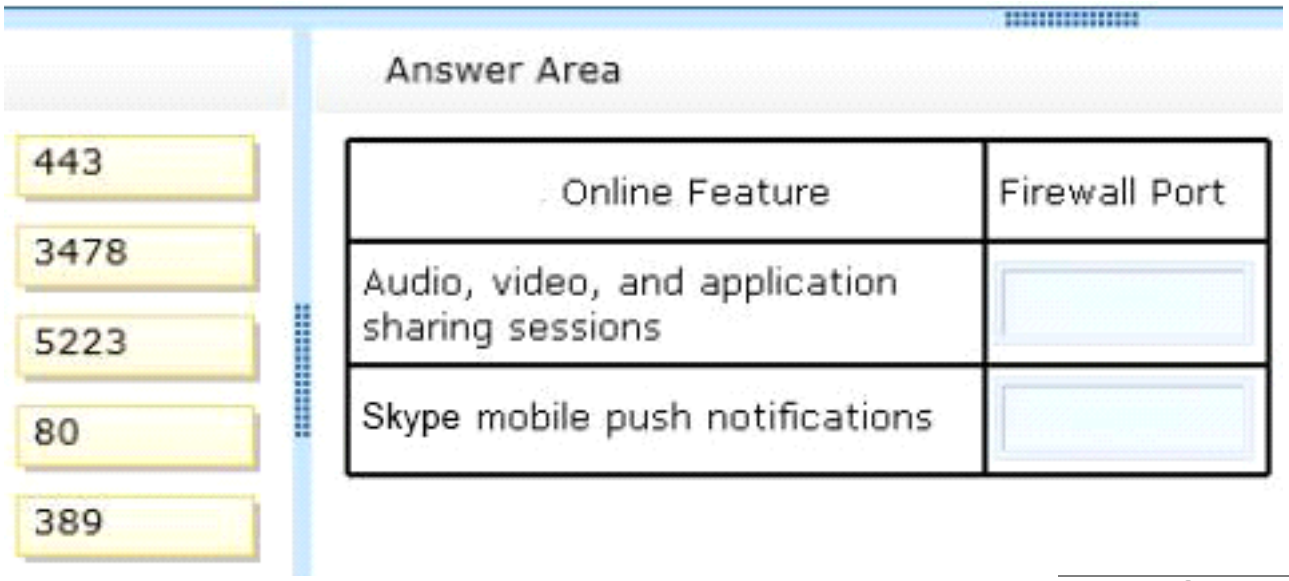
A. Configure the firewall to open Transmission Control Protocol (TCP) ports 50060-50079.
B. Configure the firewall to open Transmission Control Protocol (TCP) ports 50040-50059.
C. Create a private network connection to share files.
D. Upgrade all of the Skype for Business Online clients to use Skype for Business client application.

Answer: B

Explanation:
Skype for Business Online will allow for file sharing if the firewall is configured accordingly since it is mentioned that Skype for Business Online is already deployed. And there is connectivity by both offices to the Internet. If the TCP port number 50040-50059 is configured open on the firewall you will be able to share Audio, Video and application as well as Desktop sharing content and files.
References:
http://onlinehelp.microsoft.com/en-ca/office365-enterprises/hh416761.aspx

Question: 202

DRAG DROP
A company deploys an Office 365 tenant. All employees use Skype for Business Online.
You need to configure the network firewall to support Skype for Business Online.
Which ports must you open? To answer, drag the appropriate port number to the correct feature or features. Each port number may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:

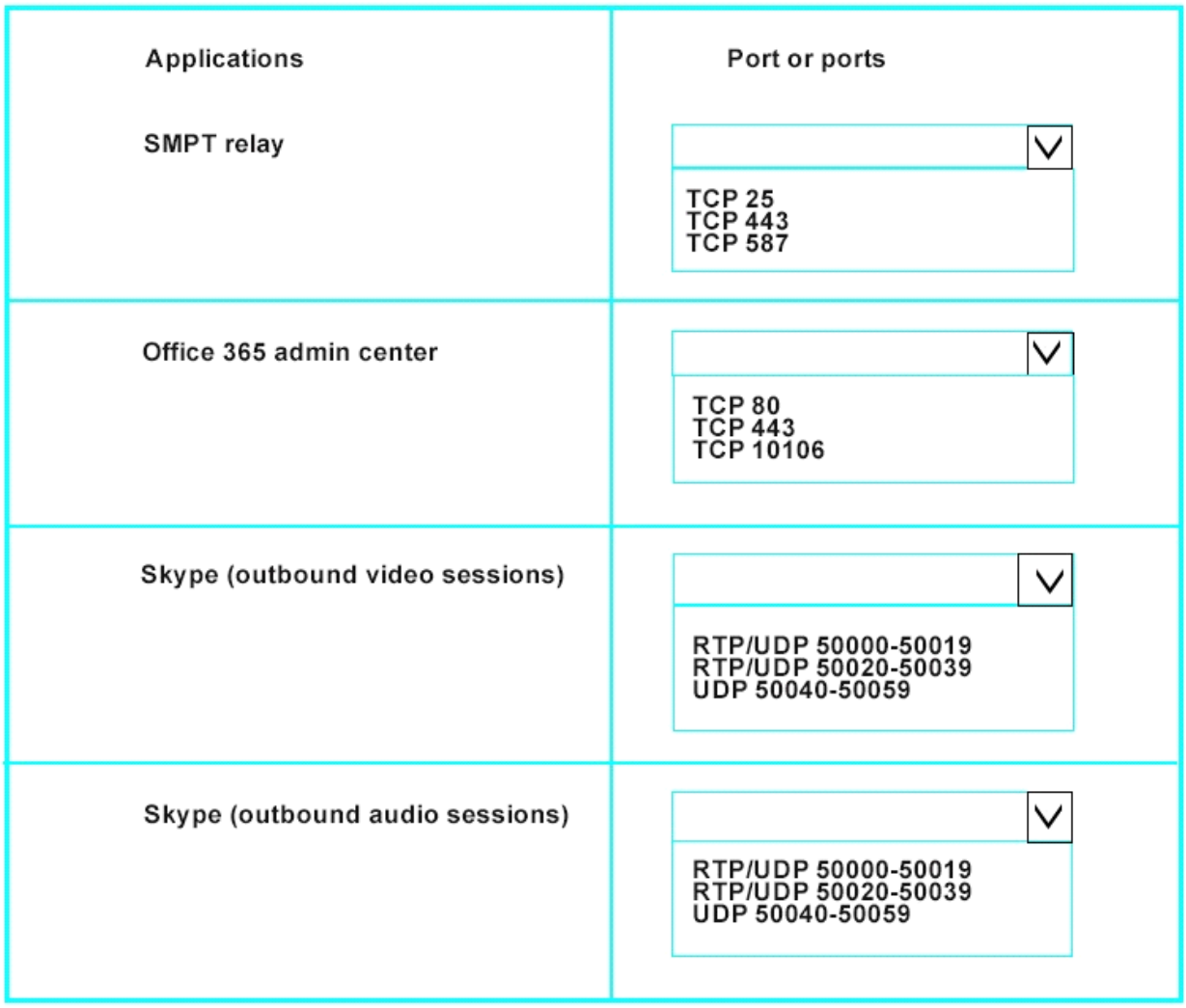
Online Feature	Firewall Port
Audio, video, and application sharing sessions	443
Skype mobile push notifications	5223

Transport Control Protocol(TCP), User Datagram Protocol(UDP) ports, and Protocol Numbers are important to TCP/IP networking, intranets, and the Internet. Ports and protocol numbers provide access to a host computer. However, they also create a security hazard by allowing uninvited access. Therefore, knowing which port to allow or disable increases a network's security. If the wrong ports or protocol numbers are disabled on a firewall, router, or proxy server as a security measure, essential services might become unavailable.
Port 443 is used for Audio, video and application sharing sessions as well as data sharing sessions - For HTTPS.
Port 5223 is used for mobile push notifications - Extensible Messaging and Presence Protocol (XMPP) client connection over SSL.

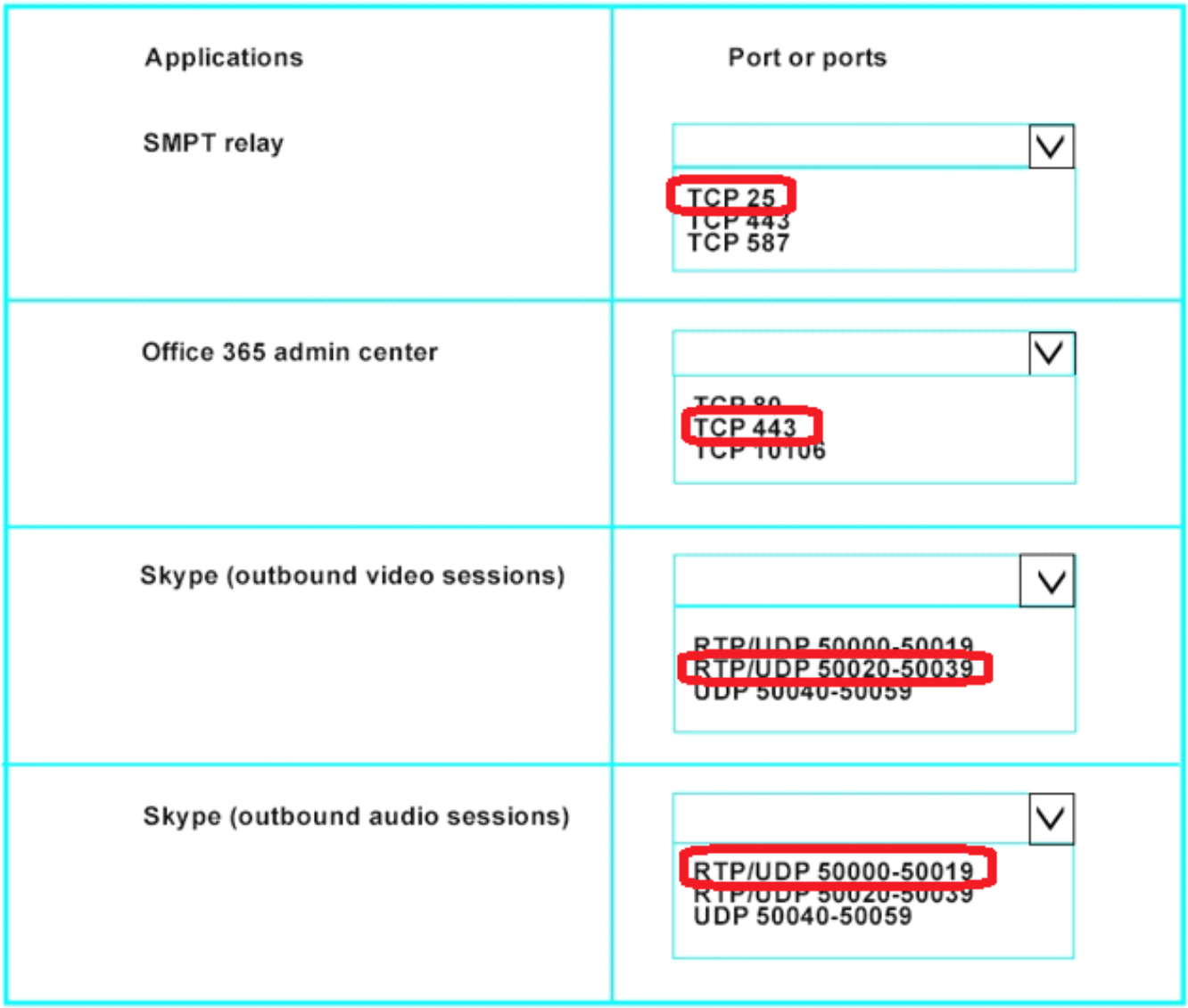
Question: 203

HOTSPOT
A company plans to deploy an Office 365 tenant.
You have the following requirements:
Administrators must be able to access the Office 365 admin center.
Microsoft Exchange Online must be used as a Simple Mail Transfer Protocol (SMTP) relay for a line-of-business application that sends email messages to remote domains.
All users must be able to use the audio and video capabilities in Microsoft Skype for Business.
You need to configure the ports for the firewall.
Which port should you use for each application? Select the correct answer from each list in the answer area.

Answer Area



Answer:



Transport Control Protocol(TCP), User Datagram Protocol (UDP) ports, and Protocol Numbers are important to TCP/IP networking, intranets, and the Internet. Ports and protocol numbers provide access to a host computer. However, they also create a security hazard by allowing uninvited access. Therefore, knowing which port to allow or disable increases a network's security. If the wrong ports or protocol numbers are disabled on a firewall, router, or proxy server as a security measure, essential services might become unavailable.
TCP port 25 is used for simple mail transfer protocol which is used to e-mail routing between mail servers.
TCP port 443 is used for Audio, video and application sharing sessions as well as data sharing sessions.
RTP/UDP port 50020-50039 must be used for outbound video sessions.
RTP/UDP port 50000-50019must be used for outbound audio sessions.

Question: 204

Your company has a subscription to Office 365 for midsize business and enterprises. The company uses Microsoft Skype for Business Online.
You need to open ports on the network firewall to enable all of the features of Skype for Business Online.
Which port or ports should you open? (Each correct answer presents part of the solution. Choose all that apply.)

A. inbound TCP443
B. outbound TCP 5061
C. outbound UDP 3478

D. outbound TCP 443
E. outbound UDP 50000 to outbound UDP 59999
F. inbound TCP 8080

Answer: A,C,D,E

Explanation:
A: inbound TCP 443 is the port for the Skype for Business for Business client service.
C: outbound UDP 3478 is the UDP port for Skype for Business audio and video sessions.
D: outbound TCP 443 is the port for the Skype for Business data sharing sessions as well as the Video and Audio and application sharing sessions.
E: outbound UDP 50000 to outbound UDP 59999 is the port for Skype for Business audio and video sessions.
References:
https://adam-hand.com/cloud-technologies/firewall-ports-for-office-365/

Question: 205

An organization plans to migrate to Office 365.
You need to estimate the post-migration network traffic.
Which tool should you use?

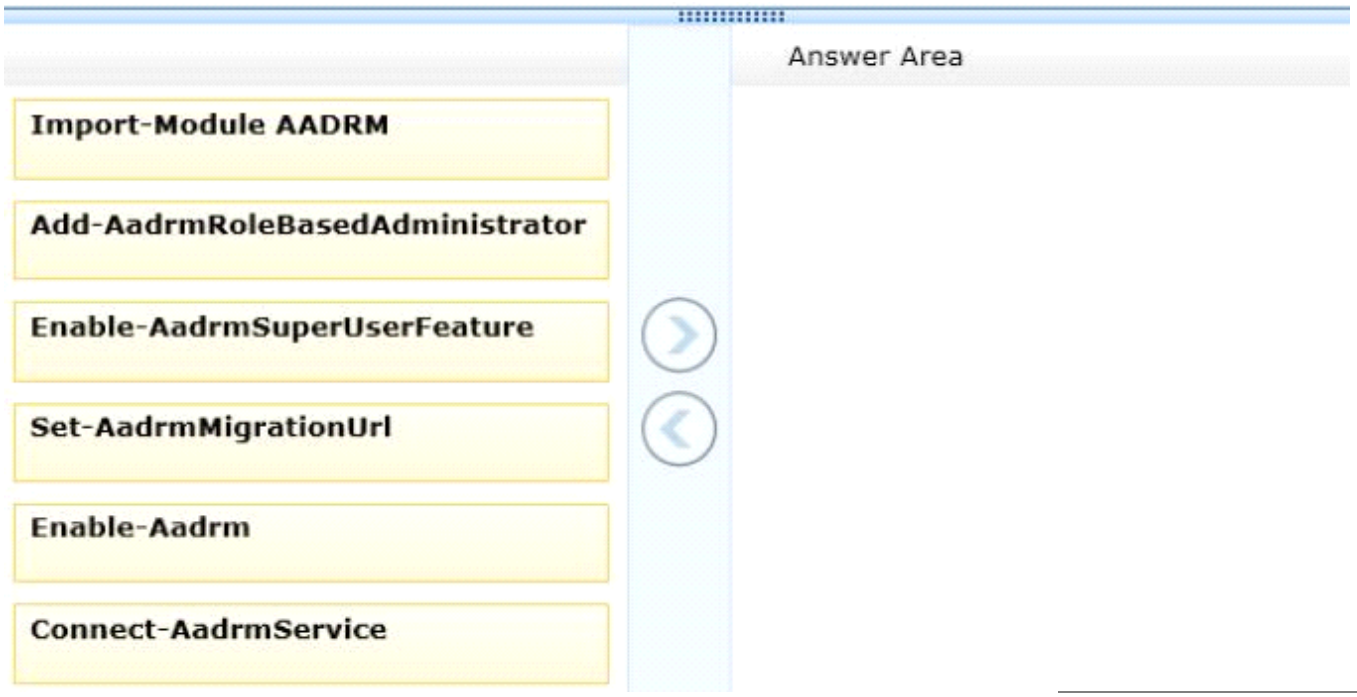
A. Microsoft Online Services Diagnostics and Logging (MOSDAL) Support Kit
B. Microsoft Network Monitor
C. Skype for Business Bandwidth Calculator
D. Microsoft Remote Connectivity Analyzer

Answer: C

Explanation:
There are calculators available to assist you with estimating network bandwidth requirements. These calculators work for on-premises as well as Office 365 deployments. You can use the Exchange client network bandwidth calculator to estimate the bandwidth required for a specific set of Outlook, Outlook Web App, and mobile device users in your Office 365 deployment. With the Skype for Business bandwidth calculator, you enter information about users and the Skype for Business features you want to deploy, and the calculator helps you determine bandwidth requirements.
Skype for Business Bandwidth Calculator - A Microsoft Excel spreadsheet that calculates WAN bandwidth requirements for a Skype for Business Server deployment based on administrator-specified user profiles and network information.

Question: 206

DRAG DROP
You are the Office 365 administrator for your company.
You need to ensure that trusted applications can decrypt rights-protected content.
Which four Windows PowerShell cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.



Answer:

Box 1:

Import-Module AADRM

Box 2:

Connect-AadrmService

Box 3:

Enable-Aadrm

Box 4:

Enable-AadrmSuperUserFeature

Microsoft Azure Rights Management (previously known as Windows Azure Active Directory Rights Management). To be able to decrypt rights protected documents you need to make sure that Microsoft Azure Rights Management is set up. Also you will need to enable a SuperUser account because The Active Directory Rights Management Services (AD RMS) super users group is a special group that has full control over all rights-protected content managed by the cluster. Its members are granted full owner rights in all use licenses that are issued by the AD RMS cluster on which the super users group is configured. This means that members of this group can decrypt any rights-protected content file and remove rights-protection from it.

The super users group is not enabled and is not assigned a group by default.

This can be done by running the appropriate commands in sequence which are:

References:

https://technet.microsoft.com/en-us/library/dn569291.aspx

https://technet.microsoft.com/en-us/library/dn151475%28v=exchg.150%29.aspx

Question: 207

Your company has an Office 365 subscription. You create a new retention policy that contains several retention tags. A user named Test5 has a client computer that runs Microsoft Office Outlook 2007. You install Microsoft Outlook 2010 on the client computer of Test5. Test5 reports that the new retention tags are unavailable from Outlook 2010.
You verify that other users can use the new retention tags. You need to ensure that the new retention tags are available to Test5 from Outlook 2010.
What should you do?

A. Instruct Test5 to repair the Outlook profile.
B. Modify the retention policy tags.
C. Run the Set-Mailbox cmdlet.
D. Force directory synchronization.

Answer: A

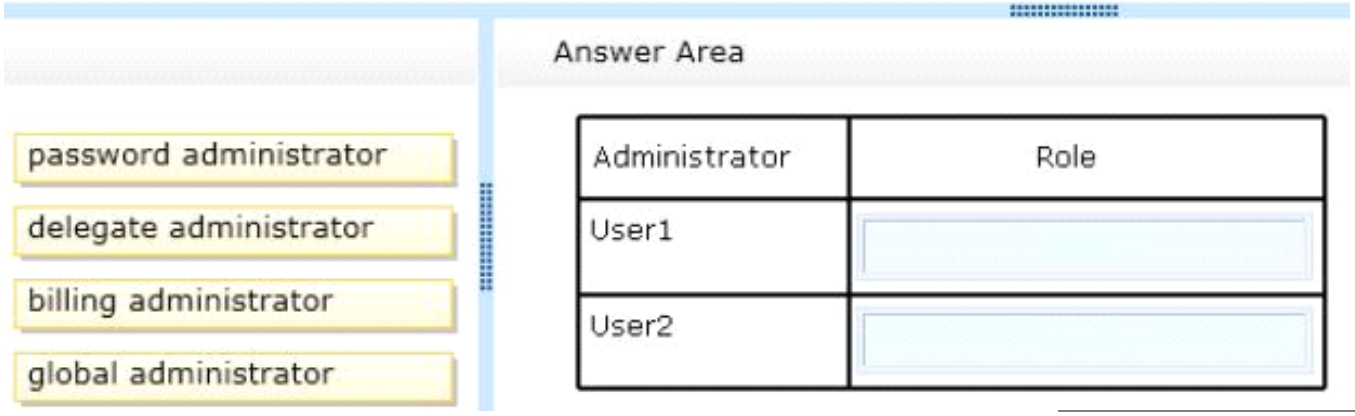
Explanation:
When deploying retention policies it is part of the procedure to create the tags and add it to the retention policies prior to the deployment. Also part of the procedure is to determine which Microsoft Outlook client versions are in use. In this case the Test5version has been changed and Test5 will then have to repair his/her Outlook profile accordingly.

Question: 208

DRAG DROP
You are the Office 365 administrator for your company. The company has two administrators named User1 and User2. Users must be able to perform the activities as shown in the following table:

Administrator	Activities
User1	o Reset passwords for standard user accounts. o Reset passwords for other members of the same role. o Must **NOT** reset passwords for other administrator accounts.
User2	o Reset passwords for all administrator accounts.

You need to grant the appropriate administrative role to each user.
What should you do? To answer, drag the appropriate role to the correct user. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:

Administrator	Role
User1	password administrator
User2	global administrator

User1 has to be the Password administrator which will allow for User1 to reset passwords, manage service requests, and monitor service health. Password admins are limited to resetting passwords for users and other password admins.
User2 has to be the global administrator to have access to all administrative features. Global admins are the only admins who can assign other admin roles. This will enable User2 the ability to reset passwords for all administrator accounts.

Question: 209

You create an Office 365 tenant. You assign administrative roles to other users. You hire a new user named User2.
User2 must NOT be able to change passwords for other users.
You need to assign an administrative role to User2.
Which role should you assign?

A. Service administrator
B. Global administrator
C. Delegate administrator
D. Password administrator

Answer: A

Explanation:
Being the Service Administrator will allow User2 to mage service requests and monitor service health, while not allowing User2 to ability to change passwords for other users.

Question: 210

A company deploys an Office 365 tenant. You assign the roles to users as shown in the following table:

User	Role Assigned
User1	global administrator
User2	user management administrator
User3	no roles are assigned to User3

User3 must be able to monitor the health of the Exchange Online service. You must use the principle of least privilege to assign permissions to User3.
You need to assign permissions to User3.
Which three actions should you perform? Each correct answer presents part of the solution.

A. Assign User3 the service administrator role in Office 365.

B. Sign in to the Office 365portal as User1.
C. Sign in to the Office 365 portal as User2.
D. GrantUser3 administrative permissions in Exchange Online.
E. Assign User3 the global administrator role in Office 365.

Answer: A,B,D

Explanation:
A: User3 must be the Service administrator role because that role allows for managing service requests and monitoring service health.
B: User1 has the global administrator role assigned. Only the global administrator can delegate service administrator role. This means that you should sign in with the User1 account for that will allow you to assign other admin roles.
D: If User3 is to monitor the health of the Exchange Online service he/she will require the appropriate administrative permissions.
References:
http://technet.microsoft.com/en-us/library/hh852528.aspx

Question: 211

A company deploys an Office 365 tenant.
You must provide an administrator with the ability to manage company information in Office 365.
You need to assign permissions to the administrator by following the principle of least privilege.
Which role should you assign?

A. Global administrator
B. Service administrator
C. Billing administrator
D. User management administrator

Answer: A

Explanation:
Global admin: Has access to all administrative features. Global admins are the only admins who can assign other admin roles. You can have more than one global admin in your organization. The person who signs up to purchase Office 365 becomes a global admin. Only the global administrator role will allow you to manage company information by means of editing the organization profile. None of the other roles are enabled to manage organization information.
References:
https://support.office.com/en-US/Article/Assigning-admin-roles-eac4d046-1afd-4f1a-85fc-8219c79e1504

Question: 212

HOTSPOT
You manage a team of three administrators for an organization that uses Office 365.
You must assign roles for each of the administrators as shown in the table. You must assign the minimum permissions required to perform the assigned tasks.

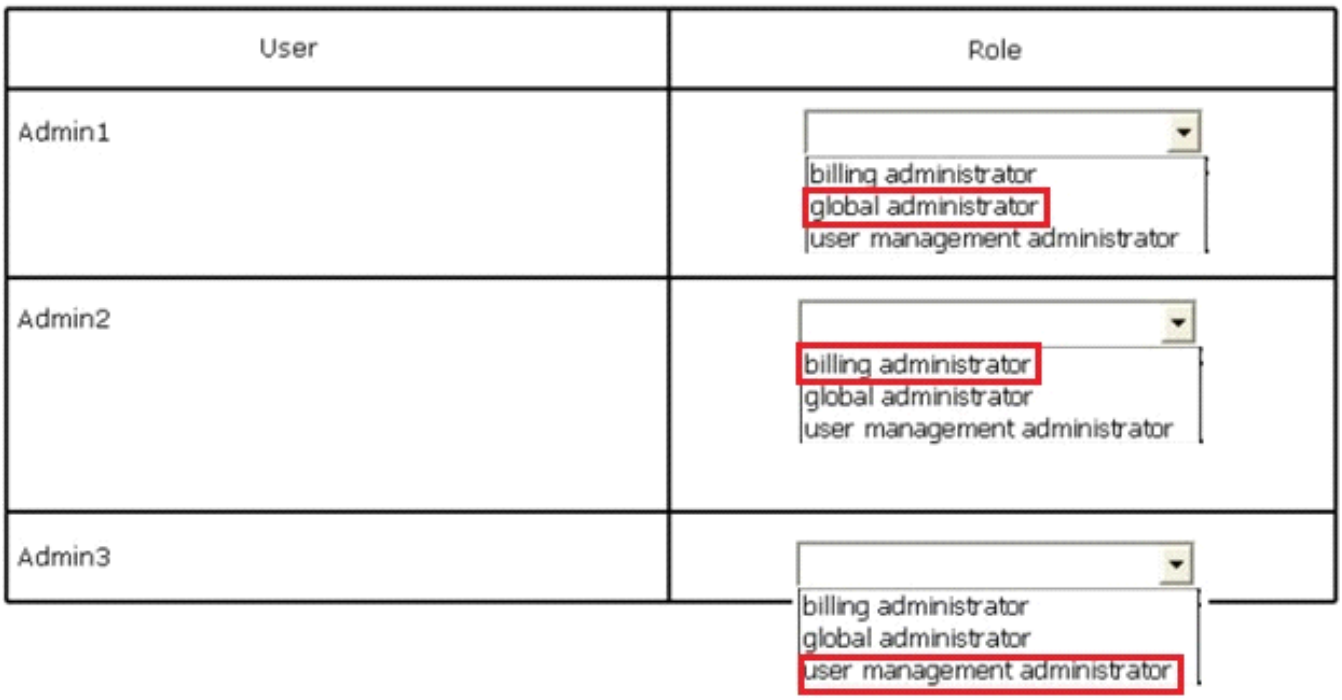
User	Requirements
Admin1	Reset user passwords for administrators
Admin2	Perform purchasing operations
Admin3	Create and manage user views

You need to assign the correct role to each administrator.
Which administrative role should you configure for each user? Select the correct answer from each list in the answer area.

User	Role
Admin1	
Admin2	
Admin3	

User	Role
Admin1	billing administrator global administrator user management administrator
Admin2	billing administrator global administrator user management administrator
Admin3	billing administrator global administrator user management administrator

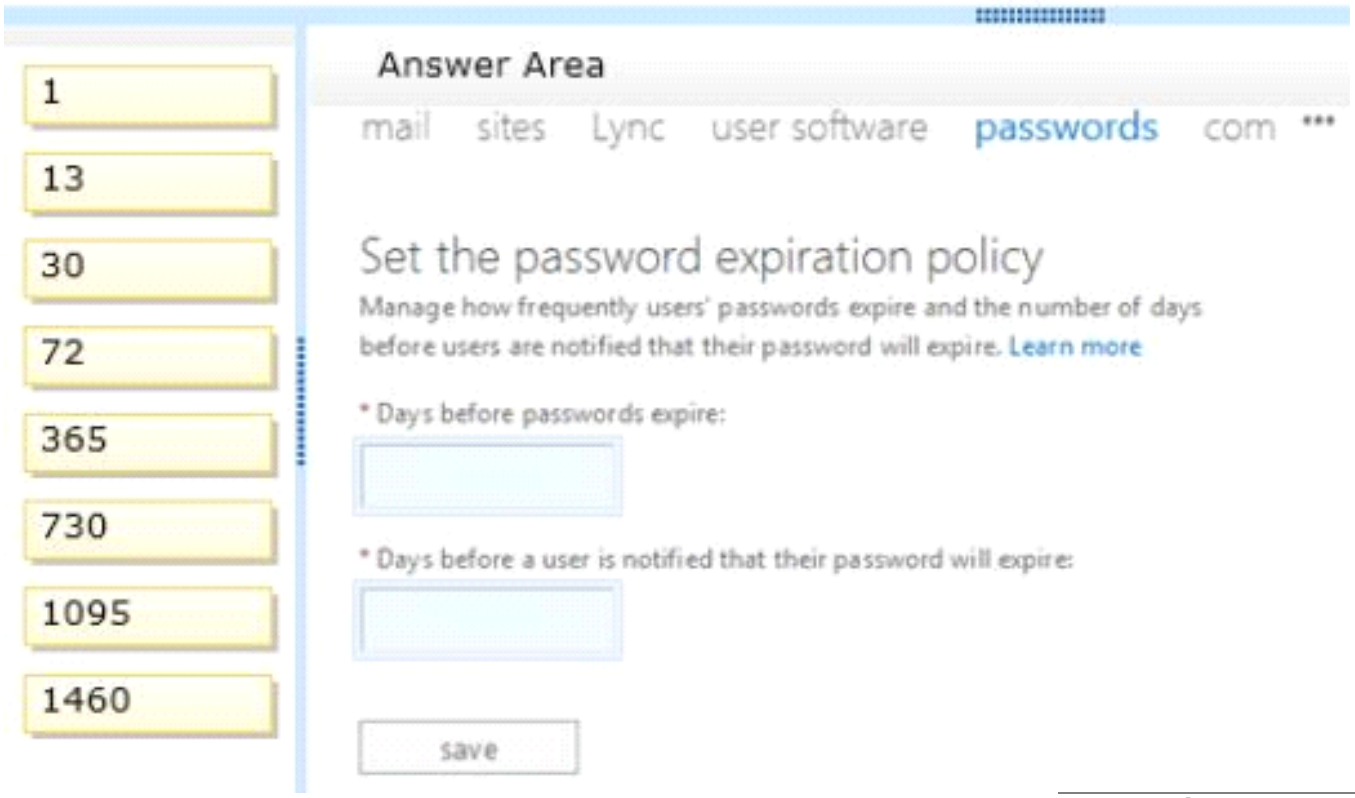
Answer:



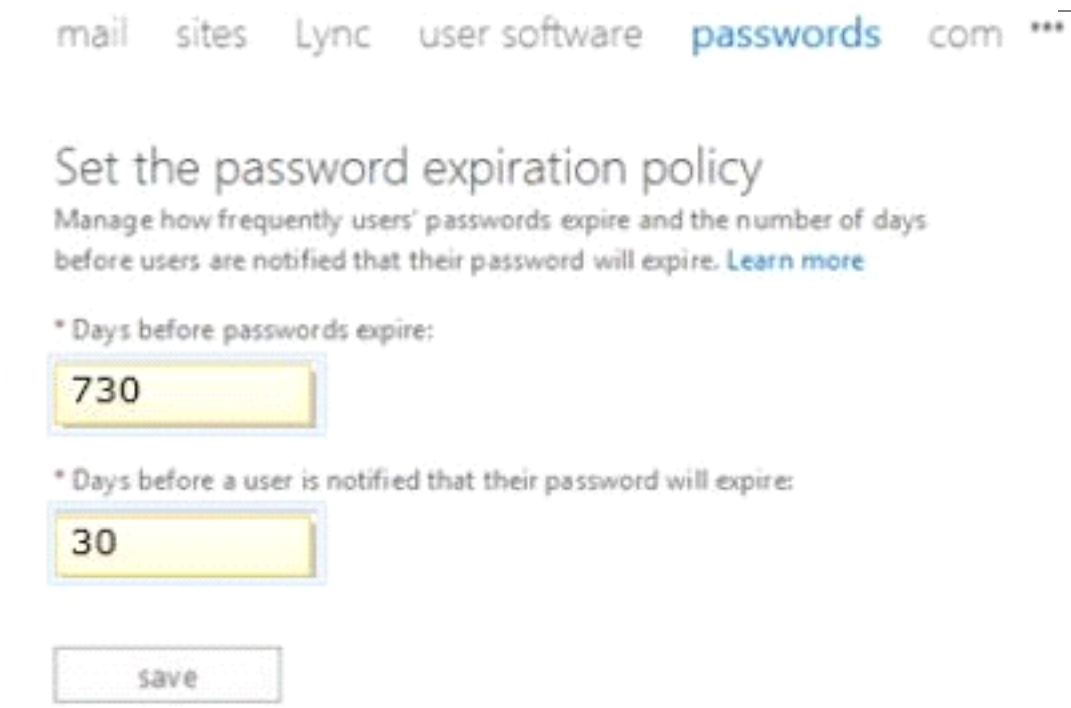
Admin1 must be the global admin that will grant him/her access to all administrative features. Global admins are the only admins who can assign other admin roles. You can have more than one global admin in your organization. The person who signs up to purchase Office 365 becomes a global admin.
Admin2 must be the billing admin to enable him/her to make purchases, manage subscriptions, and monitor service health.
Admin 3 must be the User Management admin to allow him/her to reset passwords, monitor service health, and manage user accounts, user groups, and service requests. The user management admin can't delete a global admin, create other admin roles, or reset passwords for billing, global, and service admins.
References:
https://support.office.com/en-IN/article/assigning-admin-roles-d58b8089-cbfd-41ec-b64c-9cfcbef495ac
http://onlinehelp.microsoft.com/en-in/office365-enterprises/gg243432.aspx#bkmk_EditProfile

Question: 213

DRAG DROP
You are the Office 365 administrator for your company.
Users report that their passwords expire too frequently, and they do not receive adequate notice of password expiration.
Account passwords must remain active for the longest duration allowed. Users must receive password expiration notifications as early as possible.
You need to configure the password expiration policy.
How should you set the policy on the password page of the Office 365 admin center? To answer, drag the appropriate duration to the correct location. Each duration may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:



The maximum number of days you can set the 'Days before password expire' to is 730. This will make the password valid for the longest duration.

To be notified as early as possible on that the password is about to expire, we should set the maximum value, which is 30, to the ' days before users are notified that their password will expire' setting.

Note: Set a user's password expiration policy

References:

https://support.office.com/en-us/article/Set-a-users-password-expiration-policy-0f54736f-eb22-414c-8273-498a0918678f

Question: 214

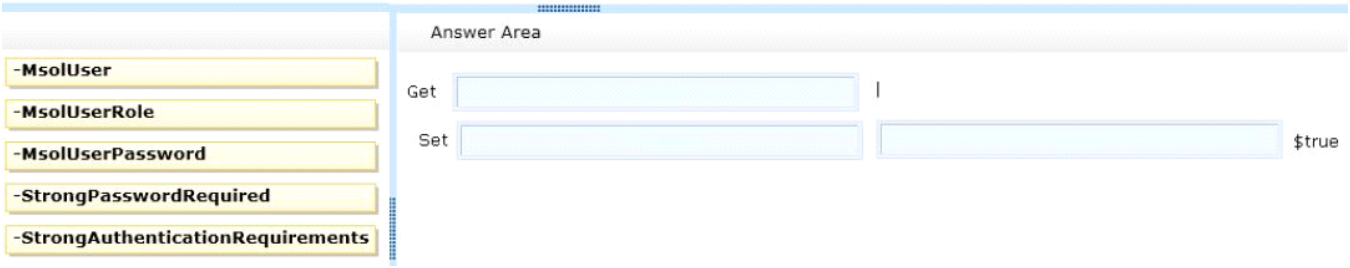
DRAG DROP

A company has 50 employees that use Office 365.

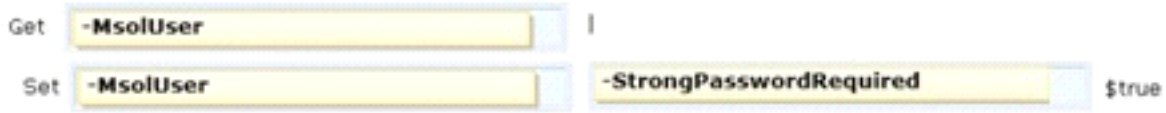
You need to enforce password complexity requirements for all accounts.

How should you complete the relevant Windows PowerShell command? To answer, drag the appropriate Windows PowerShell segment to the correct location in the answer are

a. Each Windows PowerShell segment may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:



We use Get –MsolUser to get all users. We then enforce strong password complexity to each of these users through StrongPassWordRequired parameter of the Set –MsolUser command. The output of get command is used in the set command through the concatenating function (the symbol |).

Box 1: -MsolUser

The Get-MsolUser cmdlet can be used to retrieve an individual user, or list of users. An individual user will be retrieved if the ObjectId or UserPrincipalName parameter is used.

Box 2: MsolUser

The Set-MsolUser cmdlet is used to update a user object. This cmdlet should be used for basic properties only.

Parameter: -StrongPasswordRequired <Boolean>

Sets whether or not the user requires a strong password.

Question: 215

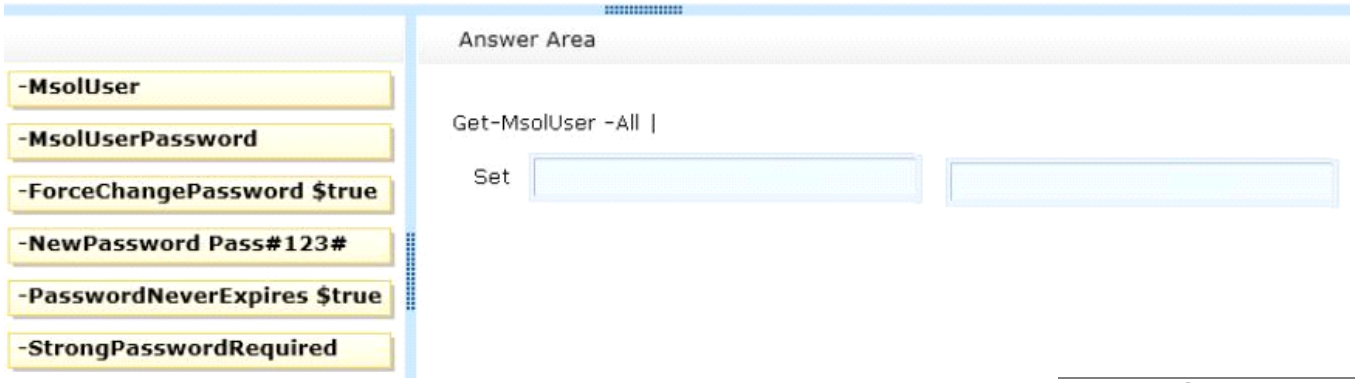
DRAG DROP

You are the Office 365 administrator for your company. Your company uses Office 365 for collaboration.

You must reset the password for all of the employees in your company.

You need to ensure that all employees create a new password the next time they sign in to Office 365.

How should you complete the relevant Windows PowerShell command? To answer, drag the appropriate Windows PowerShell segment to the correct location or locations. Each Windows PowerShell segment may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

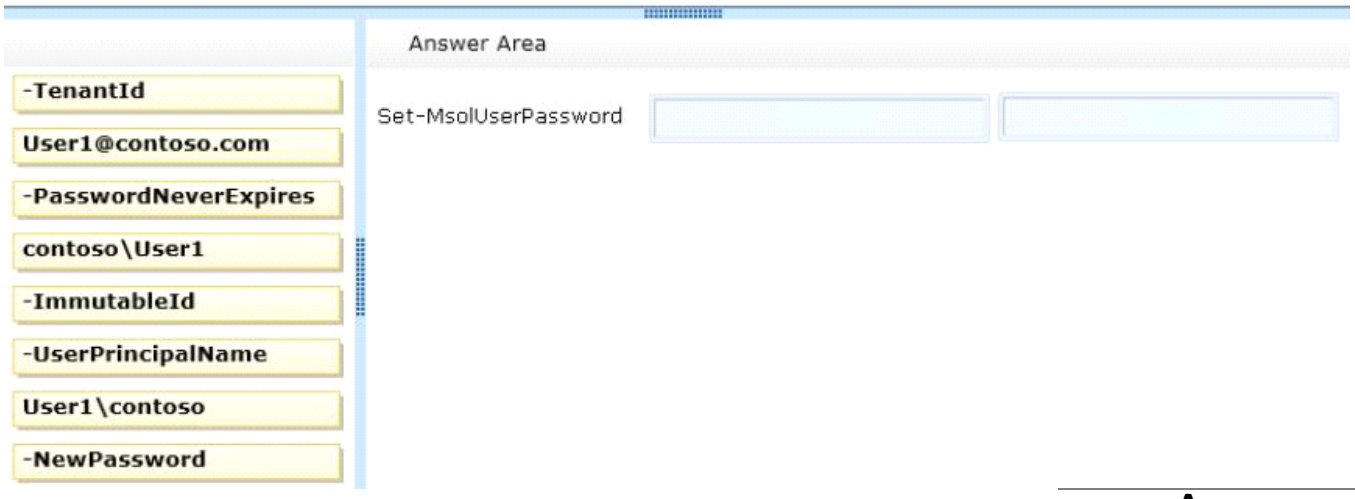


Answer:

Box 1: -MsolUserPassword
The Set-MsolUserPassword cmdlet is used to change the password of a user.
Box 2: -NewPassword Pass#123#
The Set-MsolUserPassword -NewPassword <string> sets the new password for the user.

Question: 216

DRAG DROP
You are the Office 365 administrator for Contoso, Ltd.
User1 is unable to sign in.
You need to change the password for User1 and ensure that the user is prompted to reset her password the next time she signs in.
How should you complete the relevant Windows PowerShell command? To answer, drag the appropriate Windows PowerShell segments to the correct location or locations. Each Windows PowerShell segment may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:

The Set-MsolUserPassword cmdlet is used to change the password of a user.
The parameter -UserPrincipalName is used to specify the user to set the password for.
The following command resets the password foruser@contoso.com. A random password will be generated. The user will be required to reset the password on next sign in.

Set-MsolUserPassword -UserPrincipalNameuser@contoso.com

Question: 217

Your company has a hybrid deployment of Office 365. You need to create a group. The group must have the following characteristics:
Group properties are synchronized automatically.
Group members have the ability to control which users can send email messages to the group.
What should you do?

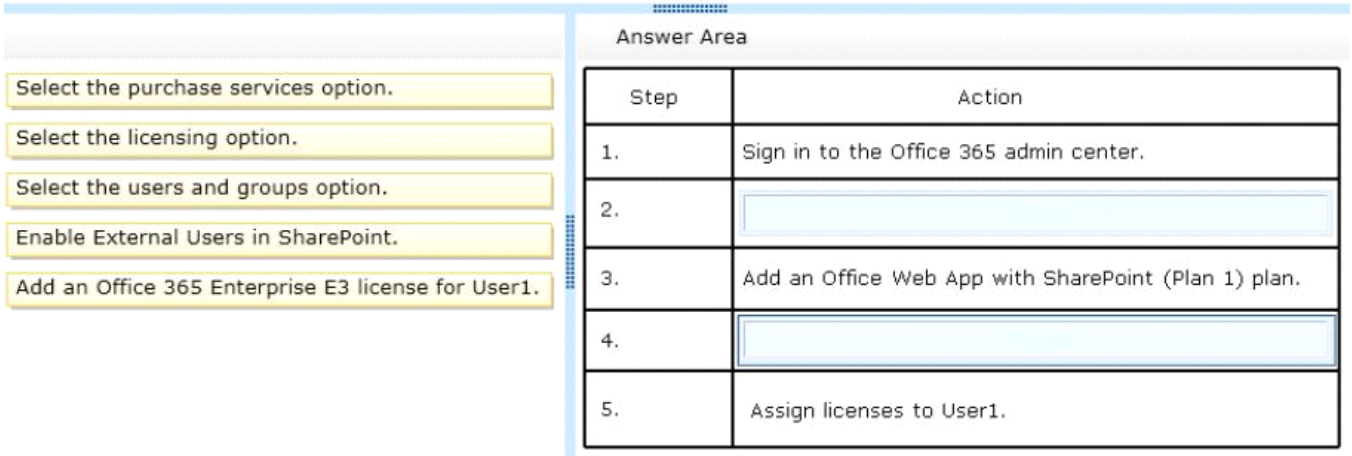
A. Create a distribution group and configure the Mail Flow Settings.
B. Create a dynamic distribution group.
C. Create a new role group.
D. Create a distribution group and configure the Membership Approval settings.

Answer: C

Explanation:
The member of the role group can all do administrative tasks. When you create a role group you can select between the following three roles:
Application Impersonation
Distribution Groups
Mail Recipients.
References:
https://blogs.perficient.com/microsoft/2015/04/office-365-allowing-users-to-edit-exchange-groups-they-manage/

Question: 218

DRAG DROP
You are the Office 365 administrator for your company. The company has Office 365 Enterprise E3 licenses for each of its 250 employees. The company does not allow email or Skype for Business Online licenses to be assigned to external contractors.
User1 is an external contractor who requires access to SharePoint and Office Web Apps only.
You need to add a license for User1's account.
What should you do? To answer, drag the appropriate action to the correct location or locations. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:

Step	Action
1.	Sign in to the Office 365 admin center.
2.	Select the purchase services option.
3.	Add an Office Web App with SharePoint (Plan 1) plan.
4.	Select the users and groups option.
5.	Assign licenses to User1.

Question: 219

A company uses Office 365 services. You implement the Windows Azure Active Directory Sync tool in the local environment.
An employee moves to a new department. All Office 365 services must display the new department information for the employee.
You need to update the employee's user account.
Where should you change the value of the department attribute for the employee?

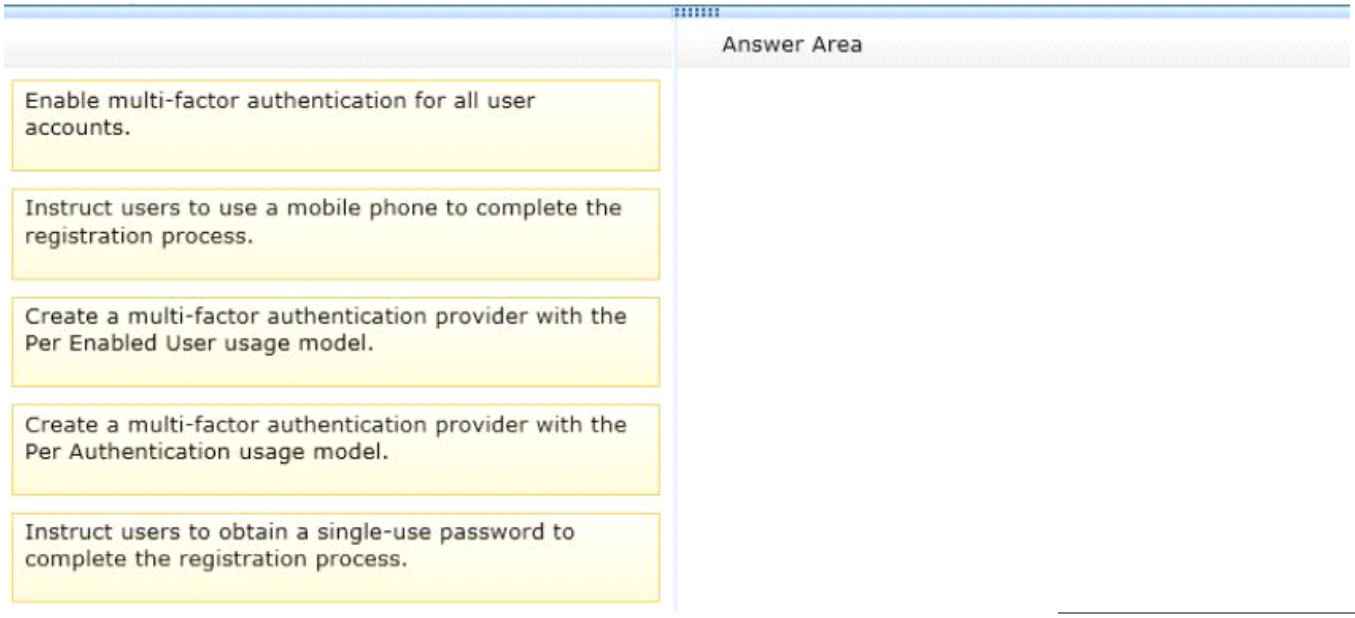
A. The Active Directory management page in the Windows Azure Management Portal
B. The Users and groups page in the Office 365 admin center
C. The on-premises Active Directory
D. The Metaverse Designer

Answer: C

Explanation:
The Active Directory Synchronization allows you to sync your Active Directory Objects such as users and groups to your Office 365 account. This is a one-way synchronization, which means you continue to manage users On-Premises, and your changes will appear on Office 365 SharePoint. So if you want to change the user information of employee you must use the On-Premises Active Directory.

Question: 220

DRAG DROP
A company deploys an Office 365 tenant.
You need to enable multi-factor authentication for Office 365.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Box 1: Create a multi-factor authentication provider with the Per Enabled User usage model.
Box 2: Enable multi-factor authentication for all user accounts.
Box 3: Instruct users to use a mobile phone to complete the registration process.
Adding Multi-Factor Authentication to Azure Active Directory (for Office 365 users)
Step 1: First we create the usage model of the MFA provider.
We should use PerEnabled User which is used for Office 365.
Note:
Per Authentication – purchasing model that charges per authentication. Typically used for scenarios that use the Azure Multi-Factor Authentication in an application.
Per Enabled User – purchasing model that charges per enabled user. Typically used for scenarios such as Office 365.
Step 2: Enable Multi-Factor Authentication for all your user accounts.
You need to enable multi-factor authentication on your Office 365 users.
Step 3: Have a user sign-in and complete the registration process.
The users can use their mobile phones to complete the auto-enrollment process.
Details: After being enrolled for multi-factor authentication, the next time a user signs in, they see a message asking them to set up their second authentication factor. Using the enrollment process the users will be able to specify your preferred method of verification.
The following methods exist: Mobile Phone Call, Mobile Phone Text Message, Office Phone Call, or Mobile App.
References:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/multi-factor-authentication/multi-factor-authentication-get-started-auth-provider.md

Question: 221

You are the Office 365 administrator for your company. The company uses Active Directory Federation Services (AD FS) to provide single sign-on to cloud-based services. You enable multi-factor authentication.
Users must NOT be required to use multi-factor authentication when they sign in from the company's main office location. However, users must be required to verify their identity with a password and token when they access resources from remote locations.
You need to configure the environment.
What should you do?

A. Disable AD FS multi-factor authentication.
B. Configure an IP blacklist for the main office location.

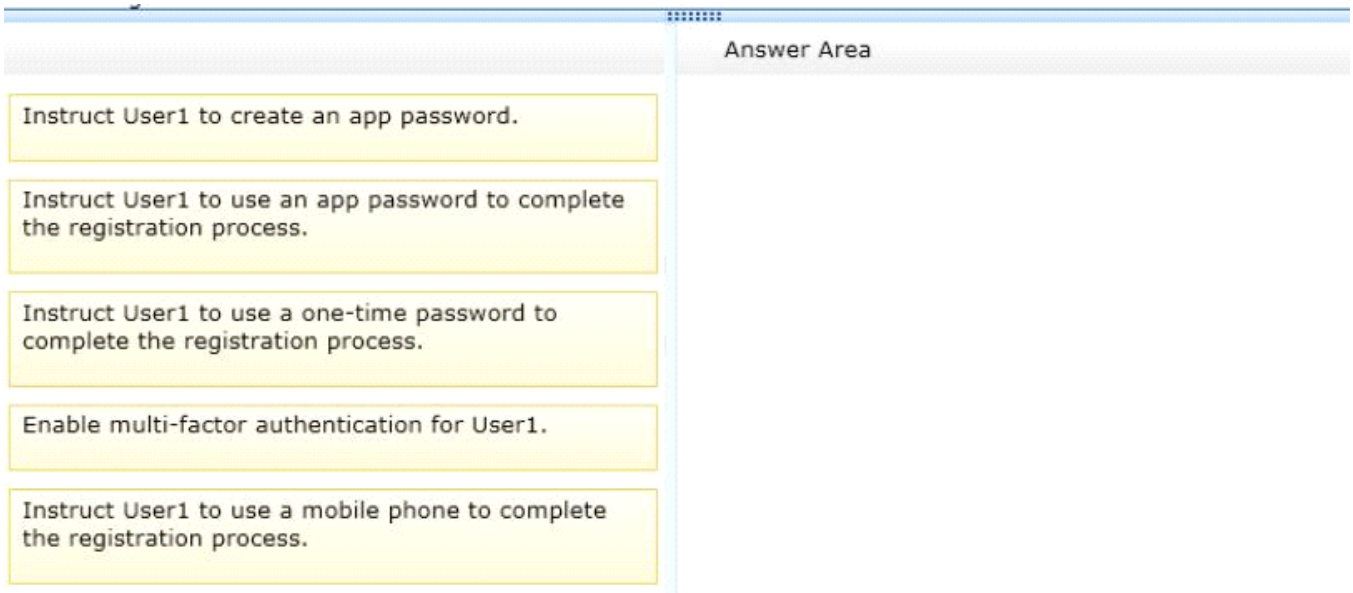
C. Disable the AD FS proxy.
D. Configure an IP whitelist for the main office location.

Answer: D

Explanation:
With ADFS you now get the option to whitelist an IP for multi-factor authentication (MFA).
For example, if you enable multi- factor authentication. Users must NOT be required to use multi-factor authentication when they sign in from the company's main office location. However, users must be required to verify their identity with a password and token when they access resources from remote locations.
References:
https://msdn.microsoft.com/en-us/library/azure/dn807156.aspx

Question: 222

DRAG DROP
A company deploys an Office 365 tenant.
All employees in the human resources (HR) department must use multi-factor authentication. They must use only the Microsoft Outlook client to access their email messages. User1 joins the HR department.
You need to help User1 configure his account.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Box 1: Enable multi-factor authentication for User1.
Box 2: Instruct User1 to use a mobile phone to complete the registration process.
Box 3: Instruct User1 to create an app password.
(Step 1) First we need to enable multi-factor authentication for this Office 365 users.
(Step 2) After being enrolled for multi-factor authentication, the next time a user signs in, they see a message asking them to set up their second authentication factor.
Any of the following may be used for the second factor of authentication: Mobile Phone Call, Mobile Phone Text Message, Office Phone Call, or Mobile App.
(Step 3) Configure app passwords for non-browser apps (such as …Outlook etc.).
User1 should create an app password. The app password should then be used to set up Microsoft Outlook.
After the registration process (step 2) has been completed, users can setup application passwords for non-browser

apps (such as …Outlook etc.). This is required because the non-browser apps (such as …Outlook etc.) do not support multi-factor authentication and you will be unable to use them unless an app password is configured.
References:
http://msdn.microsoft.com/en-us/library/azure/dn383636.aspx#enablemfaoffice365

Question: 223

Your company subscribes to an Office 365 Plan E3. A user named User1 installs Office Professional Plus for Office 365 on a client computer. From the Microsoft Online Services portal, you assign User1 an Office Professional Plus license. One month after installing Office, User1 can no longer save and edit Office documents on the client computer. User1 can open and view Office documents.
You need to ensure that User1 can save and edit documents on the client computer by using office.
What should you do?

A. Install the Office Customization Tool.
B. Reinstall Office Professional Plus.
C. Install the Microsoft Online Services Sign-in Assistant.
D. Upgrade the subscription to Plan E4.

Answer: C

Explanation:
Office 365 ProPlus is offered as a monthly subscription. The subscription for User1 has run out and the program has been deactivated. The user should choose Sign In to activate Office 365 ProPlus. This is done through the Microsoft Online Services Sign-in Assistant.
References:
http://technet.microsoft.com/en-us/library/gg702619(v=office.15).aspx

Question: 224

You are the Office 365 administrator for your company. A user named User1 from a partner organization is permitted to sign in and use the Office 365 services.
User1 reports that the password expires in ten days. You must set the password to never expire. Changes must NOT impact any other accounts.
You need to update the password policy for the user.
Which Windows PowerShell cmdlet should you run?

A. Set-MsolPasswordPolicy
B. Set-MsolPartnerInformation
C. Set-MsolUser
D. Set-MsolUserPassword

Answer: C

Explanation:
The Set-MsolUser cmdlet is used to update a user object.
The parameter -PasswordNeverExpires <Boolean>
Sets whether or not the user's password willexpireperiodically.
So the command Set-MsolUser –PasswordNeverExpires $true would make the appropriate configuration.

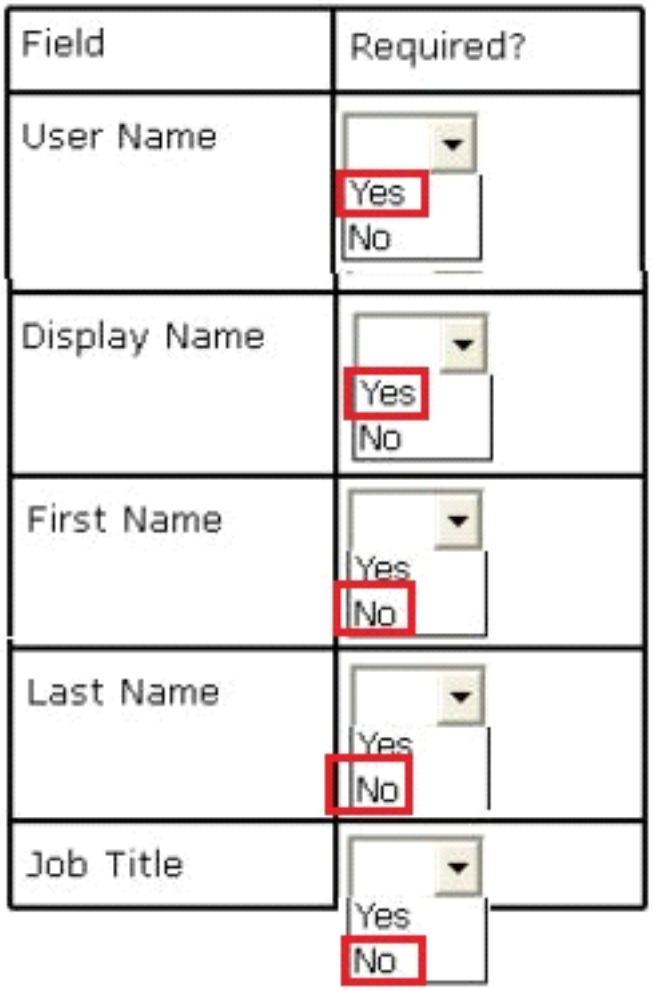
Question: 225

HOTSPOT
A company deploys an Office 365 tenant.
You prepare to use the bulk add tool to add users to Office 365.
You need to prepare a file to use with the bulk add tool.
Which fields must you include in the file? Select the correct answer from each list in the answer area.
NOTE: Each correct selection is worth one point.

Field	Required?
User Name	
Display Name	
First Name	
Last Name	
Job Title	

Field	Required?
User Name	Yes / No
Display Name	Yes / No
First Name	Yes / No
Last Name	Yes / No
Job Title	Yes / No

Answer:



How to add multiple users with bulk import in Office 365
Only the user name and display name are required entries.
The bulk import feature of Office 365 allows you to import multiple users' information into Office 365 from a single file source. The file must be a comma-separated values (CSV)file and adhere to the required format. It will then automatically do the resto f the thing for you. Only the user name and display name are required entries in the CSV file.

Question: 226

You use a centralized identity management system as a source of authority for user account information. You export a list of new user accounts to a file on a daily basis. Your company uses a local Active Directory for storing user accounts for on-premises solutions. You are configuring the Windows Azure Active Directory Sync tool.
New user accounts must be created in both the local Active Directory and Office 365. You must import user account data into Office 365 daily.
You need to import the new users. What should you do?

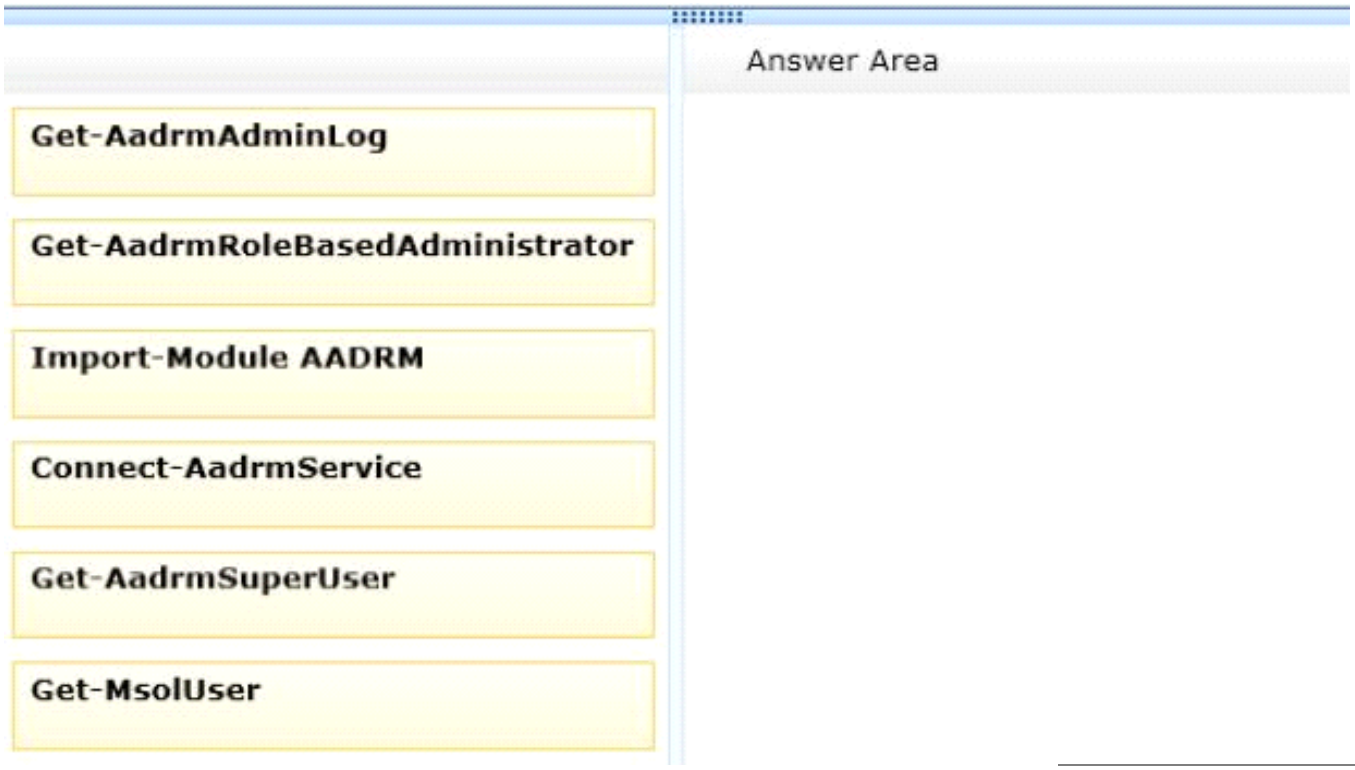
A. Use the Office 365 admin center to import the file.
B. Create a Windows PowerShell script to import account data from the file into Active Directory.
C. Use the Windows Azure Management Portal to import the file.
D. Create a Windows PowerShell script that uses the MSOnline module to import account data from the file.

Answer: B

Explanation:
To force a sync with the Windows Azure Active Directory Sync tool:
Open Powershell (as admin)
Type Import-Module DirSync
Then Type Start-OnlineCoExistenceSync
To simplify further you can write the commands as a PowerShell script.

Question: 227

DRAG DROP
You are the Office 365 administrator for your company. You audit the Windows Azure Active Directory Rights Management configuration for the company.
You need to view a log of the recent administrative commands performed against the Microsoft Rights Management Service.
Which three Windows PowerShell cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of actions to the answer area and arrange them in the correct order.



Answer:

Box 1: Import-AadrmTpd
Box 2: Connect-AadrmService
Box 3: Get-AadrmAdminLog
Although you can activate Azure Rights Management by using the Office 365 admin center or the Azure Management Portal, you can also use the Windows PowerShell module for Azure Rights Management to do this. First we active Azure Rights Management by import it through Import-AadrmTpd, then we connect to the service with Connect-AadrmService, and finally we generate the log with Get-AadrmAdminLog.
Step 1: The Import-AadrmTpd cmdlet imports an Active Directory Rights Management Services (AD RMS) trusted publishing domain (TPD) over the Internet into your tenant for Azure Rights Management so that you can migrate Rights Management from on-premises to the cloud.
Step 2: The Connect-AadrmService cmdlet connects you to the Azure Rights Management service. This cmdlet can also be used by a partner company that manages your tenant.

Connect by using this cmdlet before you configure Rights Management by using other cmdlets in this module.
Step 3: The Get-AadrmAdminLog cmdlet generates logs for all Rights Management administrative commands.
References:
http://technet.microsoft.com/en-us/library/jj585027.aspx

Question: 228

You plan to deploy an Office 365 tenant to multiple offices around the country.
You need to modify the users and groups who are authorized to administer the Rights Management service.
Which Windows PowerShell cmdlet should you run?

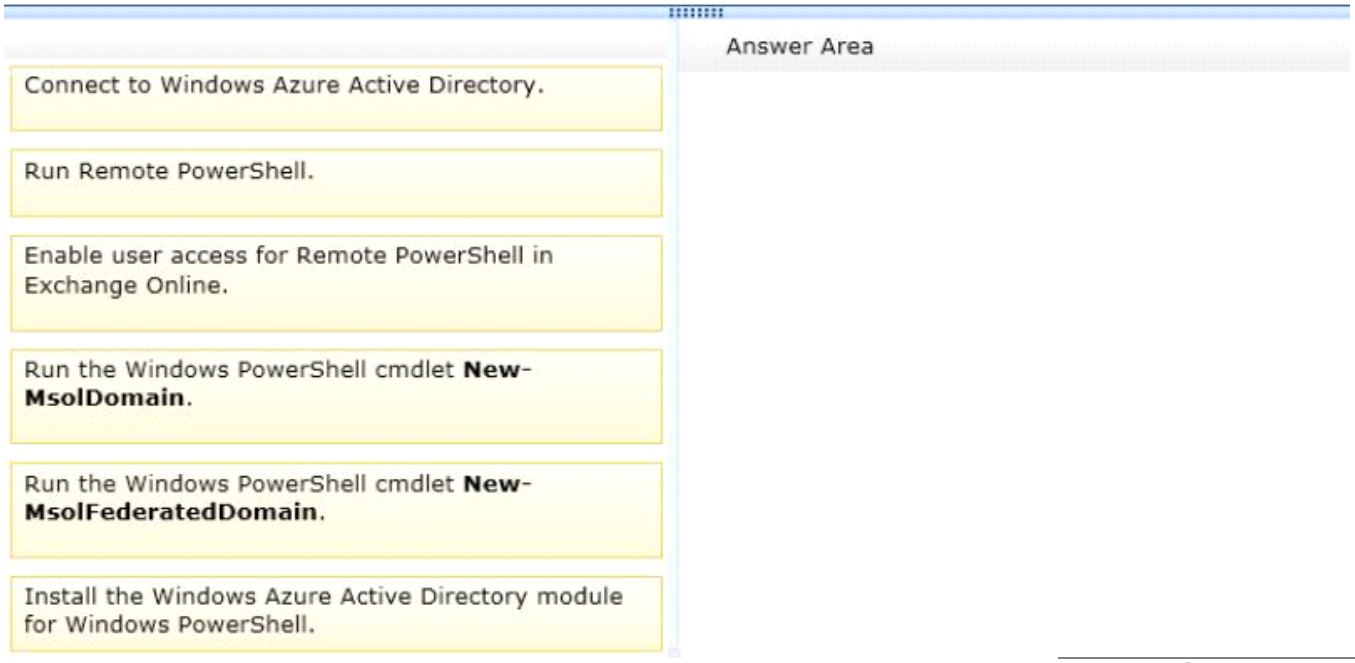
A. Add-MsolGroupMember
B. Get-Add rm Role Based Administrator
C. Remove-AadrmRoleBasedAdministrator
D. Enable AadrmSuperUserFeature

Answer: D

Explanation:
The Enable-AadrmSuperUserFeature cmdlet enables the super user feature. With this feature enabled, you can add or remove super users for Azure Rights Management. By default, the super users feature is not enabled, and no users are assigned to this feature. By enabling this feature we can modify the users and groups that are able to administer the Rights Management service.
References:
https://docs.microsoft.com/en-us/powershell/module/aadrm/enable-aadrmsuperuserfeature?view=azureipps

Question: 229

DRAG DROP
A company plans to use Office 365 to provide email services to employees. The company obtains a custom domain name to use with Office 365.
You need to add the domain name to Office 365.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Box 1:

Install the Windows Azure Active Directory module for Windows PowerShell.

Box 2:

Connect to Windows Azure Active Directory.

Box3:

Run the Windows PowerShell cmdlet **New-MsolDomain**.

Manage Azure AD using Windows PowerShell

You can use the Azure Active Directory Module for Windows PowerShell cmdlets for Azure AD administrative tasks such as user management, domain management and for configuring single sign-on.

Step 1: Install the Azure AD Module

Step 2: Connect to Azure AD

Click the Microsoft Azure Active Directory Module for Windows PowerShell shortcut to open a Windows PowerShell workspace that has the cmdlets. Alternatively, you can load the cmdlets manually by typing import-module MSOnline at the Windows PowerShell command prompt.

Step 3: The New-MsolDomain cmdlet is used to create a new domain object. This cmdlet can be used to create a domain with managed or federated identities

Question: 230

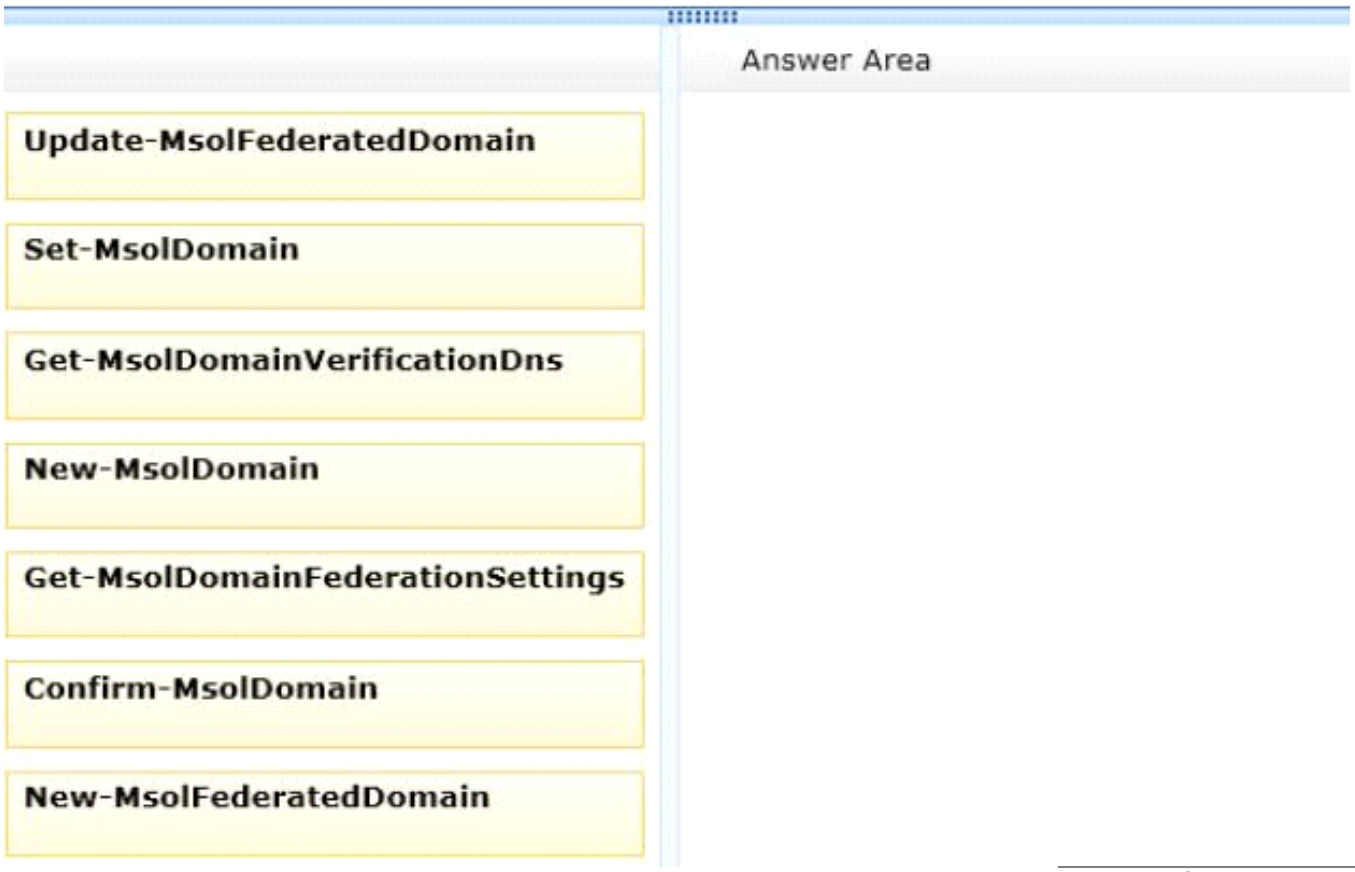
DRAG DROP

Fabrikam Inc. plans to use the domain fabrikam.com for Office 365 user identities, email addresses, Session Initiation Protocol (SIP) addresses, and a public-facing home page.

Single sign-on (SSO) between Office 365 and the on-premises Active Directory is NOT required.

You need to configure the Office 365 plan.

Which four Windows PowerShell cmdlets should you run in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Box 1: New-MsolDomain
Box 2: Get-MsolDomainVerificationDNS
Box 3: Confirm-MsolDomain
Box 4: Set-MsolDomain
Box1. First we need to add the domain.
The New-MsolDomain cmdlet is used to create a new domain object. This cmdlet can be used to create a domain with managed or federated identities.
Box2. Next we need to check the DNS before the domain can be confirmed.
The Get-MsolDomainVerificationDns cmdlet is used to return the DNS records that need to be set to verify a domain.
Box3. Now we can confirm the domain.
The Confirm-MsolDomain cmdlet is used to confirm ownership of a domain. In order to confirm ownership, a custom TXT or MX DNS record must be added for the domain. The domain must first be added using the New-MsolDomain cmdlet (step 1), and then the Get-MsolDomainVerificationDNS cmdlet (step 2) should be called to retrieve the details of the DNS record that must be set.
Box4. Next we can set fabrikam.com as the default domain.
The Set-MsolDomain cmdlet is used to update settings for a domain. This cmdlet can be used to change the default domain setting for the company.

Question: 231

You have an Office 365 environment. Synchronization between the on-premises Active Directory and Office 365 is enabled.
You need to deactivate directory synchronization.
Which Windows PowerShell cmdlet should you run?

A. Update-MsolFederatedDomain
B. Remove-MsolDomain

C. Remove-MsolFederatedDomain
D. Set-MsolDirSyncEnabled

Answer: D

Explanation:
The Set-MsolDirSyncEnabled cmdlet is used to enable or disable directory synchronization for a company. The complete command to disable directory Sync is Set-MsolDirSyncEnabled –EnableDirSync $false
References:
http://support.microsoft.com/kb/2619062

Question: 232

Your company has a hybrid deployment of Office 365. You need to verify whether free/busy information sharing with external users is configured.
Which Windows PowerShell cmdlet should you use?

A. Test-OutlookConnectivity
B. Test-FederationTrust
C. Get-OrganizationRelationship
D. Get-MSOLDomainFederationSettings

Answer: C

Explanation:
How to troubleshoot free/busy issues in a hybrid deployment of on-premises ExchangeServer and Exchange Online in Office 365
Use the Get-OrganizationRelationship cmdlet to retrieve settings for an organization relationship that has been created for federated sharing with other federated Exchange organizations or for hybrid deployments with ExchangeOnline. You can use this information to troubleshoot free/busy issues in a hybrid deployment.
In more detail (see step 4 below):
To help troubleshoot this issue, follow these steps:
On an on-premises computer that's running Microsoft Exchange 2010 Server Service Pack 1 (SP1), click Start, click All Programs, click Microsoft Exchange Server 2010, and then click Exchange Management Shell.
At the command line, type the following command, and then press Enter: Get-FederationInformation -domainname <Office 365Domain>In this command, the <Office 365 Domain> placeholder represents the default Office 365 domain (for example, adatum.onmicrosoft.com).
In the results, note the TargetApplicationUri and TargetAutodiscoverEpr values. These are the settings that the target domain must have to make sure that the federation trust is set up correctly.
To display the trust information that is currently set up for the default Office 365 domain, run the following command: Get-OrganizationRelationship | FL

Question: 233

A company migrates to Office 365. 2,000 active users have valid Office 365 licenses assigned.
An additional 5,000 user accounts were created during the migration and testing processes. These users do not have any licenses assigned.
You need to remove the Office 365 user accounts that do not have any licenses assigned by using the least amount of administrative effort.
Which Windows PowerShell command should you run?

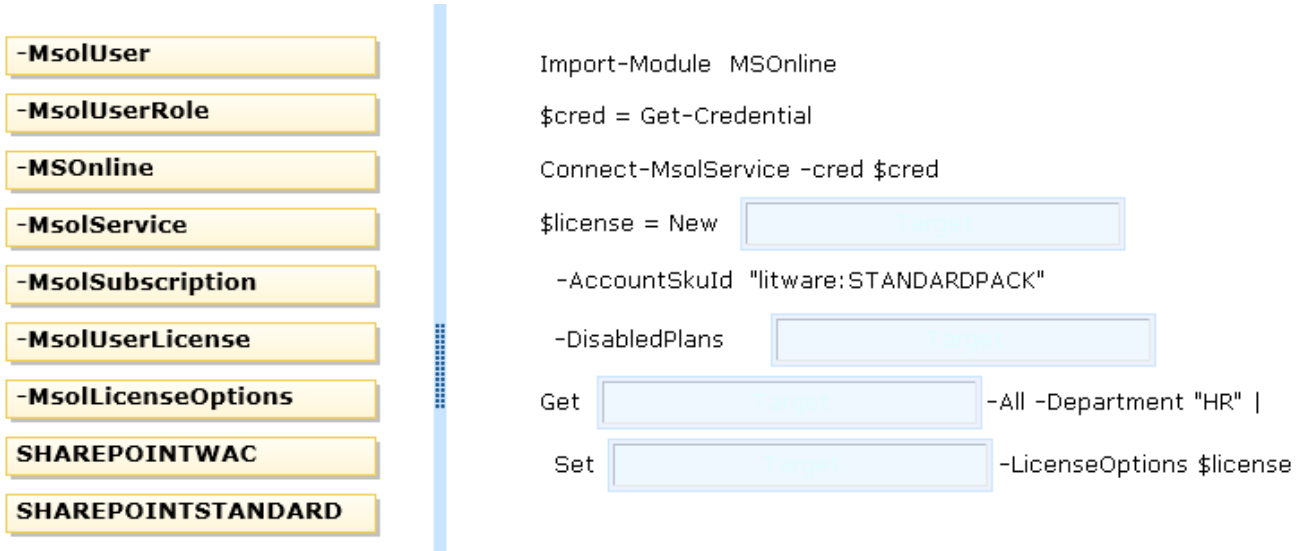
A. Get-MsolUser -All-EnabledFilter "DisabledOnly" | Remove-MsolUser -Force
B. Get-MsolUser-EnabledFilter "DisabledOnly" | Remove-MsolUser -Force
C. Get-MsolUser -All -UnlicensedUsersOnly | Remove-MsolUser -Force
D. Get-MsolUser -UnlicensedUsersOnly | Remove-MsolUser–Force

Answer: C

Explanation:
Step 1: Get all unlicensed users:
The Get-MsolUser cmdlet can be used to retrieve an individual user, or list of users. We must use both the –All and the –UnlicensedUsersOnlyparameters to retrieve all unlicensed users.
Parameters include:
All [<SwitchParameter>] If present, then all results will be returned.
UnlicensedUsersOnly [<SwitchParameter>] The filter for only users who are not assigned a license.
Step 2: Remove these users through the Remove-MsolUser –Force command.

Question: 234

DRAG DROP
Litware Inc. has an Office 365 Enterprise E1 plan. Employees have access to all Office 365 services.
Employees in the human resources (HR) department must continue to use the on-premises SharePoint 2013 deployment due to legal requirements.
You need to disable access to SharePoint Online for all HR department employees.
How should you complete the relevant Windows PowerShell commands? To answer, drag the appropriate Windows PowerShell segment to the correct location or locations in the answer are
a. Each Windows PowerShell segment may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:

```
Import-Module  MSOnline
$cred = Get-Credential
Connect-MsolService -cred $cred
$license = New -MsolLicenseOptions
 -AccountSkuId "litware:STANDARDPACK"
 -DisabledPlans SHAREPOINTSTANDARD
Get -MsolUser -All -Department "HR" |
 Set -MsolUserLicense -LicenseOptions $license
```

Box 1: -MsolLicenseOptions
We must create license object. The New-MsolLicenseOptions cmdlet creates a new License Options object.
Box 2: SHAREPOINTSTANDARD
We must disable SharePoint Online. SharePoint Online is denoted by SHAREPOINTSTANDARD.
The New-MsolLicenseOptions-DisabledPlans <string[]> produces a list of service plans to disable when assigning this license to the user.
Box 3: We get all HR department users through the Get –MsolUser –All –Department "HR" command.
The Get-MsolUser cmdlet can be used to retrieve an individual user, or list of users.
Box 4: For these retrieved users we use the Set-MsolUserLicense command to apply the license we constructed.
The Set-MsolUserLicense cmdlet can be used to adjust the licenses for a user.

Question: 235

Your company uses Office 365. You need to identify which users do NOT have a Microsoft Exchange Online license assigned to their user account.
Which Windows PowerShell cmdlet should you use?

A. Get-ManagementRoleAssignment
B. Get-User
C. Get-RoleGroupMember
D. Get-LogonStatistics
E. Get-RemovedMailbox
F. Get-MSOLContact
G. Get-Recipient
H. Get-Mailbox
I. Get-Group
J. Get-MailboxStatistics
K. Get-MSOLUser
L. Get-MailContact

Answer: K

Explanation:
We use the Get-MsolUser –UnlicensedUsersOnly command to retrieve all users which do not have a Microsoft Exchange Online license.

The Get-MsolUser cmdlet can be used to retrieve an individual user, or list of users.
The -UnlicensedUsersOnly [<SwitchParameter>] parameter filters for only users who are not assigned a license.

Question: 236

You are the Office 365 administrator for your company. The company synchronizes the local Active Directory objects with a central identity management system.
The environment has the following characteristics:
Each department has its own organizational unit (OU).
The company has OU hierarchies for partner user accounts.
All user accounts are maintained by the identity management system.
You need to ensure that partner accounts are NOT synchronized with Office 365.
What should you do?

A. Configure OU-based filtering by using Azure Active Directory Connect (Azure AD Connect).
B. In the Azure Active Directory portal, configure OU-based filtering.
C. Configure user attribute-based filtering by using Azure Active Directory Connect (Azure AD Connect).
D. In the Azure Active Directory portal, configure user attribute-based filtering.

Answer: A

Explanation:
You can use Azure AD Connect to enable Active Directory synchronization filtering. This allows you to filter out objects that should not be synchronized to the cloud. The objects that can be filtered are: Organizational-units (OUs), domains, and user-attributes.

Question: 237

An organization plans to migrate to Office 365. You use the Windows Azure Active Directory (AD) Sync tool.
Several users will not migrate to Office 365. You must exclude these users from synchronization. All users must continue to authenticate against the on-premises Active Directory.
You need to synchronize the remaining users.
Which three actions should you perform? Each correct answer presents part of the solution.

A. Populate an attribute for each user account.
B. Disable the user accounts in Active Directory.
C. Perform a full synchronization.
D. Configure the connection filter.
E. Run the Windows PowerShell command Set-MsolDirSyncEnabled -EnableDirSync $false.

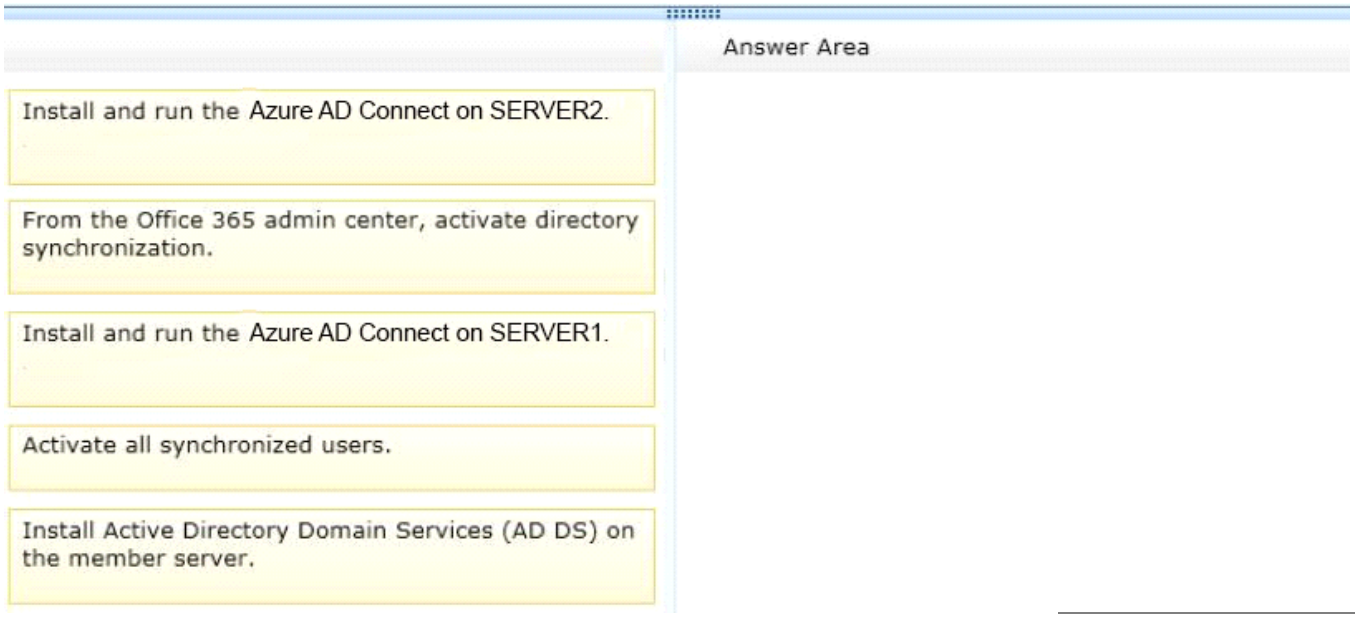
Answer: A,C,D

Explanation:
To implement user attribute-based Directory synchronization filtering you need to add an attribute to each user object that is to be filtered in your on-premises Active Directory. Then you need to enable Active Directory synchronization filtering and configure the connection filter to use the user attribute. Finally, you must perform a full synchronization.

Question: 238

DRAG DROP

An organization plans to deploy an Office 365 tenant. The company has two servers named SERVER1 and SERVER2. SERVER1 is a member server of the Active Directory forest that you are synchronizing. SERVER2 is a standalone server. Both servers run Windows Server 2012.
You need to use the Azure Active Directory Connect to provision users
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Box 1:
From the Office 365 admin center, activate directory synchronization.
Box 2:
Install and run the Azure AD Connect on SERVER1.
Box 3:
Activate all synchronized users.
You must activate directory synchronization before you install the Directory Sync tool.
The Directory Sync tool must be installed on a computer that is joined to the Active Directory forest that you plan to synchronize. As SERVER2 is a standalone server, it is not joined to the Active Directory forest and cannot be used for synchronization.
Finally, assign license to activate services for the synchronized users.

Question: 239

An organization deploys an Office 365 tenant.
User accounts must be synchronized to Office 365 by using the Windows Azure Active Directory Sync tool.
You have the following password policies:
Passwords for the on-premises Active Directory Domain Services (AD DS) user accounts are at least six characters long.
Passwords for Office 365 user accounts are at least eight characters long.
You need to ensure that the user accounts will be synchronized. Which user accounts will be synchronized?

A. All user accounts
B. No user accounts
C. User accounts with a password length of at least 8characters
D. User accounts with a password length of at least 14 characters

Answer: A

Explanation:
Password Sync is an extension to the directory synchronization implemented by the Directory Sync tool and synchronizes user passwords from your on-premises Active Directory to Azure Active Directory. When password sync is enabled, the password complexity policies configured in the on-premises Active Directory override any complexity policies that are defined in the cloud for synchronized users.

Question: 240

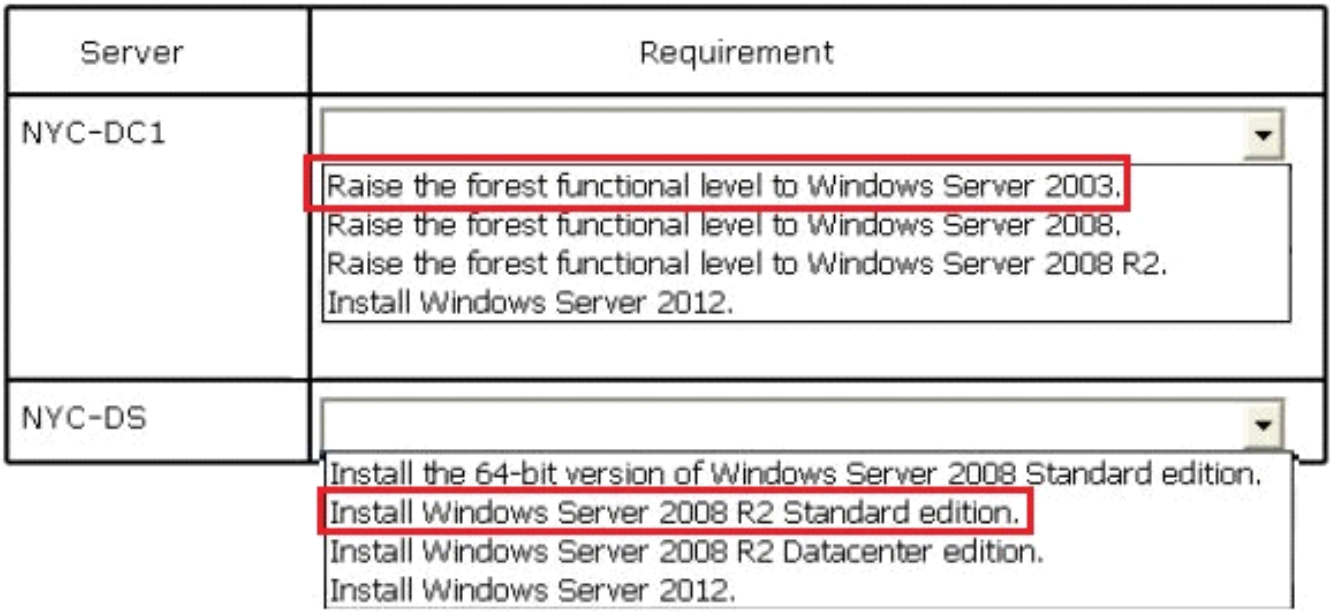
HOTSPOT
An organization prepares to migrate to Office 365. The organization has one domain controller named NYC-DC1 and one server named NYC-DS that is designated as the directory synchronization computer.
The organization has the following servers:

Server	Operating System	Forest Function Level
NYC-DC1	Windows Server 2008 R2	Windows 2000
NYC-DS	Windows Server 2003	

You plan to upgrade the servers to support directory synchronization.
You must upgrade each server to meet only the minimum requirements by using the least amount of administrative effort.
You need to ensure that you can use the Azure AD Connect to synchronize the local Active Directory with Office 365.
What should you do? Select the correct action from each list in the answer area.

Server	Requirement
NYC-DC1	Raise the forest functional level to Windows Server 2003. Raise the forest functional level to Windows Server 2008. Raise the forest functional level to Windows Server 2008 R2. Install Windows Server 2012.
NYC-DS	Install the 64-bit version of Windows Server 2008 Standard edition. Install Windows Server 2008 R2 Standard edition. Install Windows Server 2008 R2 Datacenter edition. Install Windows Server 2012.

Answer:



The minimum forest functional level requirement for Office356 is Windows Server 2003.
The minimum domain controller requirement for office 356 is 32-bit Windows Server 2003 Standard Edition with Service Pack 1 (SP1). From the available options, the minimum requirement is met by Windows Server 2008 R2 Standard Edition.
References:
http://msdn.microsoft.com/en-us/library/azure/jj151831.aspx

Question: 241

An organization purchases an Office 365 plan for 10,000 user accounts. You have a domain controller that runs Windows Server 2008 R2. The forest functional level is set to Windows Server 2000.
The organization must be able to synchronize user attributes from the on-premises Active Directory Domain Services environment to Office 365.
You need to prepare to install the Azure AD Connect
Which two actions should you perform? Each correct answer presents part of the solution.

A. Upgrade the domain controller to Windows Server 2012.
B. Install Microsoft .NET Framework 3.5SP1 and Microsoft .NET Framework 4.0.
C. Install Windows Server 2012 Standard edition.
D. Raise the forest functional level to Windows Server 2008 R2.
E. Join a workstation to an Active Directory domain.

Answer: B,D

Explanation:
B: The directory synchronization computer must run the Microsoft .NET Framework 3.5 SP1 and the Microsoft .NET Framework 4.0 or higher.
D: The minimum forest functional level requirement for Office 356 is Windows Server 2003. We must therefore raise the forest functional level.

Question: 242

HOTSPOT
You are the Office 365 administrator for your company.

User1 leaves the company. You must delete the account for User1.
In the table below, identify when each type of data will be deleted. Make only one selection in each column. Each correct selection is worth one point.

User1 Exchange Online mailbox	Documents Created by User1 on SharePoint Online	Timeframe
○	○	Never removed
○	○	Removed immediately
○	○	Removed after 30-day grace period
○	○	Removed after 90-day grace period

Answer:

User1 Exchange Online mailbox	Documents Created by User1 on SharePoint Online	Timeframe
○	○	Never removed
○	○	Removed immediately
○	○	Removed after 30-day grace period
○	○	Removed after 90-day grace period

References:
https://support.office.com/en-us/article/Manage-SharePoint-Online-user-profiles-from-the-SharePoint-admin-center-494bec9c-6654-41f0-920f-f7f937ea9723?CorrelationId=bd632ebb-fd74-4030-a971-13b99cb02f8e&ui=en-US&rs=en-US&ad=US#_Toc351377085

Question: 243

Your company has a hybrid deployment of Office 365. All mailboxes are hosted on Office 365. All users access their Office 365 mailbox by using a user account that is hosted on-premises. You need to delete a user account and its associated mailbox.
Which tool should you use?

A. The Remove-MSOLUser cmdlet
B. The Remove-Mailbox cmdlet
C. The Office 365 portal
D. Active Directory Users and Computers

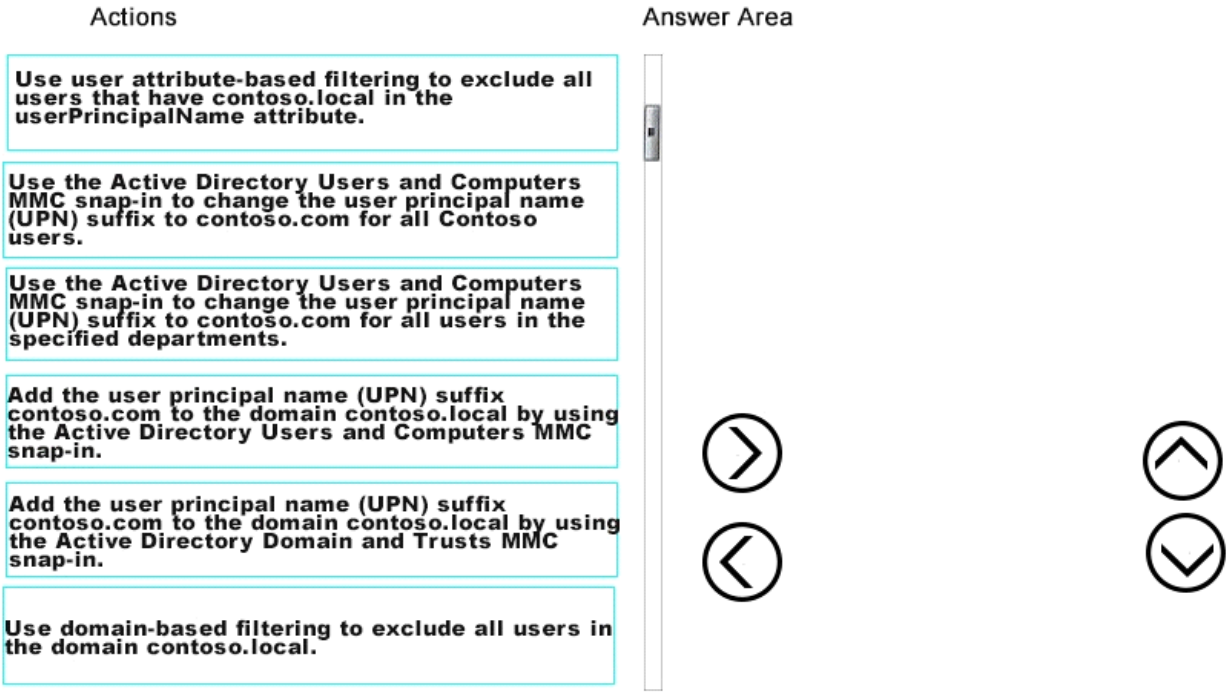
Answer: D

Explanation:
With directory synchronization enabled, the on premise Active Directory becomes the master for all changes to the synchronized mail-enabled objects in Microsoft Azure Active Directory. You should thus delete accounts from Active Directory and when directory synchronization runs the associated object will be deleted from Azure and the associated mailbox will be soft-deleted.

Question: 244

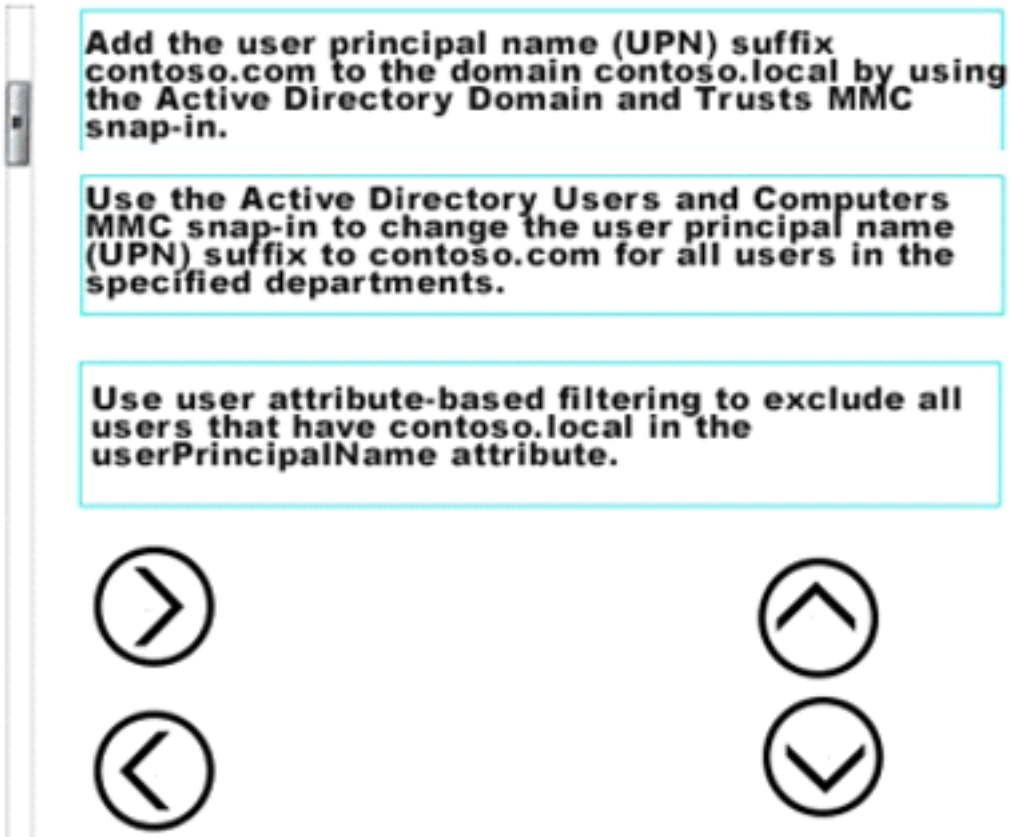
DRAG DROP

Contoso Ltd. plans to use Office 365 services for collaboration between departments. Contoso has one Active Directory Domain Services domain named contoso.local. You deploy Azure AD Connect.
You plan to implement single sign-on (SSO) for Office 365.
You need to synchronize only the user accounts that have valid routable domain names and are members of specified departments.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Answer Area



The domain we want to federate must be registered as a public internet domain with a domain registrar or within our own public DNS servers. We cannot use contoso.local as it is not routable outside of the intranet. We can then use Active Directory Domains and Trusts to add user principal name (UPN) suffixes to the domain. The default UPN suffix is the Domain Name System (DNS) domain name of the contoso.local domain that contains the user account. We can add contoso.com as an alternative UPN suffixes for logon processes.
We should then use Active Directory Users and Computers to change the UPN of user accounts in the specified departments to contoso.com.
Finally, we can use user attribute-based filtering to exclude all have non-routable domain names, i.e., those that have a contoso.local as their UPN suffix.

Question: 245

You are the Office 365 administrator for your company.
The environment must support single sign-on.
You need to install the required certificates.
Which two certificates should you install? Each correct answer presents part of the solution.

A. Secure Sockets Layer (SSL)
B. Privacy-enhanced mail (PEM)
C. Token signing
D. Personal
E. Software publisher

Answer: A,C

Explanation:

Certificates are used to secure communications between federation servers, Web Application Proxies, federation server proxies, the cloud service, and web clients.
A: A Secure Sockets Layer (SSL) certificate is used to secure communications between federation servers, clients, Web Application Proxy, and federation server proxy computers.
C: A Token-signing certificate is a standard X.509 certificate that is used to securely sign all tokens that the federation server issues and that the cloud service will accept and validate.

Question: 246

Contoso Ltd. uses Office 365 for collaboration. You are implementing Active Directory Federation Services (AD FS) for single sign-on (SSO) with Office 365 services. The environment contains an Active Directory domain and an AD FS federation server.
You need to ensure that the environment is prepared for the AD FS setup.
Which two actions should you perform? Each correct answer presents part of the solution.

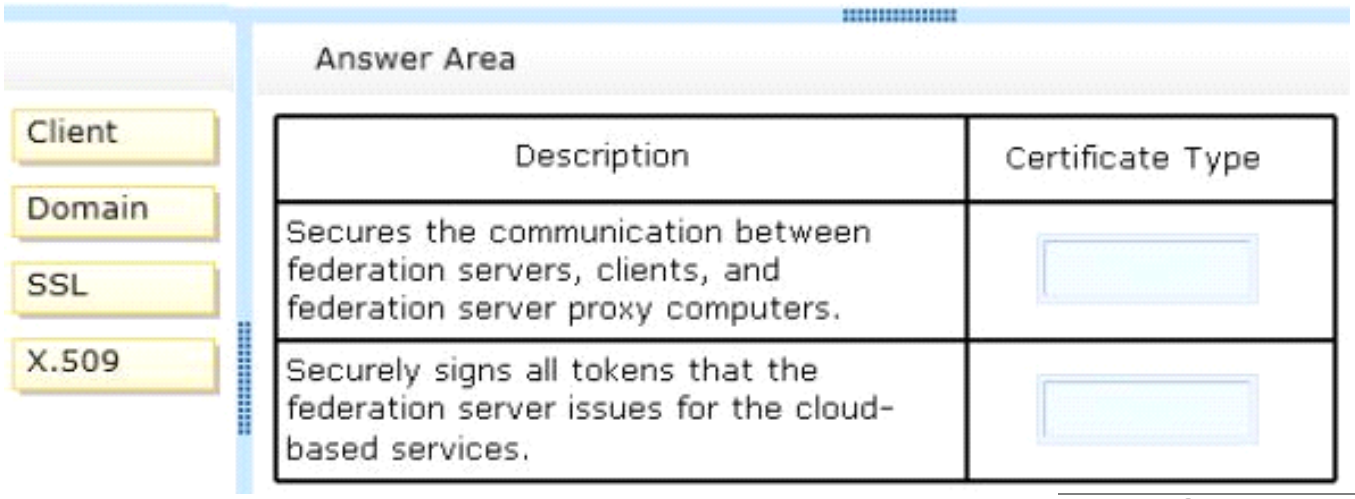
A. Configure Active Directory to use the domain contoso.com.
B. Configure Active Directory to use the domain contoso.local.
C. Create a server authentication certificate for the federation server by using fs.contoso.com as the subject name and subject alternative name.
D. Create a server authentication certificate for the federation server by using fs.contoso.local as the subject name and subject alternative name.

Answer: A,C

Explanation:
A: The domain we want to federate must be registered as a public internet domain with a domain registrar or within our own public DNS servers. We cannot use contoso.local as it is not routable outside of the intranet.
C: The Subject Name of the SSL certificate must match the names used in the AD FS configuration. The default sub-domain for AD FS is fs. As we use contoso.com as the domain, we are probably using fs,contoso.com as the AD FS name and we must also use it in the subject name for the certificate.

Question: 247

DRAG DROP
You are the Office 365 administrator for your company.
You must configure a trust between the on-premises Active Directory domain and the Office 365 environment by using Active Directory Federation Services.
You need to assign the correct certificate to the description of your on-premises server environment below.
Which certificate types should you assign? To answer, drag the appropriate certificate type to the correct test description. Each certificate type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:

Description	Certificate Type
Secures the communication between federation servers, clients, and federation server proxy computers.	SSL
Securely signs all tokens that the federation server issues for the cloud-based services.	X.509

Certificates are used to secure communications between federation servers, Web Application Proxies, federation server proxies, the cloud service, and web clients.

A Secure Sockets Layer (SSL) certificate is used to secure communications between federation servers, clients, Web Application Proxy, and federation server proxy computers.

A Token-signing certificate is a standard X.509 certificate that is used to securely sign all tokens that the federation server issues and that the cloud service will accept and validate.

References:

https://technet.microsoft.com/en-us/library/dn151311.aspx

http://blogs.technet.com/b/adfs/archive/2007/07/23/adfs-certificates-ssl-token-signing-and-client-authentication-certs.aspx

Question: 248

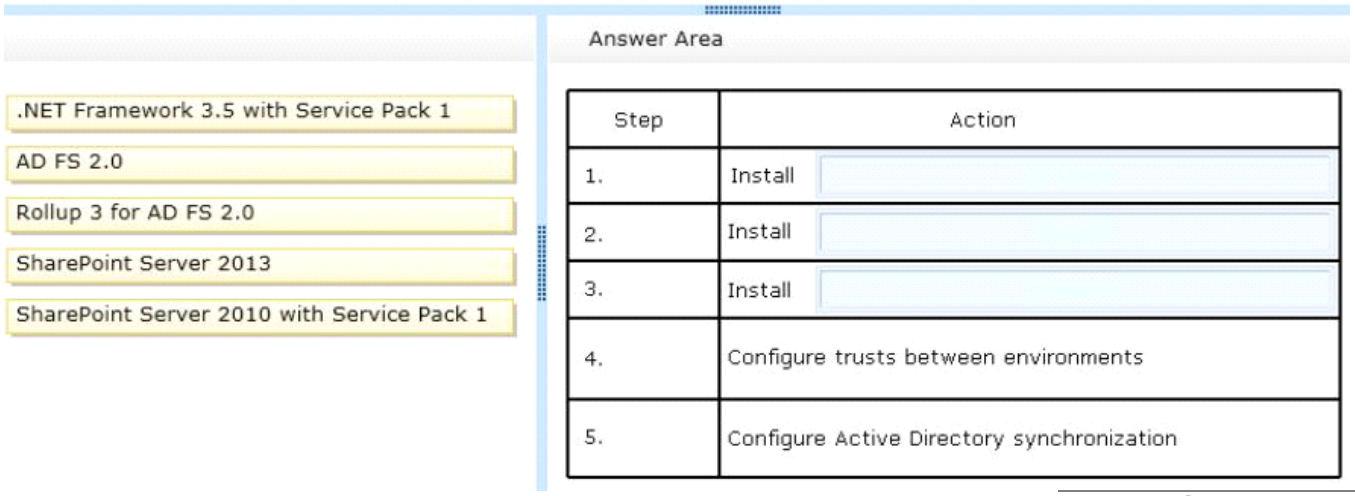
DRAG DROP

A company has a Windows Server 2008 domain controller and a SharePoint 2007 farm. All servers on the network run Windows Server 2008.

You must provide single sign-on for Office 365 SharePoint sites from the company's network.

You need to install the required software.

What should you install? To answer, drag the appropriate action to the correct location. Each answer may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:

Step	Action
1.	Install .NET Framework 3.5 with Service Pack 1
2.	Install AD FS 2.0
3.	Install Rollup 3 for AD FS 2.0
4.	Configure trusts between environments
5.	Configure Active Directory synchronization

Active Directory Federated Services (AD FS) is required to support single sign-on.
On a Windows Server 2008 computer AD FS can be installed as a separate installation package known as AD FS 2.0. The .NET Framework 3.5 with Service Pack 1 is a prerequisite for AD FS 2.0 software and is not automatically be installed by the AD FS 2.0Setup Wizard. We must therefore install the .NET Framework 3.5 with Service Pack 1 first.
Once .NET Framework 3.5 with Service Pack 1 is installed, we can run the AD FS 2.0 installation package.
Once AD FS 2.0 is installed, we must install the AD FS hotfixes. The hotfixes are included in Update Rollup 3 for AD FS 2.0.
References:
https://technet.microsoft.com/en-us/library/dn151311.aspx
http://technet.microsoft.com/en-us/library/cc771145.aspx

Question: 249

You are the Office 365 administrator for your company. You prepare to install Active Directory Federation Services (AD FS).
You need to open the correct port between the AD FS proxy server and the AD FS federation server.
Which port should you open?

A. TCP 80
B. TCP 135
C. TCP 389
D. TCP 443
E. TCP 636

F. TCP 1723

Answer: D

Explanation:
Secure Sockets Layer (SSL) is used to secure communications between federation servers, clients, Web Application Proxy, and federation server proxy computers. HTTP over SSL (HTTPS) uses TCP port 443.

Question: 250

You are the Office 365 administrator for your company. The company has a single office.
You have the following requirements:
You must configure a redundant Active Directory Federation Services (AD FS) implementation.
You must use a Windows Internal Database to store AD FS configuration data.
The solution must use a custom login page for external users.
The solution must use single sign-on for internal users.
You need to deploy the minimum number of servers.
How many servers should you deploy?

A. 2
B. 4
C. 6
D. 16

Answer: B

Explanation:
To provide redundancy, we would need to create AD FS farms with at least two servers. This can be used to allow internal users to use single sign-on (SSO).
As we are using Windows Internal Database (WIM) to store AD FS configuration data, we do not need any additional servers for the database as WIM is included in Windows Server 2008 and later versions. Redundancy for WIM is possible when an AD FS farm is set up.
To support external users, we would need to set up an AD FS proxy server. In order to provide redundancy we would need to set up an AD FS proxy farm. This would require a minimum of 2 more servers.
The custom login page for external users can be created on the AD FS proxy server, which the external users would access. There is thus no need for additional servers.
Thus the minimum number of server we would require is four: two for the AD FS farm and two for the AD FS proxy farm.
References:
https://technet.microsoft.com/en-us/library/gg982488.aspx
http://blogs.technet.com/b/askpfeplat/archive/2013/07/22/faq-on-adfs-part-1.aspx

Question: 251

Contoso uses Office 365 for collaboration services. You implement single sign-on (SSO) with Office 365 by using Active Directory Federation Services (AD FS).
You need to implement Windows Azure multi-factor authentication.
Which three actions should you perform? Each correct answer presents part of the solution.

A. On the AD FS federation server, run PhoneFactorAgentSetup.exe.

B. On the AD FS Federation server, run WindowsAzureSDK-x64.exe.
C. On the AD FS Federation server, run the Windows PowerShell cmdlet Register-AdfsAuthenticationProvider.
D. On the AD FS Federation server, run FsConfigWizard.exe.
E. Run the Active Directory Domains and Trusts MMC snap-in. Register Windows Azure Multi-Factor Authentication Server as an additional authentication provider.
F. Run the Windows Azure Multi-Factor Authentication Server Authentication Configuration Wizard.

Answer: B,C,F

Explanation:
To implement Windows Azure multi-factor authentication in AD FS, we must install the Windows Azure Multi-Factor Authentication Server, register it in AD FS and configure multi-factor authentication.
B: The Windows Azure Multi-Factor Authentication Server can be installed by running WindowsAzureSDK-x64.exe.
C: The Register-AdfsAuthenticationProvider cmdlet registers an external authentication provider in Active Directory Federation Services (AD FS).
F: Run the Windows Azure Multi-Factor Authentication Server Authentication Configuration Wizard to configure multi-factor authentication.

Question: 252

Your company has an Office 365 subscription. You need to add the label "External" to the subject line of each email message received by your organization from an external sender.
What should you do?

A. From the Exchange Control Panel, add a MailTip.
B. From the Forefront Online Protection Administration Center, set the footer for outbound email.
C. Run the Enable-InboxRule cmdlet.
D. From the Exchange Control Panel, run the New Rule wizard.

Answer: D

Explanation:
Transport rules can apply messaging policies to email messages flowing through your organization. It can be used to prepend the subject of the message with a text label.

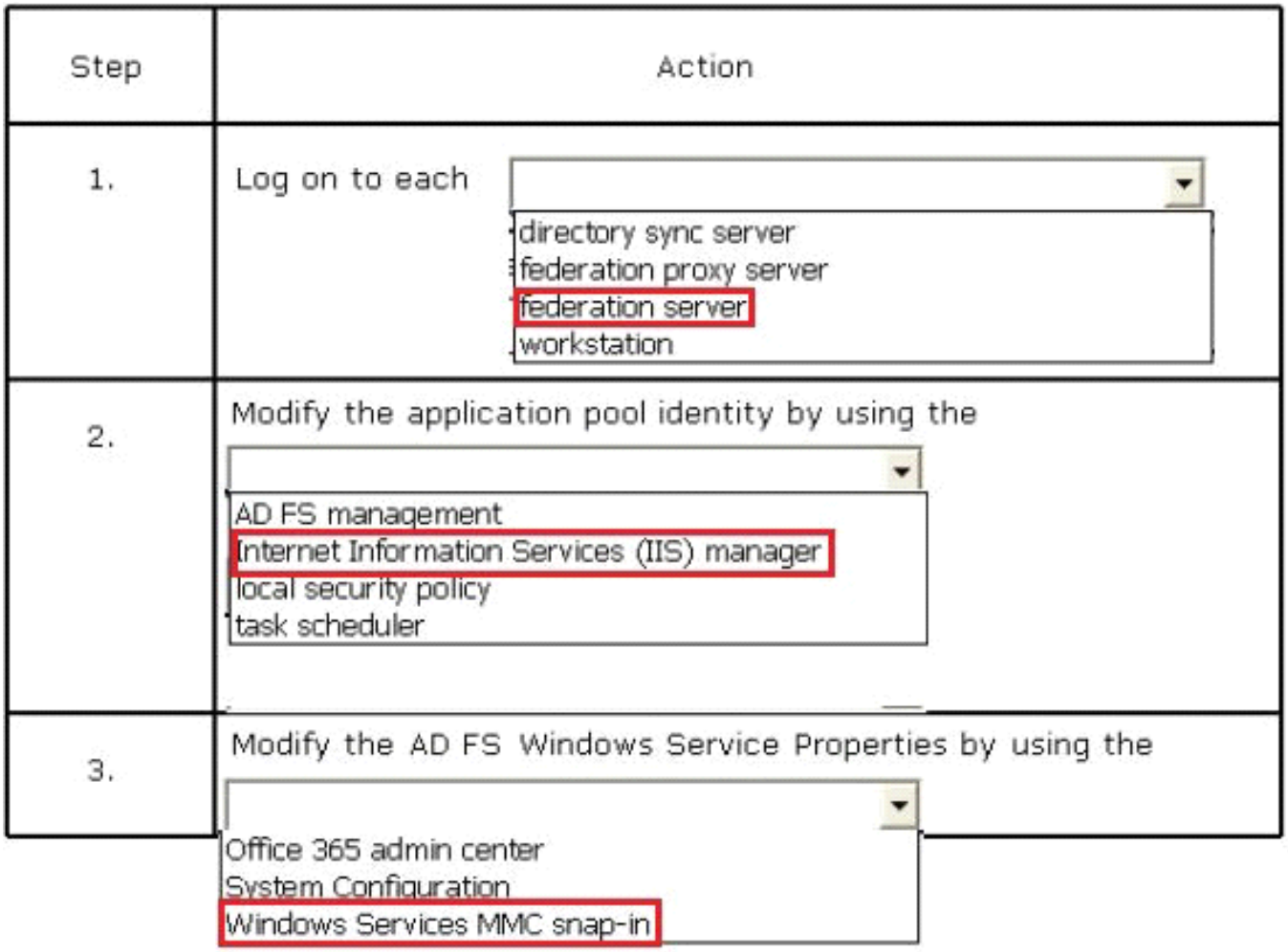
Question: 253

HOTSPOT
An organization has over 10,000 users and uses a SQL-based Active Directory Federation Services (AD FS) 2.0 server farm.
You need to change the AD FS 2.0 service account password.
What should you do? Select the correct answer from each list in the answer area.

Step	Action
1.	Log on to each [ ]
2.	Modify the application pool identity by using the [ ]
3.	Modify the AD FS Windows Service Properties by using the [ ]

Step	Action
1.	Log on to each [ ] directory sync server federation proxy server federation server workstation
2.	Modify the application pool identity by using the [ ] AD FS management Internet Information Services (IIS) manager local security policy task scheduler
3.	Modify the AD FS Windows Service Properties by using the [ ] Office 365 admin center System Configuration Windows Services MMC snap-in

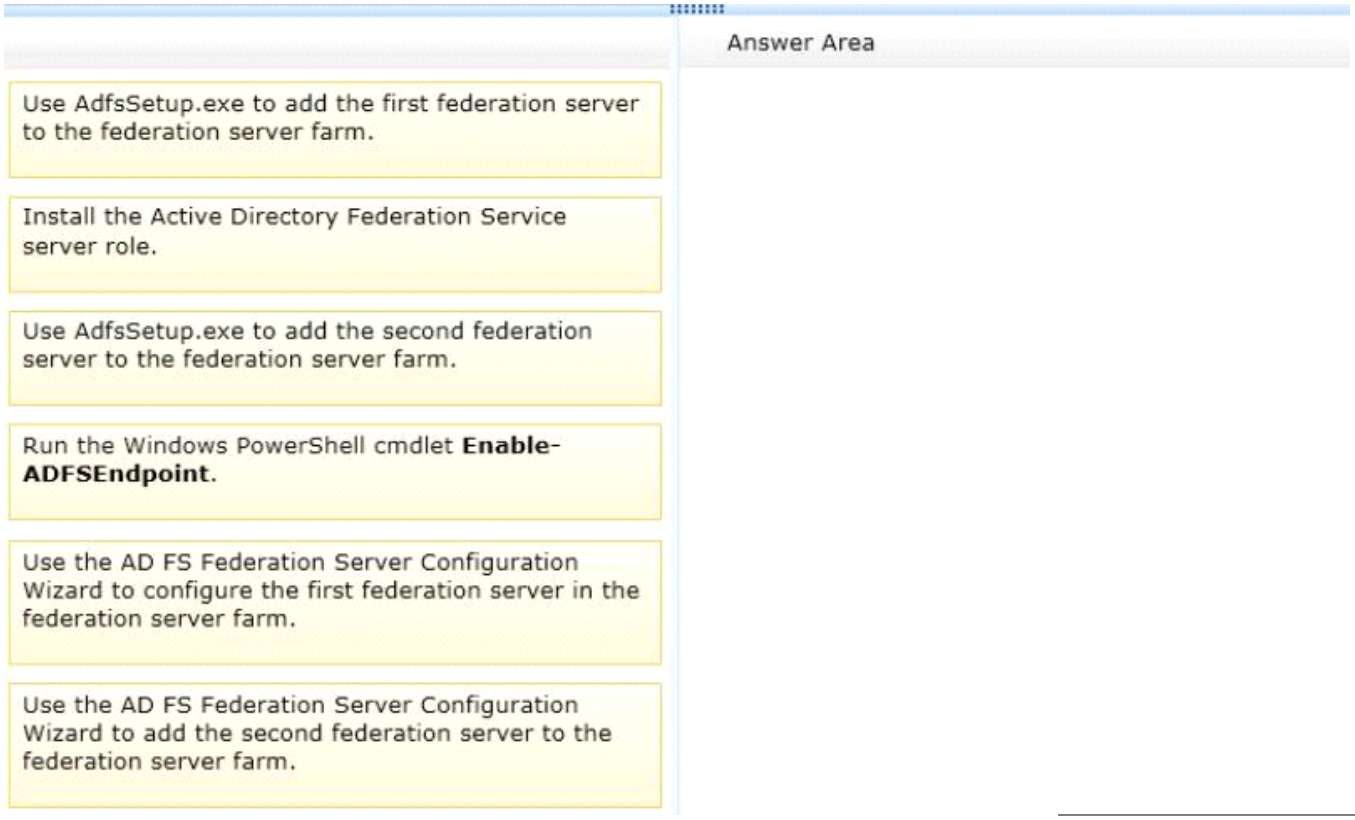
Answer:



We must update the domain password for the AD FS 2.0 service account in Active Directory Domain Services (AD DS) and then update the AD FS AppPool and the AD FS service account on all federation servers in the federation server farm to mirror the new domain password.
The AD FS AppPool is configured through Internet Information Services (IIS) Manager.
The AD FS 2.0 Windows Service Properties is configured through the Windows Services snap-in.
References:
https://technet.microsoft.com/en-us/library/hh344806%28v=ws.10%29.aspx

Question: 254

DRAG DROP
A company is deploying an Office 365 tenant.
You need to deploy a Windows Server 2012 R2 federation server farm.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Box 1:

Install the Active Directory Federation Service server role.

Box 2:

Use the AD FS Federation Server Configuration Wizard to configure the first federation server in the federation server farm.

Box 3:

Use the AD FS Federation Server Configuration Wizard to add the second federation server to the federation server farm.

To deploy a Windows Server 2012 R2 federation server farm we need to install AD FS on the computers that will become federation servers; configure AD FS to create the first federation server in a new farm; and add the additional servers to the farm.

Question: 255

A company deploys an Office 365 tenant.
You need to configure single sign-on (SSO) for all user accounts.
Which two actions should you perform? Each correct answer presents part of the solution.

A. Run the Windows PowerShell cmdlet Convert-MsolDomainToStandard.
B. Run the Windows PowerShell cmdlet Enable-ADFSEndpoint.

C. Run the Windows PowerShell cmdlet Convert-MsolDomainToFederated.
D. Deploy a federation server proxy.
E. Run the Windows PowerShell cmdlet New-ADFSOrganization.
F. Deploy a federation server farm.

Answer: C,F

Explanation:
C: The Convert-MSOLDomainToFederated cmdlet converts the specified domain from standard authentication to single sign-on (SSO).
F: Single sign-on (SSO) requires Active Directory Federation Services (AD FS) which can be installed as a federation farm.
References:
http://technet.microsoft.com/en-us/library/dn194092.aspx

Question: 256

A company plans to deploy an Office 365 tenant. You have two servers named FS1 and FS2 that have the Federation Service Proxy role service installed.
You must deploy Active Directory Federation Services (AD FS) on Windows Server 2012.
You need to configure name resolution for FS1 and FS2.
What should you do?

A. On FS1 and FS2, add the cluster DNS name and IP address of the federation server farm to the hosts file.
B. On FS1 only, add the cluster DNS name and IP address of the federation server farm to the hosts file.
C. On FS1 only, add the cluster NetBIOS name and IP address of the federation server farm to the LMHOSTS file.
D. On FS1and FS2, add the cluster NetBIOS name and IP address of the federation server farm to the LMHOSTS file.

Answer: A

Explanation:
A: To properly configure a federation proxy server, the host file on the federation proxy server must have an entry that points to the federation server farm's cluster DNS name and its IP address. This must be performed on all federation proxy servers.
References:
http://office365support.ca/setting-up-adfs-proxy-server-part-1/

Question: 257

You are the Office 365 administrator for your company. You have a server that runs Windows Server 2012. You plan to install an Active Directory Federation Services (AD FS) proxy server.
You need to install and configure all of the required roles.
Which two roles should you install and configure? Each correct answer presents part of the solution.

A. Web Server (IIS)
B. AD FS
C. Application Server
D. Network Policy and Access Service
E. Active Directory Certificate Services (AD CS)
F. Remote Access

Answer: A,B

Explanation:
The Active Directory Federation Services role and the Web Server Role (IIS) role are required for setting up an AD FS proxy server.
References:
http://technet.microsoft.com/en-us/library/dd807096.aspx
https://technet.microsoft.com/en-us/library/dd807080.aspx
https://technet.microsoft.com/en-us/network/bb545879.aspx
https://technet.microsoft.com/en-us/library/cc754521%28v=ws.10%29.aspx
https://mshiyas.wordpress.com/howto-adfs-adfs-proxy-on-windows-server-2012-r2-with-office-365/

Question: 258

A company named Fabrikam, Inc. is deploying an Office 365 tenant. You install Active Directory Federation Services (AD FS) on a server that runs Windows Server 2012.
The company's environment is described in the following table:

Description	Fully Qualified Domain Name
Cluster DNS Name	fs.fabrikam.com
Server node in cluster	server1.fabrikam.com
Server node in cluster	server2.fabrikam.com

You must obtain a certificate from a certification authority and install it on the federation servers.
You need to specify the subject name for the certificate.
Which name should you specify?

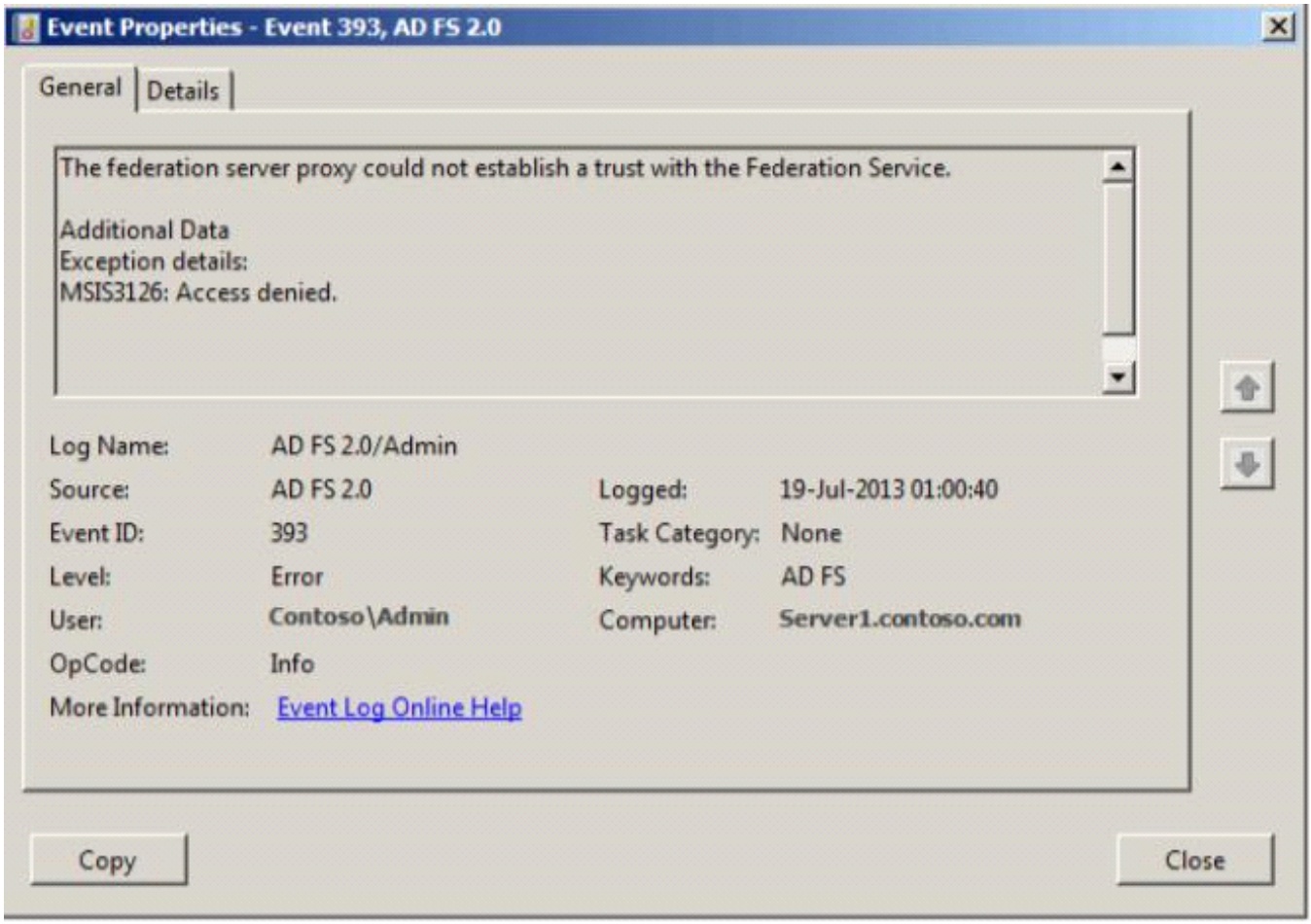
A. fs.fabnkam.com
B. server1.fabrikam.com
C. fabrikam.com
D. server2.fabrikam.com

Answer: A

Explanation:
The Subject Name for the certificate must match the names used for AD FS. The cluster DNS name must match the Federation Service name. As the cluster DNS name is fs.fabnkam.com, we are using it for AD FS, and we must use it in the subject name for the certificate.
References:
http://blogs.technet.com/b/askds/archive/2012/01/05/understanding-the-ad-fs-2-0-proxy.aspx

Question: 259

An organization implements single sign-on (SSO) for use with Office 365 services. You install an Active Directory Federation Services (AD FS) proxy server.
Users report that they are unable to authenticate. You launch the Event Viewer and view the event information shown in the following screen shot:



You need to ensure that users can authenticate to Office 365.
What should you do?

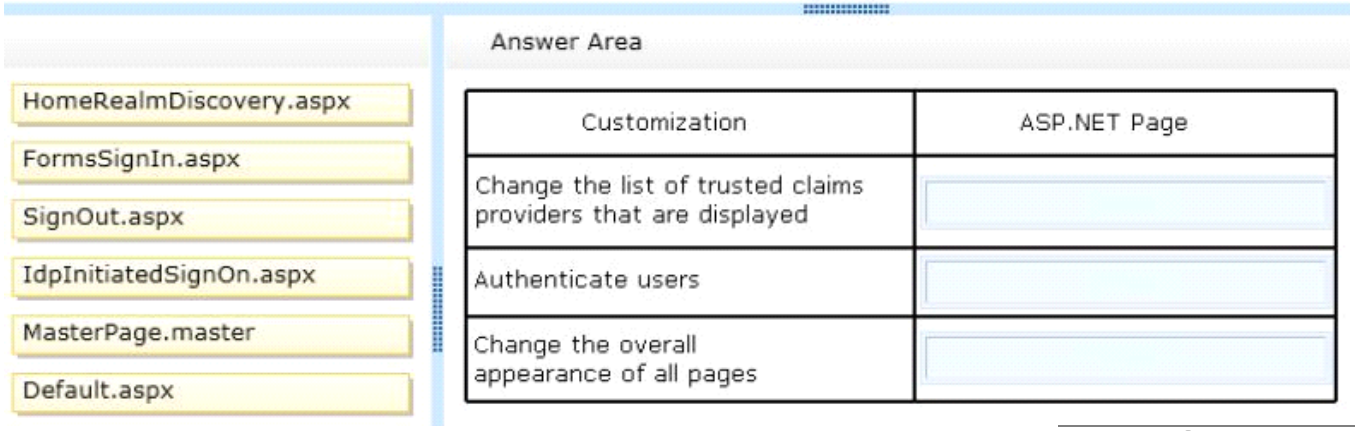
A. Re-enter the credentials used to establish the trust.
B. Verify the federation server proxy is trusted by the federation service.
C. Re-install the Secure Sockets Layer (SSL) certificate for the federation service.
D. Verify network connectivity between the Federation Service Proxy and federation server.

Answer: A

Explanation:
The exhibit indicates that the federation server proxy could not establish a trust with the Federation Service. Possible causes for this problem are:
The credentials that are used to establish the trust between the federation server proxy and the Federation Service are not valid, or the Federation Service cannot be reached.
The federation server proxy trust was revoked.
The federation server proxy has been inactive for a long period of time (such as 30 days or more).
Possible solutions are:
Ensure that the credentials that are being used to establish a trust between the federation server proxy and the Federation Service are valid, and that the Federation Service can be reached.
Run the AD FS 2.0 Proxy Configuration Wizard again to renew trust with the Federation Service.

Question: 260

DRAG DROP
A company deploys an Office 365 tenant. You install the Active Directory Federation Services (AD FS) server role on a server that runs Windows Server 2012. You install and configure the Federation Service Proxy role service. Users sign in by using the Security Assertion Markup Language (SAML) protocol.
You need to customize the sign-in pages for Office 365.
Which pages should you customize? To answer, drag the appropriate page to the correct customization. Each page may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:

Customization	ASP.NET Page
Change the list of trusted claims providers that are displayed	HomeRealmDiscovery.aspx
Authenticate users	IdpInitiatedSignOn.aspx
Change the overall appearance of all pages	MasterPage.master

The HomeRealmDiscovery.aspx page shows a drop-down list that contains the list of trusted claims providers configured for AD FS.
The IdpInitiatedSignOn.aspx page is used to handle SAML-based IdP-initiated single sign-on (SSO).
The MasterPage.master is a template for all .aspx pages and can be used to change the overall appearance of all pages.

Question: 261

HOTSPOT
An organization deploys an Office 365 tenant.
The Service health page displays the following information:

SERVICE	TODAY	NOV 13
Exchange Online		
Identity Service		
Lync Online		
Office 365 Portal		
Office Subscription		
Rights Management Service		
SharePoint Online		
Yammer Enterprise		

You need to report the status of service interruptions for Exchange Online and SharePoint Online.
Use the drop-down menus to complete each statement based on the information presented in the screen shot. Each correct selection is worth one point.

Answer Area

What is the current status of Exchange Online and SharePoint Online?

When is the earliest date that a post-incident review will be available for SharePoint Online?

Answer Area

What is the current status of Exchange Online and SharePoint Online?

SharePoint Online is available. Exchange Online is available, but service is degraded.
SharePoint Online is available. Issues with the Exchange Online service are under investigation.
The SharePoint Online subscription is expired. The Exchange Online subscription will expire soo
The SharePoint Online subscription is expired. Issues with the Exchange Online service are unde

When is the earliest date that a post-incident review will be available for SharePoint Online?

November 13
November 21
November 30
December 1

Answer:

Answer Area

What is the current status of Exchange Online and SharePoint Online?

SharePoint Online is available. Exchange Online is available, but service is degraded.
SharePoint Online is available. Issues with the Exchange Online service are under investigation.
The SharePoint Online subscription is expired. The Exchange Online subscription will expire soo
The SharePoint Online subscription is expired. Issues with the Exchange Online service are unde

When is the earliest date that a post-incident review will be available for SharePoint Online?

November 13
November 21
November 30
December 1

You can log in to Office 365 as an Office 365 Administrator and view the Service Health Page to view the status of your Office 365 services. You can use the Service Health Page to view information on the status of your services for the current day or you can select the last 6 days or 30 days for a historical view.
The following icons are used in the Service Health Page:
Microsoft says that they will publish a post-incident review within five business days. Therefore, it is possible that a post-incident review could be issued today.

References:
http://office.microsoft.com/en-in/office365-suite-help/view-the-status-of-your-services-HA102817837.aspx#_Status_icon_descriptions
http://technet.microsoft.com/en-us/library/office-365-service-continuity.aspx

Question: 262

You are the Office 365 administrator for your company.
You must use Windows PowerShell to manage cloud identities in Office 365. You must use a computer that runs Windows 8 to perform the management tasks.
You need to ensure that the Windows 8 computer has the necessary software installed.
What should you install first?

A. Microsoft Office 365 Best Practices Analyzer for Windows PowerShell
B. Windows PowerShell 4.0
C. Remote Server Administration Tools for Windows
D. Microsoft Online Services Sign-in Assistant

Answer: D

Explanation:
Cloud identities in Office 365 are user accounts in Azure Active Directory.
You can use Windows PowerShell to administer Office 365 and Azure Active Directory. However, the default installation of Windows PowerShell on Windows 8 (or any other version of Windows) does not include the PowerShell cmdlets required to manage Office 365 or Azure Active Directory.
You need to install the PowerShell module that includes the necessary cmdlets for managing Azure Active Directory. This module is the Windows Azure Active Directory Module for Windows PowerShell module. This module also requires that Microsoft .NET Framework 3.5 is installed and enabled.
Before the Windows Azure Active Directory Module for Windows PowerShell, can be installed, the Microsoft Online Services Sign-in Assistant must be installed. This will allow you to connect to your Office 365/Azure subscription from a PowerShell session on a remote computer.

Question: 263

You are the Office 365 administrator for your company.
Users report that they have received significantly more spam messages over the past month than they normally receive.
You need to analyze trends for the email messages received over the past 60 days.
From the Office 365 admin center, what should you view?

A. The Mail protection reports
B. The Mailbox content search and hold report
C. Messages on the Message center page
D. The Office 365 Malware detections in sent mail report

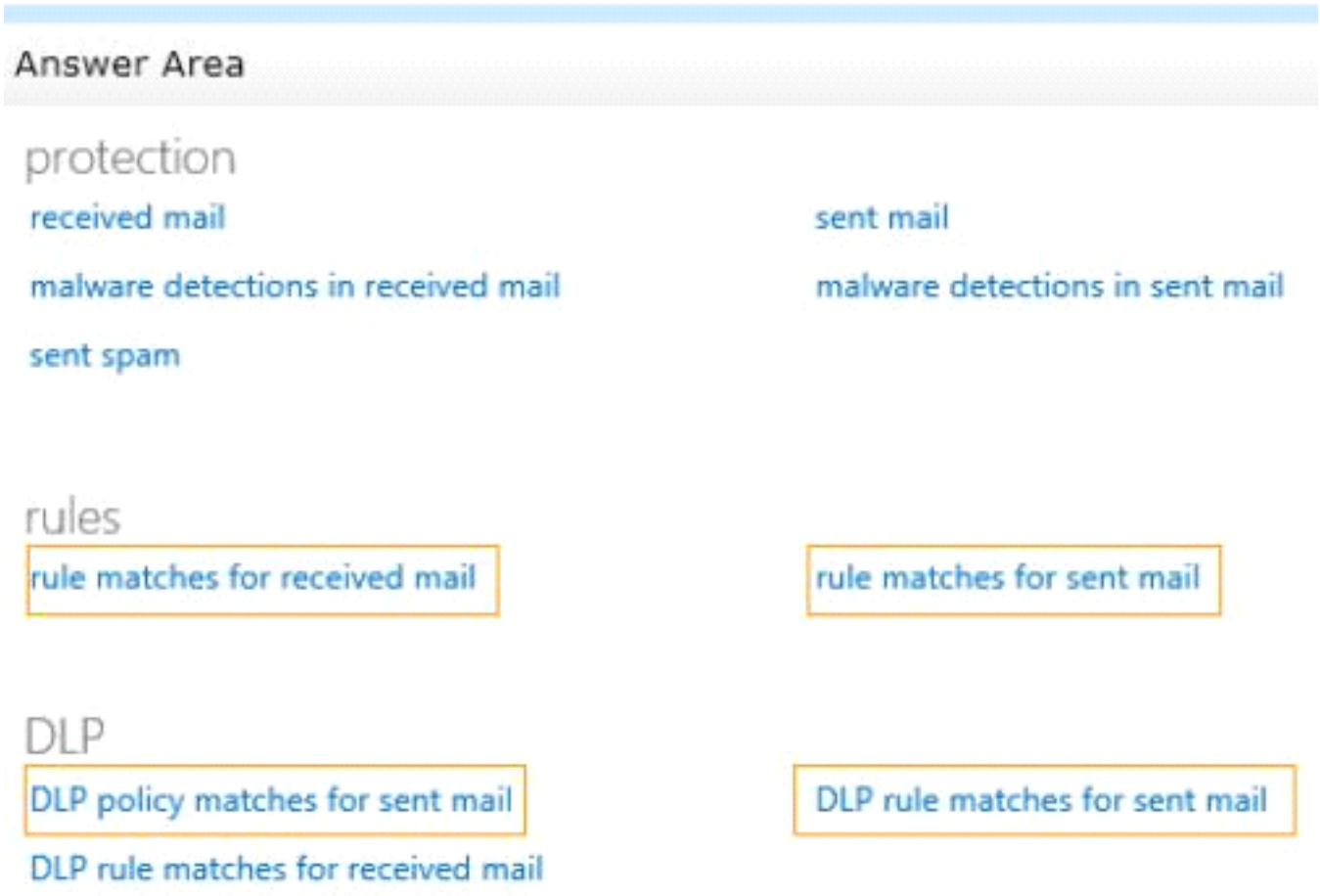
Answer: A

Explanation:
An Office 365administrator can use the Mail Protection Reports in Office 365 to view data about malware, spam, and rule detections for up to the last 90 days.
The reports can be viewed as a graph to display trends for email messages over a period of time; in this question, for

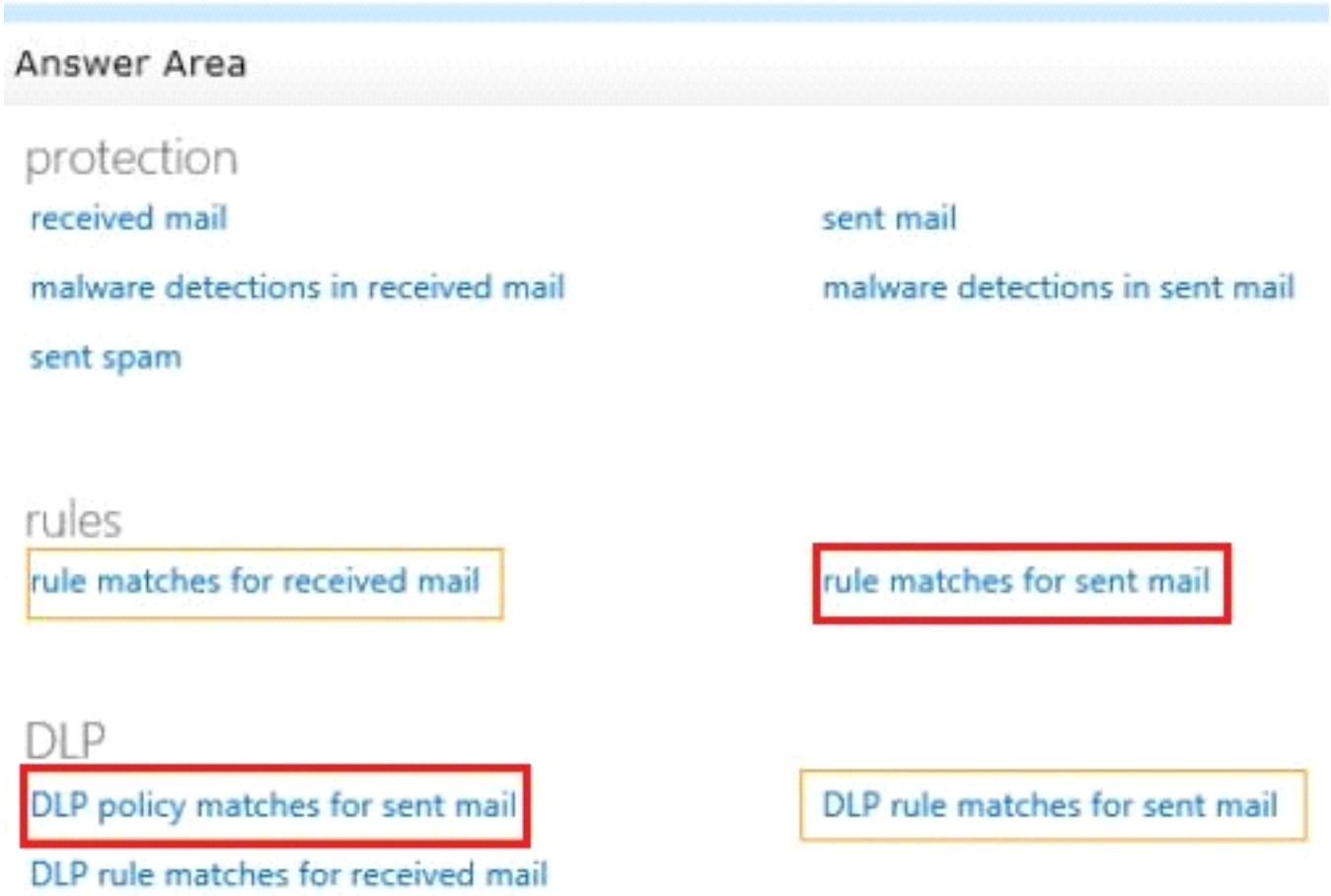
the last 60 days. The graph view will tell you if the amount of good mail, malware and spam detected has increased or decreased over the time period of the report.
References:
https://technet.microsoft.com/en-us/library/dn500744(v=exchg.150).aspx

Question: 264

HOTSPOT
The legal department in your organization creates standardized disclaimers for all of their email messages. The disclaimers explain that any transmissions that are received in error should be reported back to the sender. You track any confidential documents that are attached to email messages.
Your security team reports that an employee may have mistakenly sent an email message that contained confidential information.
You need to identify whether the email message included the disclaimer and whether it contained confidential information.
Which two options should you configure? To answer, select the appropriate objects in the answer area.



Answer:



DLP stands for DataLossPrevention. A DLP policy is used to define exactly what constitutes a confidential email. For example: any email that has a credit card number of bank account number would be deemed to be confidential.
The DLP policy matches for sent mail report is used to display which emails contained content that matched a condition defined in a DLP policy. The DLP policy matches for sent mail report can be downloaded as a table that lists every single email that matched a DLP policy. This would identify in this question if the email did actually contain confidential information.
To identify whether the email message included the disclaimer, we need to view the "rule matches for sent mail" report. The disclaimer is added to an email by a transport rule. The rule defines which emails should have the disclaimer appended. A common example of this is all email sent to recipients outside the organization. By viewing the rule matches for sent mail, we can verify if the email in this question did match a rule and therefore did have the disclaimer appended.

Question: 265

You are the Office 365 administrator for your company. You have a workstation that runs Windows 8.
You need to install the prerequisite components so that you can view mail protection reports on the workstation.
Which two items must you install? Each correct answer presents part of the solution.

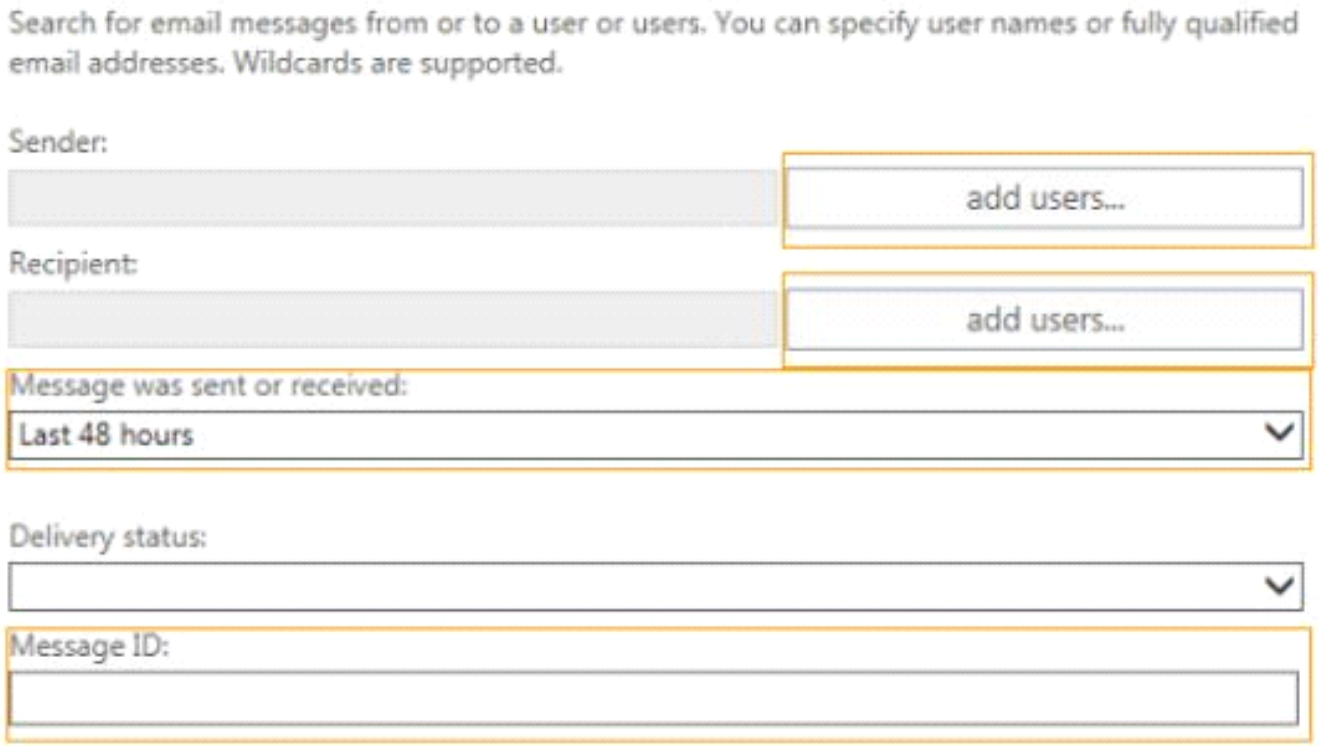
A. SQL Server Analysis Services
B. Microsoft Connectivity Analyzer Tool
C. Microsoft Access 2013
D. .NET Framework 4.5
E. Microsoft Excel 2013

Answer: D,E

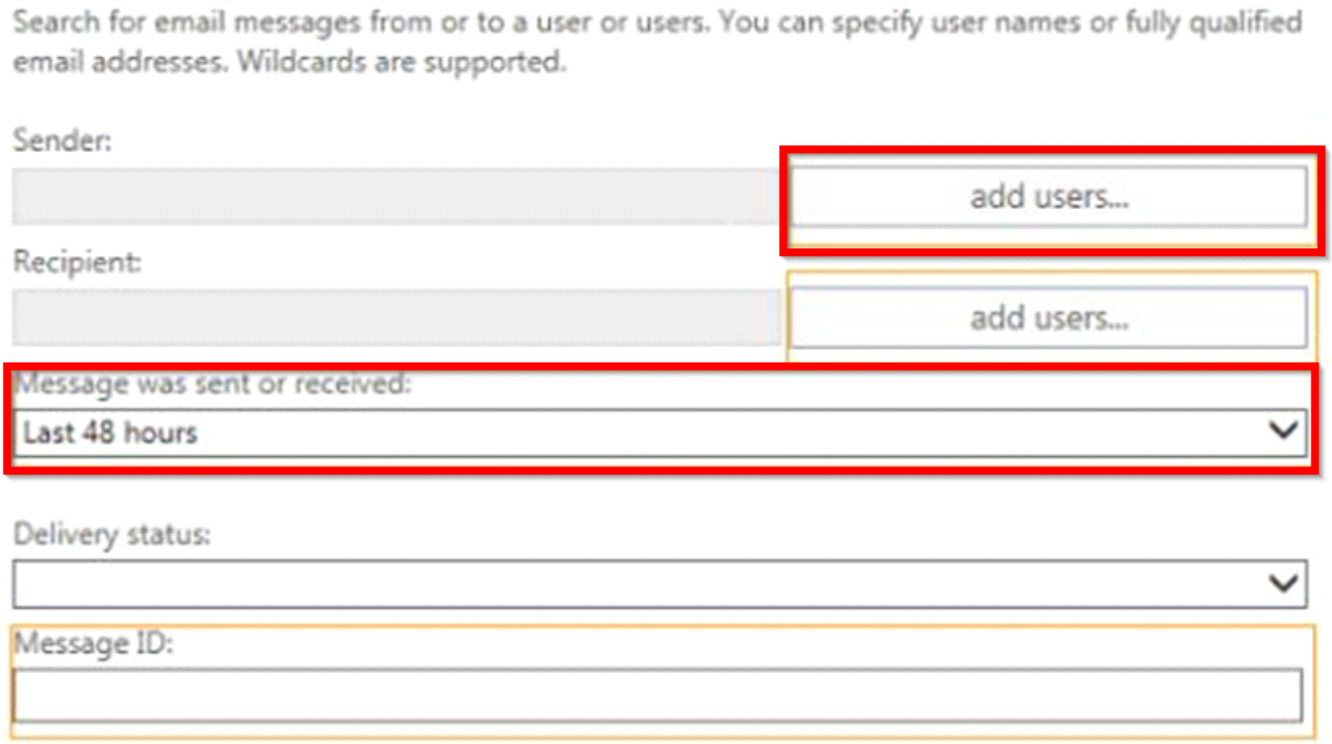
Explanation:
To view the Mail Protection Reports for Office 365 on your computer, you need to install the "Microsoft Excel plugin for Exchange Online Reporting" component which is a free download from Microsoft.
The "Microsoft Excel plugin for Exchange Online Reporting" component has the following system requirements:
Supported Operating System:
Windows 7, Windows 8, Windows Server 2008
Required Software:
Microsoft Office Excel 2013
Additional Requirements:
Microsoft .NET Framework 4.5
Microsoft Online Services Sign-In Assistant (for Exchange Online Protection customers only)
An Office 365 subscription that contains Exchange Online or Exchange Online Protection
Email address you use to sign in to Office 365

Question: 266

HOTSPOT
You are the Exchange Online administrator for an organization. The organization migrates all users to Exchange Online. An employee works for a partner organization named Contoso, Ltd. The employee uses the email alias employeel@contoso.com.
Users report that over the past week, they have not received email messages from employeel@contoso.com.
You need to trace email messages that originate from employeel@contoso.com to users inside your organization.
In the message trace window, which two settings should you configure? To answer, select the appropriate objects in the answer area.



Answer:



None of the fields in the Message Tracking window arec ompulsory.
In this question, the users have not received emails from employeel@contoso.com for the last week. To view tracking information for emails from employeel@contoso.com for the last week, we need to add employeel@contoso.com asa sender. For a sender outside the organization, you can manually type in the email address.
The default search period is 48 hours. To view one week's worth of tracking data, we need to change the search period to 7 days.

Question: 267

An organization with an Active Directory Domain Services (AD DS) domain migrates to Office 365. You need to manage Office 365 from a domain-joined Windows Server 2012 Core server.
Which three components should you install? Each answer presents part of the solution.

A. Azure Active Directory module for Windows PowerShell
B. Microsoft .NET Framework 3.5
C. Microsoft Office 365 Integration Module for Windows Small Business Server 2011 Essentials
D. Microsoft .NET Framework 4.0
E. Microsoft Online Services Sign-in Assistant
F. Rights Management module for Windows PowerShell

Answer: A,B,E

Explanation:
You can use Windows PowerShell to administer Office 365 and Azure Active Directory. However, the default installation of Windows PowerShell on Windows Server 2012 (or any other version of Windows) does not include the PowerShell cmdlets required to manage Office 365 or Azure Active Directory.
You need to install the PowerShell module that includes the necessary cmdlets for managing Azure Active Directory. This module is the Windows Azure Active Directory Module for Windows PowerShell module. This module also requires that Microsoft .NET Framework 3.5 is installed and enabled.
Before the Windows Azure Active Directory Module for Windows PowerShell, can be installed, the Microsoft Online Services Sign-in Assistant must be installed. This will allow you to connect to your Office 365/Azure subscription from

a PowerShell session on a remote computer.

Question: 268

An organization migrates to Office 365.
The Office 365 administrator must be notified when Office 365 maintenance activities are planned.
You need to configure the administrator's computer to receive the notifications.
What should you configure?

A. Office 365 Management Pack for System Center Operations Manager
B. Service requests
C. Service health page
D. Office 365 Service Health RSS Notifications feed

Answer: D

Explanation:
You can log in to Office 365 as an Office 365 Administrator and view the Service Health Page to view the status of your Office 365 services. You can use the Service Health Page to view information on the status of your services for the current day or you can select the last 6 days or 30 days for a historical view.
In the top right corner of the Service Health page, there is an RSS icon. You can click on the RSS icon to sign up for the service health RSS feed, which will email you when a new event is added or an existing event is updated.
References:
http://technet.microsoft.com/en-us/library/office-365-service-health.aspx

Question: 269

Your company deploys an Office 365 tenant.
You need to ensure that you can view service health and maintenance reports for the past seven days.
What are two possible ways to achieve this goal? Each correct answer presents a complete solution.

A. Run the Microsoft Online Services Diagnostics and Logging (MOSDAL) Support Kit.
B. View the service health current status page of the Office 365 admin center.
C. View the service settings page of the Office 365 admin center.
D. Subscribe to the Office 365 Service Health RSS Notifications feed.

Answer: B,D

Explanation:
You can log into Office 365 as an Office365Administrator and view the Service Health Page to view the status of your Office 365 services. You can use the Service Health Page to view information on the status of your services for the current day or you can select the previous 6 days or 30 days for a historical view.
The following icons are used in the Service Health Page:
A plain green tick indicates that the service is available and there have been no incidents during the reported time period.
A grey question mark in a circle indicates that a potential issue is currently under investigation.
A plain green tick with a plus sign indicates that a reported issue was a false positive.
A white down arrow in a red circle indicates that the service is offline.
A white up arrow in an orange circle indicates that a service incident is currently being resolved.
A white right-facing arrow in an orange circle indicates that the service is degraded.

A white exclamation mark in a blue circle indicates that there was an incident during a previous day and that more information is displayed in the Today column.
A white square indicates that a post incident report has been published.
In the top right corner of the Service Health page, there is an RSS icon. You can click on the RSS icon to sign up for the service health RSS feed, which will email you when a new event is added or an existing event is updated.

Question: 270

You are the Office 365 administrator for your company.
Users report that they have received significantly more spam messages over the past month than they normally receive.
You need to analyze trends for the email messages received over the past 60 days.
From the Office 365 admin center, what should you view?

A. Messages on the Service health page
B. The Received mail report
C. The Office 365Malware detections in sent mail report
D. The Mailbox content search and hold report

Answer: B

Explanation:
An Office 365 administrator can use the Mail Protection Reports in Office 365to view data about malware, spam, and rule detections for up to the last 90 days.
The reports can be viewed as a graph to display trends for email messages over a period of time; in this question, for the last 60 days. The graph view will tell you if the amount of good mail, malware and spam detected has increased or decreased over the time period of the report.
The Received Mail report shows the received mail grouped by traffic type:
Good mail – messages that were received and not identified as spam or malware.
Spam – messages identified as spam.
Malware – messages that contained malware.
Transport rules – messages that matched at least one rule.
References:
https://technet.microsoft.com/en-us/library/dn500744(v=exchg.150).aspx

Question: 271

A company deploys an Office 365 tenant in a hybrid configuration with Exchange Server 2016.
Office 365 users cannot see free/busy information that is published from the on-premises Exchange Server. In addition, Exchange Server users cannot see free/busy information that is published from Office 365.
You need to troubleshoot why users cannot access free/busy information from both Office 365 and Server 2016.
Which tool should you run?

A. the Hybrid Configuration wizard
B. the Remote Connectivity Analyzer with the Exchange Server tab selected
C. the Microsoft Connectivity Analyzer Tool
D. the Remote Connectivity Analyzer with the Office 365 tab selected

Answer: D

Explanation:
Microsoft Remote Connectivity Analyzer is a website offered by Microsoft for testing remote connectivity to server services such as Exchange Server, Skype for Business Server and Office 365.
The Office 365 tab on the Remote Connectivity Analyzer has several options for performing different tests regarding Office 365 connectivity. These tests include:
Office 365 General Tests
Microsoft Exchange ActiveSync Connectivity Tests
Microsoft Exchange Web Services Connectivity Tests
Microsoft Office Outlook Connectivity Tests
Internet Email Tests
Mail Flow Configuration
Free/Busy Test
The description given for the Free/Busy test is as follows:
"This test verifies that an Office365 mailbox can access the free/busy information of an on-premises mailbox, and vice versa (one direction per test run)."

Question: 272

You are the Office 365 administrator for your company. You configure new user accounts for User1 and User2. User1 has an on-premises mailbox. User2 has an Office 365 mailbox.
Each user must be able to view the availability of the other user.
You need to ascertain whether users can share their free/busy information.
What should you use?

A. Transport Reliability IP Probe (TRIPP Tool)
B. Microsoft Remote Connectivity Analyzer Tool
C. Business Connectivity Services
D. Windows Azure Active Directory Rights Management

Answer: B

Explanation:
Microsoft Remote Connectivity Analyzer is a website offered by Microsoft for testing remote connectivity to server services such as Exchange Server, Skype for Business Server and Office 365. In this question, we need to run the Free/Busy test in the Microsoft Remote Connectivity Analyzer website.
The Office 365 tab on the Remote Connectivity Analyzer has several options for performing different tests regarding Office 365 connectivity. These tests include:
Office 365 General Tests
Microsoft Exchange ActiveSync Connectivity Tests
Microsoft Exchange Web Services Connectivity Tests
Microsoft Office Outlook Connectivity Tests
Internet Email Tests
Mail Flow Configuration
Free/Busy Test
The description given for the Free/Busy test is as follows:
"This test verifies that an Office 365 mailbox can access the free/busy information of an on-premises mailbox, and vice versa (one direction per test run)."

Question: 273

Your company has an Office 365 subscription. The network contains an Active Directory domain. You configure single sign-on for all users.
You need to verify that single sign-on functions for the users who access Office 365 from the Internet.
What should you run?

A. the Get-MSOLFederationProperty cmdlet
B. the Test-OrganizationRelationship cmdlet
C. the Microsoft Remote Connectivity Analyzer
D. the Microsoft Exchange Server Deployment Assistant

Answer: C

Explanation:
Microsoft Remote Connectivity Analyzer is a website offered by Microsoft for testing remote connectivity to server services such as Exchange Server, Skype for Business Server and Office 365.
The Office 365 tab on the Remote Connectivity Analyzer has several options for performing
different tests regarding Office 365 connectivity. These tests include:

Office 365 General Tests
Microsoft Exchange ActiveSync Connectivity Tests
Microsoft Exchange Web Services Connectivity Tests
Microsoft Office Outlook Connectivity Tests
Internet Email Tests
Mail Flow Configuration
Free/Busy Test
The Office 365 General Tests section includes the following tests:
Office 365 Exchange Domain Server (DNS) Connectivity Test
Office 365 Lync Domain Server (DNS) Connectivity Test
Office 365 Single Sign-OnTest

The description for the Single Sign-OnTest is as follows:
"This test will validate your ability to log on to Office 365 with your on-premises credentials. It also validates some basic Active Directory Federated Services (AD FS) configuration."
This test will meet the requirement in this question of verifying that single sign-on functions for the users who access Office 365 from the Internet.

Question: 274

You are the Office 365 administrator for your company.
Users report that they cannot sign in to Skype for Business from their mobile devices, but they are able to send and receive Skype for Business messages by using their laptop computers.
You need to troubleshoot the issue.
What should you do?

A. From the Office 365 message center, confirm Skype for Business settings.
B. Use the Microsoft Connectivity Analyzer tool to confirm settings.
C. Confirm Skype for Business user licenses for the affected users.
D. From the Skype for Business admin center, verify the external access settings.

Answer: B

Explanation:
The Microsoft Connectivity Analyzer (MCA) tool is a companion to the Microsoft Remote Connectivity Analyzer web site. The MCA tool provides administrators and end users with the ability to run connectivity diagnostics for five common connectivity symptoms directly from their local computer.
One of the five symptoms that can be tested using MCA is:
"I can't log on to Skype for Business on my mobile device or the Skype for Business Windows Store App" – This test checks for the Domain Name Server (DNS) records for your on-premise domain to ensure they are configured correctly for supporting Mobile Skype for Business clients. Also it connects to the Autodiscover web service and makes sure that the authentication, certificate, web service for Mobility is correctly set up.