Question 1
Which cmdlet should you use?
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
Correct Answer: D
Explanation/Reference:
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 [email protected]

Question 2
Which tool should you use?
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 the 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
Correct Answer: B
Explanation/Reference:
The Microsoft Connectivity Analyzer Tool includes multiple different tests that can be run online.

Question 3
Which two settings should you configure?
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 [email protected] Users report that over the past week, they have not received email messages from [email protected] You need to trace email messages that originate from [email protected] 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.
Hot Area:
As we want to trace the emails originated from [email protected] we must specify him as the sender. We also know that email messages from this user have not been received for the last 7 days. We should therefore change the start date and put it back 7 days.

References:

Question 4
Which Windows PowerShell command should you run?
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-MailboxActivityReport-Expression
B. Get-StaleMailboxReport-StartDate
C. Get-MailboxActivityReport-StartDate
D. Get-StaleMailboxReport-Organization

Correct Answer: B
Explanation/Reference:
Explanation:
Use the Get-StaleMailboxDetailReport cmdlet to view mailboxes that haven’t been accessed for at least 30 days. The StartDate parameter specifies the date to start the search.
start date of the date range.

References:

**Question 5**
What are two possible ways to achieve this goal?
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.

Correct Answer: AD

Explanation/Reference:
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 RSS feed, 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-b938-6e44e88e33b0

**Question 6**
HOTSPOT
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.
Hot Area:

**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

Correct Answer:
Box 1: 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.


Question 7
What should you do?

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.

Select and Place:

Correct Answer:
**Question 8**

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 [email protected]
B. In the Office 365 admin center, create a user named [email protected]
C. In Active Directory Domain Services Users and Computers, create a user named [email protected]
D. In Active Directory Domain Services Users and Computers, create a user named [email protected]

Correct Answer: A

**Explanation/Reference:**

One of the first steps is to create SPO administrative account. You should always plan to create this account as Cloud ID, E.g. [email protected] Having this as Cloud ID, it allows you to access your tenant even if On-Premises AD FS 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 9**

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.

Correct Answer: C

**Explanation/Reference:**

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.

**PROBLEM**

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**

---

Question 10
Which three actions should you perform to ensure users excluded from migration are not synchronized?

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.

Correct Answer: BCD

Explanation/Reference:

D: With filtering, you can control which objects should appear in Azure AD from your on-premises directory. For example, you can create a filter to exclude 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://support.microsoft.com/en-us/kb/3061396

Question 11
What should you do?

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.

Correct Answer: A

Explanation/Reference:

To force a full sync with the Azure AD Connect tool from Windows PowerShell, run the following command:

```
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 12
Does this meet the goal?

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 can use the Convert-MsolDomainToFederated cmdlet. Does this meet the goal?

A. Yes
B. No

Correct Answer: A

Explanation/Reference:

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 and the Azure AD domain. 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:

Question 13
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

Does this meet the goal?
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
Correct Answer: A
Explanation/Reference:
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 and Microsoft Azure Active Directory. Due to domain verification requirements, you may need to run this cmdlet several times inorder to complete the process of adding the new single sign-on domain.
References:

Question 14
Does this meet the goal?
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
Correct Answer: B
Explanation/Reference:
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).

Question 15
Does this meet the goal?
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 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
Correct Answer: A
Explanation/Reference:
Explanation:
Azure AD Connect sync Staging mode can be used for several scenarios, including:
* High availability.
* Test and deploy new configuration changes.
* Introducte 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 16
Does this meet the goal?
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

Correct Answer: B

Explanation/Reference:

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/
need to enable the uses 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.

**Correct Answer:**

- Initially, open the Microsoft Azure Active Directory Module.
- Run `Get-Credential`. When the cmdlet prompts you for credentials, type your cloud service administrator account credentials.
- Run `Connect-MsolService -Credential $cred`. This cmdlet connects you to Azure AD. Creating a context that connects you to Azure AD is required before running any of the additional cmdlets installed by the tool.
- Run `Set-MsolAdfscontext -Computer $computer`, where `$computer` is the internal FQDN name of the primary AD FS server. This cmdlet creates a context that connects you to AD FS.
- Run `Convert-MsolDomainToFederated -DomainName $domainName`, where `$domainName` is the domain to be converted. This cmdlet changes the domain from standard authentication to single sign-on.

**References:**

**Question 19**

Which Windows PowerShell cmdlet should you run?

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
Question 20
Which Windows PowerShell cmdlet should you run?
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

Correct Answer: A
Explanation/Reference:
Explanation:
The Set-MsolUser cmdlet is used to update a user object. This cmdlet should be used for basic properties only.
Parameter -PasswordNeverExpires
Sets whether or not the user’s password will expire periodically.

References:

Question 21
Which tool should you run?
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)

Correct Answer: A
Explanation/Reference:
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 userPrincipalName (UPN), mailNickname, proxyAddress, sAMAccountName, targetAddress, and others. The IdFix tool also provides assistance for migrating from a non-routable name (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.

Question 22
What should you do?
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 split bar between panes or scroll to view content.

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 nameserver (or NS) records at your domain registrar to point to the Office 365 primary and secondary nameservers.

* Use (A) DNS record for the web site.

**Explanation/Reference:**

When you change your domain’s nameserver (NS) records, you are updating the DNS records to point to the Office 365 nameservers instead of your current nameservers. This step is necessary to allow Office 365 to manage your domain's DNS records.

**References:**

* Change your domain’s nameserver (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 nameserver (or NS) records at your domain registrar to point to the Office 365 primary and secondary nameservers.

**Question 23**

Which Windows PowerShell command should you run?

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

Correct Answer: D

**Explanation/Reference:**

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 enddate of the date range.

**References:**

* Question 24*

What should you do?

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.
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.

References:

Question 25
Which versions of each product should you implement?
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 4.5.1
D. .Net 4.5.2
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
Correct Answer: DF

Explanation/Reference:

* 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 100,000 objects. This is fine for the scenario in this question.

If you need to manage 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.

References:

**Question 26**
Which Windows PowerShell cmdlet should you run?
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

Correct Answer: D

Explanation/Reference:

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 [email protected] to [email protected]
Set-MsolUserPrincipalName -UserPrincipalName [email protected] -NewUserPrincipalName [email protected]

References:

**Question 27**
Which two name resolution strategies can you use?
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

Correct Answer: AB

Explanation/Reference:

Configure Name Resolution for Federation Server Proxy in a DNS Zone That Serves Only the Perimeter Network
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:

**Question 28**
Which report solution should you choose?
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

Correct Answer: D

Explanation/Reference:

The Office 365 Reporting web service enables developers to integrate information on email and spam, antivirus activity, compliance status, and Lync Online activities into their custom service reporting applications and web portals.

References:
Question 29
Which three actions should you perform in sequence?

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:
1. two servers named Server1 and Server2
2. a partner collaboration website for the domain contoso.com that points to a SharePoint Online team site
3. 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.

Select and Place:

Correct Answer:

Explanation/Reference:
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 server farm.
/ The parameter -CertificateThumbprint
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
Specifies the DNS name 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.

Question 30
When each type of data will be deleted.
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.
Hot Area:

<table>
<thead>
<tr>
<th>Timeframe</th>
<th>User1 Exchange Online mailbox</th>
<th>Documents Created by User1 on SharePoint Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never removed</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Removed immediately</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Removed after 30-day grace period</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Removed after 90-day grace period</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

Correct Answer:

Explanation/Reference:
* 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://support.office.com/en-sg/article/View-restore-or-delete-items-in-the-Recycle-Bin-of-a-SharePoint-site-6df466b6-53f2-4898-bd6e-c0df851d8be

Question 31
Which Windows PowerShell command should you run?
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 Active Directory Synchronization Services (AAD Sync) 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

Correct Answer: A

Explanation/Reference:
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:
**Question 32**
What are two possible ways to achieve this goal?
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.

Correct Answer: AB
Explanation/Reference:

**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.

References:

**Question 33**
What should you view?
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

Correct Answer: A
Explanation/Reference:

**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.

References:

**Question 34**
Which tool should you use?

Correct Answer: A
Explanation/Reference:

**Explanation:**
Office 365 includes Lync 2013. With this latest version of the Microsoft Lync Server 2010 and 2013 Bandwidth Calculator, you can enter information about your users and the Lync 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 Lync client real-time traffic.

References:

**Question 35**
Which two passwords can you use?
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.


Correct Answer: AG
Explanation/Reference:

**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.

**Question 36**
**HOTSPOT**
**HOTSPOT**
You manage an Office 365 tenant. The subscription details for the tenant are displayed in the following screenshot.

![Office 365 Subscription Details](image)

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

For each user, what is the maximum number of devices on which you can install Microsoft Office?

<table>
<thead>
<tr>
<th>Number of Devices</th>
<th>Incorrect</th>
<th>Correct</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Which services does the tenant have licensing rights to use?

<table>
<thead>
<tr>
<th>Service</th>
<th>Incorrect</th>
<th>Correct</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange and SharePoint</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange and Skype for Business</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange, SharePoint, and Yammer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange, SharePoint, Skype for Business, and Yammer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Maximum Number of User Accounts</th>
<th>Incorrect</th>
<th>Correct</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>200</td>
<td></td>
<td></td>
</tr>
<tr>
<td>300</td>
<td></td>
<td></td>
</tr>
<tr>
<td>400</td>
<td></td>
<td></td>
</tr>
<tr>
<td>500</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Correct Answer:**

For each user, what is the maximum number of devices on which you can install Microsoft Office?

- 5

Which services does the tenant have licensing rights to use?

- Exchange, SharePoint, Skype for Business, and Yammer

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

- 500

**Explanation/Reference:**

Office 365 Business Premium

- 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 365 Small Business Premium supports a maximum of 300 users

**Question 37**
What should you do?
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.

Correct Answer: A

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

References:

Question 38

Which two permission levels should you assign to the account for each task?

HOTSPOT

A company plans to synchronize users in an existing Active Directory organizational unit with Office 365. You must configure the Azure Active Directory Synchronization (AAD Sync) tool 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.

Hot Area:

Correct Answer:

Explanation/Reference:
* 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:
Replicating Directory Changes Replicating Directory Changes All

References:
Which Windows PowerShell cmdlet should you run?

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

Correct Answer: E

Explanation/Reference:
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 with the 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:

Question 40
Which settings should you use?

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

Correct Answer: C

Explanation/Reference:

For Office 365 for business, use the following settings.

IMAP4 outlook.office365.com
993 implicit

References:

Question 41
What should you do?

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 90 days 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.

Correct Answer: B

Explanation/Reference:

After you’ve verified that 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:

Question 42
Which report solution should you choose?

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

Correct Answer: B

Explanation/Reference:

The Office 365 Reporting web service enables developers to integrate information on email and spam, antivirus activity, compliance status, and Lync 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.
cmdlets, are accessible using the Reporting web service.

References:

Question 43
Which Windows PowerShell cmdlet should you run?
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

Correct Answer: E
Explanation/Reference:
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.
References:

Question 44
Which Windows PowerShell cmdlet should you run?
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

Correct Answer: C
Explanation/Reference:
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 [email protected] -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:

Question 45
Which Windows PowerShell cmdlet should you run?
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

Correct Answer: A
Explanation/Reference:
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 [email protected] -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 policies 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.
References:
Question 46
Which four actions should you perform in sequence?

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.

Select and Place:

Correct Answer:

Explanation/Reference:
Note:
Prepare the Base Servers Box 1, Box 2: AD FS Server
Basebuild the AD FS server with Windows Server 2012
Setup a connection to the internal network
Add the server to the local domain
Once the necessary WAP role services are installed, we are then able to launch the Web Application Proxy Wizard to configure WAP. Note:

- Base Build the AD FS Proxy server with Windows Server 2012
- Setup a connection to the DMZ network (verify connectivity to the AD FS server on port 443)
- DO NOT add the server to the local domain
- Update the server with all Windows Updates

References:

**Question 47**

What should you use?

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 Lync Connectivity Analyzer Tool
B. OCSLogger
C. ClsController
D. Remote Connectivity Analyzer

Correct Answer: C

Explanation/Reference:

Centralized Logging Service (CLS) is a new feature in Lync Server 2013. It provides a mechanism to enable/disable logging across all Lync 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, AudioVideoConferencing, Issue, HybridVoice, IncomingAndOutgoingCall, VoiceMail, IMAndPresence, AddressBook, DeviceUpdate, LYSSAndUCS, CLS, SP, WAC, UserReplicator, HostedMigration, MonitoringAndArchiving, LILRLYSS, MeetingJoin, RGS, CPS, XMPP, and CAA.

References:

**Question 48**

What should you use?

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

Correct Answer: C

Explanation/Reference:

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

References:

**Question 49**

Which Windows PowerShell command should you run?

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-Organization
C. Get-MailboxActivityReport-Expression
D. Get-MailboxActivityReport-EndDate

Correct Answer: A

Explanation/Reference:

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

References:

**Question 50**

What should you do?

**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.

Select and Place:
**Question 51**
Which tool should you run?
A company deploys an Office 365 tenant in a hybrid configuration with Exchange Server 2013. 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 Exchange Server 2013. 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

Correct Answer: D
Explanation/Reference:
Microsoft Remote Connectivity Analyzer is a website offered by Microsoft for testing remote connectivity to server services such as Exchange Server, Lync 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 52**
What should you use?
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. BusinessConnectivity Services
D. Windows Azure Active Directory Rights Management

Correct Answer: B
Explanation/Reference:
Microsoft Remote Connectivity Analyzer is a website offered by Microsoft for testing remote connectivity to server services such as Exchange Server, Lync 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 53
What should you run?
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

Correct Answer: C
Explanation/Reference:
Explanation:
Microsoft Remote Connectivity Analyzer is a website offered by Microsoft for testing remote connectivity to server services such as Exchange Server, Lync 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-On Test

The description for the Single Sign-On Test 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 54
What should you do?
You are the Office 365 administrator for your company. Users report that they cannot sign in to Lync from their mobile devices, but they are able to send and receive Lync messages by using their laptop computers.

You need to troubleshoot the issue. What should you do?
A. From the Office 365 message center, confirm Lync settings.
B. Use the Microsoft Connectivity Analyzer tool to confirm settings.
C. Confirm Lync user licenses for the affected users.
D. From the Lync admin center, verify the external access settings.

Correct Answer: B
Explanation/Reference:
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 log on to Lync on my mobile device or the Lync 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 Lync clients. Also it connects to the Autodiscover web service and makes sure that the authentication, certificate, web service for Mobility is correctly set up.

Question 55
Which three components should you install?
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. Windows 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

Correct Answer: AB
Explanation/Reference:
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 56
What should you configure?
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 ManagementPack for System Center Operations Manager
B. Service requests
C. Service health page
D. Office 365 Service Health RSS Notifications feed

Correct Answer: D
Explanation/Reference:
Explanation:
You can log in to Office 365 as an Office 365 Administrator and view the Service Health Page to view information on 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 57
What are two possible ways to achieve this goal?
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 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.

Correct Answer: BD
Explanation/Reference:
Explanation:
You can log in to Office 365 as an Office 365 Administrator and view the Service Health Page to view information on 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 58
What should you view?
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 365 Malware detections in sent mail report
D. The Mailbox content search and hold report

Correct Answer: B
Explanation/Reference:
Explanation:
An Office 365 administrator 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 past 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.

**Question 59**
Which two options should you configure?

**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.

**Explanation/Reference:**
DLP stands for Data Loss Prevention. A DLP policy is used to define exactly what constitutes a confidential email. For example: any email that has a credit card number or 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 60**
Which two items must you install?
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

**Correct Answer:** DE

**Explanation/Reference:**

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:
- 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 61
Which two settings should you configure?
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 [email protected]
Users report that over the past week, they have not received email messages from [email protected] You need to trace email messages that originate from [email protected] 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.
Hot Area:

Correct Answer:

Explanation/Reference:
None of the fields in the Message Tracking window are compulsory.
In this question, the users have not received emails from [email protected] for the last week. To view tracking information for emails from [email protected] for the last week, we need to add [email protected] as a 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 62
Which pages should you customize?
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.
Select and Place:
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 63
HOTSPOT
HOTSPOT
An organization deploys an Office 365 tenant.
The Service health page displays the following information:

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.

Correct Answer:
Explanation/Reference:
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:
- 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 an orange 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.
- A white tick in a green square indicates that an incident was active earlier today, but service has been restored.

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:

Question 64
What should you install first?
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

Correct Answer: D
Explanation/Reference:
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 65
What should you view?
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

Correct Answer: A
Explanation/Reference:
An Office 365 administrator 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.

Question 66
Which two roles should you install and configure?

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

Correct Answer: AB

Explanation/Reference:
The Active Directory Federation Services role and the Web Server Role (IIS) role are required for setting up an AD FS proxy server.
References:

Question 67
Which name should you specify?

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:

<table>
<thead>
<tr>
<th>Description</th>
<th>Fully Qualified Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster DNS Name</td>
<td>fs.fabrikam.com</td>
</tr>
<tr>
<td>Server node in cluster</td>
<td>server1.fabrikam.com</td>
</tr>
<tr>
<td>Server node in cluster</td>
<td>server2.fabrikam.com</td>
</tr>
</tbody>
</table>

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.fabrikam.com
B. server1.fabrikam.com
C. fabrikam.com
D. server2.fabrikam.com

Correct Answer: A

Explanation/Reference:
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.fabrikam.com, we are using it for AD FS, and we must use it in the subject name for the certificate.

Question 68
What should you do?

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.

Correct Answer: A

Explanation/Reference:

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 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 69

Which three actions should you perform in sequence?

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.

Select and Place:

Correct Answer:

Explanation/Reference:

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 70
Which two actions should you perform?
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.
B. Run the Windows PowerShell cmdlet Enable-ADFSFederated.
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.

Correct Answer: CF
Explanation/Reference:
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.

Question 71
What should you do?
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 FS1 and FS2, add the cluster NetBIOS name and IP address of the federation server farm to the LMHOSTS file.

Correct Answer: A
Explanation/Reference:
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.

Question 72
What should you do?
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.

Correct Answer: D
Explanation/Reference:
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 73
What should you do?
HOTSPOT
An organization has over 10,000 users and uses a SQL-based Active Directory Federation Services (AD FS) 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.
Hot Area:
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:

**Question 74**
Which port should you open?
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

Correct Answer: D
Explanation/Reference:
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 75**
How many servers should you deploy?
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

Correct Answer: B

Explanation/Reference:

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:

**Question 76**

Which three actions should you perform?
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.
F. Run the Windows Azure Multi-Factor Authentication Server Authentication Configuration Wizard.

Correct Answer: BCF

Explanation/Reference:

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).

**Question 77**

Which two actions should you perform?
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.

Correct Answer: AC

Explanation/Reference:

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 78**

Which certificate types should you assign?

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.
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:

Question 79
What should you install?
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.

Select and Place:
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 2.0 Setup 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:

Question 80
Which two certificates should you install?

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

Correct Answer: AC

Explanation/Reference:
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 81
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.

Correct Answer:
**Question 82**

Which tool should you use?

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  

Correct Answer: D

**Explanation/Reference:**

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 83**

Which three actions should you perform in sequence?

**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.

Select and Place:

Correct Answer:
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 suffix 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 84**

Which user accounts will be synchronized?

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 8 characters  
D. User accounts with a password length of at least 14 characters

Correct Answer: A

**Explanation/Reference:**

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 85**

What should you do?

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:

<table>
<thead>
<tr>
<th>Server</th>
<th>Operating System</th>
<th>Forest Function Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>NYC-DC1</td>
<td>Windows Server 2008 R2</td>
<td>Windows 2000</td>
</tr>
</tbody>
</table>

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 Windows Azure Active Directory Sync tool to synchronize the local Active Directory with Office 365. What should you do? Select the correct action from each list in the answer area.

Hot Area:
Correct Answer:

**Question 86**
Which two actions should you perform?  
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 Windows Azure Active Directory Sync tool.  
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 Framework3.5 SP1 and Microsoft .NET Framework 4.0.  
D. Raise the forest functional level to Windows Server 2008 R2.  
E. Join a workstation to an Active Directory domain.  
Correct Answer: BD  
Explanation/Reference:  
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 365 is Windows Server 2003. We must therefore raise the forest functional level.

**Question 87**
Which Windows PowerShell cmdlet should you use?  
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  
Correct Answer: K  
Explanation/Reference:  
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 $false parameter filters for only users who are not assigned a license.
Question 88
What should you do?
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 the Windows Azure Active Directory Sync tool.
B. In the Windows Azure Active Directory portal, configure OU-based filtering.
C. Configure user attribute-based filtering by using the Windows Azure Active Directory Sync tool.
D. In the Windows Azure Active Directory portal, configure user attribute-based filtering.

Correct Answer: A
Explanation/Reference:
Explanation:
You can use the Windows Azure Active Directory Sync tool 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 89
Which three actions should you perform?
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.

Correct Answer: ACD
Explanation/Reference:
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 90
Which three actions should you perform in sequence?
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 Windows Azure Active Directory Sync tool 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.
Select and Place:

Correct Answer:
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 91
Which Windows PowerShell cmdlet should you run?
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

Correct Answer: D
Explanation/Reference:
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.

Question 92
Which four Windows PowerShell cmdlets should you run in sequence?
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.

Correct Answer:

Box 1. 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. The Get-MsolDomainVerificationDns cmdlet is used to return the DNS records that need to be set to verify a 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. The Set-MsolDomain cmdlet is used to set fabrikam.com as the default domain.

Box 2. Next we need to check the DNS before the domain can be confirmed.

Box 3. Now we can confirm the domain.

Box 4. Next we can set fabrikam.com as the default domain.

Question 93
Which three actions should you perform in sequence?
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.
Select and Place:
Manage Azure AD using Windows PowerShell

You can use the Azure Active Directory Module for Windows PowerShell cmdlets for AzureAD 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 94
Which Windows PowerShell cmdlet should you run?
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

Correct Answer: D
Explanation/Reference:
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`.

Question 95
Which Windows PowerShell cmdlet should you use?
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

Correct Answer: C
Explanation/Reference:
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 Exchange Online. 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 In this command, the 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`

IncorrectAnswers:
A: The Test-OutlookConnectivity cmdlet is used to test end-to-end Microsoft Outlook client connectivity in the Microsoft Exchange Server 2013 organization, but it isn’t used to troubleshoot free/busy issues in a hybrid deployment.
B: The Test-FederationTrust cmdlet is used to verify that the federation trust is properly configured and functioning as expected. It isn’t used to troubleshoot free/busy issues in a hybrid deployment.
C: The Get-OrganizationRelationship cmdlet used to retrieve settings for an organization relationship that has been created for federated sharing with
other federated Exchange organizations or for hybrid deployments with Exchange Online. It isn’t used to troubleshoot free/busy issues in a hybrid deployment.

References:
https://support.microsoft.com/en-us/kb/2555008

Question 96
Which Windows PowerShell command should you run?
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
C. Get-MsolUser -All -UnlicensedUsersOnly | Remove-MsolUser -Force
D. Get-MsolUser -UnlicensedUsersOnly | Remove-MsolUser-Force

Correct Answer: C
Explanation/Reference:
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 –UnlicensedUsersOnly parameters to retrieve all unlicensed users.
Parameters include:
  All [If present, then all results will be returned.]
  UnlicensedUsersOnly [Filter for only users who are not assigned a license.]
Step 2: Remove these users through the Remove-MsolUser -Force command.

Question 97
How should you complete the relevant Windows PowerShell commands?
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 area. 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.
Select and Place:

Correct Answer:

Explanation/Reference:
Box 1: -MsoLicenseOptions
We must create license object. The New-MsoLicenseOptions 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` 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 98**
Which fields must you include in the file?

**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? To answer, drag the appropriate response to each field. Each response 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.

**Hot Area:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Yes</td>
</tr>
<tr>
<td>Display Name</td>
<td>Yes</td>
</tr>
<tr>
<td>First Name</td>
<td>No</td>
</tr>
<tr>
<td>Last Name</td>
<td>No</td>
</tr>
<tr>
<td>Job Title</td>
<td>No</td>
</tr>
</tbody>
</table>

**Correct Answer:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Yes</td>
</tr>
<tr>
<td>Display Name</td>
<td>Yes</td>
</tr>
<tr>
<td>First Name</td>
<td>No</td>
</tr>
<tr>
<td>Last Name</td>
<td>No</td>
</tr>
<tr>
<td>Job Title</td>
<td>No</td>
</tr>
</tbody>
</table>

**Explanation/Reference:**

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 rest of the thing for you. Only the user name and display name are required entries in the CSV file.

**Question 99**
What should you do?

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.

**Correct Answer:** B
Question 100
Which three Windows PowerShell cmdlets should you run in sequence?

Correct Answer:

Get-AaadrmAdminLog
Get-AaadrmRoleBasedAdministrator
Get-AaadrmSuperUser
Get-MsolUser

Step 1: The Import-AaadrmTpd 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-AaadrmService cmdlet connects you to the Azure Rights Management service. This cmdlet can also be used by a partner company that manages your tenant.


References:

Answer Area

Explanation/Reference:
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-AaadrmTpd, then we connect to the service with Connect-AaadrmService, and finally we generate the log with Get-AaadrmAdminLog.

Question 101
Which three actions should you perform in sequence?

Correct Answer:

Get-AaadrmAdminLog
Get-AaadrmRoleBasedAdministrator
Get-AaadrmSuperUser
Get-MsolUser

Step 1: The Import-AaadrmTpd 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-AaadrmService cmdlet connects you to the Azure Rights Management service. This cmdlet can also be used by a partner company that manages your tenant.


References:
Correct Answer: C

Explanation/Reference:
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.

Question 103
Which Windows PowerShell cmdlet should you run?
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

Correct Answer: C
Explanation/Reference:
Explanation:
The Set-MsolUser cmdlet is used to update a user object.
The parameter-PasswordNeverExpires
Sets whether or not the user’s password will expire periodically.
So the command Set-MsolUser -PasswordNeverExpires $true would make the appropriate configuration.

Question 104
Where should you change the value of the department attribute for the employee?
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

Correct Answer: C
Explanation/Reference:
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 105
Which three actions should you perform in sequence?

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.
Select and Place:

Correct Answer:
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 Per Enabled User which is used for Office 365.

Note:
- Per Authentication – purchasing model that charges per authentication. Typically used for scenarios that use 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 their preferred method of verification.

The following methods exist: Mobile Phone Call, Mobile Phone Text Message, Office Phone Call, or Mobile App.

Incorrect Answers:
- The users do not use a single-use password to complete the registration. Instead they can use their mobile phone. This is one of the two notification modes of Azure Multi-Factor Authentication.
- The Per Authentication provider model is not used for Office 365.

References:
- https://msdn.microsoft.com/library/azure/dn376346.aspx#create

Question 106
What should you do?
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.

Correct Answer: D
Explanation:
With AD FS, 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.

Question 107
What should you do?
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 Lync 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.

Select and Place:
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 108
How should you complete the relevant Windows PowerShell command?

**Correct Answer:**

We use Get -MsolUser to get all users. We then enforce strong password complexity to each of these users through StrongPasswordRequired parameter.
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
Sets whether or not the user requires a strong password.

Question 109
How should you complete the relevant Windows PowerShell command?

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.

Correct Answer:

Explanation/Reference:
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 sets the new password for the user.

Question 110
How should you complete the relevant Windows PowerShell command?

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.

Select and Place:
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 for [email protected]. A random password will be generated. The user will be required to reset the password on next sign in.

Set-MsolUserPassword [email protected]

Question 111
What should you do?
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.
Correct Answer: C
Explanation/Reference:
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.
In this case we should use a Mail Recipients rolegroup as we want this group to receive mails.

Question 112
How should you set the policy on the password page of the Office 365 admin center?
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. Select and Place:
Correct Answer:

Explanation/Reference:
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
. Sign in to Office 365 with your work or school account.
. Go to the Office 365 admin center.
. Go to Service settings > Passwords.
. If you don’t want users to have to change passwords, select Passwords never expire. If you select this option, users won’t get any reminders anymore to change their passwords.
. If you want user passwords to expire, type the number of days before the password should expire. Choose a number of days from 14 to 730.
. Type the number of days before users are notified that their password will expire, and then click Save. Choose a number of days from 1 to 30.

References:

Question 113
Which role should you assign?
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

Correct Answer: A

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

Question 114
Which three actions should you perform?
A company deploys an Office 365 tenant. You assign the roles to users as shown in the following table:
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 365 portal as User1.
C. Sign in to the Office 365 portal as User2.
D. Grant User3 administrative permissions in Exchange Online.
E. Assign User3 the global administrator role in Office 365.

Correct Answer: ABD

Explanation/Reference:
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.

Question 115
Which role should you assign?
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

Correct Answer: A
Explanation/Reference:
Explanation:
A: 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.

Question 116
Which administrative role should you configure for each user?
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.

Which administrative role should you configure for each user? Select the correct answer from each list in the answer area.

Hot Area:
Correct 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 cannot 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-cbf8-41ec-b64c-9cfcbef495ac

Question 117
What should you do?

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:

You need to grant the appropriate administrative role to each user.

Select and Place:

Correct Answer:

Explanation/Reference:
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 118
Which four Windows PowerShell cmdlets should you run in sequence?
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.

Select and Place:

Correct Answer:

Explanation/Reference:
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: Import-Module AADRM Connect-AADRMService Enable-AADRM Enable-AADRMSuperUserFeature

References:

Question 119
What should you do?
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.

Correct Answer: A
Explanation/Reference:
A: 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 Test5 version has been changed and Test5 will then have to repair his/her Outlook profile accordingly.
Question 120
Which port or ports should you open?

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

A. inbound TCP 443
B. outbound TCP 5061
C. outbound UDP 3478
D. outbound TCP 443
E. outbound UDP 50000 to outbound UDP 59999
F. inbound TCP 8080

Correct Answer: ACDE
Explanation/Reference:
A. inbound TCP 443 is the port for the Lync for Business client service.
C. outbound UDP 3478 is the UDP port for Lync audio and video sessions.
D. outbound TCP 443 is the port for the Lync 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 Lync audio and video sessions.

Question 121
Which tool should you use?

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. Lync 2013 Bandwidth Calculator
D. Microsoft Remote Connectivity Analyzer

Correct Answer: C
Explanation/Reference:
C: 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 and 2013 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. Lync 2010 and 2013 Bandwidth Calculator – A Microsoft Excel spreadsheet that calculates WAN bandwidth requirements for a Lync Server deployment based on administrator-specified user profiles and network information.

Question 122
Which ports must you open?

DRAG DROP

A company deploys an Office 365 tenant. All employees use Lync Online. You need to configure the network firewall to support Lync 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.

Select and Place:

Correct Answer:

Explanation/Reference:
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 unwanted 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 123**
Which port should you use for each application?

**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 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 Lync 2013.
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.

<table>
<thead>
<tr>
<th>Hot Area:</th>
<th>Correct Answer:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Applications</strong></td>
<td><strong>Port or Ports</strong></td>
</tr>
<tr>
<td>SMTP relay</td>
<td>TCP 25, TCP 443, TCP 5025</td>
</tr>
<tr>
<td>Office 365 admin center</td>
<td>TCP 80, TCP 443, TCP 10101</td>
</tr>
<tr>
<td>Lync (outbound video sessions)</td>
<td>RTP/UDP 50000-50019, RTP/UDP 50050-50059</td>
</tr>
<tr>
<td>Lync (outbound audio sessions)</td>
<td>RTP/UDP 50000-50019, RTP/UDP 50050-50059</td>
</tr>
</tbody>
</table>

**Explanation/Reference:**
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 50000-50019 must be used for outbound audio sessions.

**Question 124**
Which two DNS entries should you create?
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

Correct Answer: CD
Explanation/Reference:
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 125
Which DNS entries should you create?
DRAG DROP
You implement Office 365 for an organization.
You must create the correct DNS entries needed to configure Office 365.
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.
Select and Place:

Correct Answer:

Explanation/Reference:
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 126
How should you configure the DNS settings?
HOTSPOT
You are the SharePoint Online administrator for Contoso, Ltd. The company purchases an Office 365 Enterprise E1 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.
Hot Area:
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 the first domain name with the CNAME, and then looks up the new name.

Question 127
What should you do?
You deploy Lync 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 Lync Online. You need to ensure that users in both offices can transfer files by using Lync 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 Lync Online clients to use Lync 2013.

Correct Answer: B
Explanation/Reference:
Explanation:
B: Lync Online will allow for file sharing if the firewall is configured accordingly since it is mentioned that Lync 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.

Question 128
Which two domain names should you exclude from the migration?
Contoso, Ltd. plans to use Office 365 for email services and Lync 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

Correct Answer: BC
Explanation/Reference:
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 129
What should you do first?
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.
Correct Answer: A
Explanation/Reference:
Explanation:
A: 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 130
Which DNS record types should you use?
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 area. 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.
Select and Place:

Correct Answer: 

Explanation/Reference:
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 131
How should you configure the trial plan?
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.
Hot Area:

Correct Answer: 

Explanation/Reference:
Office 365 Enterprise E 3 offers include unlimited number of users and since you are signing up for a trial 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:
Katzer, Matthew and Don Crawford, Office 365 Migrating and Managing your Business in the Cloud, Apress Media, New York, 2013, pp 84-87

Question 132
HOTSPOT
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.

Hot Area:

Correct Answer:

Explanation/Reference:
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.

Question 133
What should you do?
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.

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

Question 134
Which three actions should you perform in sequence?
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.
Select and Place:
The tenant is your Office 365 account, including hosted Exchange, Lync, 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.

Step 4 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 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

Question 135
What should you do first?
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.
Correct Answer: A
Explanation/Reference:
A: 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 136
Which setting or service should you update?
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
Correct Answer: A
Explanation/Reference:
A: 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.

**Question 137**

What should you do?

Your company purchases an Office 365 plan. The company has an Active Directory Domain Services domain. User1 must 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.

Correct Answer: D

Explanation/Reference:

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).