MCSA: Office 365 Study Guide

PHOENIX TS

Table of Contents

Part I – Exam 70-346: Managing Office 365 Identities and Requirements

This guide follows the outline of the "Skills Measured" section available on the official Microsoft website for Exam 70-346: Managing Office 365 Identities and Requirements. We created this document with the intention that exam candidates utilize it as a source of guidance for studying for the exam. While the document includes exam objective overviews, terms and concepts, practice questions, this is not a comprehensive study tool.

Objectives:

I. Provision Office 365
II. Plan and Implement Network and Security in Office 365
III. Implement and Manage Identities using Azure Active Directory Connect
IV. Implement and Manage Federated Identities for Single Sign-On (SSO)
V. Monitor and Troubleshoot Office 365 Availability and Usage

Objective I: Provision Office 365

Main Topics:

1. Provision Tenants
2. Add and Configure Custom Domains
3. Plan a Pilot

Overview:

You should possess the necessary skills and knowledge to:

- Set up a tenant for your organization and create a custom domain name for the tenant.
- Set up the tenant physical region based upon your organizational location.
- Assign and manage licenses for user accounts and access to specific Office 365 services, such as Skype for Business, SharePoint Online, OneDrive for Business, and Outlook.
- Understand and assign Office 365 management roles for Global admins, Tenant admins, Billing admins, Password admins, Service admins, User Management admins.

You should know how to add a custom domain name through the Office 365 Admin Center, either by purchasing a new domain name, connecting an existing domain through GoDaddy, or through manual configuration. Be able to confirm ownership of the domain.

The process requires a strong comprehension of DNS configuration options, TXT records, and the varying options for custom DNS configurations for Office 365 services, including Skype for Business, Outlook, and SharePoint Online. Also, know how to configure primary and secondary nameservers.

Know how to designate a group of pilot users and what typical individuals make ideal pilot users. For example, the users should come from different organizational departments and hold a minimum amount of experience already in the work environment.

Understand how to develop test plans for deploying the Office 365 tenancy, configuring email, enabling services, and acquiring feedback from the pilot users.

Be able to demonstrate your ability to use the Office 365 on-ramp readiness tool for a variety of testing purposes for troubleshooting configuration issues. Know how to run the Office 365 Health, Readiness, and Connectivity checks.

Concepts, Terms, and Tools to Define and Know...

- IdFix
- Pilot users
- Office 365 Platform
- Exchange Online
- Yammer
- Skype for Business
- SharePoint Online
- OneDrive for Business
- Office Online and Other Applications
- Office 365 On-Ramp Readiness tool
- Global Administrator
- Billing Administrator
- Password Administrator
- Service Administrator
- User Management Administrator

Practice Questions:

1. Can you change the tenant name after configuring the Office 365 subscription?
2. Can you change the tenant region after initial configuration?
3. What account is assigned the Global administrator role by default?
4. What methods are appropriate for resolving license conflicts?
5. What workloads do not require migration?
6. What can you use the Office 365 on-ramp readiness tool for?

Objective II: Plan and Implement Networking and Security in Office 365

Main Topics:

- Configure DNS Records for Services
- Enable Client Connectivity to Office 365
- Administer Microsoft Azure Rights Management (RM)
- Manage Administrator Roles in Office 365

Overview:

You must have a strong understanding of configuring custom DNS records for Exchange, Skype for Business Online, and SharePoint Online. You should know which DNS record is necessary to configure for each Office 365 service and the appropriate values.

Know how to configure proxy servers and outbound firewall ports. Have familiarity with the different Office 365 tools for assessing bandwidth capabilities for various Office 365 services. Know how to configure and troubleshoot Internet connectivity for clients. Know the tools and methods for desktop deployment setup for older Office clients.

Develop a thorough grasp on the capabilities of Azure Rights management for assigning user and group roles. Pay close attention to the abilities Azure Rights Management super user.

Finally, know the technical steps and requirements for the manual configuration of DNS records for mail routing, Sender Policy Framework (SPF), Exchange federation (TXT and CNAME records), and AutoDiscover service. When will you need to manually configure the custom DNS records? When is it not necessary?

Concepts, Terms, and Tools to Define and Know…

- Azure Rights Management super user
- Exchange Client Network Bandwidth Calculator
- Skype for Business Online Bandwidth Calculator
- OneDrive for Business Synchronization Calculator
- TXT records
- CNAME records

- Autodiscover CNAME
- Sender Policy Framework (SPF)
- MX record

Practice Questions:

1. What are common network connectivity issues of clients?
2. What are the two different CNAME records necessary to configure Skype for Business Online
3. What protocols and ports must remain open for clients on an internal network to host on the Internet?
4. Is Azure Rights Management activated by default?
5. What cmdlets in Windows PowerShell do you use to add and remove users from administrator roles?

Objective III: Manage Cloud Identities

Main Topics:

- Configure Password Management
- Manage User and Security Groups
- Manage Cloud Identities with Windows PowerShell

Overview:

Administrators should possess a strong understanding of password management in the Office 365. This entails knowing the password complexity requirements configured by Microsoft, how to configure an expiration policy, password lockout policies, manual and user reset password options, and how to use Windows PowerShell cmdlets for these tasks.

For managing users and security groups, you should know the difference between a soft and hard delete, how to import a large bulk file of users in Office 365, and how to enable multi-factor authentication with the use of mobile devices, one-time passwords, phone calls, or SMS messages.

The Windows PowerShell section contains a robust number of PowerShell cmdlets to know for performing a variety of options to manage cloud identities. You should have a strong grasp on the cmdlets necessary for user, group and role, service principal, domain, single sign-on, subscription and license, company information and service, and administrative management. Practice using all of the cmdlets. Memorization is not an effective means for gaining proficiency in this section.

Concepts, Terms, and Tools to Define and Know…

- UserPrincipalName (UPN)
- Azure Active Directory Module
- Azure Active Directory Graph API
- Cloud identities

Practice Questions:

1. What are the requirements for enabling a self-service password reset for users in Office 365?
2. What benefit comes from accessing the Azure Active Directory API for system administrators?
3. Where are cloud identities stored?
4. What are the default password expiration settings for Office 365 users?
5. When soft deleting user accounts, can you recover them beyond thirty days in the Azure Active Directory Recycle Bin?
6. How would you exempt a user from password complexity requirements by using Windows PowerShell?

Objective IV: Implement and Manage Identities with DirSync

Main Topics:

- Prepare On-Premises Active Directory for Azure AD Connect
- Set Up the Azure AD Connect Tool
- Manage Active Directory Users and Groups with Azure AD Connect

Overview:

For this section you should understand the full capabilities of Azure Active Directory Sync, specifically for replicating multi-forest AD and Exchange deployments while setting up syncing rules for mapping and flow. Although Azure AD Sync is important, it is essential to know how to use Azure Active Directory Connect because it is considered the replacement tool for Azure AD sync.

You should know how to use various other tools, including IdFix, Forefront Identity Manager, and ADModify.NET for tasks such as deploying on-premises single-sign, managing certificates, and maintaining existing AD objects.

Understand the importance of UPN suffixes and the issues that could arise with non-routable domains.

Know the limitations for supporting a multiple forest environment with DirSync and how to compensate with AAD Connect and Forefront Identity Manager.

You should have a grasp on the details for installing and configuring DirSync, including knowledge of the software and hardware requirements.

Know how to create, modify, and delete users with DirSync in place. Be able to demonstrate an understanding of scheduling and forcing syncing.

Concepts, Terms, and Tools to Define and Know...

- Azure Active Directory Synchronization Tools (DirSync)
- Source of Authority
- Azure Active Directory Connect (AAD Connect)

- Forefront Identity Manager 2010 R2
- Active Directory Objects
- IdFix
- ADModify.NET
- UPN suffixes
- Microsoft.Online.DirSync.Scheduler.exe.Config
- Import-Module DirSync
- Start-OnlineCoexistenceSync
- AD Domains and Trusts console
- Microsoft.NET Framework SP1
- Microsoft.NET Framework 4.0

Practice Questions:

1. What tasks are required before deploying DirSync?
2. What port does DirSync communicate through to the Microsoft Azure Servers?
3. Does the computer hosting DirSync need a publicly routable IP address?
4. After you verify a domain, what is the limit to the number of objects for syncing with a new Office 365 tenancy?
5. If a user password expires on an on-premises Active Directory instance, can the user use the same password to sign into Office 365?
6. When adding new user accounts to on-premises AD after configuring DirSync, do you need to manually assign those accounts Office 365 licenses or will DirSync do it automatically?
7. When verifying DirSync installation, what local groups must be present on the computer where DirSync was installed?

Objective V: Implement and Manage Federated Identities

Main Topics:

- Plan Requirements for Active Directory Federation Services (AD FS)
- Install and Manage AD FS Servers
- Install and Manage WAP/AD FS Proxy Servers

Overview:

You should understand how to deploy Active Directory Federation Services (AD FS) topologies. This entails having a strong understanding of the recommendations for deploying farms based on the number of users in your present environment.

Know how to use certificates to establish secure communication across computers hosting the Web Application Proxy (WPA), AD FS federation server, and Office 365 server roles. This involves an understanding of Service Communication Certificates, the X.509 certificate, and the federation and WAP server certificate requirements. In addition to certificates, understand how to employ and configure multi-factor authentication with the Azure Multi-Factor Authentication server.

You should know how to configure an AD FS service account, configure farms, add servers to farms, convert an Office 365 domain from standard to federated, and manage the certificate lifecycle.

You should have comprehension of how to set up perimeter network name resolution with AD FS and WAP servers, know how to install necessary Windows roles and features such as the Remote Access role, configure AD FS WAP, and create custom proxy forms for the user login page prompt.

Concepts, Terms, and Tools to Define and Know...

- AD FS topologies
- Service Communications Certificate
- Web Application Proxy Server
- AD FS Configuration Wizard
- Certification Authority (CA)

- Token-signing certificate (X.509 certificate)
- Namespaces
- Kerberos
- Service Principal Name (SPN)
- Azure Multi-Factor Authentication Server
- OATH tokens
- AD FS service accounts
- Setspn.exe
- Group Managed Service Account (gMSA)
- Server Manager Console
- Connect-MsolService
- Set-MsolADFSContext
- Convert-MsolDomainToFederated
- Get-MsolDomain
- Perimeter Network Name Resolution
- Remote Access node

Practice Questions:

1. How do you block access to Office 365 users based on properties of the user accounts trying to gain access? Also, why would you restrict access?
2. When maintaining certificates, do you need to manually replace token-signing certificates?
3. Where do you place AD FS Service Communication Certificates for the Web App Proxy server?
4. What are the network requirements to configure federation between Office 365 and an on-premises AD instance?

Objective VI: Monitor and Troubleshoot Office 365 Availability and Usage

Main Topics:

- Analyze Reports
- Monitor Service Health
- Isolate Service Interruption

Overview:

You should understand how to access, view, analyze, and leverage mail, usage, auditing, and protection, rules, and Data Loss Prevention (DLP) reports. This section extends to Skype for Business, SharePoint, and OneDrive for Business reports.

Be able to demonstrate your proficiency in using the Service Health Dashboard, enabling a RSS feed for gaining instant service health updates, installing and configuring the Office 365 Management Pack for System Center Operations Manager, and using PowerShell cmdlets for auditing and reporting.

You should know how to create service requests, use the Microsoft Remote Connectivity Analyzer, Microsoft Connectivity Analyzer, and the Transport Reliability IP Probe.

Concepts, Terms, and Tools to Define and Know…

- Mail reports
- Usage reports
- Skype for Business reports
- SharePoint reports
- OneDrive for Business reports
- Auditing reports
- Azure AD reports
- eDiscovery & Hold operations
- Protection reports
- Rules reports

- IMAP
- Outlook on the web
- Exchange Active Sync
- EWS
- POP3
- Service Health Dashboard
- Office 365 Management Pack for System Center Operations Manager
- Office 365 Monitoring Dashboard
- Search-AdminAuditLog
- Write-AdminAuditLog
- Get-AdminAuditLogConfig
- New-AdminAuditLogSearch
- Office 365 tests with Remote Connectivity Analyzer
- Exchange ActiveSync tests
- Exchange ActiveSync AutoDiscover tests
- Exchange Web Services tests
- Outlook tests
- Mail flow configuration tests
- Transport Reliability IP Probe (TRIPP)
- Hybrid Free/Busy Troubleshooter
- Office 365 Client Performance Analyzer
- Microsoft Support Recovery Assistant

Practice Questions:

1. What report would enable you to see the frequency in which users utilize Skype instant messaging, application sharing, audio, video conferencing, and file transfers? Why is this important?
2. What does TRIPP test for?
3. What admin privileges are required for using the hybrid free/busy troubleshooter tool?
4. What Office 365 test reports on mail delivery or client connectivity issues pertaining to DNS?
5. What Office 365 test verifies configuration for Active Directory Federation Services?
6. What is the key difference between the Microsoft Connectivity Analyzer and Microsoft Remote Connectivity Analyzer?
7. What ports does the TRIPP firewall test review?

Practice Question Answers – Part I

Objective I

1. No, the only way to change the tenant name after configuration is to cancel the current Office 365 subscription.
2. No, you cannot change the region without cancelling the current Office 365 subscription.
3. The first tenancy account created when beginning the Office 365 subscription becomes the Global admin by default.
4. Deleting users, purchasing additional licenses, removing licenses from existing users no longer in active use at the organization.
5. Not all workloads need to be hosted on-premises, in the cloud (Microsoft datacenters). Decide what data matters, the level of confidentiality, and legal issues with hosting confidential data across state or country borders.
6. Creating new user accounts, syncing users and passwords with on-premises directories, authenticating users with single-sign on, adding domains, migrating from IMAP supportive systems, and migrations from earlier Exchange Server 2003 or 2007.

Objective II

1. Common network connectivity problems typically are:
    a. There is default gateway address to properly route traffic to the Internet,
    b. Ports of the firewall are misconfigured, resulting in blocking access for clients to the Internet
    c. Clients configured with IP addresses in APIPA range aren't able to connect to the Internet.
    d. Proxy server is configured to require authentication for Internet connections to client computers.
2. One CNAME record is configured to employ the "sip" alias for pointing to sipdir.online.lync. The second CNAME record is configured to employ the alias "lyncdiscover" enable the Skype for Business mobile device client and the Skype for Business service connect.
3. TCP ports 80 and 443.
4. No.

5. Add-MsolRoleMember and Remove-MsolRoleMember.

Objective III

1. To enable self-service password reset option in Office 365, you must have an Azure Active Directory tenant, Azure Active Directory basic or premium, and at least one admin account and one user account in the Azure Active Directory instance.
2. Admins benefit with access to the Azure Active Directory Graph API with the ability to edit large batches of users for creating, disabling, and deleting accounts, retrieving user properties, and modifying user properties.
3. Azure Active Directory and not a separate Office 365 account database. Password policy rules set by Microsoft and not admins from the Admin center.
4. Ninety days with a warning fourteen days before the expiration date arrives.
5. No, user accounts are permanently deleted from the Recycle Bin after a thirty day period.
6. Exempt a user from the password complexity requirements with the Set-MsolUser cmdlet and the StrongPasswordRequired parameter.

Objective IV

1. Remove duplicate proxy address attributes and User-Principal-Name attributes. Ensure blank or invalid User-Name-Principal name attribute settings have only valid UPNs. For group accounts, the member, alias and display name must be populated. Ensure that UPNs with Office 365 must have only letters, numbers, periods, dashes, and underscores.
2. TCP port 443 (SSL)
3. No
4. 300,000 objects, but only 50,000 are permitted before verification.
5. Yes because the password of the cloud user object is set to never expire.
6. Manually with Office 365 Admin Center or Windows PowerShell
7. FIMSyncAdmins, FIMSyncBrowse, FIMSyncJoiners, FIMSyncOperators, FIMSyncPasswordSet

Objective V

1. Restrict access to user accounts by filtering based on claims rules. You may want to restrict access to users for a number of reasons. For example, you may not want users accessing specific confidential data or Office 365 services outside of the organization's internal network.
2. No, they are automatically replaced, but you must replace the AD FS Service Communication Certificates to ensure they remain valid before expiring.
3. Personal Certificate Store .
4. You must configure TCP/IP connectivity between the WAP servers and the Internet. Requirements vary for external clients.

Objective VI

1. The user activities report in the Skype for Business reports. This report enables you to see what services and activities your current users find valuable versus the ones that go unused. If Skype for Business isn't leveraged by a majority of users, then what do they use? Should you limit access to the service, train employees on the importance of using it, or proceed towards another action? This type of thinking enables admins to best customize their environments based on user needs.
2. TRIPP tests VoIP connections, network speed, and firewalls for port availability and usage.
3. Tenant administrator privileges.
4. Office 365 Exchange Domain Name Server (DNS) Connectivity test.
5. Office 365 Single Sign-On test.
6. The Remote Connectivity Analyzer runs through a browser on the Internet. The Microsoft Connectivity Analyzers runs from an on-premises computer.
7. TCP port 443, TCP port 5061, UDP port 3478, and UDP ports ranging from 50,000 to 59,999.

Part II – Exam 70-347: Enabling Office 365 Services

This part of the guide follows the outline of the "Skills Measured" section available on the official Microsoft website for Exam 70-347: Enabling Office 365 Services and follows the same structure as Part I.

Objectives:

I. Manage Clients and End-User Devices (20-25%)
II. Provision SharePoint Online Site Collections (20-25%)
III. Configure Exchange Online and Skype for Business Online for End Users (25-30%)
IV. Plan for Exchange Online and Skype for Business Online (25-30%)

Objective I: Manage Clients and End-Users

Main Topics:

- Manage User Driven Client Deployments
- Manage IT Deployments for Office 365 ProPlus
- Set Up Telemetry and Reporting
- Plan for Office Clients

Overview:

You should know how to set limits on user self-provisioning for their Office 365 ProPlus licenses. This involves knowledge of the software available through this offering, such as Microsoft Access, Excel, Outlook, OneNote, PowerPoint, Word, Publisher, InfoPath, Visio, and Skype for Business. Prior to granting access to end-users to download Office 365 software on their computers, assess the full range of your computing environment. Do user's have proper administrator privileges for downloading and installing software? Ask this and similar questions to address potential conflicts.

Be able to educate and manage end-user access to Office 365 mobile applications. Know the difference between normal Office 365 user activation and reduced functionality mode. Also, understand the steps to deactivate Office 365 ProPlus for specific users.

You should understand how to manually deploy Office 365 ProPlus on an end-user's computer. Know the methods for performing a central deployment with the Office Deployment Tool. Understand how to use this tool and its full capabilities as a command line tool.

Be able to locate and modify the configuration.xml file for various tasks, such as editing languages or display options for Office 365 installations.

To gather telemetry data on Office 365 application usage, know how to enable it through Group Policy, set up and deploy the service, specifically deploying and installing the Telemetry Processor role.

You should know how to configure Skype for Business Online and Outlook clients for users. Understand the difference between click-to-run Office 365 ProPlus and MSI Office for deploying, updating, and managing Office applications for users.

Concepts, Terms, and Tools to Define and Know…

- Reduced functionality mode
- Office Deployment Tool
- Key Management Services (KMS) server
- App-V packages
- Configuration.xml file
- Telemetry data
- Office Telemetry
- Telemetry Dashboard
- Telemetry Processor role
- Group Policy
- UNC path

Practice Questions:

1. How many copies of Office 365 ProPlus is allotted to users?
2. What are the main capabilities of the Office Deployment Tool?
3. List and describe examples of attributes available in the configuration.xml file.
4. What SQL server versions are compatible for hosting the back-end database for Telemetry dashboard?
5. What similarities do Click-to-Run and MSI formats share?

Objective II: Provision SharePoint Online Site Collections

Main Topics:

- Configure External User Sharing
- Create SharePoint Site Collection
- Plan a Collaboration Solution

Overview:

Admins should be able to enable external user sharing globally and by site collection. For external user sharing, ensure that your IT team and organizational users know sharing permissions and restrictions. Pay close attention to the cons of enabling and permitting user sharing globally for SharePoint Online tenancy and site collections.

After proper configuration, be able to educate users on the different methods for sharing content with external users. This includes sharing an entire SharePoint sites, sharing individual documents, or using guest links. Know how to revoke access and change permissions for external users after they accept share invitations.

Be able to describe how to set up a Site Collection Administrator. Understand the full capabilities and default permissions of this admin.

Understand the importance of monitoring resource quotas for Site Collections. Be able to set storage quotas based on the size of your environment.

Know how to create, delete, and restore Site Collections from the Web user interface and from Windows PowerShell.

Understand how to configure a number of Office 365 collaboration tools, including Yammer, Delve, OneDrive for Business, Enterprise eDiscovery, and coauthoring.

Concepts, Terms, and Tools to Define and Know...

- SharePoint Admin Center
- Site Collection Administrator
- Resource quotas

- Storage quotas
- Pooled storage model vs per-site collection storage
- Enterprise eDiscovery
- SharePoint App Store
- Office 365 groups
- SharePoint newsfeed
- Yammer newsfeed
- Coauthoring
- Delve
- Data Loss Prevention (DLP)
- Office 365 video

Practice Questions:

1. When sharing content with external users, when will the invitations expire if the users do not accept it?
2. Do sharing settings at the Site Collection level take precedence over settings at the SharePoint Online level?
3. What is the recommended storage space set aside by SharePoint Online based on the number of users in the environment?
4. If a deleted site collection remains in the Recycle Bin and you have not met the SharePoint Online tenancy storage quota, can you restore that site collection?
5. How does a user block a document temporarily from coauthoring?

Objective III: Configure Exchange Online and Skype for Business Online for End-Users

Main Topics:

- Configure Extra Email Addresses for Users
- Create and Manage External Contacts, Resources, and Groups
- Configure Personal Archive Policies
- Configure Skype for Business Online End-User Communication Settings

Overview:

Admins should have a thorough understanding of email and SIP address management. This entails initiating changes through the Office 365 Admin Center and Windows PowerShell for variety of tasks. You should know how to add additional secondary email aliases for existing users and set their primary (reply-to) email addresses.

Add external contacts to address book through the browser UI and Windows PowerShell.

Know how to add, modify, and remove SIP addresses for users.

Know the differences between the different types of distribution groups and lists.

Know how to enable personal archives for mailboxes with PowerShell.

Understand the importance of retention tags for managing email messages, specifically retention actions and retention periods.

Be able to demonstrate proficiency in managing retention tags and policies via Windows PowerShell.

You should be capable of configuring presence, per user external communication, and user settings for end-user communications for Skype for Business. You should understand the implications for enabling and disabling meeting records, specifically in how this feature impacts potential compliance issues.

Office 365 enables admins to configure external communication settings and control for the entire tenancy or for individual users. This allows admins to permit as much or as little control for users who communicate with contacts on Skype outside of the organization.

You can adjust the configuration for user settings on a more granular level by enabling or blocking specific features, such as audio, video meeting and conversion recordings.

Concepts, Terms, and Tools to Define and Know...

- Reply-to email address
- Secondary email aliases
- Session Initiation Protocol (SIP) addresses
- Resource mailboxes
- Room mailboxes
- Equipment mailboxes
- Distribution group
- Mail-enabled security group
- Dynamic distribution group
- Personal archive mailboxes
- Retention tags
- Retention policies
- Messaging Records Management (MRM)

Practice Questions:

1. What is the name of the default retention policy?
2. What period of time must pass before email messages are automatically transferred to the mailbox archive?
3. When "For Compliance, Turn Off Non-Archived Features" is enabled, what Skype for Business features are disabled?

Objective IV: Plan for Exchange Online and Skype for Business Online

Main Topics:

- Manage Anti-malware and Anti-Spam Policies
- Mailbox Migration Strategy Recommendations
- Plan for Exchange Online
- Manage Skype for Business

Overview:

Be able to configure the malware detection response, anti-malware notifications, administrator notifications, and custom notifications. Be able to create anti-malware policies and apply those policies to different groups of users in your environment.

Be able to demonstrate proficiency in using Windows PowerShell cmdlets for creating and modifying anti-malware policies.

Know how to create IP Allow and IP block lists for connection filter policies to reduce spammers from reaching user inboxes. Also, know how to set up the spam filter block and allow lists. Even be capable of modifying advanced options for spam mail, such as specifying the spam score based on content in email messages (image links, numeric IP addresses in URL, empty messages, URL redirects, etc.). Ensure you know PowerShell cmdlets for configuring spam filter policies.

Understand the various options for migrating on-premises mailboxes to Exchange Online. Strategies in this objective include the remote move, staged migration, and IMAP migration. Based on the number of mailboxes and the type of on-premises environment, know which migration strategies apply best to different situations.

When planning for Exchange Online, first know how to plan for the client requirements for setting up and enabling mailbox archives. Know what versions of Outlook enable archiving and how to set it up in each version.

Understand the difference between in-place and litigation holds, as well as how to create and remove both types through Windows PowerShell.

Know how to enable and disable OWA access for users, depending on the security policies of your computing environment.

Know how to configure, enable, and disable ActiveSync for users through the Exchange admin center in Office 365 and PowerShell.

Be able to dive deeper into the PowerShell cmdlets for managing external communications for Skype for Business end users in your environment. This entails also having proficiency in configuring allow and blocked domain lists. Also, for Skype, know how to disable push notifications and public IM connectivity through the Office 365 Admin Center and PowerShell.

Concepts, Terms, and Tools to Define and Know...

- Exchange Online anti-malware policies
- Malware detection response
- Malware filter lists
- Connection filter policies
- Spam filter policy settings
- Spam filter block and allow lists
- Advanced policy options for spam
- Spam Confidence Level (SPL) ratings
- Outbound spam policy
- Quarantine
- Remote move migration
- Cutover migration
- Staged migration
- IMAP migration
- ActiveSync
- In-place hold
- Litigation hold
- Outlook Web App (OWA)
- Skype Meeting Broadcast
- Cloud PBX
- PSTN Conferencing

Practice Questions:

1. If an IP address is located on the block and allow lists, what will happen with email messages from that IP address?
2. Based on the default or custom spam filter policy settings enabled, what are the options for handling potential spam email messages?
3. After how many days in Quarantine will spam messages be deleted?
4. Explain the difference between in-place and litigation holds? Also, how do you enable and remove each type of hold with Windows PowerShell?
5. What PowerShell cmdlets are applied to enable OWA access for users?

Practice Question Answers – Part II

Objective I

1. Each Office 365 user has access to five copies to Office 365 ProPlus.
2. The Office Deployment Tool enables admins to perform click-to-run for Office 365 installation source and clients. Also, it allows you to create application virtualization (App-V) packages.
3. Configuration.xml file attributes include Version, Display, OfficeClientEdition, ExcludeApp, SourcePath, Logging, Product ID, Updates, and Language ID.
4. SQL Server 2005, 2008, 2008 R2, 2012, 2014, and corresponding Express versions.
5. Click-to-Run and MSI formats are configurable through Group Policy. They both offer telemetry data accessible in the Telemetry tool dashboard.

Objective II

1. Share invitations expire after seven days
2. No, the exact opposite is true. Configured share settings for SharePoint Online take priority.
3. 10 GB for SharePoint Online tenancy and 500 MB per user in the environment.
4. The ability to restore a site collection depends on the SharePoint Online tenancy usage quota. If it hasn't been met, then it is possible to restore it. But you must also ensure that the site collection URL does not conflict with an existing site collection URL.
5. The user must have the document their editing "Checked Out" to prevent other users from coauthoring and editing the document. However, this feature is disabled by default.

Objective III

1. Default MRM Policy
2. Two years.
3. PowerPoint presentation annotations, file transfers, and shared OneNote pages.

Objective IV

1. If on both lists, emails are permitted.
2. Delete, Quarantine, or Move to Junk Email Folder.
3. Spam messages remain in Quarantine for fifteen days before being deleted.
4. Litigation holds (legal holds) are employed when individuals within an organization are under internal or legal investigation and the administrators must preserve the current state of their mailboxes. In-place holds vary from litigation holds in that the holds are set on mailboxes based on defined queries and criteria. For enabling litigation holds in PowerShell, the appropriate cmdlets to use are Set-Mailbox and Get-Mailbox with the "-LitigationHold" and "-LitigationHoldEnabled" parameters. To create in-place holds in PowerShell, use the "New-MailboxSearch", "Set-MailboxSearch", and "Remove-MailboxSearch" with the "-InPlaceHoldEnabled" parameter.
5. Set-CasMailbox and the –OwaEnabled $True (or False) parameter.