Objective Domain

Exam 697: Configuring Windows Devices

Audience Profile
Candidates for this exam are Windows device support technicians or Windows Device System Administrators who are responsible for building solid identities, protection of content (data loss protection), mobile device management policy, virtualization with Hyper-V, and application management using the Company Portal or the Microsoft Store.

Candidates should have experience with Windows desktop administration, maintenance, troubleshooting, Windows 10 security, and integrated Azure features. Candidates should have a basic understanding of Windows networking technologies, Active Directory, and Microsoft Intune.

Skills Measured
Note: This document shows tracked changes that are effective as of December 15, 2017.

Manage Identity (10-15%)

Support Microsoft Store, Microsoft Store for Education, Microsoft Store for Business, and cloud apps.

> Install and manage software by using Microsoft Office 365, Microsoft Store for Business apps, or Microsoft Store for Education apps; sideload apps by using Microsoft Intune; sideload apps into online and offline images; deeplink apps by using Microsoft Intune; integrate Microsoft account, including personalization settings

Support authentication and authorization.

> Identify and resolve issues related to multi-factor authentication, Windows Hello for Business, virtual smart cards, picture passwords, and biometrics; implement workgroup and domain authentication; implement Homegroup; configure computer and user authentication using secure channel, account policies, credential caching, and Credential Manager; implement local accounts and Microsoft accounts; configure Windows Hello for Business; implement Azure AD Join; connect Microsoft accounts to domain accounts

Plan Desktop and Device Deployment (10-15%)

Migrate and configure user data.

> Migrate user profiles; configure folder location; configure profiles, including profile version, local, roaming, and mandatory

Configure Hyper-V.

> Create and configure virtual machines including integration services; create and manage checkpoints; create and configure virtual switches; create and configure virtual disks; move a

virtual machine's storage

Configure mobility options.

Configure offline file policies, power policies (powercfg), Windows to Go, sync options, Sync Center, and Wi-Fi direct

Configure security for mobile devices.

Configure BitLocker; configure startup key storage

Plan and Implement a Microsoft 365 Solution (10-15%)

Support mobile devices.

Support mobile device policies including security policies, remote access, and remote wipe; support mobile access and data synchronization including Work Folders and Sync Center; support broadband connectivity including broadband tethering and metered networks; support Mobile Device Management by using Microsoft Intune including, Windows 10, Windows 10 Mobile, iOS, and Android

Deploy software updates by using Microsoft Intune.

Use reports and In-Console Monitoring to identify required updates; approve or decline updates; configure automatic approval settings; configure deadlines for update installations; deploy third-party updates

Manage devices with Microsoft 365 Solution.

Provision user accounts; enroll devices; view and manage all managed devices; configure the Microsoft Intune subscriptions; configure the Microsoft Service Connection Point role; manage user and computer groups; configure monitoring and alerts; manage policies; manage remote computers

Configure information protection.

Manage and configure Office 365 Data Loss Prevention, Windows Information Protection and BitLocker, Azure Information Protection, Microsoft Cloud App Security, Office 365 Advanced Security Management

Configure Networking (10-15%)

Configure IP settings.

Configure name resolution; connect to a network; configure network locations

Configure networking settings.

Connect to a wireless network; manage preferred wireless networks; configure network adapters

Configure and maintain network security.

Configure Windows Firewall; configure Windows Firewall with Advanced Security; configure connection security rules (IPsec); configure authenticated exceptions; configure network discovery

Configure Storage (10-15%)

Support data storage.

Identify and resolve issues related to the following: DFS client including caching settings; storage spaces including capacity and fault tolerance; OneDrive

Support data security.

Identify and resolve issues related to the following: Permissions including share, NTFS, and Dynamic Access Control (DAC); Encrypting File System (EFS) including Data Recovery Agent; access to removable media; BitLocker and BitLocker To Go including Data Recovery Agent and Microsoft BitLocker Administration and Monitoring (MBAM)

Manage Data Access and Protection (10-15%)

Configure shared resources.

Configure shared folder permissions; configure HomeGroup settings; configure libraries; configure shared printers; configure OneDrive

Configure file and folder access.

Encrypt files and folders by using EFS; configure NTFS permissions; configure disk quotas; configure file access auditing Configure authentication and authorization.

Manage Remote Access (10-15%)

Configure remote connections.

Configure remote authentication; configure Remote Desktop settings; configure VPN connections and authentication; enable VPN Reconnect; configure broadband tethering; configure Remote Desktop client for Windows 10 Mobile, iOS, and Android; protect remote desktop credentials with Remote Credential Guard; enable restricted admin mode for RDP in Windows 8.1 and Windows 2012 R2

Configure mobility options.

Configure offline file policies; configure power policies; configure Windows to Go; configure sync options; configure Wi-Fi direct.

Manage Apps (10-15%)

Deploy and manage RemoteApp

Configure RemoteApp and Desktop Connections settings, configure Group Policy Objects (GPOs) for signed packages, subscribe to the Desktop Connections feeds, export and import RemoteApp configurations, support iOS and Android, configure remote desktop web access for distribution

Support desktop apps.

Support desktop app compatibility using Windows Assessment and Deployment Kit (ADK)~~Application Compatibility Toolkit (ACT) including shims and compatibility database~~; desktop application co-existence using Hyper-V and App-V; configuration of User Experience Virtualization (UE-V); deploy desktop apps by using Microsoft Intune

Manage Updates and Recovery (10-15%)

Configure system recovery.

Configure a recovery drive; configure system restore; perform a refresh or recycle; perform a driver rollback; configure restore points

Configure file recovery.

Restore previous versions of files and folders; configure File History; recover files from OneDrive

Configure and manage updates.

Configure update settings; configure Windows Update policies; manage update history; roll back updates; update Microsoft Store apps