Device Configuration and Management

Candidates for this exam have fundamental knowledge of computer hardware, connections, operation, and management. Candidates should have hands-on experience with Windows 10 installation and configuration, network connections, application and peripheral device management, data access and management, and basic device security in a Windows business environment. Candidates should have at least 150 hours of instruction or hands-on experience with Windows device configuration and management.

To be successful on the test, the candidate is also expected to have the following prerequisite knowledge and skills:

- 8th grade reading skills
- Basic computer operation
- An understanding of hardware components
- Basic safety practices around hardware
- Digital literacy skills, including the ability to research, create content, and solve problems using technology

1. Windows Installation and Configuration

1.1 Install Windows using the default settings

- Time zone options, Microsoft account vs. local account, upgrade vs. custom install

1.2 Configure user account options

- User account (cloud or local), local user and administrative account types

1.3 Configure desktop settings

- Start menu, display settings, application shortcuts, time zone settings, Taskbar settings, power settings, window management (minimize, close, snap)

1.4 Manage accessibility settings

- Display settings, mouse settings, color filters, high-contrast settings, audio settings, closed captions, speech recognition, Magnifier, Narrator, Sticky Keys, on-screen keyboard

1.5 Manage updates

- Windows Update settings, software updates and patches, optional updates, device driver updates, update history

2. Application and Peripheral Management

2.1 Manage applications and Windows features

- Identify user account requirements and permissions for application installation, modify application installations, remove desktop applications, locate and identify optional Windows features, describe the purpose of the Microsoft Store, understand application default locations for 32-bit and 64-bit applications

INFORMATION TECHNOLOGY SPECIALIST

2.2 Compare and contrast capabilities of peripheral connection types

- HDMI, DisplayPort, DVI, VGA, mini-HDMI, USB, USB-C, converting between connection types

3. Data Access and Management

3.1 Describe cloud services

- Cloud storage and collaboration concepts; identify common cloud storage and service providers (Azure, SharePoint, OneDrive, Exchange, Teams, Intune, Yammer etc.), file sharing capabilities and permissions, capabilities of local and hosted virtual machines, offline file synchronization

3.2 Describe and configure storage, file sharing, and permissions

- File and share permissions; effective permissions; basic and advanced permissions; public, basic, and advanced shares; map drives; differentiate between file systems including NTFS, FAT, FAT32, and ExFAT; identify the effect on permissions of copying or moving data between file systems; describe taking ownership of files or folders

3.3 Manage backup and restore

- Describe backup types, (full, differential, incremental, and mirroring) perform full backup and restore operations, restore previous versions

3.4 Describe data access and retention policies

- Memorandums of understanding, Acceptable Use Policies (AUPs), ownership of and access to data and history, use of remote wipe

4. Device Security

4.1 Describe network firewall settings

- Why and how to disable or enable Windows Defender Firewall, compare and contrast private, public, and guest networks

4.2 Describe user authentication

- Multifactor authentication, smart cards, biometric authentication methods, and secure password requirements for BYOD mobile devices and corporate-managed devices

4.3 Given an attack type, describe mitigation methods

- Methods of mitigating attacks (computer viruses, worms, Trojan horses, spyware, adware, ransomware, phishing, keyloggers, social engineering attacks, and physical attacks), antivirus and antimalware program configuration options, analyze antivirus and antimalware program results, social engineering training

4.4 Manage User Account Control (UAC) settings

- Describe the function of UAC, identify appropriate UAC settings for specific purposes, elevate permissions in UAC

4.5 Manage mobile device security

- Mobile Device Management (MDM), methods of securing mobile devices, installing agents on devices, connect mobile devices to corporate networks, limitations on transporting corporate devices

INFORMATION TECHNOLOGY
SPECIALIST

5. Windows Management and Troubleshooting

5.1 Perform troubleshooting tasks

- Locate and identify Windows troubleshooting tools, gather data to describe issues and support troubleshooting, research how to remedy issues, identify when to escalate issues, update group policies in a Windows domain (gpupdate /force, gpresult), differentiate between local and group security policies and precedence, recognize that a policy has been applied or could cause a problem

5.2 Troubleshoot operating system and application issues

- Reset or roll back the operating system, advanced startup, file and setting retention options, features of safe mode, use troubleshooting tools to identify application compatibility issues, resolve Store app installation issues, reinstall or repair desktop applications

5.3 Manage and troubleshoot devices

- Hardware troubleshooting methods (connections, ports, power), update or roll back drivers, uninstall or reinstall a device to reconfigure drivers, describe the purpose and capabilities of Device Manager and Disk Management

5.4 Manage and troubleshoot device connections to networks and domains

- Wired and wireless connections (physical cable, signal, APIPA), joining devices to domains

5.5 Manage and troubleshoot peripheral device connections

- Keyboard, mouse, display, headset, microphone, camera, local and network storage devices, printers, scanners, drivers, connection cables