70-697: Configuring Windows Devices
Course 6 – Sharing Data and Printers

WORKBOOK
Course 6 - Sharing Data and Printers

- Managing Hard Disks
- Creating and Managing Storage Spaces
- Overview of Data Access
- Configuring and Managing File Access
- Configuring and Managing Shared Folders
- Understanding Work Folders
- Managing Printers
Windows 10 simplifies the task of managing drives in the local system and allocating free space with options that have been previously unavailable.

Administrators need to understand:
- Types of partitions and volumes
- How to create partitions and volumes
- How to perform disk maintenance
- How to troubleshoot disks
- How to work with virtual hard drives
- Situations requiring multiple disks
Managing Hard Disks

Partition Styles

- **Master Boot Record (MBR)**
  - MBR is created on the first sector of the disk
  - Lists sizes and locations of partitions
  - Limited to four partitions
  - 2 TB maximum partition size
  - No redundancy

- **GUID Partition Table (GPT)**
  - Disk contains an array of partition entries
  - Each partition identified by GUID
  - Up to 128 partitions per disk
  - Maximum volume size of 18 EB
  - CRC used for redundancy
Managing Hard Disks

- Disk Management Tools
  - Storage in Settings app
    - Identify storage utilization
    - Clean up disks
    - Configure default save locations
  - Disk Management
    - Advanced disk management
  - Diskpart and Windows PowerShell
  - Storage Spaces in Control Panel
Managing Hard Disks

◆ Converting Disks from MBR to GPT
  o System partition must be MBR in BIOS systems
  o Only UEFI systems support booting to GPT
  o GPT is supported for data disks
  o Only use GPT if you need partitions > 2 TB
  o Considerations
    • Administrator or Backup Operators
    • Always backup data first
    • Disks must be online
    • One way conversion unless you wipe the data
MBR disks are either basic or dynamic with dynamic providing additional functionality:
- Ability to be extended
- Creation of multiple volume types
- Repair mirrored volumes
- Reactivate missing or offline disks
- No limit to number of volumes that can be created
Volume Types

**Simple**
- Contiguous space on a single disk
- Not fault tolerant
- No increase in performance
- Can be extended using unallocated space
- Conversion to dynamic performed automatically

**Spanned**
- Space from multiple dynamic disks
- No fault tolerance
- No performance increase
- Can shrink or extend
Volume Types

- Striped (RAID-0)
  - Uses identical allocated space from three or more disks
  - Provides faster throughput
  - No fault tolerance
  - Cannot resize

- Mirrored (RAID-1)
  - Uses two identical dynamic disks
  - Duplicates data across both disks
  - Provides fault tolerance
  - Enhances read access
Managing Hard Disks

- Drive Letters and Mount Points
  - Each volume is formatted using a file system
  - Drive letters are assigned for access
  - Mount points provide more flexibility
Resizing Volumes
- Creates additional space for use by applications or data
- Simple and spanned dynamic disks
  - Extend a simple volume on same disk
  - Extend a spanned volume to another disk in same computer
  - Shrink to free up space
- Before shrinking you should
  - Defragment the disks
  - Move page files
Managing Hard Disks

- Fragmentation
  - Data written to hard disks is broken up into pieces
  - Pieces are placed in contiguous sectors when possible
  - Delete and move operations cause additional white space
  - Subsequent files are not stored contiguously
  - Performance issues for accessing data and opening programs
Managing Hard Disks

- Defragmentation
  - Performed by the Optimize Drives tool
  - Files are rearranged to the optimal location
  - Performed automatically
    - Modify volumes and frequency
    - Enable or disable

- [Diagrams representing different states or settings]
Managing Hard Disks

- **Disk Quotas**
  - Provide the ability to control disk space on NTFS partitions
  - Limits space based on file and folder ownership
  - Enabled at the volume level
- **Benefits**
  - Track and/or restrict disk consumption
  - Proactively monitor available space
  - Determine who is using space
  - Plan for storage increases
- **Tools**
  - FSUTIL
  - Group Policy
  - Disk properties UI
**Managing Hard Disks**

- A virtual hard drive represents a hard drive using a portion of space on a physical drive that is contained in a single file which supports file systems and standard disk operations

- Features
  - Primarily used with virtual machines and Hyper-V
  - Support booting to VHD or additional drives
  - VHDs are portable from one system to another
  - VHDs represent a single point of backup
  - Might not provide necessary performance
Virtual Disk Formats
- VHD
  - 2 TB limit
  - Backward compatible with Windows 7
- VHDX
  - 64 TB limit
  - Supported on Windows 8.1 and Windows Server 2012

Virtual Disk Types
- Fixed size – fixed space, better performance
- Dynamic – expanding space, better efficiency
Storage spaces are a feature in Windows 10 and Server 2012 that provide the flexibility in disk management that was only possible when using SANs.

- Storage pools are created using one or more physical or virtual drives.
- Once the storage pool is created virtual drives or LUNs are created across the physical disks.
- These virtual drives support a variety of arrangements and types:
  - Simple
  - Two way mirrors
  - Three way mirrors
  - Parity
Giving users access to the appropriate data is a critical function for an IT Professional
- Lack of access results in limited productivity
- Unauthorized access results in security breaches
Authentication and authorization are foundational to network security and are utilized by Windows 10 and other systems to control resource access.

**Authentication**
- Validating the identity of an individual or system
- Uses multiple methods
  - What you know
  - What you have
  - Who you are

**Authorization**
- Determining access to resources
- Access Control Lists
### Overview of Data Access

- Permissions are granted to local and domain user accounts on a per resource basis
  - Allow or deny access
  - Control the level of access
- In domain environments AD DS users and groups are used on the ACL
- In home and small business environments local user accounts or Homegroups can be used
Network Models
- Workgroup
  - Collection of systems
  - Decentralized administration and security
- Domain
  - Collection of systems with a common security database
  - Centralized administration and security
- HomeGroup
  - Collection of systems
  - Simplified control of systems and data access
Homegroups offer an easy way to configure accounts and sharing in small networks and home networks
- Configured via Network and sharing center
- Alleviate the problems with local accounts on multiple computers
- Provide easy sharing
  - Documents
  - Pictures
  - Music
  - Videos
  - Printers
Windows 10 uses an access control mechanism as a part of the NTFS operating system to provide secure access to authorized users locally and over the network.

- Shared folders provide access over the network
  - Permissions apply at the folder level

- NTFS files and folders protected by DACLs
  - List defines access using ACEs
  - Users/groups are granted or denied access
  - Access permissions apply locally and over the network
All objects on NTFS partitions are secured using DACLs and permissions

- Standard Permissions
  - Read
  - Read and Execute
  - List Folder contents
  - Write
  - Modify
  - Full Control
Configure and Managing File Access

- **Special Permissions**
  - Provide more granular access when necessary
  - Traverse Folder / Execute File
  - List Folder / Read Data
  - Read attributes
  - Read Extended Attributes
  - Create Files / Write Data
  - Create Folders / Append Data
  - Write Attributes
  - Write Extended Attributes
  - Delete Subfolders and Files
  - Read Permissions / Change Permissions
  - Take Ownership
Configuring and Managing File Access

- **NTFS Permission Rules**
  - Explicit Permissions
  - Implicit Permissions (inherited)
  - Permissions can be allowed or denied
  - If no access is assigned none is granted
  - Precedence
    - Explicit Deny
    - Explicit Allow
    - Inherited Deny
    - Inherited Allow
  - Permission inheritance can be controlled
    - Block permissions from being inherited by the child object
    - Prevent inheritance from parent
**Configuring and Managing File Access**

- Permissions are cumulative
  - Combining permissions assigned to users and groups results in the *least restrictive*
  - All explicit and inherited permissions are evaluated
  - File permissions override folder permissions

- Effective Permissions
  - Tool used to determine effective NTFS permissions
  - Does not include shared folder permissions
Windows 10 provides the ability to add conditions that must be met for a permission to take effect
- Based on group membership
- Based on the device being used to access

Group Condition
- Member of any
- Member of each
- Not member of any
- Not member of each
Effects of copying and moving files and folders on permissions
- Copying within the same partition > file inherits new permissions
- Copying to a different partition > file inherits new permissions
- Moving in the same partition > file retains permissions
- Moving to a different partition > file inherits new permissions
In addition to permissions Windows 10 provides file compression which reduces storage space requirements by minimizing the size of a file as stored on the disk.

Two methods of compression:
- NTFS file and folder compression
  - File attribute
  - Only applicable on NTFS partitions
  - Susceptible to copy and move procedures
- Compressed zipped folders
  - Functions similar to third party applications
  - Consolidate multiple files into a single compressed file
  - Works with all file systems
  - Used to transport compressed files
Topic E - Managing Shared Folders

- Sharing folders provides access to data across the network
  - Only folders are shared not individual files
  - Only data in shared folders is accessible
  - Sharing folders adds additional permissions
## Managing Shared Folders

- **Two types of sharing**
  - Any folder sharing
  - Public folder sharing

- **Basic Sharing**
  - Share folders quickly
  - Configure permissions

- **Advanced Sharing**
  - Assign share name
  - Maximum number of concurrent connections
  - Shared folder permissions
  - Caching options
Managing Shared Folders

◆Sharing Methods
  • Sharing through File Explorer
  • Share with option in the toolbar
  • Sharing tab in folder properties
  • Sharing through the command line
  • Sharing through Computer management
  • Sharing through Windows PowerShell
    • New-SmbShare
    • Get-SmbShare
    • Grant-SmbShareAccess
Managing Shared Folders

- Users require both NTFS and shared folder permissions for access
  - Shared folder permissions are cumulative
  - NTFS permissions are cumulative
  - When combined the most restrictive permission applies

- Considerations
  - Default permission for Everyone group doesn’t work in many environments
  - Grant FC Shared folder permissions
  - Use NTFS for more granular control
  - Lack of either permission will prevent access
  - Effective Permissions feature only shows NTFS permissions
Topic F - Understanding Work Folders

- Overview of Work Folders
  - Allow home and office users to access their personal files regardless of physical location and domain membership
  - Data is stored on a traditional file server but cached on local devices
  - If accessing from multiple devices files are synchronized across all devices
  - All file server features are accessible for management
    - DAC
    - Auditing and access control
    - Quotas
    - IRM
  - Policies can implement security such as encryption and remote wipe capabilities
Work Folders Components

- **File server**
  - File and Storage services role
  - Additional access protocol is added for HTTPS access
  - Installed SSL certificate

- **Sync share**
  - Unit of synchronization between Work Folders server and clients
  - Each user has a personal folder created inside the sync share
  - Exclusive access to this folder and subfolders only

- **User devices**
  - Devices connecting to sync share
  - Must trust SSL certificate
  - Synchronizes files with the server every 10 minutes by default
Understanding Work Folders

- **Configuring Work Folders**
  - Create a sync share on the server with Work Folders role service installed
  - Deploy Work Folders to clients
    - Manual deployment
      - Manage work folders option in Control Panel
      - If domain member or workplace joined an email address is used for auto discovery
      - If workgroup member the Work Folders URL is entered
    - Opt-in
      - Settings are configured using domain based Group Policy, Intune, or Config Manager
      - Users can choose to connect or not
    - Mandatory
      - Same as opt-in without the ability to modify settings
      - Work Folders are configured transparently on devices
Various components participate in the printing process

- Printer
- Print device
- Print server
- Print driver
- Page description language (PDL)
  - PostScript
  - PCL
  - XPS
- Printer port
- Spooler service
Printers are installed in various ways

- Local printers
  - USB – installed automatically
  - LPT – installed using Add Printer wizard
  - TCP/IP – installed using Add Printer wizard
- Network printers
  - Group Policy
  - Manual installation
Direct attached printers can be shared with other network hosts

Printer Permissions
- Print
- Manage Documents
- Manage Printer
## Managing Printers

- **Printer Management**
  - Devices and Printers
    - See What’s Printing manages document queue
    - Add Printer wizard
    - Device stage
  - Print Management MMC snap-in
    - Manage multiple printers and print servers
    - Manage queues
    - Manage drivers
    - Deploy printers with Group Policy
## Summary

- Managing Hard Disks
- Creating and Managing Storage Spaces
- Overview of Data Access
- Configuring and Managing File Access
- Configuring and Managing Shared Folders
- Understanding Work Folders
- Managing Printers
Review Questions:

1. You require fault tolerance so that a Windows 10 machine can still boot up to the operating system in the case of a disk failure. Which of the following volumes should you create?
   A. RAID-0
   B. RAID-1
   C. RAID-5
   D. None of the above

2. You would like to convert a local drive from the MBR drive type to the GPT drive type. Which of the following commands will achieve this goal?
   A. Convert GPT
   B. Convert MBR
   C. Convert basic
   D. Convert dynamic

3. Using the Storage Spaces feature in Windows 10 you would like to configure a storage pool for redundancy. What should you do first?
   A. Add physical disks to the computer and create a storage pool
   B. Create a virtual disk
   C. Configure thin provisioning
   D. Create a two-way mirror disk drive

4. You are looking to implement a three way mirror virtual disk using the Storage Spaces feature in Windows 10. How many physical disks are required in the pool in order to implement this configuration?
   A. 2
   B. 3
   C. 4
   D. 5

5. You would like to add device drivers into the driver store so that standard users are able to attach removable devices such as USB drives and certain printers without being prompted to install the driver and needing administrative credentials. Which of the following commands should you use to achieve this goal?
   A. Sigverif
   B. Msiexec /I /Q
   C. Pnputil /a c:\mydriver.inf
   D. Pnputil /d c:\mydriver.inf
6. In the Windows 10 Enterprise operating system with Hyper-V enabled, which of the following is a feature that is unique to the new VHDX file type?
   A. Ability to boot to VHD
   B. Importable into Hyper-V virtual machines using Client Hyper-V
   C. 64 TB limit
   D. Fixed size or dynamic sized

7. Which of the following options in Windows 10 using the NTFS file system will allow you to conserve disk space by only allocating space based on file and folder ownership with specific default and configurable limits?
   A. chkdsk
   B. Disk Defrag
   C. Diskpart.exe
   D. Fsutil.exe

8. Which of the following options for Device Management is the best when it comes to user experience in that it provides a photo-realistic view of the device with device specific options easily available?
   A. Devices and Printers
   B. Device Manager
   C. System Information
   D. Device Stage

9. Joan is a user in the Sales department and is a member of the Sales_Users and the LA_Users security groups. A data share is located on a Windows 10 machine in the marketing department with the following permissions:
   Shared: Everyone – Full Control
   NTFS: Sales_Users – Read and Execute, Read, List Folder Contents
   LA_Users - Read/Write
   Administrators – Full Control
   What are Joan’s effective permissions when accessing the data over the network?
   A. Full Control
   B. Modify
   C. Read/Write
   D. Read
10. You need to identify the precedence order for permissions on a Windows 10 machine that utilizes the NTFS file system. Which of the following correctly identifies the order of precedence when dealing with explicit and inherited permission entries?
   A. Explicit Allow, Explicit Deny, Inherited Allow, Inherited Deny
   B. Explicit Deny, Inherited Deny, Explicit Allow, Inherited Allow
   C. Explicit Deny, Explicit Allow, Inherited Allow, Inherited Deny
   D. Explicit Deny, Explicit Allow, Inherited Deny, Inherited Allow
**Answer Key:**

1. **B**
   You should create a RAID-1 volume for the operating system drive. This will mirror that volume to another physical disk and is really the only option for fault tolerance when it comes to the operating system disk. RAID-0 doesn't provide fault tolerance and RAID-5 is not supported for OS drives.

2. **A**
   The convert command inside the diskpart interactive utility will convert to GPT disk from MBR disk. You should specify the format that you would like to convert to.

3. **A**
   The first step to implementing storage spaces is to add multiple physical disks to the system and to create a storage pool using those disks.

4. **D**
   In order to implement the three way mirror configuration using Storage Spaces, you require a minimum of five physical disks in the storage pool.

5. **C**
   The Plug and Play utility (pnputil) is used to add drivers in the driver store. The driver store is an area that contains drivers which may then be installed by standard users without requiring any additional administrative privileges.

6. **C**
   The only thing here that is unique to the VHDX file type is the size. It is also only supported on Windows 10 and Windows Server 2012. The other features are shared by VHD files.

7. **D**
   Disk quotas are available with the NTFS file system and can be used to limit the amount of space a user/application can use on the drive. You can use the drive properties or the fsutil command line utility to configure disk quotas. You must configure the quotas on the properties of the drive and they will be in effect based on file/folder ownership.

8. **D**
   The Device Stage is provided using the metadata available with a device driver. That metadata is used to provide a photo-realistic icon and options that are specific to the device. It is accessed through Devices and Printers by double-clicking the device, but is a separate administrative location.
9. C
The effective permissions would be the cumulative NTFS permissions. Since the
Shared permissions are Full Control and the NTFS permissions are more
restrictive because of the Read only and Read/Write permissions, the least
restrictive NTFS permission of Read/Write will apply.

10. D
The rules of permissions on NTFS are that Explicit permissions will always
override inherited permissions and that deny permissions will always override
allow but in that order. Therefore, the Explicit Allow statement will override the
Inherited Deny, which is the one exception to the rule.