Managing Users, Workstations, and Shared Resources

Manage Users
Managing Users, Workstations, and Shared Resources

- Manage Users
- Configure Shared Resources
- Configure Active Directory Accounts and Policies
User and Group Accounts (Slide 1 of 2)

**User account:** The logon ID that identifies each user.

**Security group:** A collection of user accounts that can be assigned permissions in the same way as a single user object.

- Groups
  - Built-in local groups
  - Administrators
  - Users
  - Guests
  - Power Users
  - System Groups
  - System and Service Accounts
User and Group Accounts (Slide 2 of 2)

- System Groups
  - Everyone
  - Authenticated Users
  - Creator Owner
  - Interactive
  - Network
- System and Service Accounts
  - LocalSystem
  - LocalService
  - NetworkService
Local Users and Groups (Slide 1 of 2)

[Image of Local Users and Groups in Computer Management]

- Description: Members of this group can... Administrators have complete... Backup Operators can override sec... Members are authorized to perfor... Members of this group can chang... Members are allowed to launch, a... Members of this group can read e... Guests have the same access as m... Members of this group have comm... Built-in group used by Internet Inf... Members in this group can have s... Members of this group may sche... Members of this group can acces... Power Users are included for back... Members in this group are grant... Members of this group can acces... Supports file replication in a dom... Members of this group are mana... Users are prevented from making... HomeUsers Security Group
Local Users and Groups (Slide 2 of 2)

- Create new user
- Rename and delete user accounts
- Add a user to a group
- Use `net user` commands
Local Security Policy

Policies: A subset of a security profile, and a document that outlines the specific requirements and rules everyone must meet.
SSO and Credential Manager

**Single Sign-On (SSO):** Any authentication technology that allows a user to authenticate once and receive authorizations for multiple services.
Managing Windows User Management
Managing Users, Workstations, and Shared Resources

Configure Share Resources
**Workgroups**

**Peer-to-peer network:** A network with no dedicated server and each computer acts as both a server and a client.

**Workgroup:** A small group of computers on a network that share resources in a peer-to-peer fashion.
**Homegroups**

**Homegroup**: Windows networking feature designed to allow Windows 7 and later home networks to share files and printers easily through a simple password protection mechanism.
Network and Sharing Center (Slide 1 of 2)
Network and Sharing Center (Slide 2 of 2)

Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Home or Work

Network discovery:

- Turn on network discovery
- Turn off network discovery

File and printer sharing:

- Turn on file and printer sharing
- Turn off file and printer sharing

Public folder sharing:

- Turn on sharing so anyone with network access can read and write files in the Public folders
- Turn off Public folder sharing (people logged on to this computer can still access these folders)

Copyright (c) 2018 CompTIA Properties, LLC. All Rights Reserved. | CompTIA.org
Network Share Configuration (Slide 1 of 6)
Network Share Configuration (Slide 2 of 6)

- Share name and optional comment
- Maximum number of users allowed to connect at any one time
- Permissions
  - Full Control
  - Change
  - Read
Network Share Configuration (Slide 3 of 6)

• Shared Folders snap-in
• Administrative shares
Network Share Configuration (Slide 4 of 6)
Network drive: A local share that has been assigned a drive letter.
Network Share Configuration (Slide 6 of 6)
Offline Files and Sync Center

Synchronisation partnership details

View the items within this synchronisation partnership, synchronise now or change your synchronisation settings.

labfiles (\comptia)

Progress: 
Status: Last synchronisation on 30/09/2018 19:41
1 conflicts
The `net` Commands

- `net /?`
- `net use /?`
- `net use DeviceName \ComputerName\ShareName`
- `net use DeviceName /delete`
- `net use * /delete`
- `net view`
## NTFS File and Folder Permissions (Slide 2 of 8)

<table>
<thead>
<tr>
<th>Folder Permission</th>
<th>Allows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>View files and subfolders including their attributes, permissions, and ownership.</td>
</tr>
<tr>
<td>Write</td>
<td>Create new folders and files, change attributes, view permissions and ownership.</td>
</tr>
<tr>
<td>List</td>
<td>View the names of files and subfolders.</td>
</tr>
<tr>
<td>Read &amp; Execute</td>
<td>Pass-through folders for which no permissions are assigned, plus read and list permissions.</td>
</tr>
<tr>
<td>Modify</td>
<td>Includes Read/Execute and Write permissions, as well as the ability to rename and delete the folder.</td>
</tr>
<tr>
<td>Full Control</td>
<td>All the above, plus changing permissions, taking ownership, and deleting subfolders and files.</td>
</tr>
<tr>
<td>File Permission</td>
<td>Allows</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------</td>
</tr>
<tr>
<td>Read</td>
<td>Read the contents of the file and view attributes, ownership, and permissions.</td>
</tr>
<tr>
<td>Write</td>
<td>Overwrite the file and view attributes, ownership, and permissions.</td>
</tr>
<tr>
<td>Read &amp; Execute</td>
<td>Read permissions, plus the ability to run applications.</td>
</tr>
<tr>
<td>Modify</td>
<td>Includes Read/Execute and Write permissions, as well as the ability to rename and delete the file.</td>
</tr>
<tr>
<td>Full Control</td>
<td>All the above, plus changing permissions, taking ownership.</td>
</tr>
</tbody>
</table>
Effective Permissions and Allow Versus Deny

• Permissions usually applied at one of three levels:
  • For application folders, the read/execute permission is granted to the appropriate group.
  • For data areas, the modify or read permission is assigned as appropriate.
  • To home directories (personal storage areas on a network), full control is assigned to the relevant user.
NTFS File and Folder Permissions (Slide 5 of 8)

- Permission Propagation and Inheritance
- Ownership
<table>
<thead>
<tr>
<th>Action</th>
<th>Effect</th>
</tr>
</thead>
</table>
| Moving files and folders on the same NTFS volume                      | • Destination folder: Write permission.  
• Source folder: Modify permission.  
• NTFS permissions are retained.                                                                                                       |
| Moving files and folders to a different NTFS volume                   | • Destination folder: Write permission.  
• Source folder: Modify permission.  
• NTFS permissions are inherited from the destination folder and the user becomes the Creator/Owner.                                      |
| Copying files and folders on the same NTFS volume or different NTFS volumes | • Destination folder: Write permission.  
• Source folder: Read permission.  
• NTFS permissions are inherited from the destination folder and the user becomes the Creator/Owner.                                      |
| Moving files and folders to a FAT or FAT32 partition                  | • Source folder: Modify permission.  
• All permissions and NTFS attributes (such as encryption) are lost.                                                                        |
NTFS File and Folder Permissions (Slide 7 of 8)

Combining NTFS and Share Permissions:
• Share permissions only protect resource accessed across the network.
• NTFS permissions protect resource from unauthorized local access.
• FAT disk partitions only protected using share permissions.
• Share permissions are set at the root of the share.
  • All files and subdirectories inherit the same permissions.
• NTFS permissions are used in combination with the share permissions to provide greater flexibility.
• If both share and NTFS permissions are applied to the same resource, the most restrictive applies.
NTFS File and Folder Permissions (Slide 8 of 8)
Activity

Discussing Shared Resource Configuration
Activity

Configuring Shared Resources
Managing Users, Workstations, and Shared Resources

Configure AD Accounts and Policies
Windows Active Directory Domains

Local accounts: An account that is only associated with the computer on which it was created.

Local Security Accounts database: A local (non-network) database where local system account information is stored.

Security Accounts Manager (SAM): The Windows local security account database where local system account information is stored.

Windows Server Domain Controller (DC): Any Windows-based server that provides domain authentication services (logon services) is referred to as a domain controller (DC).
Active Directory Domain Services (AD DS): The database that contains the users, groups, and computer accounts in a Windows Server domain.
Active Directory Components (Slide 2 of 2)

**Member servers:** Any server-based systems that have been configured into the domain, but do not maintain a copy of the Active Directory database.

**Organizational Units (OUs):** In Windows Active Directory, a way of dividing the domain up into different administrative realms.
Domain Membership

• The computer has a computer account object.
• Computer users can log on to the domain with domain user accounts.
• The computer and its users are subject to centralized settings:
  • Domain security
  • Configuration
  • Policy settings
• Certain domain accounts automatically become members of local groups on the computer.
Domain Sign-In
Group Policy Objects (Slide 1 of 2)

**GPO:** A means of applying security settings (as well as other administrative settings) across a range of computers and users.

**Administrative templates:** Group Policy files for registry-based policy management, which have the .ADM file extension.

**Security templates:** Settings for services and policy configuration for a server operating in a particular application role.

**RSoP:** A Group Policy report showing all of the GPO settings and how they affect the network.
Group Policy Objects (Slide 2 of 2)
Basic AD Functions (Slide 1 of 2)
Basic AD Functions (Slide 2 of 2)
Logon Scripts

**Logon script**: A file containing commands that run each time a user logs on to a computer to set up the user environment.

**SSO**: Any authentication technology that allows a user to authenticate once and receive authorizations for multiple services.

- Windows logon scripts
- Linux login scripts
Home Folder

**Home folder**: A private network storage area located in a shared network server folder in which users can store personal files.
Folder Redirection

**Folder redirection:** A Microsoft Windows technology that allows an administrative user to redirect the path of a local folder (such as the user's home folder) to a folder on a network share, making the data available to the user when they log into any computer on the network where the network share is located.

**Roaming profiles:** A Microsoft Windows technology that redirects user profiles to a network share so that the information is available when the user logs into any computer on the network where the network share is located.

**Offline files:** Files (or folders) from a network share that are cached locally.
Account Locks and Password Resets
Discussing Active Directory Account and Policy Configuration
Activity: Configuring Active Directory Accounts and Policies
Reflective Questions

1. What experiences do you have in working with any of the technologies discussed in this lesson?

2. Which AD configuration task do you expect to perform most often in your workplace?