UNIT 1

Overview of Systems Administration and Maintenance

1.0 Learning Outcomes

After completing this module, you will be able to:

a. Configure and manage user accounts to limit security threats across an organization
b. Apply Protected Users settings, policies, and authentication silos to protect highly privileged user accounts
c. Describe and configure Windows Defender Credential Guard
d. Configure Group Policy to block the use of NTLM for authentication
e. Disable inactive accounts and require periodic password updates

1.1 Introduction

The first step in securing Windows Server is to ensure that you've properly configured user accounts. First, confirm the accounts have only the privileges needed to perform necessary tasks by using the principal of least privilege. Additionally, you need to protect user account credentials from compromise by restricting resources that accounts can use to authenticate against, and the protocols that can be used for that authentication

1.2 Configure User Account Rights

When configuring user rights, it's important to follow the principle of least privilege. This means granting users only the rights and privileges they need to perform their tasks, and no more. As a result, if an unauthorized user compromises an account, they gain access only to the limited set of privileges assigned to that account. IT staff should also have separate accounts for day-to-day activities such as answering email, separate from the privileged accounts used to perform administrative tasks.

User rights assignment policy	Function
Access Credential Manager as a trusted caller	Used by Credential Manager during backup and restore. You should not assign this privilege to user accounts.
Access this computer from the network	Determines which users and groups can connect to the computer from the network. This right does not affect Remote Desktop Services.
Act as part of the operating system	Allows a process to impersonate a user without authentication. You typically would assign the

User rights assignment policy	Function
	LocalSystem account to processes that require this privilege.
Add workstations to a domain	Allows you to join workstations to the domain.
Adjust memory quotas for a process	Determines which security principals can adjust the maximum amount of memory assigned to a process.
Allow sign in locally	Determines which users can sign in locally to a computer. Alter this policy on Privileged Access Workstations to remove members of the Users group as a way of limiting which accounts can sign in to a computer. By default, any authenticated user can sign in to any workstation or server except for a Domain Controller, which is limited to members of certain groups.
Allow sign in through Remote Desktop Services	Determines which users and groups can sign in remotely by using a Remote Desktop Service connection.
Back up files and directories	Gives permission to back up files, directories, registry, and other objects to which the user normally would not have permission. Assigning this right gives indirect access to all data on a computer because the person with that right can back that data up and then recover it in an environment over which they have complete control.
Bypass traverse checking	Allows the user with this right to traverse directories on which they don't have permission. It does not allow the user to list the contents of that directory though.
Change the system time	Allows the user with this right to alter the system time, which is separate from the time zone.
Change the time zone	Allows the user with this right to alter the time zone, but not the system time.
Create a page file	Allows the user with this right to create and modify a page file.
Create a token object	Determines which user accounts that processes can use to create tokens that allow access to local resources. Don't assign this right to any user you don't want to have complete system control, because they can use it to leverage local Administrator privileges.
Create global objects	Determines which user accounts can create global objects that are available to all sessions. Don't assign this right to any user you don't want to give complete system control, because they can use it to leverage local Administrator privileges.
Create permanent shared objects	Determines which user accounts can create directory objects by using the object manager.

User rights assignment policy	Function
Create symbolic links	Determines which user accounts can create symbolic links from the computer they are signed in to. You should assign this right only to trusted users because symbolic links can expose security vulnerabilities in apps that aren’t configured to support them.
Debug programs	Determines which user accounts can attach a debugger to processes within the operating system kernel. Only developers who are writing new system components require this ability. Developers who are writing applications do not.
Deny access to this computer from the network	Blocks specified users and groups from accessing the computer from the network. This setting overrides the policy that allows access from the network.
Deny sign in as a batch job	Blocks specified users and groups from signing in as a batch job. This overrides the sign-in as a batch job policy.
Deny sign in as a service	Blocks service accounts from registering a process as a service. This policy overrides the sign in as a service policy. However, it doesn't apply to Local System, Local Service, or Network Service accounts.
Deny sign in locally	Blocks accounts from signing on locally. This policy overrides the allow sign in locally policy.
Deny sign in through Remote Desktop Services	Blocks accounts from signing in by using Remote Desktop Services. This policy overrides the Allow sign in through Remote Desktop Services policy.
Enable computer and user accounts to be trusted for delegation	Determines whether you can configure the Trusted for Delegation setting on a user or a computer object.
Force shutdown from a remote system	Users assigned this right can shut down computers from remote network locations.
Generate security audits	Determines which accounts processes can use to add items to the security log. Because this right allows interaction with the security log, it presents a security risk when you assign this to a user account.
Impersonate a client after authentication	Allows apps that are running on behalf of a user to impersonate a client. This right can be a security risk, and you should assign it only to trusted users.
Increase a process working set	Accounts assigned this right can increase or decrease the number of memory pages available for the process to use to the process in random access memory (RAM).
Increase scheduling priority	Accounts assigned this right can change the scheduling priority of a process.

User rights assignment policy	Function
Load and unload device drivers	Accounts assigned this right can dynamically load and unload device drivers into kernel mode. This right is separate from the right to load and unload plug and play drivers. Assigning this right is a security risk because it grants access to the kernel mode.
Lock pages in memory	Accounts assigned this right can use a process to keep data stored in physical memory, blocking that data from paging to virtual memory.
Sign in as a batch job	Users with accounts that have this permission can sign in to a computer through a batch-queue facility. This right is only relevant to older versions of the Windows operating system, and you should not use it with newer versions, such as Windows 10 and Windows Server 2016 or later.
Sign in as a service	Allows a security principal to sign in as a service. You need to assign this right when any service that you configure to use a user account, rather than one of the built-in service accounts.
Manage auditing and security log	Users assigned this right can configure object access auditing options for resources such as files and AD DS (Active Directory) objects. Users assigned this right can also review events in the security log and clear the security log. Because unauthorized users are likely to clear the security log as a way of hiding their tracks, you should not assign this right to user accounts to which you would not assign local Administrator permissions on a computer.
Modify an object label	Users with this permission can modify the integrity level of objects, including files, registry keys, or processes that other users own.
Modify firmware environment values	Determines which users can modify firmware environment variables. This policy is primarily for modifying the boot-configuration settings of non-x86-based computers
Perform volume maintenance tasks	Determines which user accounts can perform maintenance tasks on a volume. Assigning this right is a security risk because users who have this permission might access data stored on the volume.
Profile single process	Determines which user accounts can leverage performance-monitoring tools to monitor nonsystem processes.

User rights assignment policy	Function
Profile system performance	Determines which user accounts can leverage performance-monitoring tools to monitor system processes.
Remove computer from docking station	When assigned, a user account can remove a portable computer from a docking station without signing in.
Replace a process-level token	When assigned, a user account can call the **CreateProcessAsUser** API so that one service can trigger another.
Restore files and directories	Allows users assigned this right to bypass permissions on files, directories, and the registry and overwrite these objects with restored data. This right is a security risk, as a user account with this right can overwrite registry settings and replace existing permissions.
Shut down the system	Assigns the ability for a locally signed-in user to shut down the operating system.
Synchronize directory service data	Assigns the ability to synchronize AD DS data.
Take ownership of files or other objects	When assigned, this user account can take ownership of any securable object, including AD DS objects, files, folders, registry keys, processes, and threads. This represents a security risk because it allows the user to take control of any securable object.

You can also configure additional account security options that limit how and when an account can be used, including:

- **Logon Hours**. Use this setting to configure when users can use an account.
- **Logon Workstations**. Use this setting to limit the computers an account can sign in to. By default, users can use an account to sign in to any computer in the domain.
- **Password Never Expires**. You should never configure this option for privileged accounts because it will exempt the account from the domain password policy.
- **Smart card is required for interactive logon**. In high-security environments, you can enable this option to ensure that only an authorized person that has both the smart card and the account credentials can use the privileged account.
- **Account is sensitive and cannot be delegated**. When you enable this option, you ensure that trusted applications cannot forward an account's credentials to other services or computers on the network. You should enable this setting for highly privileged accounts.
- **Use only Kerberos Data Encryption Standard (DES) encryption types for this account**. This option configures an account to use only DES encryption, which is a weaker form of encryption than Advanced Encryption Standard (AES). You should not configure this option on a secure network.

- **This account supports Kerberos AES 128-bit encryption**. When you enable this option, you are allowing Kerberos AES 128-bit encryption to occur.
- **This account supports Kerberos AES 256-bit encryption**. When possible, you should configure this option for privileged accounts and have them use this form of Kerberos encryption over the AES 128-bit encryption option.
- **Do not require Kerberos preauthentication**. Kerberos preauthentication reduces the risk of replay attacks. Therefore, you should not enable this option.
- **Account expires**. Allows you to configure an end date for an account so that it doesn't remain in AD DS after it is no longer used.

1.3 Protect user accounts with the Protected Users group

The AD DS (Active Directory) security group Protected Users helps you protect highly privileged user accounts against compromise. The Protected Users group members have several security-related configuration settings applied that cannot be modified except by leaving the group.

1.3.1 Protected Users Group Prerequisites

To provide protection for members of the Protected Users group:

- The group must be replicated to all domain controllers.
- The user must sign in to a device running Windows 8.1 or Windows Server 2012 R2 or later.
- Domain controller protection requires that domains must be running at a Windows Server 2012 R2 or higher domain functional level. Lower functional levels still support protection on client devices.

1.3.2 Protected Users Group Protections

When a user is a member of the Protected Users group, on their workstation or local device:

- User credentials are not cached locally.
- Credential delegation (CredSSP) will not cache user credentials
- Windows Digest will not cache user credentials.
- NTLM will not cache user credentials.
- Kerberos will not create DES (Data Encryption Standard) or RC4 keys, or cache credentials or long-term keys.
- The user can no longer sign-in offline.

On domain controllers running Windows Server 2012 R2 or later:

- NTLM authentication is not allowed.
- DES and RC4 encryption in Kerberos preauthentication cannot be used.

- Credentials cannot be delegated using constrained delegation.
- Cannot be delegated using unconstrained delegation.

1.3.3 Authentication Policies

Authentication policies enable you to configure TGT lifetime and access-control conditions for a user, service, or computer account. For user accounts, you can configure the user's TGT lifetime, up to the maximum set by the Protected Users group's 600-minute maximum lifetime. You can also restrict which devices the user can sign in to, and the criteria that the devices need to meet.

1.3.4 Authentication Policy Silos

Authentication policy silos allow administrators to assign authentication policies to user, computer, and service accounts. Authentication policy silos work with the Protected Users group to add configurable restrictions to the group's existing non-configurable restrictions. In addition, policy silos ensure that the accounts belong to only a single authentication policy silo.

When an account signs in, a user that is part of an Authentication policy silo is granted an Authentication Policy Silo claim. This silo claim controls access to claims-aware resources to verify whether the account is authorized to access that device. For example, you might associate accounts that can access sensitive servers with a specific Authentication policy silo.

1.4 Describe Windows Defender Credential Guard

Windows Defender Credential Guard helps protect you against NTLM Pass-the-Hash attacks or Kerberos Pass-the-Ticket attacks. It protects you by restricting access to NTLM password hashes (Pass-the-Hash), Kerberos TGTs (Pass-the-Ticket), and application credentials stored as domain credentials to special processes and memory that manage and store that authorization and authentication-related data. Therefore, only specific, digitally authorized elements of the host operating system—which verifies those elements—can access the special processes and memory. This blocks unauthorized operations or unauthorized software from gaining access to the protected processes and memory, and subsequently limiting their access to authorization and authentication-related data. Windows Defender Credential Guard also provides hardware security by utilizing hardware security features such as secure boot and virtualization for NTLM, Kerberos, and Credential Manager.

1.4.1 How Windows Defender Credential Guard Works

Windows Defender Credential Guard protects user credentials from compromise by isolating those credentials within a protected, virtualized container, separate from the rest of the operating system. Only privileged system software can access the credentials.

The virtualized container's operating system runs in parallel with, but independent from the host operating system. This operating system protects these processes from attempts by any external entity to read information that those processes store and use. This means that credentials are more protected, even if malware has penetrated the rest of your system.

1.4.2 Windows Defender Credential Guard Requirements

You can deploy Windows Defender Credential Guard only on devices that meet certain hardware requirements. Windows Defender Credential Guard should be used on any computer where IT staff use privileged credentials, especially workstations dedicated to privileged access.

Windows Defender Credential Guard requires the following:

- Windows 10 Enterprise or Windows Server 2016 or later
- 64-bit CPU
- CPU virtualization extensions plus extended page tables (Intel VT-x or AMD-V)
- Trusted Platform Module (TPM) 1.2 or 2.0
- Unified Extensible Firmware Interface (UEFI) firmware version 2.3.1.c or newer
- UEFI Secure boot
- UEFI secure firmware update

Windows Defender Credential Guard can protect secrets in a Microsoft Hyper-V virtual machine when:

- The Hyper-V host has an input/output memory management unit (IOMMU) and runs Windows Server 2016 or later, or runs Windows 10 Enterprise.
- The virtual machine must be Generation 2, have virtual TPM enabled, and run an operating system that supports Windows Defender Credential Guard.

Windows Defender Credential Guard does not support:

- Unconstrained Kerberos delegation
- NTLMv1
- MS-CHAPv2
- Digest authentication
- Credential (CredSSP) delegation
- Kerberos DES (Data Encryption Standard) encryption

Windows Defender Credential Guard is not supported on domain controllers. It also does not provide protections for the AD DS (Active Directory) database or Security Accounts Manager (SAM).

1.5 Block NTLM Authentication

The NTLM authentication protocol is less secure than the Kerberos authentication protocol. You should block the use of NTLM for authentication and use Kerberos instead.

1.5.1 Audit NTLM Traffic

Prior to blocking NTLM, you need to ensure that existing applications are no longer using the protocol. You can audit NTLM traffic by configuring the following Group Policy settings under Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options:

- **Network security: Restrict NTLM: Outgoing NTLM Traffic to remote servers**. Configure this policy with the Audit All setting.
- **Network security: Restrict NTLM: Audit Incoming NTLM Traffic**. Configure this policy with the Enable auditing for all accounts setting.

Network security: Restrict NTLM: Audit NTLM authentication in this domain. Configure this policy with the Enable for domain accounts to domain servers setting on domain controllers. You should not configure this policy on all computers.

1.5.2 Block NTLM

After you have determined that you can block NTLM in your organization, you need to configure the Restrict NTLM: NTLM authentication in this domain policy in the previous Group Policy node. The configuration options are:

- **Deny for domain accounts to domain servers**. This option denies all NTLM authentication sign-in attempts for all servers in the domain that use domain accounts, unless the server name is listed in the **Network Security: Restrict NTLM: Add server exceptions for NTLM authentication** setting in this domain policy.
- **Deny for domain accounts**. This option denies all NTLM authentication attempts for domain accounts unless the server name is listed in the **Network Security: Restrict NTLM: Add server exceptions for NTLM authentication** setting in this domain policy.
- **Deny for domain servers**. This option denies NTLM authentication requests to all servers in the domain unless the server name is listed in the **Network Security: Restrict NTLM: Add server exceptions** setting for NTLM authentication in this domain policy.

- **Deny all**. This option ensures that all NTLM pass-through authentication requests for servers and accounts will be denied unless the server name is listed in the **Network Security: Restrict NTLM: Add server exceptions** setting for NTLM authentication in this domain policy.

1.6 Locate Problematic Accounts

You should check your AD DS environment for accounts that have not signed in for a specific period of time, or that have passwords with no expiration date.

Inactive user accounts usually indicate a person that has left the organization and organization processes have failed to remove or disable the account. The account might also have originally been shared by IT staff, but is no longer in use. These extra accounts represent additional opportunities for unauthorized users to gain access to your network resources.

Accounts with fixed passwords are less secure than accounts that are required to update their password periodically. If a third-party user obtains a user's password, that knowledge is only valid until the user updates the password. If you configure an account with a password that the user doesn't have to update periodically, then a potential cybercriminal could have access to your network indefinitely. Ensuring regular password updates is especially important for highly privileged accounts.

When you find accounts that haven't signed in for a specified number of days, you can disable those accounts. Disabling them allows you to reenable them should the person return. After you've located accounts that are configured with passwords that don't expire, you can take steps to ensure that an appropriate password update policy is enforced.

Note

User accounts with credentials shared by multiple IT staff members should be avoided, even if they have a strong password policy. Shared accounts make it hard to track which individual performed a specific administrative task.

You can use Windows PowerShell or the AD DS Administrative Center to find problematic users. To use Windows PowerShell to find active users with passwords set to never expire, use the following command:

PowerShellCopy

```
Get-ADUser -Filter {Enabled -eq $true -and PasswordNeverExpires -eq $true}
```

Use the following Windows PowerShell command to find users that have not signed in within the last 90 days, using Windows PowerShell:

PowerShellCopy

```
Get-ADUser -Filter {LastLogonTimeStamp -lt (Get-Date).Adddays(-(90))-and enabled -eq
$true} -Properties LastLogonTimeStamp
```

ASSESSMENT NO. 1

Name:_________________________ Year, Course and Section: _____________

Subject: ________________________

Check your knowledge

1. Which security setting when enabled reduces rather than improves the security of administrative user accounts?

   A. This account supports Kerberos AES (Advanced Encryption Standard) 256-bit encryption.
   B. Don't require Kerberos preauthentication.
   C. Account is sensitive and cannot be delegated.

2. Which feature allows you to configure TGT (Ticket-granting tickets) lifetime and access-control conditions for a user?

   A. Authentication policies.
   B. Protected Users group.
   C. Authentication policy silos.

3. Which of the following problematic user accounts you should check for regularly?

   A. Users with passwords that do not expire.
   B. Users with few administrative permissions.
   C. Users with complex passwords.

The following table shows the rubric that will be used in evaluating your answer.

	Excellent **5**	**Good** **3**	**Average** **2**	**Needs improvement** **1**
Knowledge and argumentation	Strong use of sources - including summary, quotations, interpretation and analysis. Argumentation.	Good use of sources and some argumentation.	Some use of sources and very little or unclear argumentation.	Insufficient use of sources and/or sources misunderstood. Unclear or lacking argumentation.
Vocabulary and style	Wide and growing vocabulary. Variety of sentence types.	Most elements achieved.	Some elements achieved.	Vocabulary in this paper is limited. There are several instances of incorrect word choices. There is a narrow range of sentence variety.
Paragraphs and punctuation	Main ideas appropriately divided by paragraphs. Sentences divided by proper punctuation.	Good control.	Paper has examples of proper use of paragraphs and punctuation.	Use of paragraphs and punctuation needs improvement.
Spelling and grammar	Precise and consistent control.	Good control. Paper has some errors that do not interfere with understanding.	Paper has several errors that could interfere with understanding or affect readability.	Several sentences and/or ideas are difficult to understand because of errors.

1.7 References

Learn.microsoft.com

1.8 Acknowledgement

All the figures and information presented in this module were taken from the references enumerated above.