Microsoft

**

AZ-801

Tag 4

Configure Windows Server Hybrid Advanced Services

Guten Morgen!

Agenda AZ-801

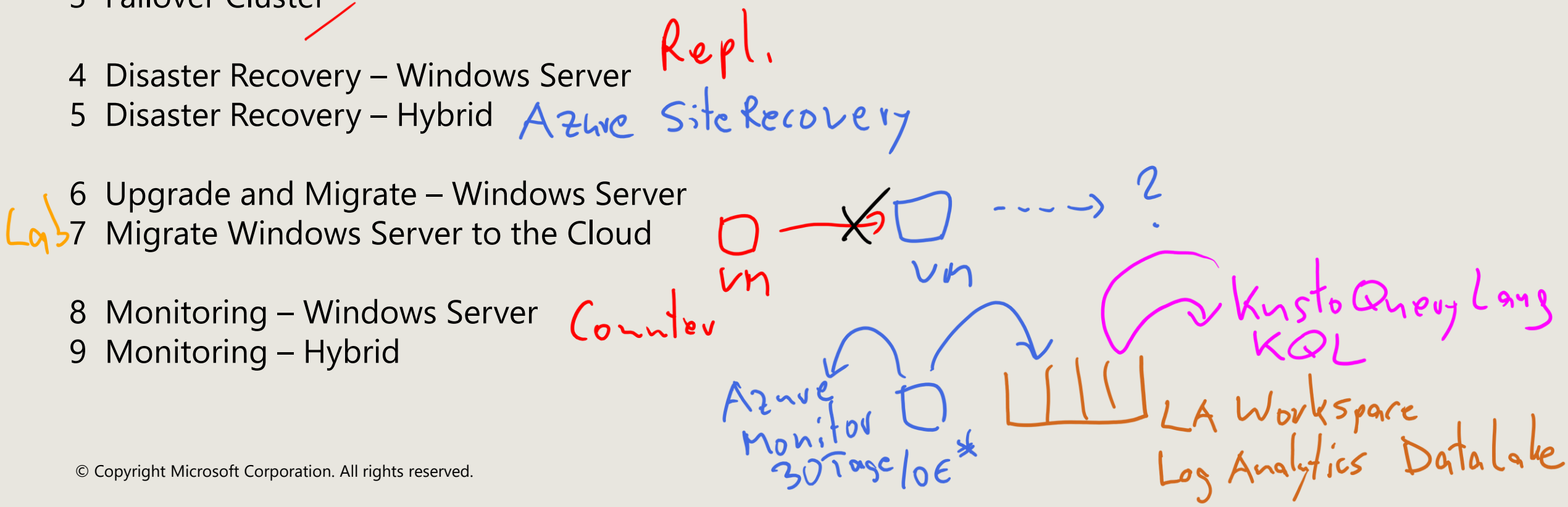
1 Security – Windows Server
2 Security – Hybrid

3 Failover Cluster

4 Disaster Recovery – Windows Server
5 Disaster Recovery – Hybrid

6 Upgrade and Migrate – Windows Server
7 Migrate Windows Server to the Cloud

8 Monitoring – Windows Server
9 Monitoring – Hybrid



Secure Windows Server on-premises and hybrid infrastructures *(Windows Server security)*

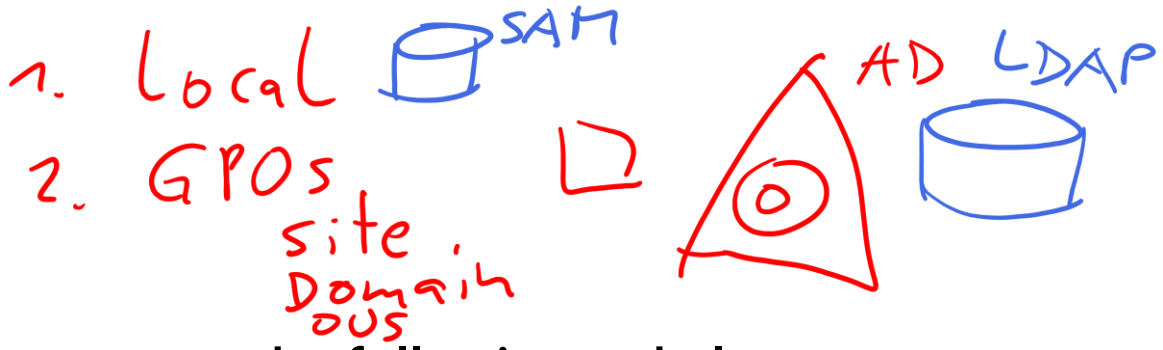
- Secure Windows Server user accounts
- Hardening Windows Server
- Windows Server update management
- Lab 01 – Configuring security in Windows Server

Secure Windows Server user accounts

Learning Objectives – Secure Windows Server user accounts

- Configure User Account Rights, Security Options, and Password Policies
- Protect user accounts
- Implement Microsoft Defender Credential Guard
- Block NTLM authentication
- Locate problematic accounts
- Implement Exploit Protection and Windows Defender Application Control
- Implement Microsoft Defender for Endpoint
- Microsoft Defender SmartScreen
- Learning recap

Configure User Account Rights

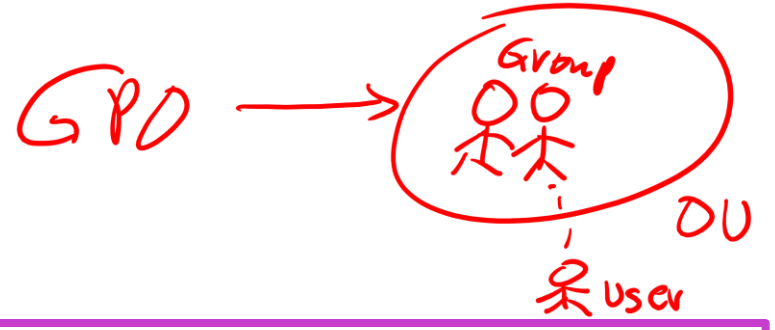


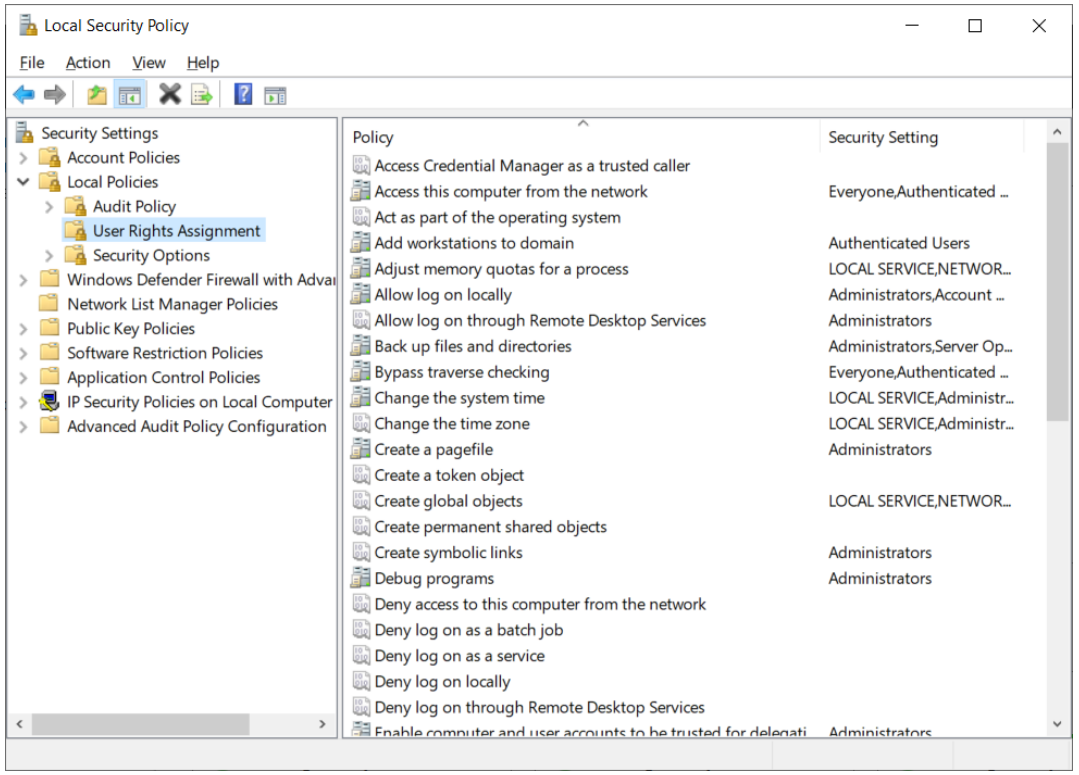
- When configuring user rights, follow the principle of least privilege
- Grant users only the rights and privileges they need to perform their tasks
- This approach helps to limit access in the event of account compromise

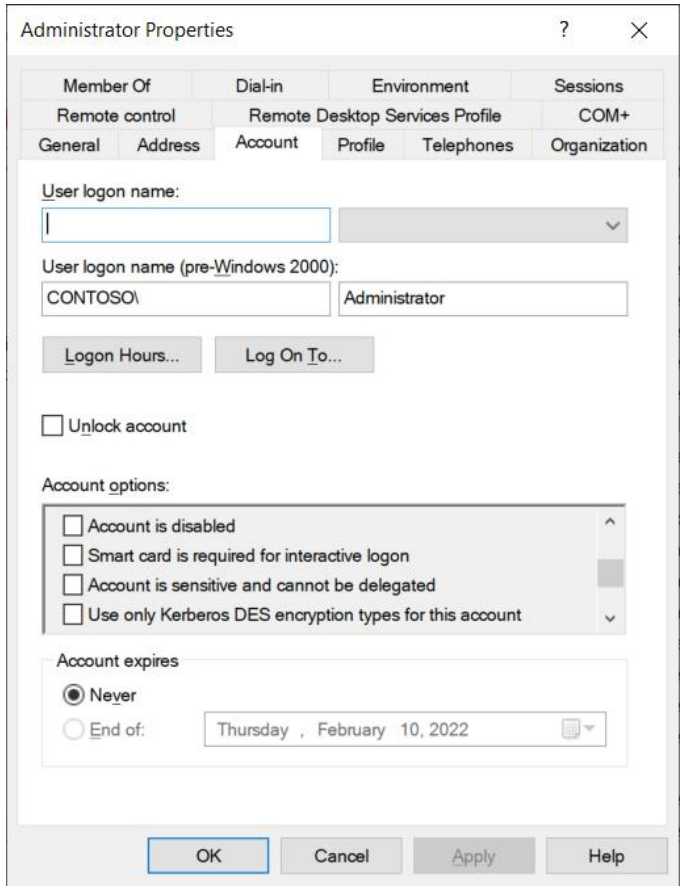
You can use the following to help manage user rights:

- User rights assignment policy, such as:
  - Take ownership of files or other objects
  - Load and unload device drivers
- Account security options, including:
  - Logon hours
  - Logon workstations
  - Account is sensitive and cannot be delegated

Configure User Account Rights

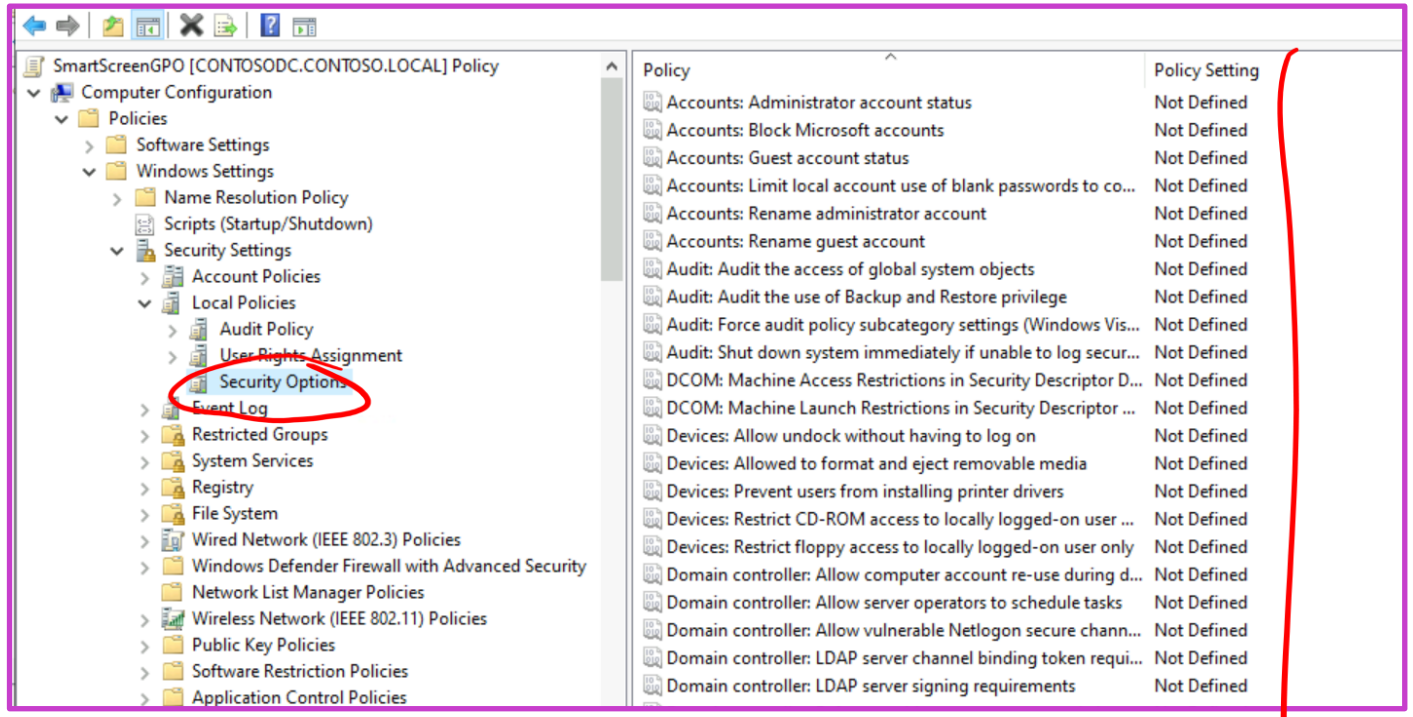






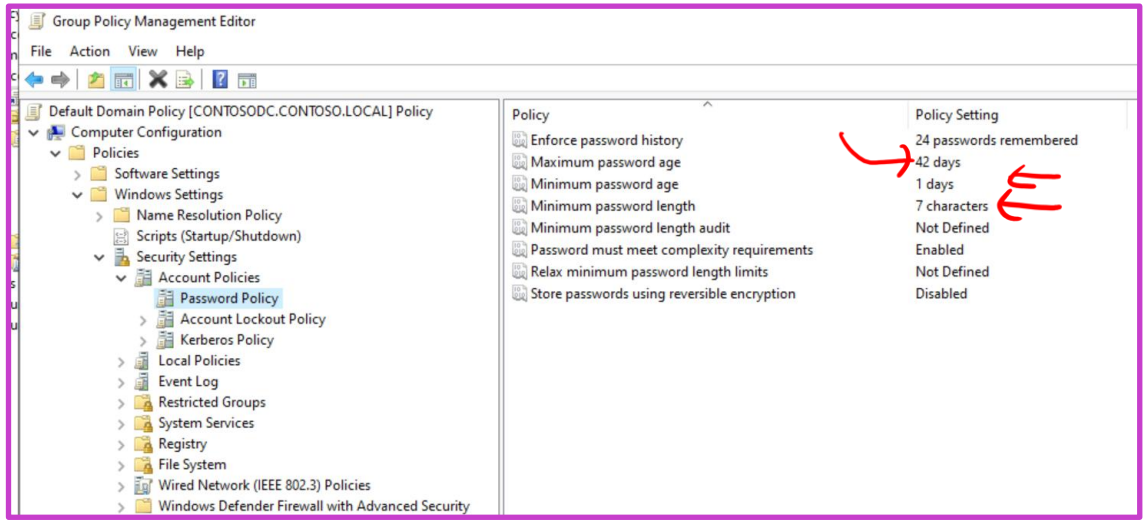
Configure Security Options

Security policy settings are rules that are configured on a computer or multiple devices for protecting resources on a device or network.



- The Security Settings extension of the Local Group Policy Editor snap-in allows you to define security configurations as part of a Group Policy Object (GPO).
- GPOs are linked to Active Directory containers such as sites, domains, or organizational units, and they enable you to manage security settings for multiple devices from any device joined to the domain.

Configure password policies



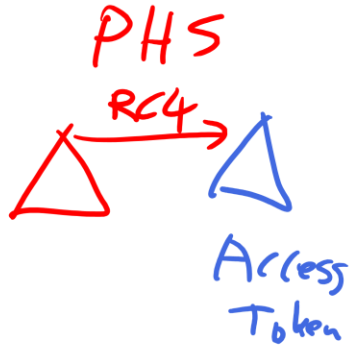
Topic	Description
Enforce password history	Describes the best practices, location, values, policy management, and security considerations for the **Enforce password history** security policy setting.
Maximum password age	Describes the best practices, location, values, policy management, and security considerations for the **Maximum password age** security policy setting.
Minimum password age	Describes the best practices, location, values, policy management, and security considerations for the **Minimum password age** security policy setting.
Minimum password length	Describes the best practices, location, values, policy management, and security considerations for the **Minimum password length** security policy setting.
Password must meet complexity requirements	Describes the best practices, location, values, and security considerations for the **Password must meet complexity requirements** security policy setting.
Store passwords using reversible encryption	Describes the best practices, location, values, and security considerations for the **Store passwords using reversible encryption** security policy setting.

- Windows Server password policies control how users authenticate with Windows servers.
- Default password policies are set using GPOs linked to the domain.
- Microsoft Entra Password Protection for Active Directory Domain Services (AD DS) gives another level of control and security.
- You can implement fine-grained password policies using Active Directory Administrative Center (or PowerShell) and assign them to a user or a global security group.

Protect User Accounts – with the Protected Users Group

When a user is a member of the Protected Users group:

- 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 Data Encryption Standard (DES) or RC4 keys, or cache credentials or long-term keys
- The user can no longer sign-in offline
- 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
- Ticket-granting tickets (TGTs) cannot renew past the initial lifetime



klist tgt

Protect User Accounts – with the Protected Users Group

Protected Users group prerequisites:

- The Protected Users group is a universal group and replicated across all domain controllers.
- The user must sign in to a device running Windows 8.1 or Windows Server 2012 R2 or newer.
- Domain controller protection requires that domains must be running at a Windows Server 2012 R2 or higher domain functional level.

Note: Lower functional levels still support protection on client devices

Protect User Accounts – with Authentication Policies

Authentication policies:

- Enable you to configure:
  - TGT lifetime
  - Access-control conditions for a user, service, or computer account
- For user accounts, you can:
  - Configure the user's TGT lifetime
  - Restrict devices the user can sign in to
  - Define criteria that the devices must meet

Authentication policy silos:

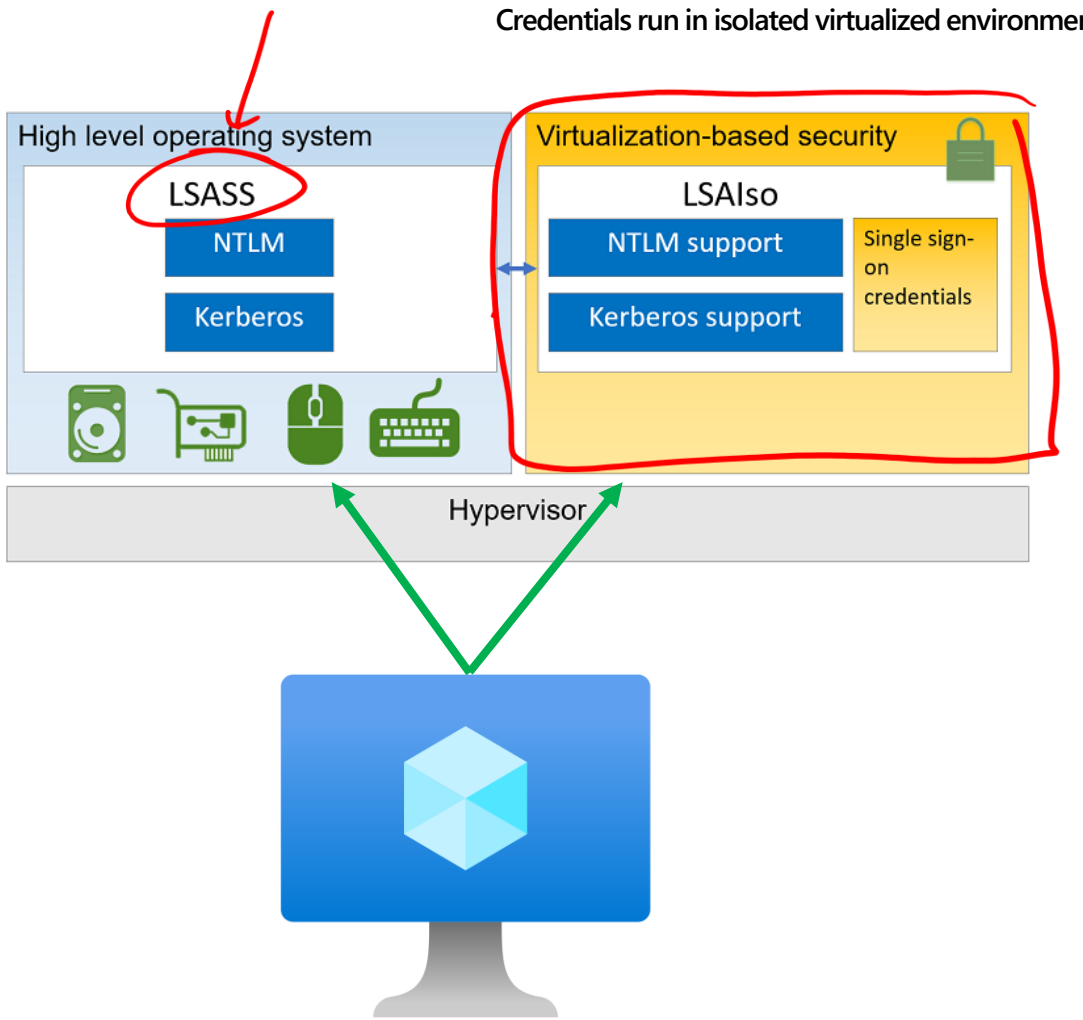
- Enable you to assign authentication policies to user, computer, and service accounts
- Work with the Protected Users group to add configurable restrictions to the group's existing non-configurable restrictions
- Ensure that the accounts belong to only a single authentication policy silo

When an account signs in, a user that is part of an Authentication Policy Silo is granted a claim. This claim controls access to claims-aware resources.

Describe Microsoft Defender Credential Guard (1 of 3)

Golden Ticket mimikatz

- Microsoft 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.
- The virtualized container's operating system runs in parallel with, but independent from, the host operating system.



Describe Microsoft Defender Credential Guard (2 of 3)

Requirements:

- Windows 10 Enterprise or Windows Server 2016 or newer
- 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

Describe Microsoft Defender Credential Guard (3 of 3)

Microsoft Defender Credential Guard does not support:

- Unconstrained Kerberos delegation
- NTLMv1 or MS-CHAPv2
- Digest authentication
- CredSSP delegation
- Kerberos DES encryption
- Use on domain controllers
- Protections for the AD DS database or Security Accounts Manager (SAM)

Block NTLM Authentication

The NTLM authentication protocol:

- Is less secure than the Kerberos authentication protocol
- Should be blocked in favor of using Kerberos

Prior to blocking NTLM, you must:

- Ensure that existing applications are no longer using the protocol

You can audit NTLM traffic by configuring the following Group Policy settings:

- Network security: Restrict NTLM: Outgoing NTLM Traffic to remote servers.
- Network security: Restrict NTLM: Audit Incoming NTLM Traffic.
- Network security: Restrict NTLM: Audit NTLM authentication in this domain.

Navigate to: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Block NTLM Authentication

After you have determined that you can block NTLM in your organization, you must configure the **Restrict NTLM: NTLM authentication in this domain** policy. The configuration options are:

- Deny for domain accounts to domain servers
- Deny for domain accounts
- Deny for domain servers
- Deny all

Navigate to: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Locate Problematic Accounts

You should check your AD DS environment for accounts that:

- Haven't signed in for a period of time
- Have passwords with no expiration date

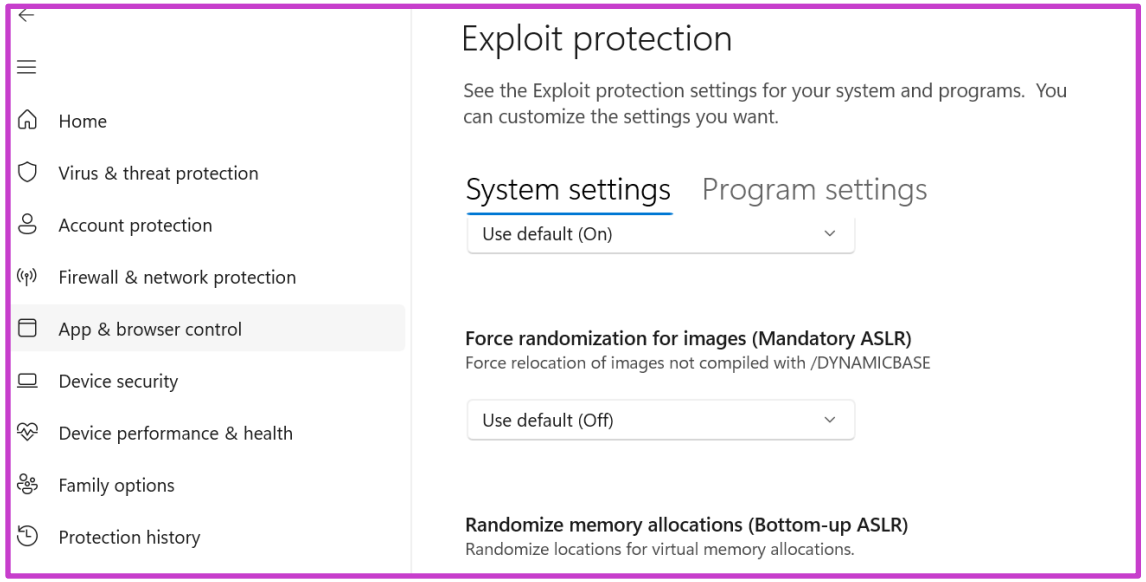
Inactive user accounts usually indicate a person that has left the organization and organization processes have failed to remove or disable the account.

Accounts with fixed passwords are less secure than accounts that are required to update their password periodically.

When you find accounts that haven't signed in for a specified number of days, you can disable those accounts.

Note: User accounts with credentials shared by multiple IT staff members should be avoided, even if they have a strong password policy.

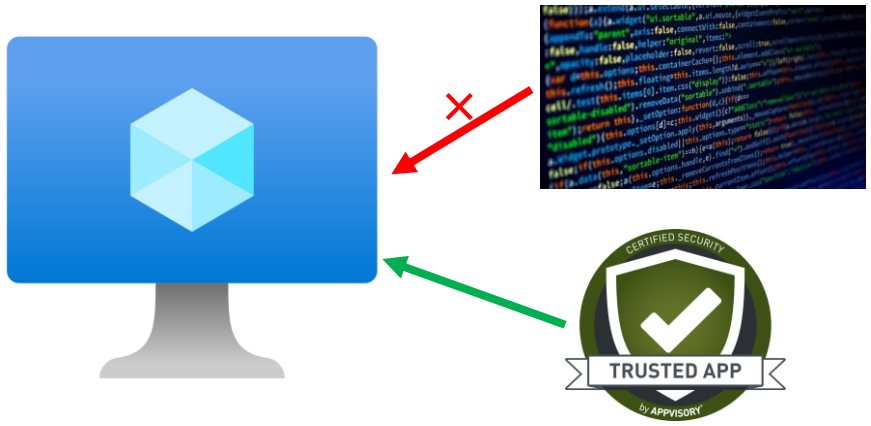
Implement Exploit Protection



Attack Surface reduction
Prevent Exploit of System
Prevent Exploit of programs

1. **Configure exploit protection settings in Windows Security app**
2. **Export the settings to an XML configuration file**
3. **Use Group Policy or Microsoft Intune to apply the same settings to multiple devices in your organization**

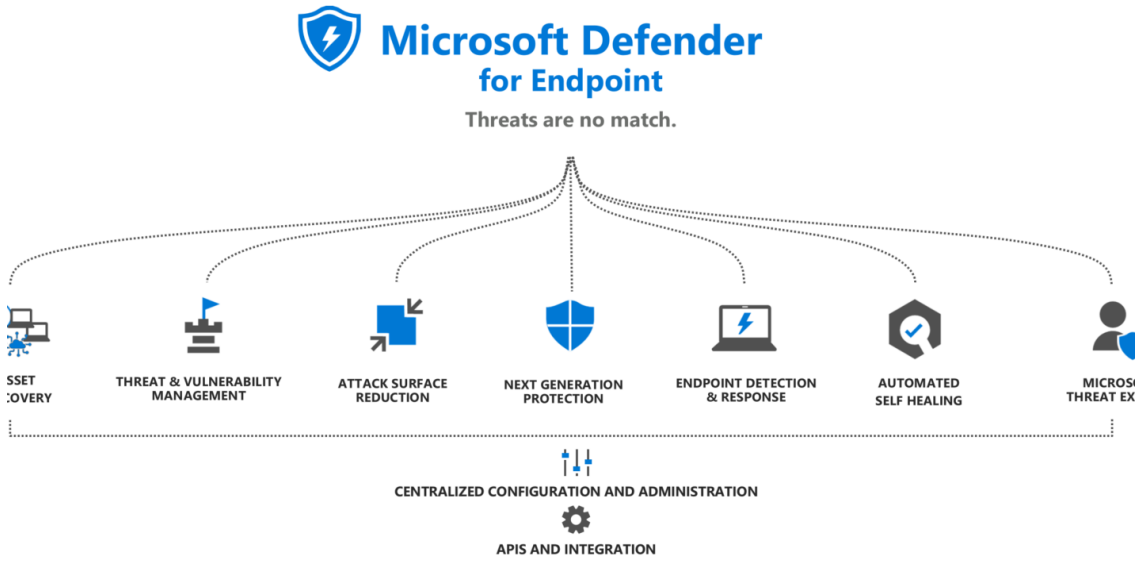
Configure and manage Windows Defender Application Control

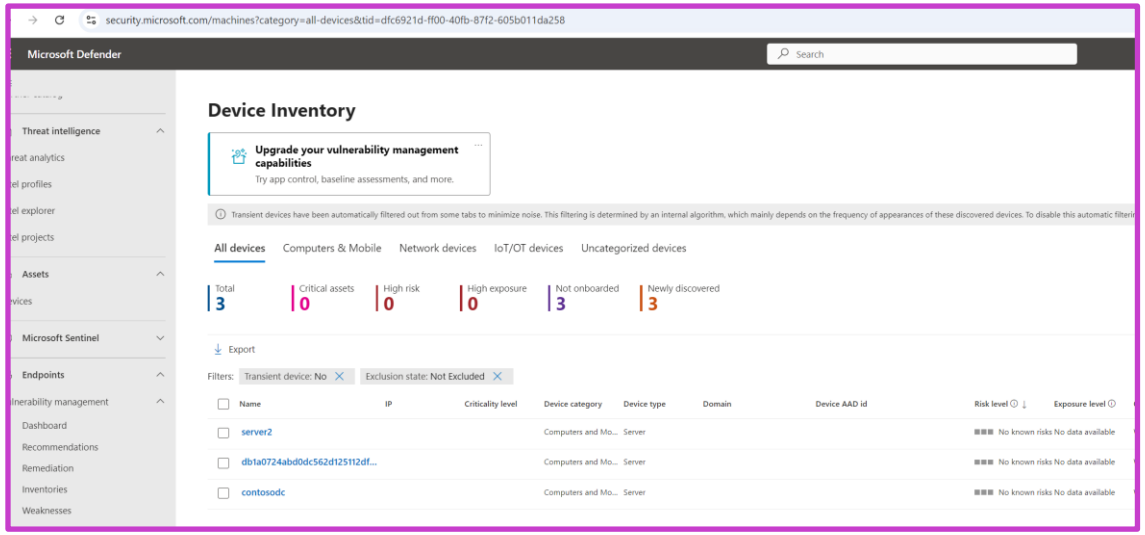


Establishing Series of Trusted and Untrusted Applications

- Windows Defender Application Control is designed to protect devices against malware and other untrusted software.
- It prevents malicious code from running by ensuring that only approved code, that you know, can be run.

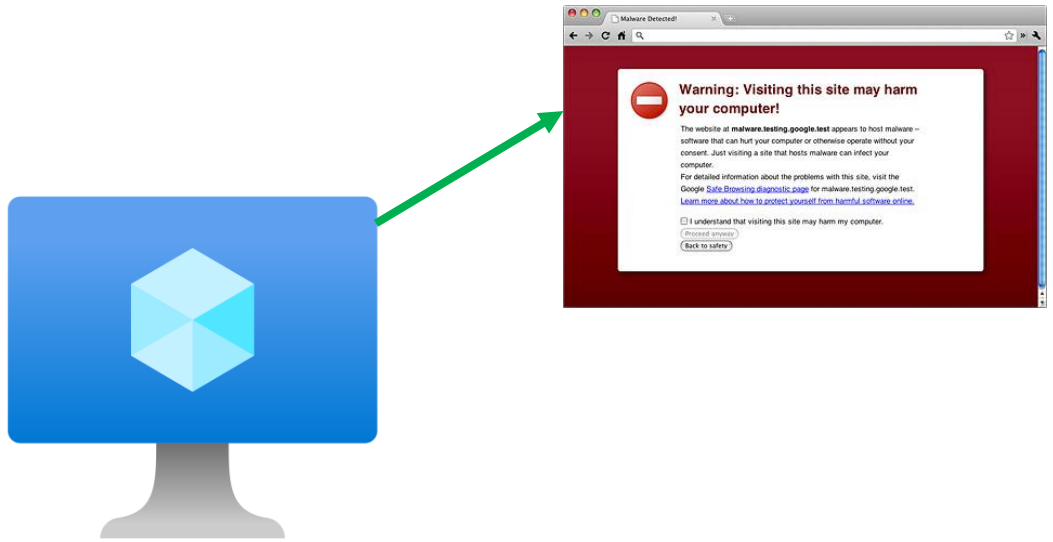
Implement Microsoft Defender for Endpoint

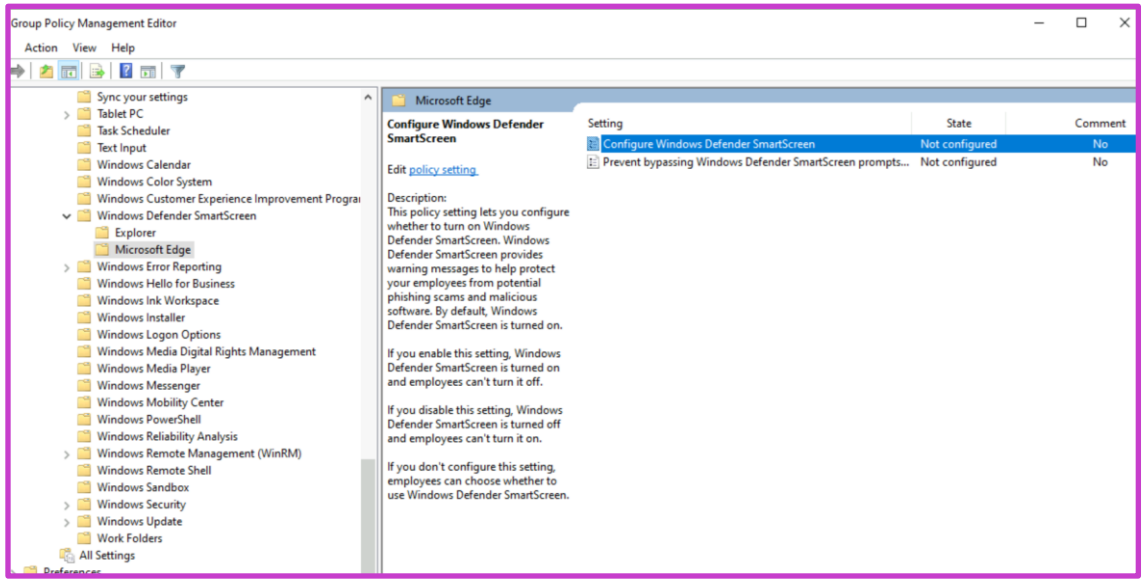




- Maximize available security capabilities and better protect your enterprise from cyber threats
- Onboarding your devices enables you to identify and stop threats quickly, prioritize risks, and evolve your defenses across operating systems and network devices

Microsoft Defender SmartScreen





Microsoft Defender SmartScreen determines whether a site is potentially malicious by:

- Analyzing visited webpages and looking for indications of suspicious behavior. If Microsoft Defender SmartScreen determines that a page is suspicious, it shows a warning page to advise caution.
- Checking the visited sites against a dynamic list of reported phishing sites and malicious software sites. If it finds a match, Microsoft Defender SmartScreen shows a warning to let the user know that the site might be malicious.

Learning recap – Secure Windows Server User Accounts

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Secure Windows Server user accounts

Hardening Windows Server

Learning Objectives – Hardening Windows Server Introduction

- OSConfig
- Local Administrator Password Solution (Windows LAPS)
- Privileged Access Workstations
- Secure Domain Controllers
- Security Compliance Toolkit
- Secure SMB traffic
- Recap

OSConfig

Capability	Description
Scenario based security configuration	Applies and enforces security baselines like Secured-core, CIS, and STIGs
Drift control	Detects drift from desired state and remediates automatically
Reporting and auditing	Generates reports on compliance and configuration status
Cross-platform support	Works on Windows Server, Azure Arc, and Linux Edge devices
Integration	Compatible with PowerShell, Azure Policy, Windows Admin Center, and GitOps

Describe Windows Local Administrator Password Solution

Windows Local Administrator Password Solution (Windows LAPS) provides organizations with a central local administrator passwords repository for domain-member machines.

Features:

- Back-up passwords in Windows Server Active Directory OR Microsoft Entra ID
- Encrypt passwords in Windows Server Active Directory
- Local administrator passwords are unique on each computer that Windows LAPS manages
- Windows LAPS randomizes and changes local administrator passwords regularly
- Windows LAPS stores local administrator passwords and secrets securely within AD DS
- Configurable permissions control access to passwords in AD DS or Microsoft Entra ID
- Passwords that Windows LAPS retrieves are transmitted to the client in a secure, encrypted manner

Describe Local Administrator Password Solution

How Windows LAPS works:

1. Windows LAPS determines if the password of the local Administrator account has expired
2. If the password hasn't expired, Windows LAPS does nothing
3. If the password has expired, Windows LAPS performs the following steps:
   a) Changes the local Administrator password to a new, random value based on the configured parameters for local Administrator passwords
   b) Transmits this new password and the new password-expiration date to AD DS or Microsoft Entra ID
   c) AD DS stores these properties in a special, confidential attribute associated with the computer account of the computer that has had its local Administrator account password updated

Note: authorized users can read passwords from AD DS, and an authorized user can trigger a local Administrator password change on a specific computer

Describe Local Administrator Password Solution

Configure and manage passwords using Windows LAPS:

There are several steps that you need to take to configure and manage passwords by using Windows LAPS.

1. Move computers targeted for LAPS to a specific OU
2. Using the **Set-LapsADComputerSelfPermission** cmdlet to assign the computer accounts the ability to update their computer's local Administrator account password when it expires

Policies that you can configure after you have installed the templates:

- Enable local admin password management.
- Password settings.

Configure Privileged Access Workstations

When configuring a PAW, you should:

- Ensure that only authorized users can sign in to the PAW
- Enable Microsoft Defender Credential Guard
- Enable BitLocker Drive Encryption
- Use Microsoft Defender Device Guard policies to restrict app execution to only trusted apps
- Block PAWs from accessing the internet.
- Install all the tools your administrative tasks require
- Limit physical access to the PAWs

Configure Privileged Access Workstations

After you have configured your PAWs, perform the following configuration tasks:

- Block RDP, Windows PowerShell, and management console connections to your servers that come from any computer that isn't a PAW
- Implement IPsec Connection specific rules so that traffic between servers and PAWs is authenticated and encrypted to help protect against replay attacks
- Configure sign-in restrictions for administrative accounts so that those accounts can only sign in to a PAW

Configure Privileged Access Workstations

Combining a daily-user workstation and a PAW:

- Combine these computers by hosting one of the operating systems in a virtual environment
- Host the daily-use workstation VM within the PAW host, and not a PAW virtual machine within a daily-user host

Note: this is recommended because if the PAW is hosted in the daily user workstation, and the workstation is compromised, the PAW could be compromised as well.

Secure Domain Controllers

Take the following precautions to help secure your organization's domain controllers:

- Ensure domain controllers are running the most recent version of the Windows Server and have current security updates
- Deploy domain controllers using the Server Core installation option
- Keep physically deployed domain controllers in dedicated, secure racks separate from other servers
- Run virtualized domain controllers either on separate virtualization hosts or as a shielded VM on a guarded fabric
- Deploy domain controllers on hardware that includes a TPM and configure all volumes with BitLocker

Secure Domain Controllers

Take the following precautions to help secure your organization's domain controllers:

- Use Microsoft Defender Device Guard to control the execution of scripts and executables on the domain controller
- Limit RDP connections by configuring RDP through Group Policy assigned to the Domain Controllers' OU
- Configure the perimeter firewall to block outbound connections to the internet from domain controllers
- Review Center for Internet Security (CIS) benchmark for Windows Server for security guidance specific to domain controllers

Analyze Security Configuration with Security Compliance Toolkit

What is Microsoft Security Compliance Toolkit?

- The Microsoft SCT is a set of tools provided by Microsoft that you can use to download and implement security configuration baselines
- You can also use the SCT to compare your current GPOs to the recommended GPO security baselines
- You can then edit the recommended GPOs and apply them to devices in your organization

Contents included in SCT:

- Policy Analyzer tool
- LGPO tool

Analyze Security Configuration with Security Compliance Toolkit

Policy Analyzer tool:

- Highlights redundant or inconsistent settings
- Highlights differences between sets of GPOs
- Compares GPOs to local policy and registry settings
- Exports results to Microsoft Excel

LGPO tool:

- Helps you verify the effects of GPO settings on a local host
- Enables you to manage systems that are not domain joined
- Can export and import Registry Policy settings files, security templates, Advanced Auditing backup files, and from LGPO files, text files with a special formatting

Secure SMB traffic

What is SMB 3.1.1 protocol security?

SMB 3.1.1, provides several enhancements over SMB 3.0 security, including:

- Preauthentication integrity checks
- Encryption improvements

These are discussed on the following slide

Note: Server Message Block (SMB) protocol is a network protocol primarily used for file sharing

Secure SMB traffic

Preauthentication integrity

With preauthentication integrity, while a session is being established the “negotiate” and "session setup" messages are protected by using a strong (SHA-512) hash

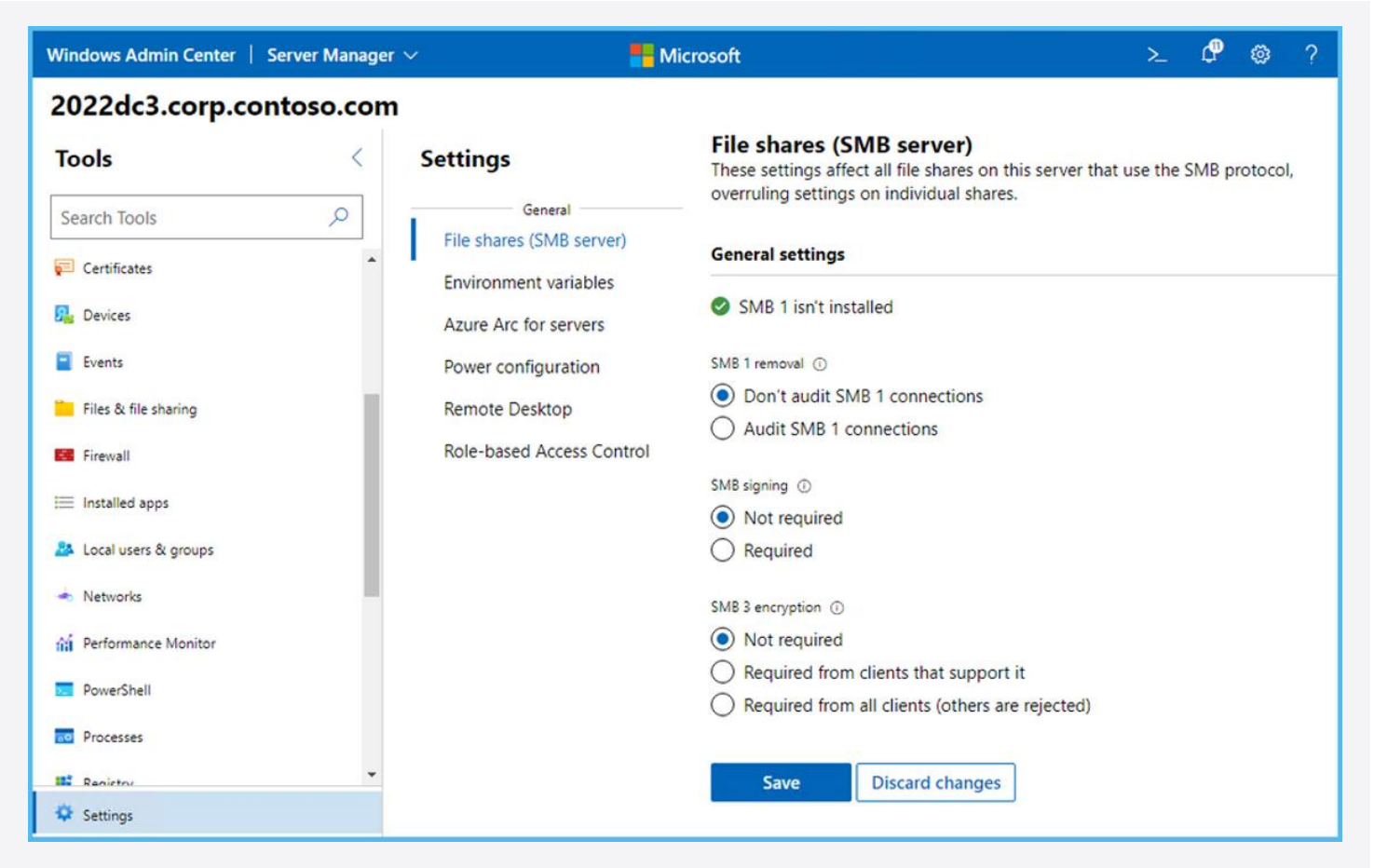
SMB encryption improvements

- SMB encryption
- Directory Caching
- Rolling cluster upgrade support
- Support for FileNormalizedNameInformation API calls
- Write-through to disk
- Guest access to file shares
- SMB global mapping
- SMB dialect control

Secure SMB traffic

You can configure SMB encryption:

- On a per-share basis or for an entire file server
- Using Windows Admin Center
- Using Windows PowerShell:
  - Set-SmbShare –Name <sharename> -EncryptData $true
  - Set-SmbServerConfiguration –EncryptData $true
  - New-SmbShare –Name <sharename> -Path <pathname> –EncryptData $true
  - Set-SmbServerConfiguration –RejectUnencryptedAccess $false



Learning recap – Hardening Windows Server

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Hardening Windows Server

Windows Server Update Management

Learning Objectives – Windows Server Update Management

- Explore Windows Update
- Outline Windows Server Update Services server deployment options
- Define Windows Server Update Services update management process
- Describe the process of Update Management
- Learning recap

Explore Windows Update

Windows Update is a Microsoft service that provides updates to Microsoft software. This includes service packs, security patches, drive updates, and even firmware updates.

The Windows Update Orchestrator scans for and downloads updates. You can configure the orchestrator to get updates from a Windows Server Update Services (WSUS) by using Group Policy.

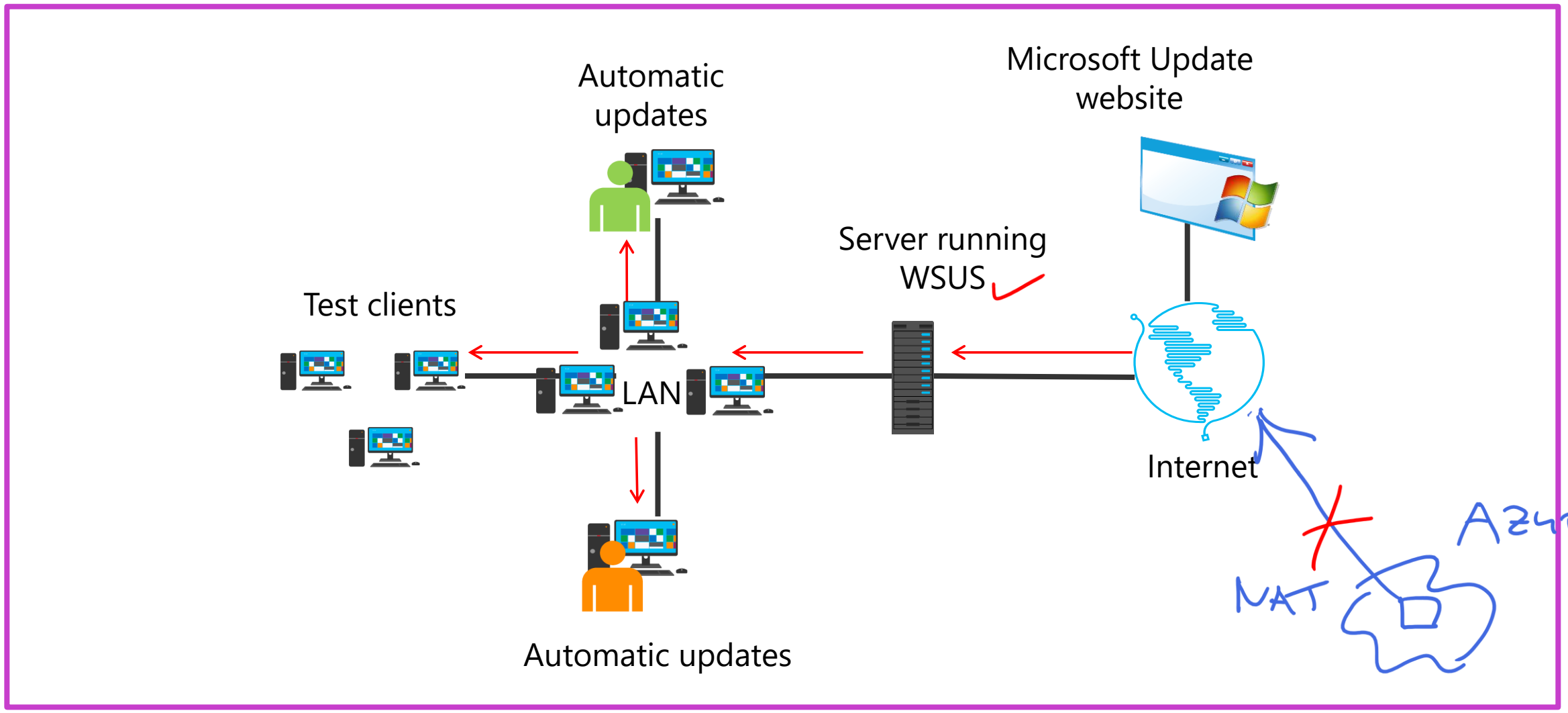
What is WSUS?

WSUS is a server role that helps you download and distribute updates to Windows clients and servers.

What does WSUS provide?

WSUS provides a central management point for updates to your computers running Windows operating systems.

Explore Windows Update



Outline Windows Server Update Services Server Deployment Options

WSUS implementations vary in size and configuration depending on your network environment and how you want to manage updates.

1. Single WSUS server
2. Multiple WSUS servers
3. Disconnected WSUS servers
4. WSUS server hierarchies

Define Windows Server Update Services Update Management Process

The update management process enables you to manage and maintain WSUS (Windows Server Update Services) and the updates retrieved by WSUS. The four phases in the update management process are:

1. The assess phase
2. The identify phase
3. The evaluate and plan phase
4. The deploy phase

Define Windows Server Update Services Update Management Process

Troubleshooting WSUS

List of common problems you could encounter when managing a WSUS environment:

- Computers not displaying in WSUS
- WSUS server stops with a full database
- You cannot connect to WSUS

Knowledge Check and Resources – Windows Server Update Management

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Windows Server update management

Lab 01: Configuring Security in Windows Server

Lab 01 – Configuring Security in Windows Server

Lab scenario

Contoso Pharmaceuticals is a medical research company with about 5,000 employees worldwide. They have specific needs for ensuring that medical records and data remain private. The company has a headquarters location and multiple worldwide sites. Contoso has recently deployed a Windows Server and Windows client infrastructure. You have been asked to implement improvements in the server security configuration.

Objectives

- Configure Microsoft Defender Credential Guard
- Locate problematic user accounts
- Implement and verify Windows LAPS

End of presentation