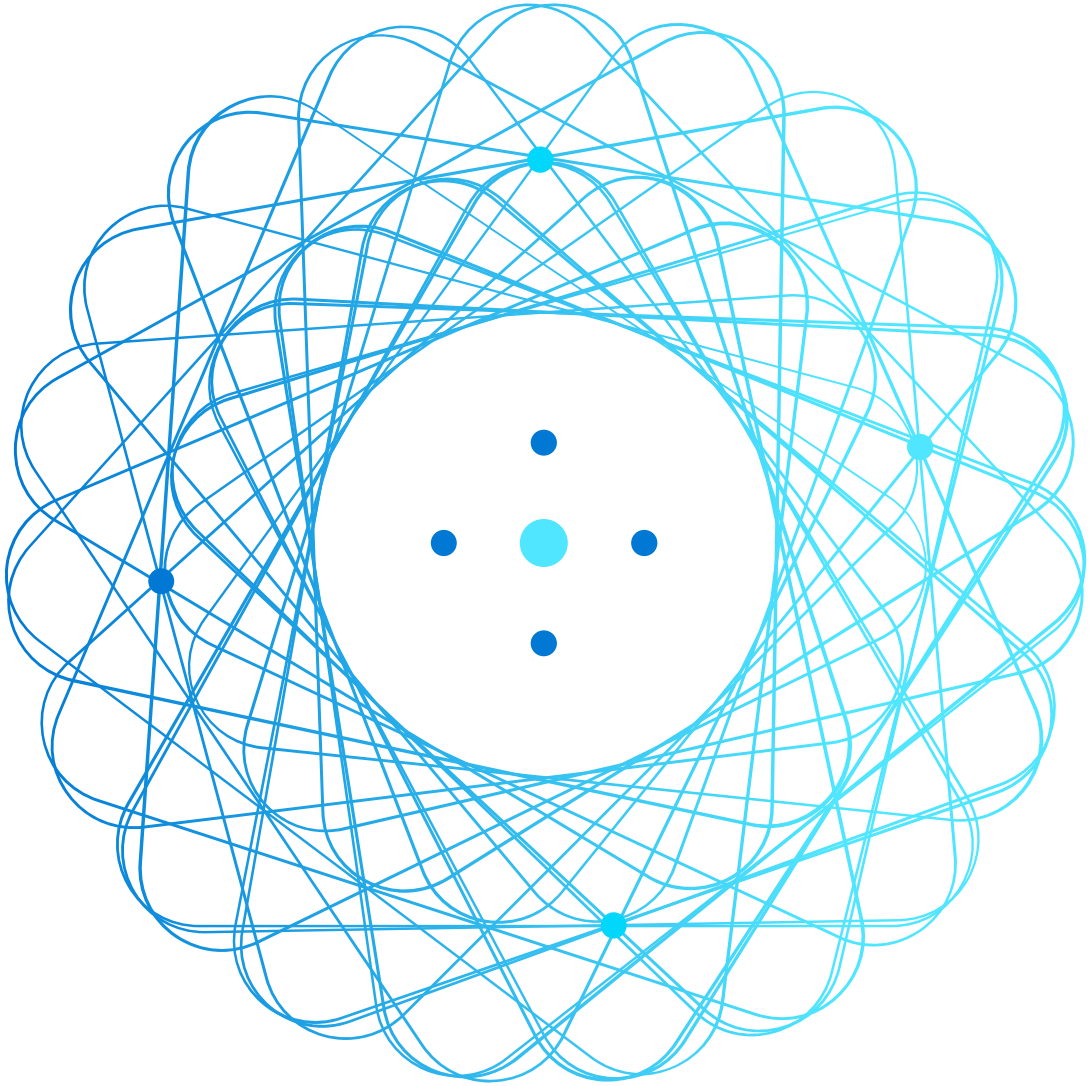
Microsoft Azure

AZ-801

Configuring Windows Server Hybrid Advanced Services



Course Outline

LP Number	Learning Path	Coverage
1	Secure Windows Server on-premises and hybrid infrastructures	Windows Server security
1	Secure Windows Server on-premises and hybrid infrastructures	Implementing security solutions in hybrid scenarios
2	Implement Windows Server high availability	Implementing Windows Server high availability
3	Implement disaster recovery in Windows Server on-premises and hybrid environments	Disaster recovery in Windows Server
3	Implement disaster recovery in Windows Server on-premises and hybrid environments	Implementing recovery services in hybrid scenarios
4	Migrate servers and workloads in on-premises and hybrid environments	Upgrade and migrate in Windows Server
4	Migrate servers and workloads in on-premises and hybrid environments	Implementing migration in hybrid scenarios
5	Monitor and troubleshoot Windows Server environments	Server and performance monitoring in Windows Server
5	Monitor and troubleshoot Windows Server environments	Implementing operational monitoring in hybrid scenarios

Learning Path 1: Secure Windows Server on-premises and hybrid infrastructures

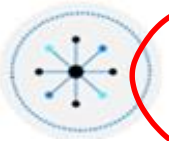
(Windows Server security)

Secure Windows Server user accounts

Hardening Windows Server

Windows Server update management

Secure Windows Server DNS



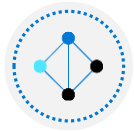
Lab 01

Skillable

- Least Privilege
- Shared Resonsabil
- Zero Trust

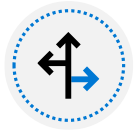
Module 1: Secure Windows Server user accounts

Secure Windows Server user accounts



Configure user account rights

Protect user accounts



Describe Microsoft Defender Credential Guard

Block NTLM authentication

Locate problematic accounts

Knowledge check and resources

Configure user account rights

When configuring user rights, follow the principle of least privilege

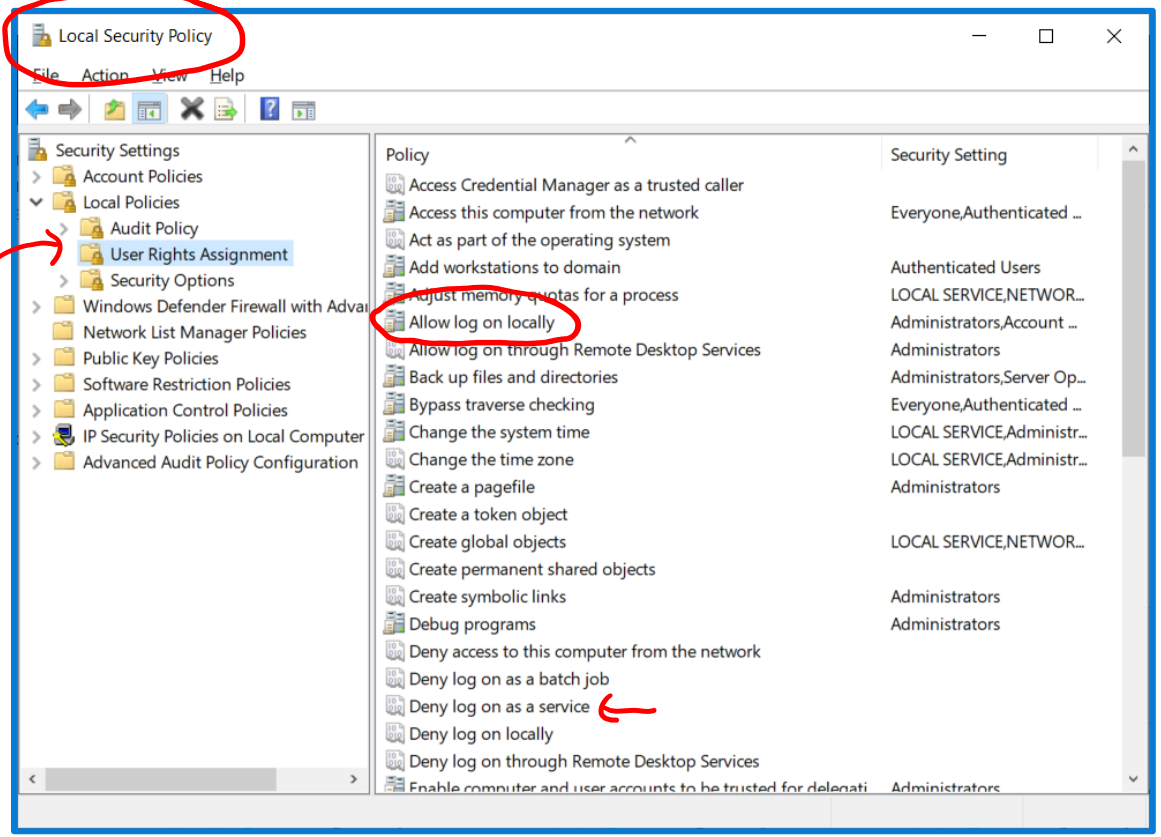
Grant users only the rights and privileges they need to perform their tasks

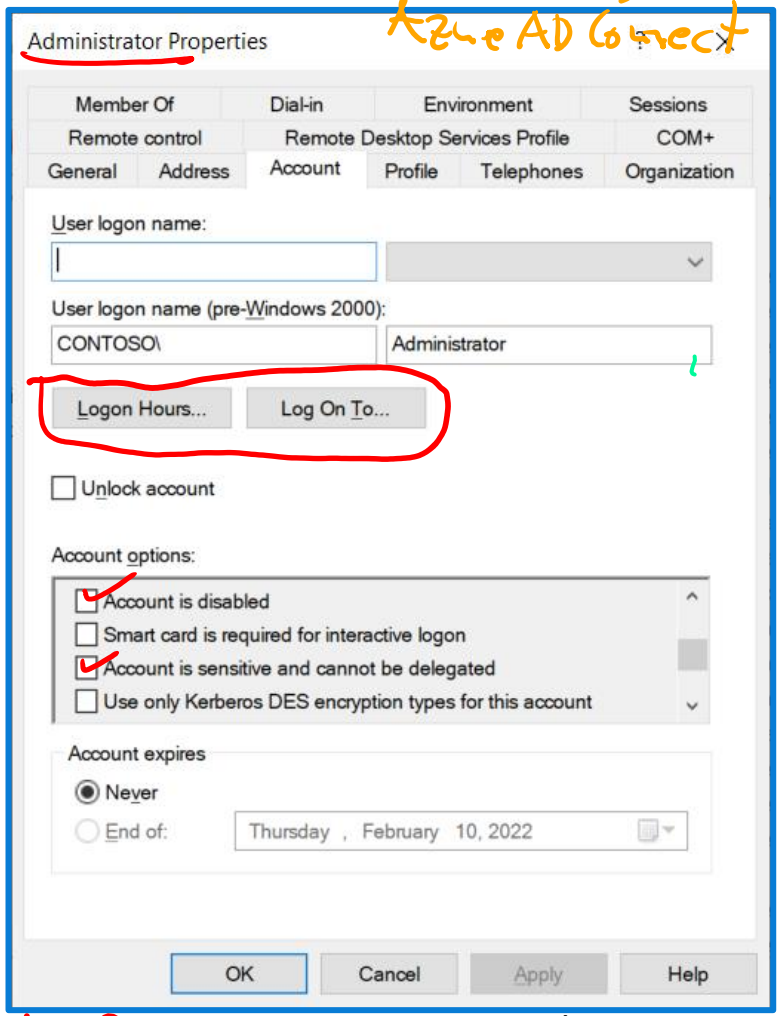
This approach helps to limit access in the event of account compromise

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

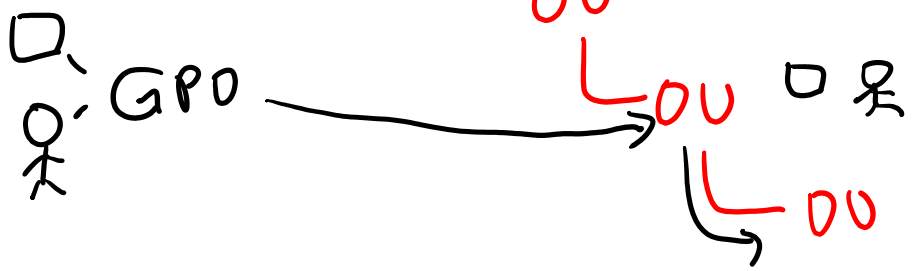




On Prem AD

LDAP

OU



:88

Kerberos (NTLM)

↳ Ticket

klist tgt

klist

Azure AD

nur ID Provider

Data Lake

Flat

AU Admin Unit

Roles → 👤👤

z.B.

UserAdmin

Sync.

Azure AD Connect (MIM)

a) PHS *

b) Fed

c) PTA

write Back Password Group Member

Refresh Token

Get-AzAccessToken

HTTP friendly

OAuth ↳ Token (JWT)

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

Protect user accounts – with the Protected Users group

Protected Users group prerequisites:

- 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 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

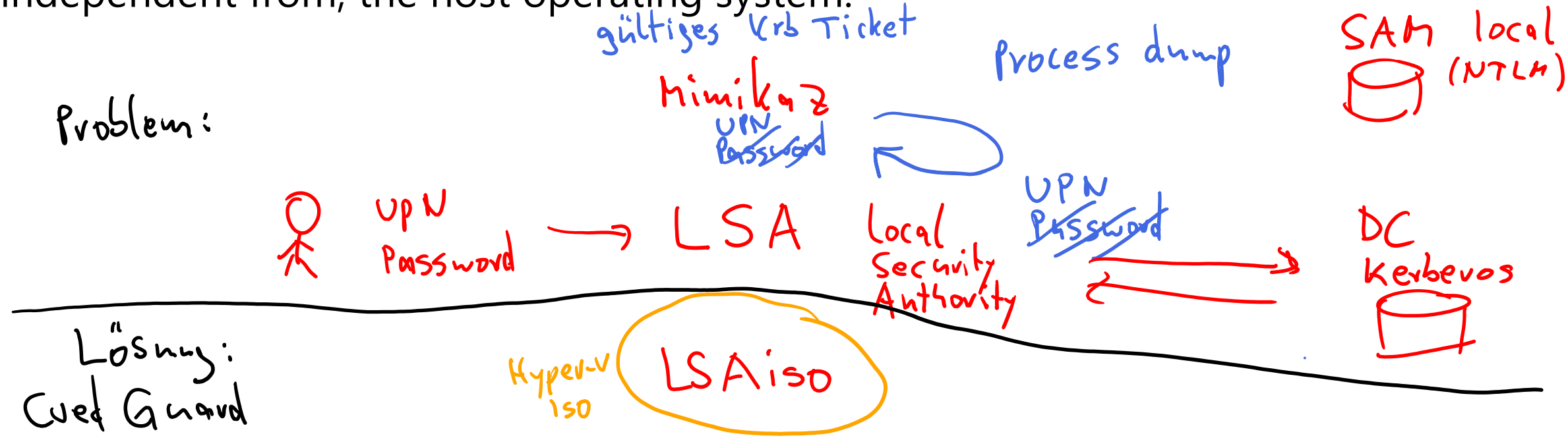
Authentication policy silos:

- 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

- 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

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

Windows 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.

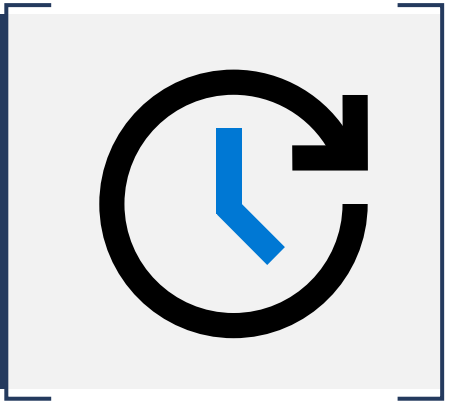
Get-ADUser

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

Knowledge check and resources – Secure Windows Server user accounts

Knowledge Check	Microsoft Learn Modules (docs.microsoft.com/Learn)
	Secure Windows Server user accounts

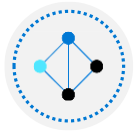
Module 2: Hardening Windows Server



LAPS Tool

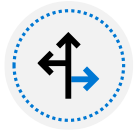
SVR2$

Hardening Windows Server Introduction



Describe Local Password Administrator Solution

Configure Privileged Access Workstations



Secure domain controllers

Analyze security configuration with Security Compliance Toolkit

Secure SMB Traffic

Knowledge check and resources

Describe Local Password Administrator Solution

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

Features:

- Local administrator passwords are unique on each computer that LAPS manages
- LAPS randomizes and changes local administrator passwords regularly
- LAPS stores local administrator passwords and secrets securely within AD DS
- Configurable permissions control access to passwords in AD DS
- Passwords that LAPS retrieves are transmitted to the client in a secure, encrypted manner

You can download LAPS from Microsoft's website

Describe Local Password Administrator Solution

How LAPS works:

1. LAPS determines if the password of the local Administrator account has expired
2. If the password hasn't expired, LAPS does nothing
3. If the password has expired, 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
    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

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 Password Administrator Solution

Configure and manage passwords using LAPS:

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

1. Move computers targeted for LAPS to a specific OU
2. Using the **Set-AdmPwdComputerSelfPermission** cmdlet to assign the computer accounts the ability to update their computer's local Administrator account password when it expires
3. Run the LAPS installer to install the GPO templates into AD DS

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 Connection Security 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

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

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

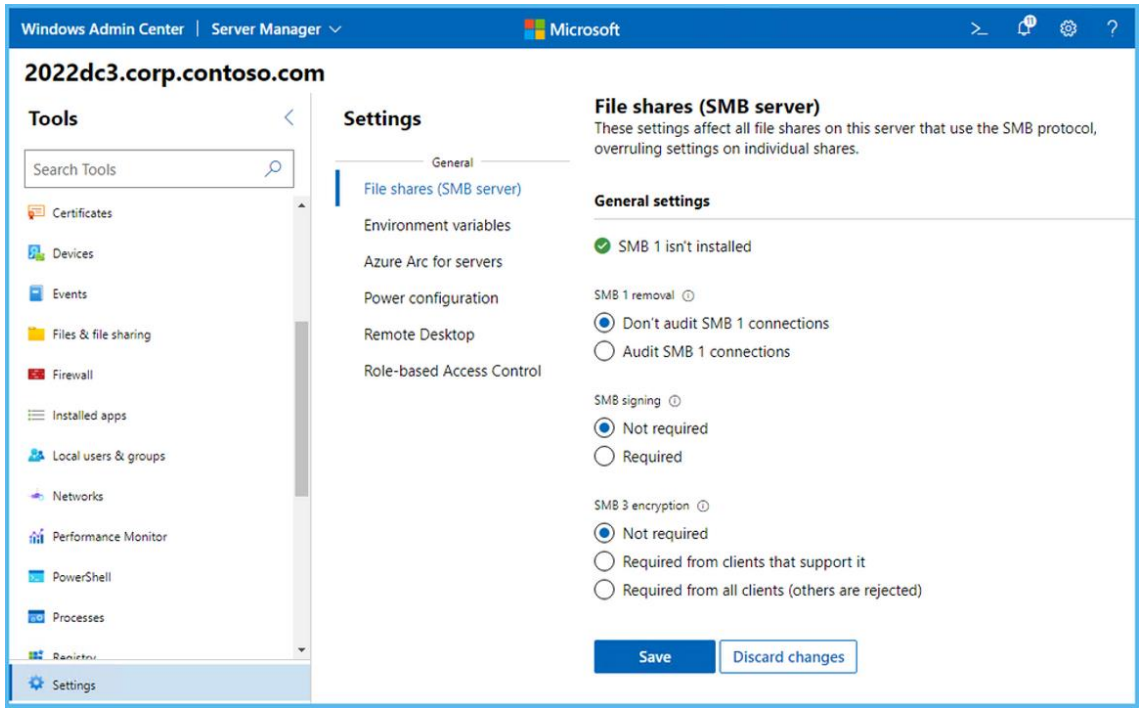
SMB encryption improvements

- 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:

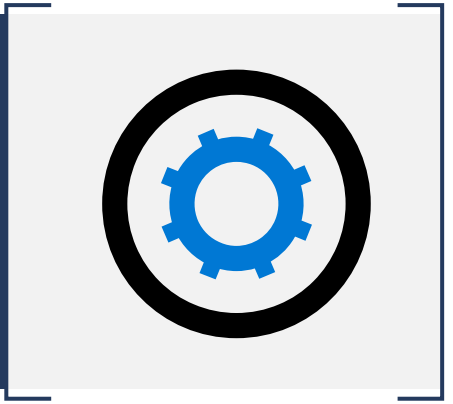
- On a per-share basis or for an entire file server
- Using Windows Admin Center
- Using Windows PowerShell:
  - Set-SmbShare –Name <sharename> -EncryptData $true
  - Set-SmbServerConfiguration –EncryptData $true
  - New-SmbShare –Name <sharename> -Path <pathname> –EncryptData $true
  - Set-SmbServerConfiguration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



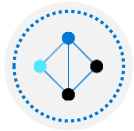
Knowledge check and resources – Hardening Windows Server

Knowledge Check	Microsoft Learn Modules (docs.microsoft.com/Learn)
	Hardening Windows Server

Module 3: Windows Server update management

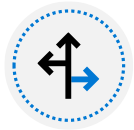


Windows Server update management Introduction



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

Knowledge check and resources

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.

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

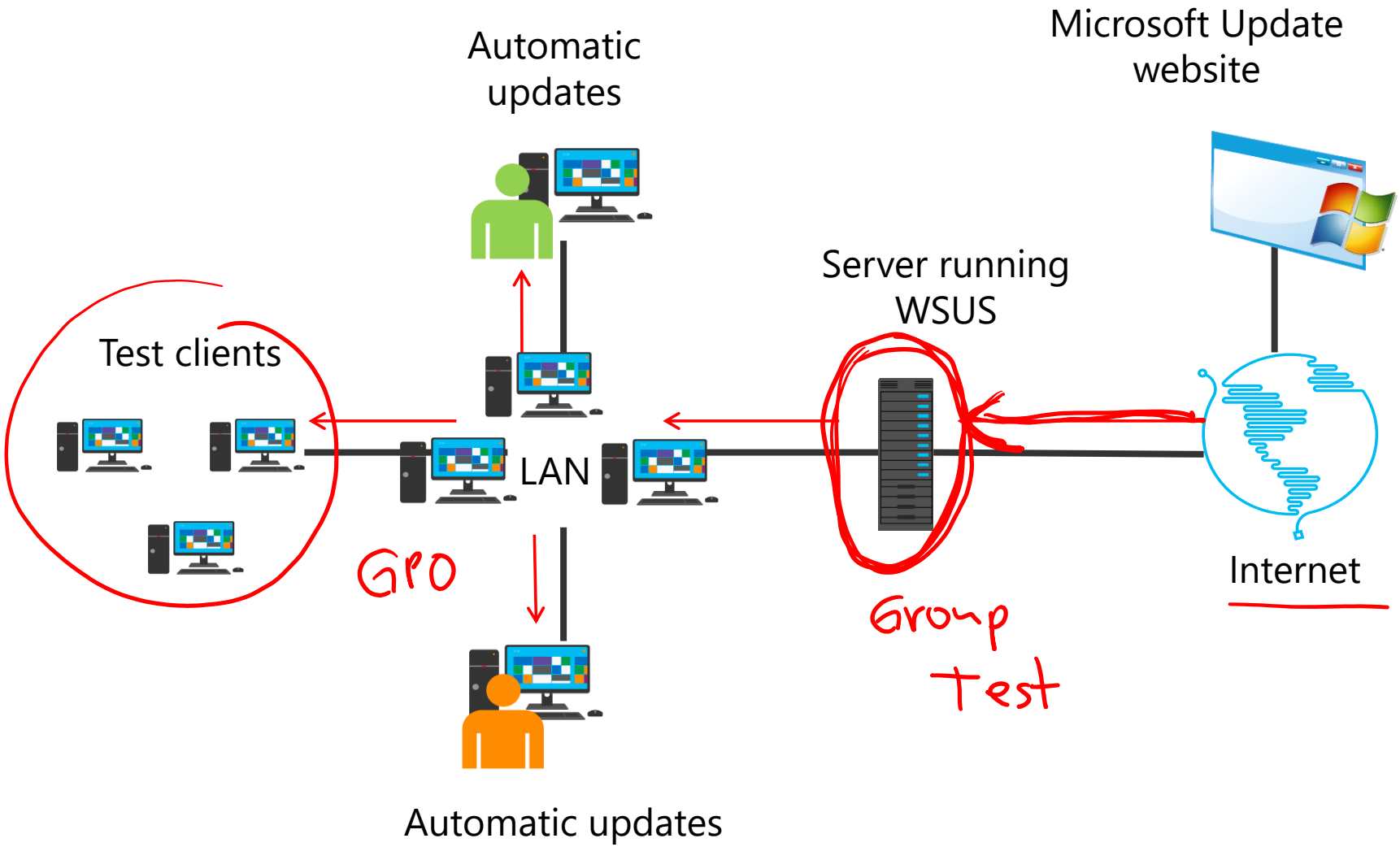
What is WSUS?

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.

Single WSUS server

Multiple WSUS servers

Disconnected WSUS servers

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

Describe the process of Update Management

You can also use Microsoft Azure Update Management, in conjunction with WSUS or instead of WSUS to manage updates on your servers.

What is Azure Automation?

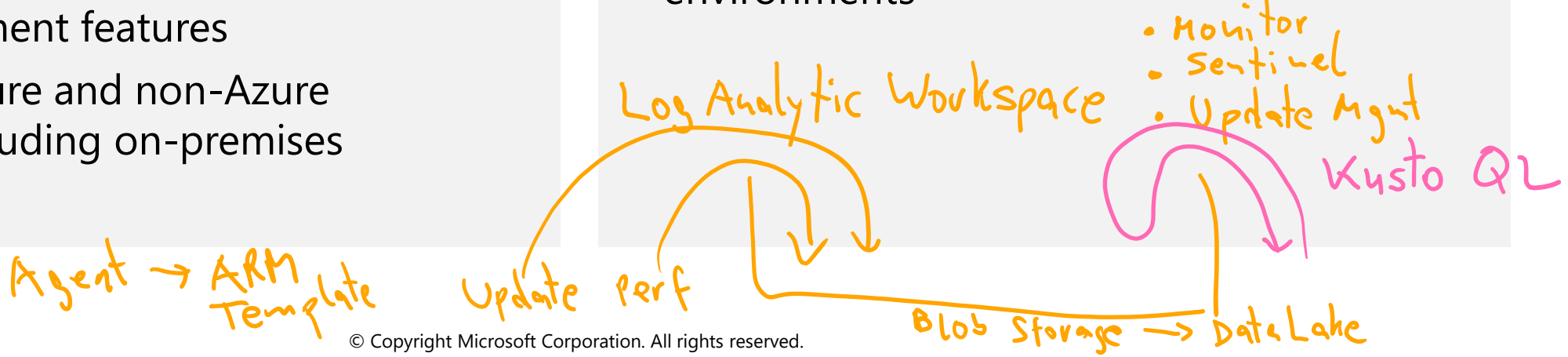
A cloud-based service that provides:

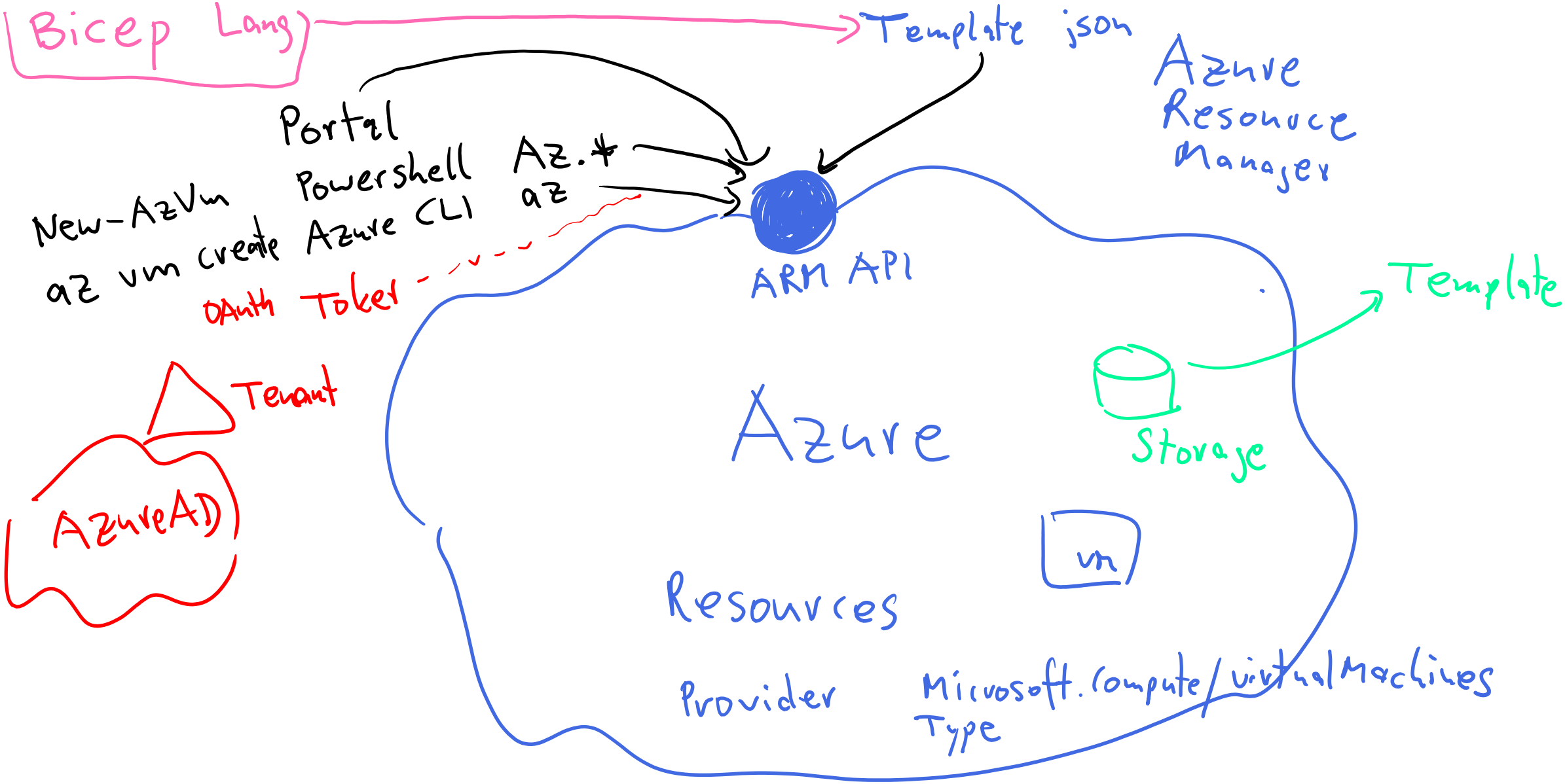
- Process automation
- Configuration management
- Update management
- Other management features

Supports both Azure and non-Azure environments, including on-premises environments.

What is Update Management?

- A free service within Azure Automation that helps you manage operating system updates for both Windows and Linux machines
- Supports both cloud and on-premises environments





Describe the process of Update Management

Update Management capabilities

Update Management includes the following capabilities related to on-premises servers:

- Check status of updates on your servers
- Configure dynamic groups of machines to target
- Search Azure Monitor logs

Onboarding your on-premises server

- You must add your on-premises servers to Update Management in Azure Automation manually
- After you enable Update Management, you then download and install the Log Analytics agent for Windows to your on-premises server

Knowledge check and resources – Windows Server update management

Knowledge Check	Microsoft Learn Modules (docs.microsoft.com/Learn)
	Windows Server update management

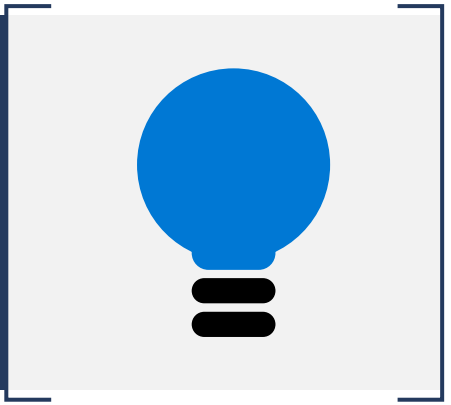
DSC

Ansible
SSH

Module 4: Secure Windows Server DNS

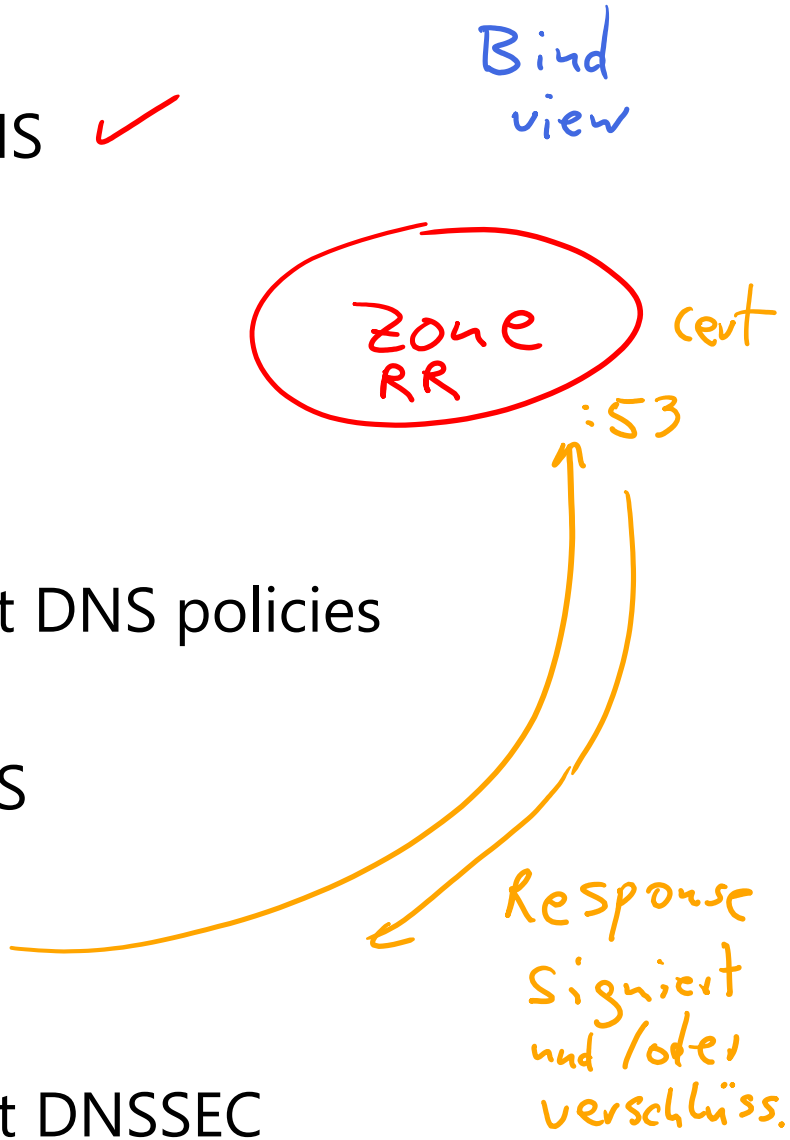
(AWS Route 53)

.53

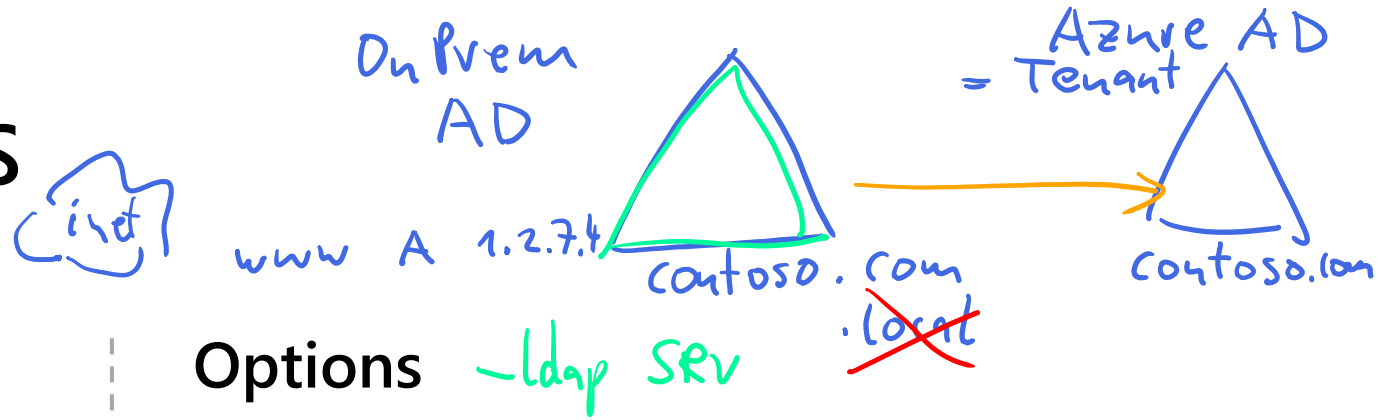


Secure Windows Server DNS Introduction

- Implement split-horizon DNS
- Create DNS policies
- Implement DNS policies
- Demonstration – Implement DNS policies
- Secure Windows Server DNS
- Implement DNSSEC
- Demonstration – Implement DNSSEC
- Knowledge check and resources



Implement split-horizon DNS



Implement split-DNS

- Split-horizon DNS, also known as split DNS, uses the same DNS domain name for both internet and internal domain-member resources.
- However, the DNS server role is assigned to separate servers: one or more servers for the internet, and the other server(s) for the AD DS domain.

Options

- Use the same namespace internally and externally
- Use unique namespaces for the internal and public namespaces
- Use a subdomain of the public namespace for AD DS

Implement split-horizon DNS

Non-split configuration

Host	Record type	IP address
www	A	131.107.1.200
Relay	A	131.107.1.201
Webserver1	A	192.168.1.200
Exchange1	A	192.168.0.201

Split-DNS configuration – internal zone

Host	Record type	IP address
www	CNAME	Webserver1.contoso.com
Relay	CNAME	Exchange1.contoso.com
Webserver1	A	192.168.1.200
Exchange1	A	192.168.0.201

SRV

Split-DNS configuration – external zone

Host	Record type	IP address
www	A	131.107.1.200
Relay	A	131.107.1.201
	MX	Relay.contoso.com

Create DNS policies

Scenarios for using DNS policies

- You can use DNS policies to manipulate how a DNS server manages queries based on different factors.

Various factors that might benefit from creating a DNS policy, based on the following scenarios:

- Application high availability
- Traffic management
- Split DNS
- Filtering
- Forensics
- Time-of-day based redirection

DNS policy objects

- You can identify the elements by the DNS policy objects, such as Client subnet, Recursion scope and Zone scopes.

Implement DNS policies

Two policy types of DNS policies:

- Query-resolution policies
- Zone-transfer policies

The high-level steps to resolve a host record differently for users from a specific IP address range are:

1. Create a DNS server client subnet for the IP address range.
2. Create a DNS server zone scope for the zone containing the host record.
3. Add a host record to the zone that is specific to the zone scope.
4. Add a DNS server query resolution policy that allows the DNS server client subnet to query the zone scope for the zone.

Implement DNS policies

```
# Create the required subnets
Add-DnsServerClientSubnet -Name "LondonSubnet" -IPv4Subnet "172.16.18.0/24"
Add-DnsServerClientSubnet -Name "SeattleSubnet" -IPv4Subnet "172.16.10.0/24“

# Create the DNS server zone scopes
Add-DnsServerZoneScope -ZoneName "Contoso.com" -Name "LondonZoneScope"
Add-DnsServerZoneScope -ZoneName "Contoso.com" -Name "SeattleZoneScope"
```

Implement DNS policies

BIND

```
# Add the required host records

Add-DnsServerResourceRecord -ZoneName "Contoso.com" -A -Name "www" -IPv4Address
"172.16.10.41" -ZoneScope "SeattleZoneScope"

Add-DnsServerResourceRecord -ZoneName "Contoso.com" -A -Name "www" -IPv4Address
"172.16.18.17" -ZoneScope "LondonZoneScope“

# Create the DNS server query resolution policies

Add-DnsServerQueryResolutionPolicy -Name "LondonPolicy" -Action ALLOW -ClientSubnet
"eq,LondonSubnet" -ZoneScope "LondonZoneScope,1" -ZoneName "Contoso.com"

Add-DnsServerQueryResolutionPolicy -Name "SeattlePolicy" -Action ALLOW -ClientSubnet
"eq,SeattleSubnet" -ZoneScope "SeattleZoneScope,1" -ZoneName Contoso.com
```

Demonstration – Implement DNS policies

Create the required subnets

Create the DNS server zone scopes

Add the required host records

Create the DNS server query resolution policies

Secure Windows Server DNS

NRPT (DA) Direct Access

Name Resolution PolicyTable

wenn dann

DNS intern

DNS extern

Several options for protecting the DNS server role, including:

- DNS cache locking
- DNS socket pool
- DANE
- RRL
- Unknown record support:
- DNSSEC

Implement DNSSEC

DNSSEC protects clients that are making DNS queries from accepting false DNS responses

The high-level steps for deploying DNSSEC are:

1. Sign the DNS zone
2. Configure the trust anchor distribution
3. Configure the NRPT on client computers

nslookup ✗

Resolve-DNSName ✓

Demonstration – Implement DNSSEC

Sign the zone

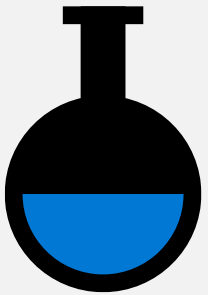
Configure the trust anchor distribution

Configure the NRPT on client computers

Knowledge check and resources – Secure Windows Server DNS

Knowledge Check	Microsoft Learn Modules (docs.microsoft.com/Learn)
	Secure Windows Server DNS

Lab 01



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 LAPS

End of presentation