Module 1

Installing, upgrading, and migrating servers and workloads

Module Overview

- Introducing Windows Server 2016
- Preparing and installing Server Core
- Preparing for upgrades and migrations
- Migrating server roles and workloads
- Windows Server activation models

Lesson 1: Introducing Windows Server 2016

- Selecting a suitable Windows Server 2016 edition
- Hardware requirements
- Overview of installation options
- Managing servers remotely
- Using Windows PowerShell 5.0 to manage servers
- What's new since Windows Server 2008 was released?
- Windows Server Servicing Channels

Selecting a suitable Windows Server 2016 edition

- Windows Server 2016 Essentials
- Windows Server 2016 Standard
- Windows Server 2016 Datacenter
- Microsoft Hyper-V Server 2016
- Windows Storage Server 2016 Workgroup
- Windows Storage Server 2016 Standard

Hardware requirements

Windows Server 2016 has the following minimum hardware requirements for Server Core installation:

Hardware	Requirement
Processor architecture	x64
Processor speed	1.4 GHz
RAM	512 MB
Hard drive space	32 GB

Overview of installation options

You can choose among the following installation options when deploying Windows Server 2016:

- Windows Server 2016 (Desktop Experience)—full server installation
- Windows Server 2016—Server Core installation
- Windows and Hyper-V containers can run on a Desktop Experience or Server Core of Windows Server 2016, and provide further application isolation

Managing servers remotely

- Use the following options to remotely manage a computer that is running Windows Server 2016:
  - Remote Server Administration Tools (RSAT)
    - Server Manager
    - Management consoles for each role/feature
  - Windows PowerShell remoting and PowerShell Direct
  - Remote shell
  - Remote Desktop
  - Group Policy (not supported on Nano Server)
- Firewall exceptions required for remote management

Using Windows PowerShell 5.0 to manage servers

Windows PowerShell is a scripting language and command-line interface that is designed to assist you in performing day-to-day administrative tasks

Administrator: Windows PowerShell

```
PS C:\> Set-Item WSMan:\localhost\Client\TrustedHosts "10.0.0.102"

WinRM Security Configuration.
This command modifies the TrustedHosts list for the WinRM client. The computers in the TrustedHosts li
authenticated. The client might send credential information to these computers. Are you sure that you
this list?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
PS C:\> $ip="10.0.0.102"
PS C:\> enter-PSSession -computername $ip -credential $ip\administrator
[10.0.0.102]: PS C:\Users\Administrator\Documents>
```

What's new since Windows Server 2008 was released?

New features and improvements introduced in Windows Server 2012 or Windows Server 2012 R2:

- Work Folders
- DHCP failover
- IPAM
- Dynamic Access Control
- Data deduplication
- Storage Spaces
- Storage tiers
- Better domain controller virtualization
- Cloning virtual domain controllers

What's new since Windows Server 2012 was released?

New features and improvements introduced in Windows Server 2016:

- Containers
- Docker support
- Rolling upgrades for Hyper-V and storage clusters
- Hot add/remove virtual memory & network adapters
- Nested virtualization
- PowerShell Direct
- Shielded virtual machines
- Windows Defender
- Storage Spaces Direct
- Storage Replica
- Remote Desktop Services
- Microsoft Passport
- Azure AD Join support
- Privileged Access Management

Windows Server Servicing Channels

Windows Server 2016 now uses the Windows-as-a-Service servicing model known as Channels

- Semi-Annual Channel
  - Contains new or updated features released every six months
  - Only available through a Microsoft SA Agreement
- LTSC
  - Traditional deployment and versioning
  - Available in Server Core or Server with Desktop Experience modes
- Both channels will release security and driver updates as required as soon as available
- Nano Server no longer supported with infrastructure roles; use Server Core or Desktop Experience modes instead

Lesson 2: Preparing and installing Server Core

- Planning for Server Core
- Installing Server Core and Server with Desktop Experience
- Post-installation configuration settings
- Discussion: selecting a suitable Windows Server edition and installation type

Planning for Server Core

- Server Core is:
  - A more security-enhanced, less resource-intensive installation option than the Desktop Experience installation
  - An installation that cannot be converted to a full graphical shell version of Windows Server 2016
  - The default installation option for Windows Server 2016
  - Managed locally by using Windows PowerShell and other standard tools
- With remote management enabled, you rarely need to sign in locally

Installing Server Core and Server with Desktop Experience

1. Perform preinstallation tasks:
   - Disconnect UPS
   - Back up server if applicable
   - Disable antivirus software
2. Run the **Windows Setup Wizard** from the installation media:
   1. Provide locale information (language, date, currency, keyboard)
   2. Select **Server Core Installation**
   3. Review and accept license
   4. Select installation location
   5. Provide administrator password

Post-installation configuration settings

After you install Windows Server 2016, you must complete the following:

- Configure the IP address
- Set the computer name
- Join an Active Directory domain
- Configure the time zone
- Enable automatic updates
- Add roles and features
- Enable the Remote Desktop feature
- Configure Windows Firewall settings

Sconfig.cmd interface screen

Administrator: C:\Windows\system32\cmd.exe - sconfig.cmd

```
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Inspecting system...


===============================================================================
                         Server Configuration
===============================================================================

1) Domain/Workgroup:                    Workgroup:  WORKGROUP
2) Computer Name:                       WIN-FNIED3G1J09
3) Add Local Administrator
4) Configure Remote Management          Enabled

5) Windows Update Settings:             DownloadOnly
6) Download and Install Updates
7) Remote Desktop:                      Disabled

8) Network Settings
9) Date and Time
10) Telemetry settings                  Enhanced
11) Windows Activation

12) Log Off User
13) Restart Server
14) Shut Down Server
15) Exit to Command Line

Enter number to select an option:
```

Lesson 3: Preparing for upgrades and migrations

- In-place upgrades vs. server migration
- In-place upgrade scenarios
- Benefits of migrating to Windows Server 2016
- Using solution accelerators
- Recommendations for server consolidation

In-place upgrades vs. server migration

- Upgrading to Windows Server 2016:
  - Can upgrade from Windows Server 2008 R2 or later
  - Can only upgrade to same or newer editions
  - Requires same processor architecture
- Migrating to Windows Server 2016:
  - Must migrate from x86 version of Windows Server
  - Can use the Windows Server Migration Tools feature

In-place upgrade scenarios

Perform an in-place upgrade when:

- Existing servers meet hardware requirements
- Software products installed on an existing server support an in-place upgrade
- You want to keep existing data and security permissions
- You want to keep existing roles, features, and settings

Benefits of migrating to Windows Server 2016

When you perform a migration, you:

- Do not affect your current Windows Server 2008 or later IT infrastructure
- Perform software product migration in a separate environment
- Perform migration of server roles, features, and settings in a separate environment
- Ensure new operating system enhancements are installed by default

Using solution accelerators

- Use Microsoft Deployment Toolkit (MDT) to:
  - Automate deployments of Windows Server 2016 or other Windows operating systems
- Use MAP Toolkit for Windows Server 2016 to:
  - Perform inventory of your organization's IT infrastructure
  - Generate a report or proposal based on the Windows Server 2016 Readiness Assessment to plan server consolidation
- Use Windows Server Migration Tools to:
  - Migrate server roles, features, operating system settings, data, and shares

Recommendations for server consolidation

- Analyze if cohosting of multiple roles is supported
- Deploy roles that are not supported for cohosting on additional servers
- Determine if cohosting multiple roles affects server performance (it should not)
- Analyze if cohosted roles are supported for high availability

Lesson 4: Migrating server roles and workloads

- Migrating server roles within a domain
- Migrating server roles across domains or forests

Migrating server roles within a domain

The roles that you can migrate from supported earlier editions of Windows Server to Windows Server 2016 include:

- AD FS Role Services
- Hyper-V
- DHCP
- DNS
- Network Policy Server
- Print and Document Services
- Remote Access
- WSUS

Migrating server roles across domains or forests

When migrating serves across domains:

- Create a new Windows Server 2016 AD DS forest
- Deploy applications on new servers
- Establish AD DS trust between the current and the new AD DS forests
- Migrate AD DS objects
- Migrate application data and settings
- Decommission and remove the old AD DS environment

Lesson 5: Windows Server activation models

- Windows Server 2016 licensing and activation

Windows Server 2016 licensing and activation

Organizations can choose between two activation strategies:

Activation strategy	**When used**
Manual	Suitable when deploying small number of servers
Automatic	Suitable when deploying larger number of servers

Module 2

Implementing failover clustering

Module Overview

- Planning a failover cluster
- Creating and configuring a new failover cluster

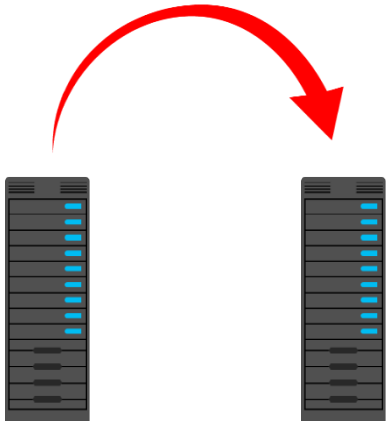
Lesson 1: Planning a failover cluster

- Preparing to implement failover clustering
- Failover-cluster storage
- Hardware requirements for a failover-cluster implementation
- Network requirements for a failover-cluster implementation
- Infrastructure and software requirements for a failover cluster
- Security considerations
- Quorum in Windows Server 2016
- Planning for migrating and upgrading failover clusters

Preparing to implement failover clustering

Features of failover clustering include:

- High availability
- Stateful application
- IP-based protocols



Preparing to implement failover clustering

Consider the following guidelines when planning node capacity in a failover cluster:

- Distribute the highly available applications from a failed node
- Ensure that each node has sufficient capacity
- Use hardware with similar capacity for all nodes in a cluster

Failover-cluster storage

- Failover clusters require shared storage to provide consistent data to a virtual server after failover
- Shared storage options include:
  - SAS
  - iSCSI
  - Fibre Channel
  - Shared .vhdx
  - Scale-Out File Server
- You can also implement clustered storage spaces to achieve high availability at the storage level

Hardware requirements for a failover-cluster implementation

The hardware requirements for a failover implementation include:

- You must use server hardware that is certified for Windows Server
- Server nodes should all have the same configuration and contain the same or similar components
- All servers must pass the tests in the **Validate a Configuration Wizard**

Network requirements for a failover-cluster implementation

The network requirements for a failover implementation include:

- Your server should connect to multiple networks to ensure communication redundancy, or it should connect to a single network with redundant hardware, to remove single points of failure
- You should ensure that network adapters are identical and that they have the same IP protocol versions, speed, duplex, and flow-control capabilities
- Your network adapters should be compatible with RSS and RDMA

Infrastructure and software requirements for a failover cluster

- The infrastructure requirements for a failover implementation include:
  - Active Directory domain controllers should run Windows Server 2008 or newer
  - Domain-functional level and forest-functional level should run Windows Server 2008 or newer
  - The application must support Windows Server 2016 high availability
- The software best practices for a failover cluster implementation require that:
  - All nodes have the same edition of Windows Server 2016 and the same service pack and updates

Security considerations

- Security considerations for failover clustering include that you must:
  - Provide a method for authentication and authorization
  - Ensure that unauthorized users do not have physical access to failover cluster nodes
  - Ensure that you use antimalware software
  - Ensure that your intra-cluster communication authenticates with Kerberos version 5
- If you use an Active Directory-detached cluster:
  - AD DS objects for network names are not created
  - Cluster network name that you register in a DNS is not necessary to create new objects in AD DS
  - We do not recommend this for any scenario that requires Kerberos authentication
  - You must run Windows Server 2012 R2 or newer on all cluster nodes

Security considerations

Windows Server 2016 introduces several cluster types, and which one you use depends on your domain-membership scenario:

- Single-domain clusters
- Workgroup clusters
- Multi-domain clusters
- Workgroup and domain clusters

Quorum in Windows Server 2016

Quorum mode	What has the vote?	When is quorum maintained?
Node majority	Only nodes in the cluster have a vote	When more than half of the nodes are online
Node and disk majority	The nodes in the cluster and a disk witness have a vote	When more than half of the votes are online
Node and file share majority	The nodes in the cluster and a file share witness have a vote	When more than half of the votes are online
No majority: disk only	Only the quorum-shared disk has a vote	When the shared disk is online
Dynamic quorum	Votes are dynamically assigned to always be odd	When half the votes are online

Quorum in Windows Server 2016

- Dynamic quorum:
  - Disk witness
  - File share witness
  - Azure Cloud Witness
- We recommend that you use dynamic quorum, which is the default configuration
- You should use all other forms of quorum in specific use cases only

Planning for migrating and upgrading failover clusters

The upgrade steps for each node in the cluster include:

- Pause the cluster node and drain all cluster resources
- Migrate cluster resources to another node in the cluster
- Replace the cluster node operating system with Windows Server 2016 and add the node back to the cluster
- Upgrade all nodes to Windows Server 2016
- Run cmdlet **Update-ClusterFunctionalLevel**

Lesson 2: Creating and configuring a new failover cluster

- The validation wizard and the cluster support-policy requirements
- The process for creating a failover cluster
- Configuring roles
- Managing failover clusters
- Configuring cluster properties
- Configuring failover and failback
- Configuring storage
- Configuring networking
- Configuring quorum options

The validation wizard and the cluster support-policy requirements

- Validation wizard performs multiple types of tests, such as:
  - Cluster
  - Inventory
  - Network
  - Storage
  - System
- You can perform validation from the **Validate a Configuration Wizard** or with the **Test-Cluster** Windows PowerShell cmdlet

The process for creating a failover cluster

1. Install the failover clustering feature
2. Verify the configuration, and create a cluster
3. Install the role on all cluster nodes by using Server Manager
4. Create a clustered application by using the Failover Clustering Management snap-in
5. Configure the application
6. Test failover

Configuring roles

- Configuring a cluster role includes:
  - Choosing a clustering role
  - Installing the role
  - Verifying the status (Running) on all cluster nodes
- You can configure a cluster role by using:
  - The **Cluster Manager** console
  - The **New-Cluster** Windows PowerShell cmdlet

Managing failover clusters

The most common management tasks include:

- Managing nodes
- Managing networks
- Managing permissions
- Configuring cluster-quorum settings
- Migrating services and applications to a cluster
- Configuring new services and applications
- Removing the cluster

Configuring cluster properties

The three aspects of managing cluster nodes include:

- Adding nodes after you create a cluster
- Pausing nodes, which prevents resources from running on that node
- Evicting nodes from a cluster, which removes the node from the cluster configuration

Configuration tasks are available in:

- The **Actions** pane of the **Failover Cluster Management** console
- Windows PowerShell

Configuring failover and failback

- During failover, the clustered instance and all associated resources move from one node to another
- Failover occurs when:
  - The node that hosts the instance becomes inactive for some reason
  - One of the resources within the instance fails
  - An administrator performs a failover
- The Cluster service can fail back after the offline node becomes active again
- Failover can be planned or unplanned

Configuring storage

Storage configuration tasks in Failover Clustering include:

- Adding storage spaces
- Adding a disk to available storage and to the CSV
- Taking a disk offline
- Bringing the disk back online

Configuring networking

Network	Description
Public network	Clients use this network to connect to the clustered service
Private network	Nodes use this network to communicate with each other
Public-and-private network	Required to communicate with external storage systems

- One network can support both client and node communications
- Multiple network adapters are recommended for enhanced performance and redundancy
- iSCSI storage should have a dedicated network

Configuring quorum options

Quorum configuration options available in the **Configure Cluster Quorum Wizard** and Windows PowerShell include:

- Use typical settings
- Add or change the quorum witness
- Advanced quorum configuration and witness selection

Dynamic quorum and quorum-configuration considerations

- Dynamic quorum management:
  - Failover cluster dynamically manages the vote assignment to nodes
  - Allows for a cluster to run on the last surviving cluster node
  - Cannot survive a simultaneous failure of a majority of voting nodes
  - If you explicitly remove a vote from a node, the cluster cannot dynamically add or remove that vote
- Quorum configuration considerations include:
  - Validating the quorum configuration by using the **Validate a Configuration Wizard** or the **Test-Cluster** Windows PowerShell cmdlet
  - Changing the quorum configuration only in specific scenarios:
    - Adding or evicting nodes
    - Node or witness have failed and cannot be recovered quickly
    - Recovering a cluster in a multisite disaster recovery scenario

Module 3

Managing, monitoring, and maintaining Windows Server

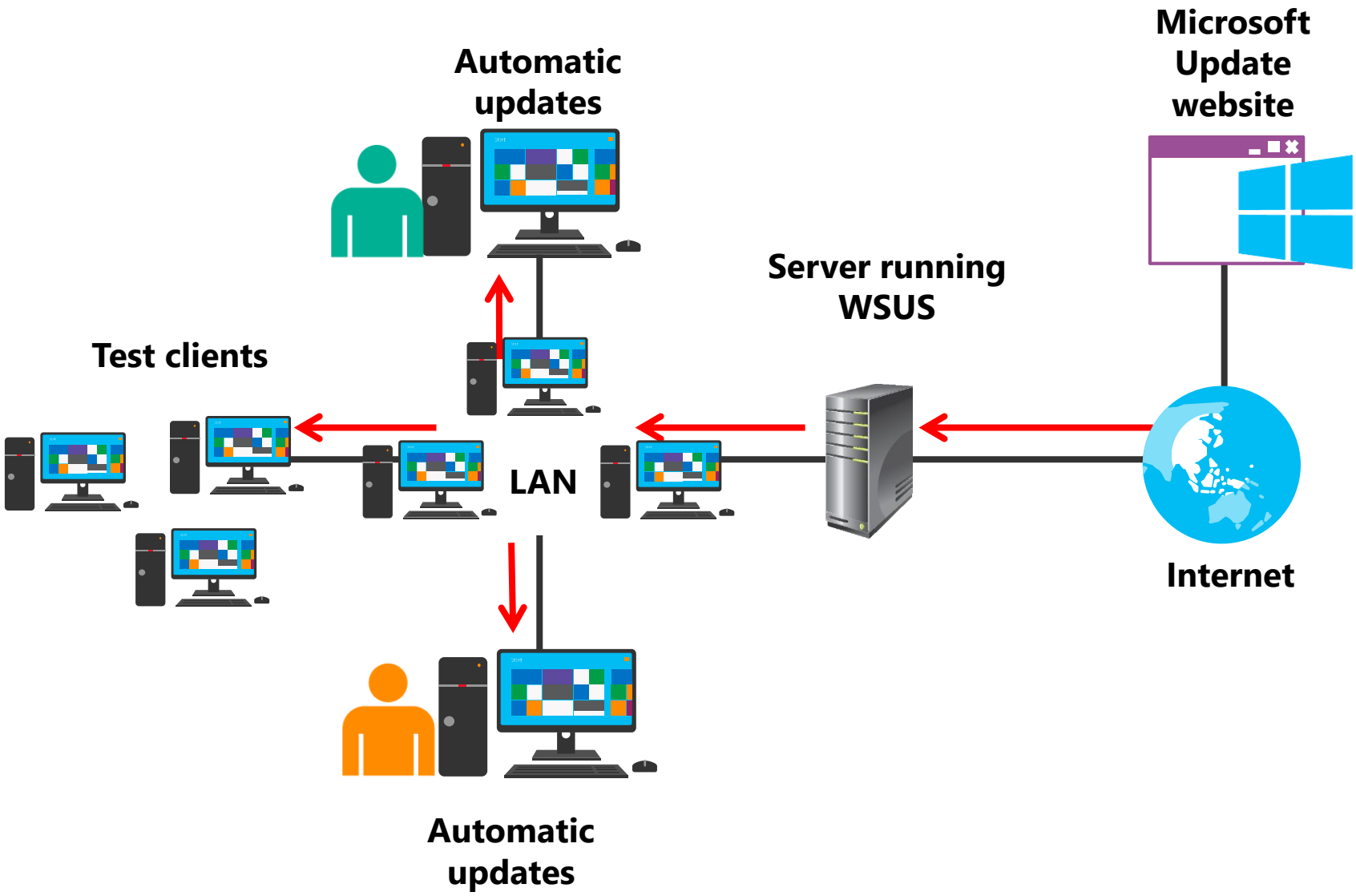
Module Overview

- WSUS overview and deployment options
- Update management process with WSUS
- Overview of Windows Server 2016 monitoring tools
- Using Performance Monitor
- Monitoring event logs

Lesson 1: WSUS overview and deployment options

- What is WSUS?
- WSUS server deployment options
- The WSUS update management process
- Server requirements for WSUS
- Configuring clients to use WSUS

What is WSUS?


Automatic updates
Microsoft Update website
Server running WSUS
Test clients
LAN
Internet
Automatic updates

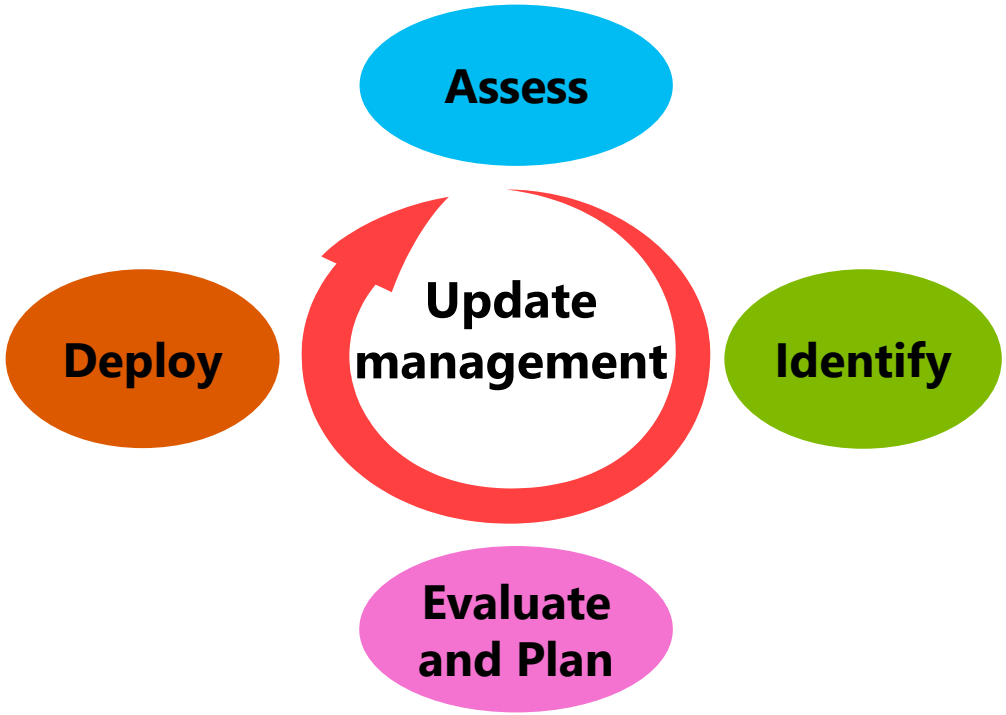
WSUS server deployment options

- WSUS implementation:
  - Single server
  - Multiple servers
  - Disconnected servers
- WSUS hierarchies:
  - Autonomous mode
  - Replica mode
- WSUS database:
  - Windows Internal Database
  - SQL Server database

The WSUS update management process

Phase 1: Assess

- Set up production environment



Phase 2: Identify

- Discover new updates
- Determine if updates are relevant

Phase 3: Evaluate and plan

- Test updates
- Determine how to update production environment

Phase 4: Deploy

- Approve and schedule updates
- Review process

Server requirements for WSUS

Software requirements:

- IIS
- Microsoft .NET Framework 4.6 or newer
- Microsoft Report Viewer Redistributable 2008 or newer
- SQL Server 2012 SP1, SQL Server 2012, SQL Server 2008 R2 SP2, SQL Server 2008 R2 SP1, or WID

Hardware requirements:

- 1.4 GHz or faster x64 processor
- 2 GB of RAM or greater
- 10 GB available disk space (40 GB or greater is recommended)

Configuring clients to use WSUS

Use a GPO to:

- Configure automatic updates
- Specify intranet Microsoft Update service location

For computers running Windows 8 and Windows Server 2012, you can use **Automatic Maintenance** to control the update process

For computers running older operating systems, you should:

- Automatically download updates
- Automatically install updates

Beginning with Windows 10, you can defer updates for up to one month

Lesson 2: Update management process with WSUS

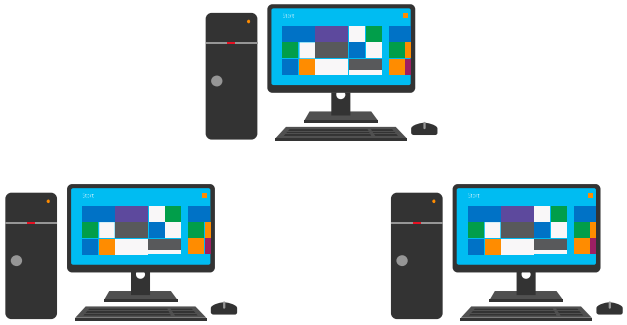
- WSUS administration
- What are computer groups?
- Approving updates
- Configuring automatic updates
- WSUS reporting
- WSUS troubleshooting

WSUS administration

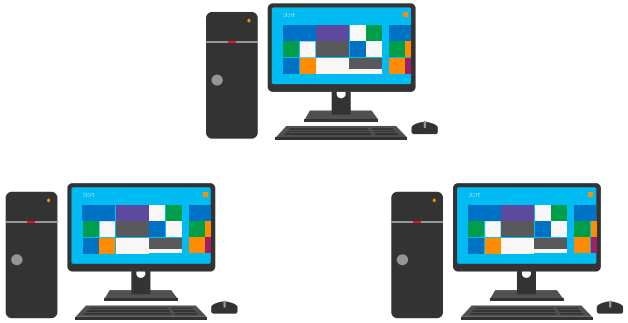
- You can use the WSUS administration console to:
  - Manage updates
  - Configure computer groups
  - View computer status
  - View synchronization information
  - Configure and view WSUS reports
  - Configure WSUS settings and options
- In Windows Server 2016, WSUS also includes Windows PowerShell cmdlets for administration

What are computer groups?

- You can use computer groups to organize WSUS clients
- The default computer groups include:



All computers



Unassigned computers

- You can create custom computer groups to control how updates are applied

Approving updates

- Updates can be:
  - Approved automatically, but it is not recommended
  - Declined if they are not needed
  - Removed if they cause problems
- You should test updates before they are approved for production

Configuring automatic updates

- You must configure the client computers to use the WSUS server as the source for updates
- You can use Group Policy to configure clients, including the following settings:
  - Update frequency
  - Update installation schedule
  - Automatic restart behavior
  - Default computer group in WSUS

WSUS reporting

- Update Reports:
  - Update Status Summary
  - Update Detailed Status
  - Update Tabular Status
  - Update Tabular Status for Approved Updates
- Computer Updates:
  - Computer Status Summary
  - Computer Detailed Status
  - Computer Tabular Status for Approved Updates
- Synchronization Updates:
  - Synchronization Results

WSUS troubleshooting

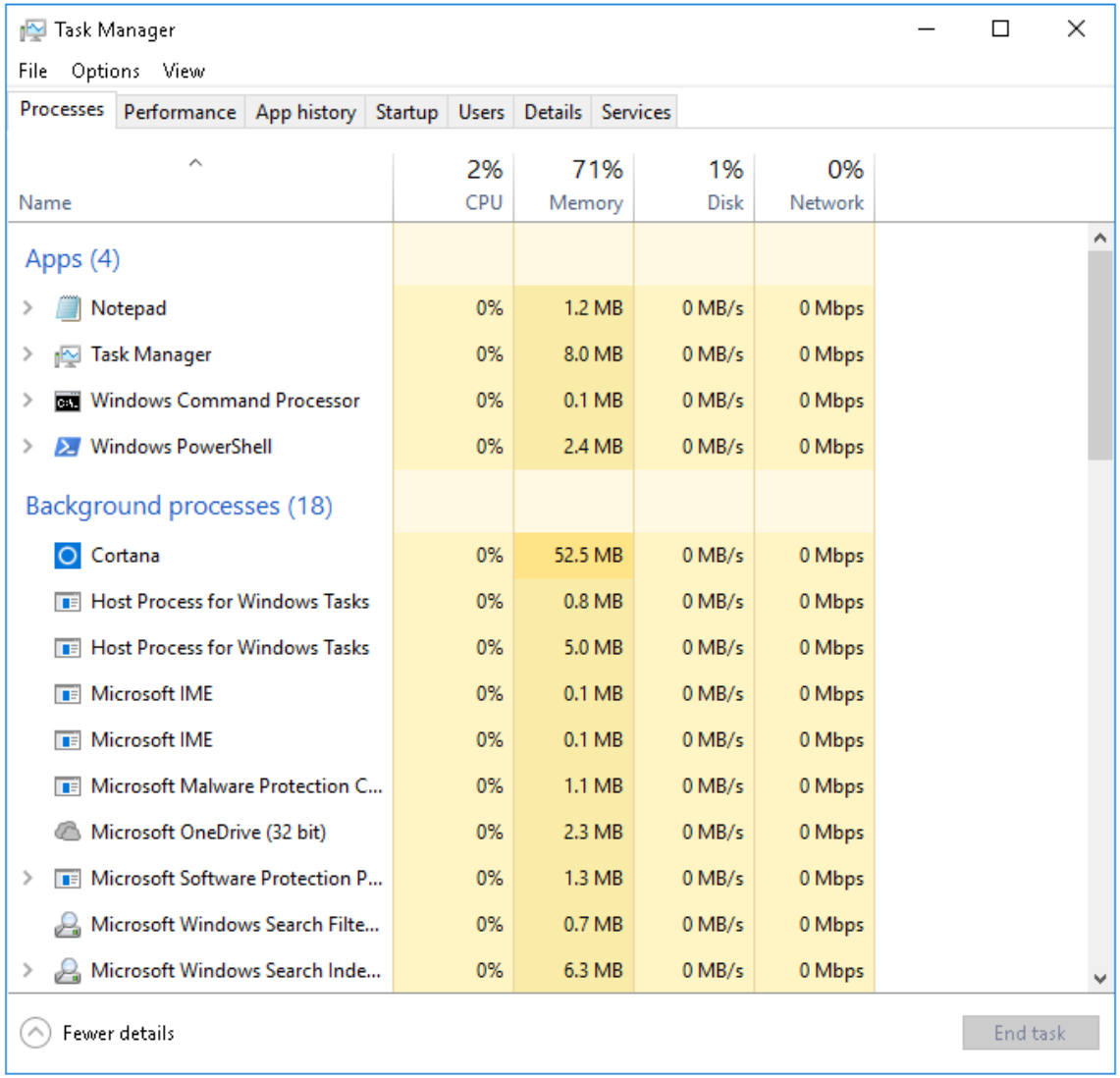
- Clients not appearing in WSUS:
  - Check GPO and client settings
- When the WSUS server stops, you should:
  - Check database server
  - Reinstall WSUS
- When you cannot connect to WSUS, you should:
  - Check network connectivity
  - Telnet to HTTP and HTTPS ports
- If you encounter other problems, you should use the:
  - Server diagnostics tool
  - Client diagnostics tool

Lesson 3: Overview of Windows Server 2016 monitoring tools

- Overview of Task Manager
- Overview of Performance Monitor
- Overview of Resource Monitor
- Overview of Reliability Monitor
- Overview of Event Viewer
- Monitoring a server with Server Manager

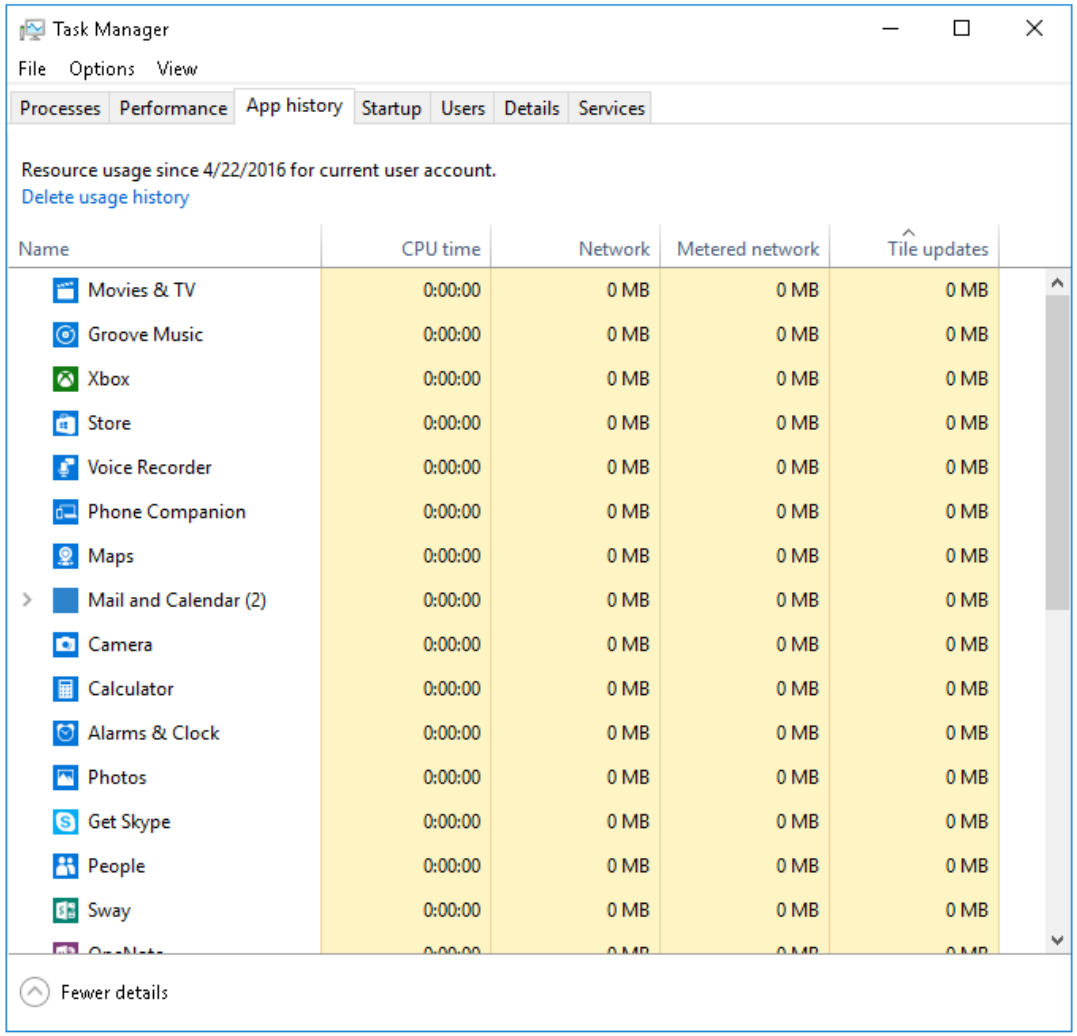
Overview of Task Manager

Task Manager helps you to identify and resolve performance-related issues



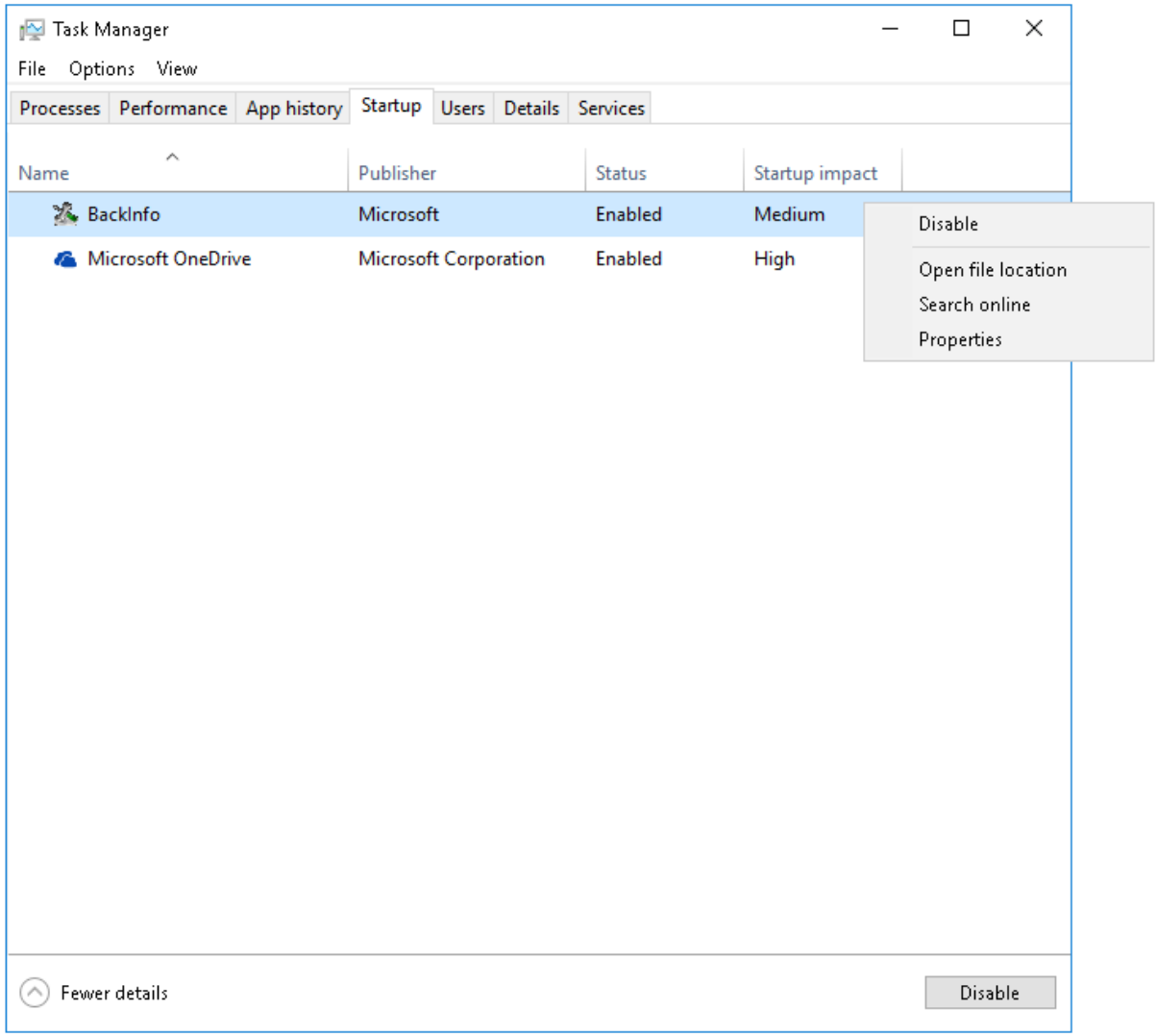
Overview of Task Manager

The **App history** tab shows the amount of resources running apps have consumed



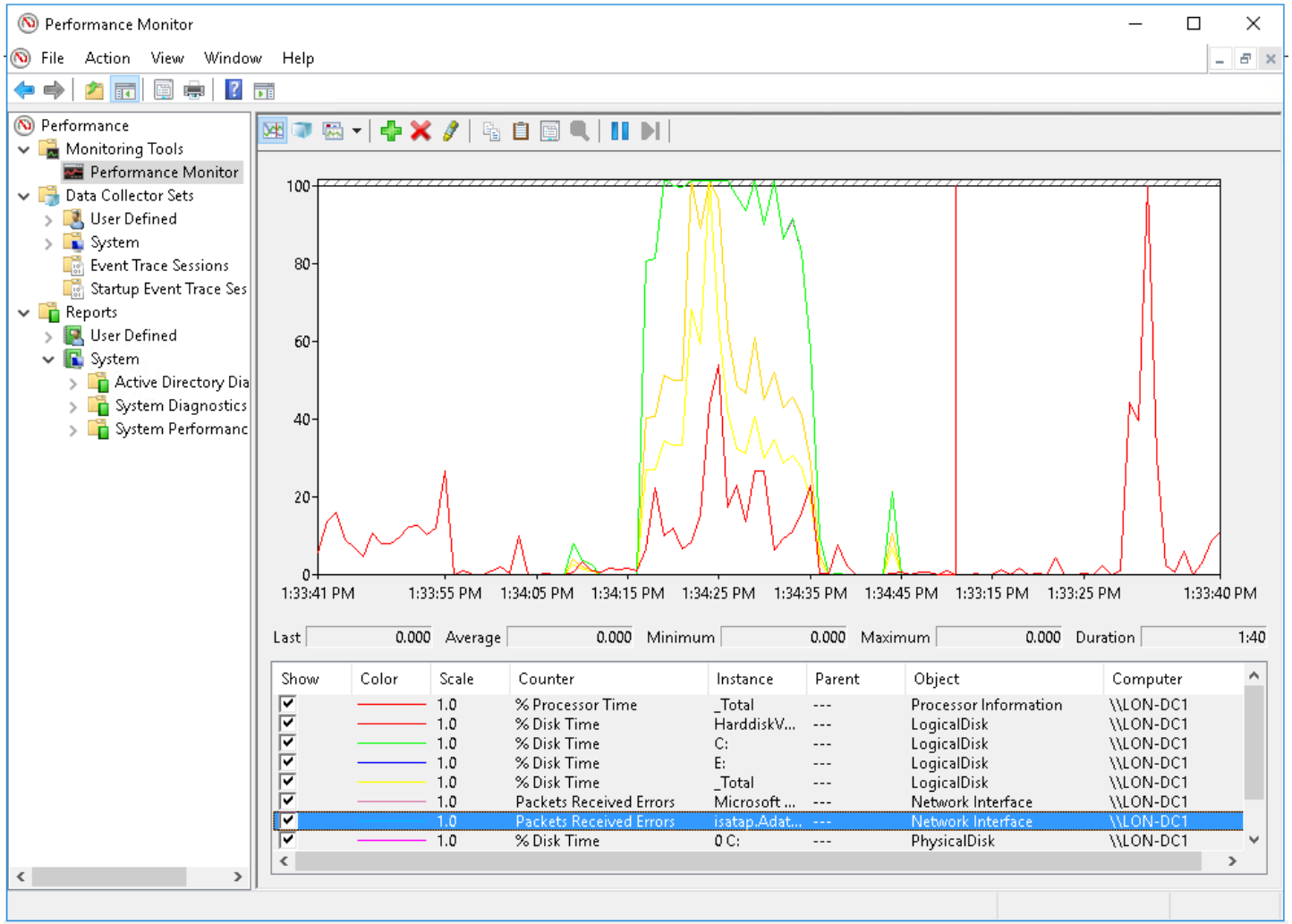
Overview of Task Manager

The **Startup** tab shows the applications that automatically start and allows you to manage them



Overview of Performance Monitor

Performance Monitor enables you to view current performance statistics or historical data that data collector sets have gathered



Overview of Performance Monitor

Primary processor counters:

- Processor > % Processor Time
- Processor > Interrupts/sec
- System > Processor Queue Length

Primary disk counters:

- Physical Disk > % Disk Time
- Physical Disk > Avg. Disk Queue Length

Primary network counters:

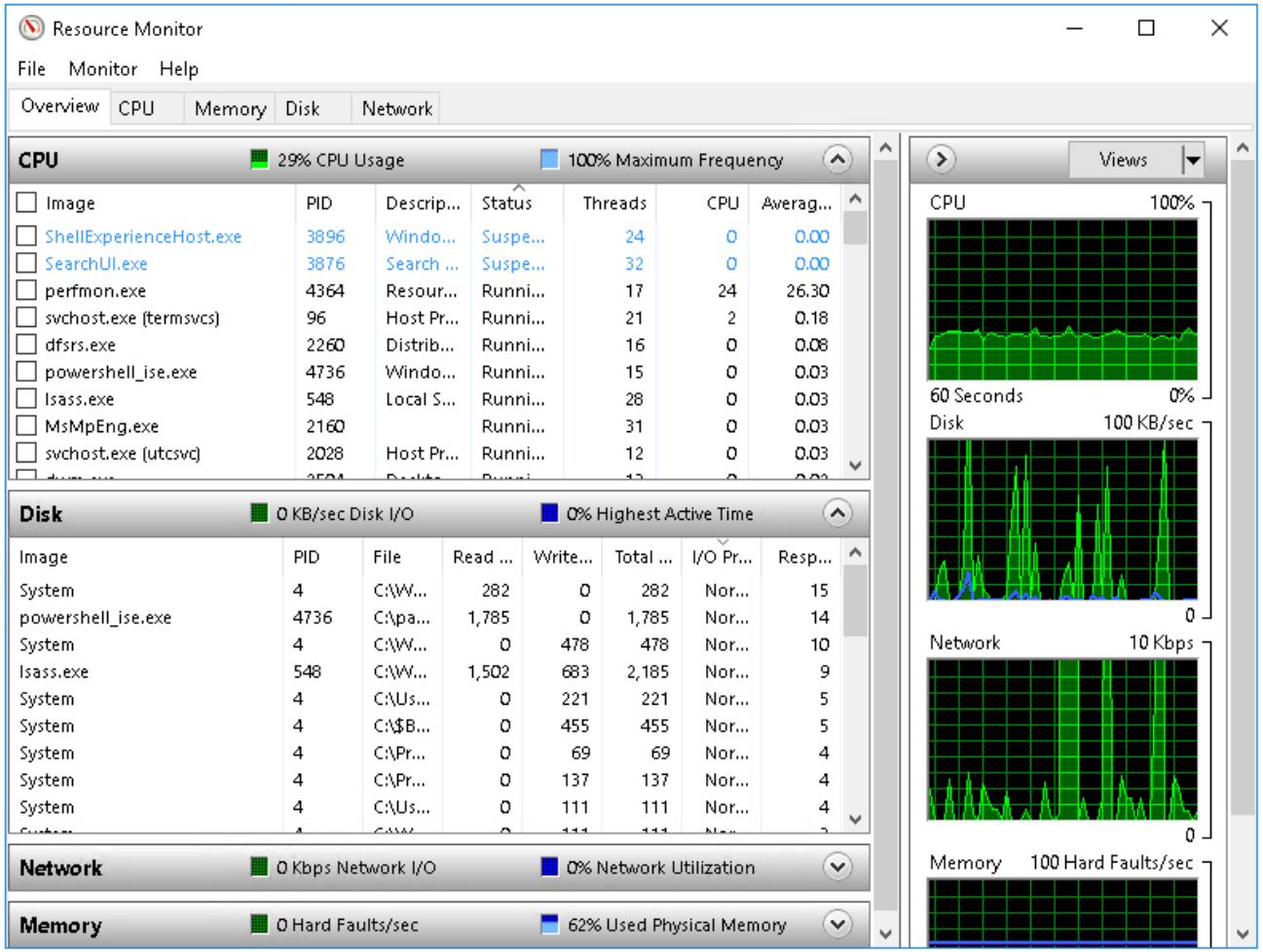
- Network Interface > Current Bandwidth
- Network Interface > Output Queue Length
- Network Interface > Bytes Total/sec

Primary memory counter:

- The Memory > Pages/sec counter

Overview of Resource Monitor

Resource Monitor provides an in-depth look at the real-time performance of your server



Overview of Reliability Monitor

- Monitors hardware and software issues
- Provides stability index number (from 1 to 10):
  - 1 represents lowest stability
  - 10 represents highest stability
- The **Reliability Monitor** window components include:
  - Historical reports on stability index
  - Reliability details
  - Action to be performed: saving historical data, starting the **Problem Reports** console, checking online for a solution to a specific problem

Overview of Reliability Monitor

Reliability Monitor tracks hardware and software issues that have impacted the system

Reliability Monitor

Control Panel › System and Security › Security and Maintenance › Reliability Monitor

Search Control Panel

Review your computer's reliability and problem history

The stability index assesses your system's overall stability on a scale from 1 to 10. By selecting a specific period in time, you may review the specific hardware and software problems that have impacted your system.

View by: Days | Weeks

Last updated: 5/22/2016 12:00 PM

10
5
1

5/3/2016 5/5/2016 5/7/2016 5/9/2016 5/11/2016 5/13/2016 5/15/2016 5/17/2016 5/19/2016 5/21/2016

Application failures
Windows failures
Miscellaneous failures
Warnings
Information

Reliability details for: 5/22/2016

Source	Summary	Date	Action
Critical events			
mmc.exe	Stopped working	5/22/2016 8:37 AM	View technical d...

Save reliability history... View all problem reports Check for solutions to all problems ...

OK

Overview of Event Viewer

Event Viewer provides categorized lists of essential Windows log events, and log groupings for individual installed applications and specific Windows component categories

Event Viewer

File Action View Help

Event Viewer (Local)
- Custom Views
  - ServerRoles
    - Active Directory Certi
    - Active Directory Dom
    - DHCP Server
    - DNS Server
    - Remote Desktop Serv
    - Web Server (IIS)
  - Administrative Events
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Lo
  - Active Directory Web Ser
  - DFS Replication
  - Directory Service
  - DNS Server
  - Hardware Events
  - Internet Explorer
  - Key Management Service
  - Microsoft
    - Windows
  - Windows PowerShell
- Subscriptions

Application Number of events: 342

Level	Date and Time	Source	Event ID	Task Category
Error	5/22/2016 1:32:06 PM	PerfNet	2001	None
Error	5/22/2016 1:32:06 PM	Perflib	1008	None
Error	5/22/2016 1:31:56 PM	PerfNet	2001	None
Information	5/22/2016 10:28:48 AM	Windows Err...	1001	None
Information	5/22/2016 10:22:24 AM	Windows Err...	1001	None
Information	5/22/2016 9:04:55 AM	Windows Err...	1001	None
Error	5/22/2016 8:37:22 AM	Application E...	1000	(100)
Information	5/22/2016 4:01:48 AM	Security-SPP	903	None
Information	5/22/2016 4:01:48 AM	Security-SPP	16384	None
Information	5/22/2016 4:01:15 AM	Security-SPP	902	None
Information	5/22/2016 4:01:15 AM	Security-SPP	1003	None
Information	5/22/2016 4:01:15 AM	Security-SPP	1066	None
Information	5/22/2016 4:01:15 AM	Security-SPP	900	None
Information	5/22/2016 2:45:52 AM	SceCli	1704	None

Event 2001, PerfNet

General Details

Unable to collect Browser performance data because the Query function was not found in the NetApi32.DLL. The first four bytes (DWORD) of the Data section contains the status code.

Log Name:	Application		
Source:	PerfNet	Logged:	5/22/2016 1:32:06 PM
Event ID:	2001	Task Category:	None
Level:	Error	Keywords:	Classic
User:	N/A	Computer:	LON-DC1.Adatum.com
OpCode:	Info		
More Information:	Event Log Online Help		

Actions

Application
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help

Event 2001, PerfNet
- Event Properties
- Attach Task To This Event...
- Save Selected Events...
- Copy
- Refresh
- Help

Overview of Event Viewer

- Event Viewer provides the ability to:
  - View multiple logs
  - Create customized views
  - Configure tasks scheduled to run in response to events
  - Create and manage event subscriptions
- Event Viewer has many built-in logs such as:
  - Application log
  - Security log
  - Setup log
  - System log
  - Forwarded events

Monitoring a server with Server Manager

Server Manager console:

- Installed by default on Windows Server 2016, and can be installed on Windows 10
- Supports monitoring of Windows Server operating systems
- Provides a centralized monitoring dashboard
- Analyzes or troubleshoots different types of issues
- Identifies critical events
- Monitors the status of Best Practices Analyzer tool

Lesson 4: Using Performance Monitor

- Overview of baseline, trends, and capacity planning
- What are data collector sets?
- Monitoring network infrastructure services
- Considerations for monitoring virtual machines

Overview of baseline, trends, and capacity planning

- By calculating performance baselines for your server environment, you can more accurately interpret real-time monitoring information
- By establishing a baseline, you can:
  - Interpret performance trends
  - Perform capacity planning
  - Identify bottlenecks
- Analyze performance trends to predict when existing capacity is likely to be exhausted
- Plan the capacity for the key hardware components: processor, disk, memory, and network

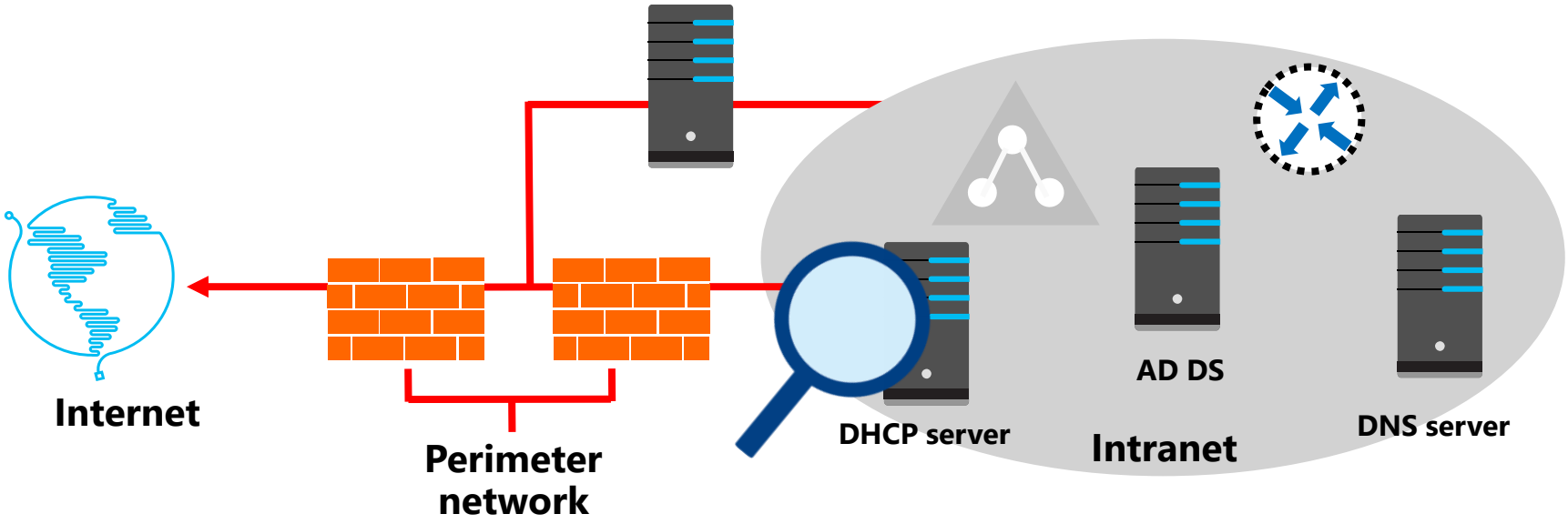
What are data collector sets?

- Data collector sets enable you to gather performance-related and other system statistics for analysis
- Data collector sets can contain the following types of data collectors:
  - Performance counters
  - Event trace data
  - System configuration information

Monitoring network infrastructure services

Monitoring is essential for:

- Optimizing network infrastructure server performance
- Troubleshooting servers



Considerations for monitoring virtual machines

- Virtual machines must be assigned sufficient resources for their workload
- If multiple virtual machines run on a host, ensure the host has enough resources
- Resources are shared, so performance of one virtual machine can affect the performance of others
- You must remember to monitor the resource utilization on the host and the guests

Lesson 5: Monitoring event logs

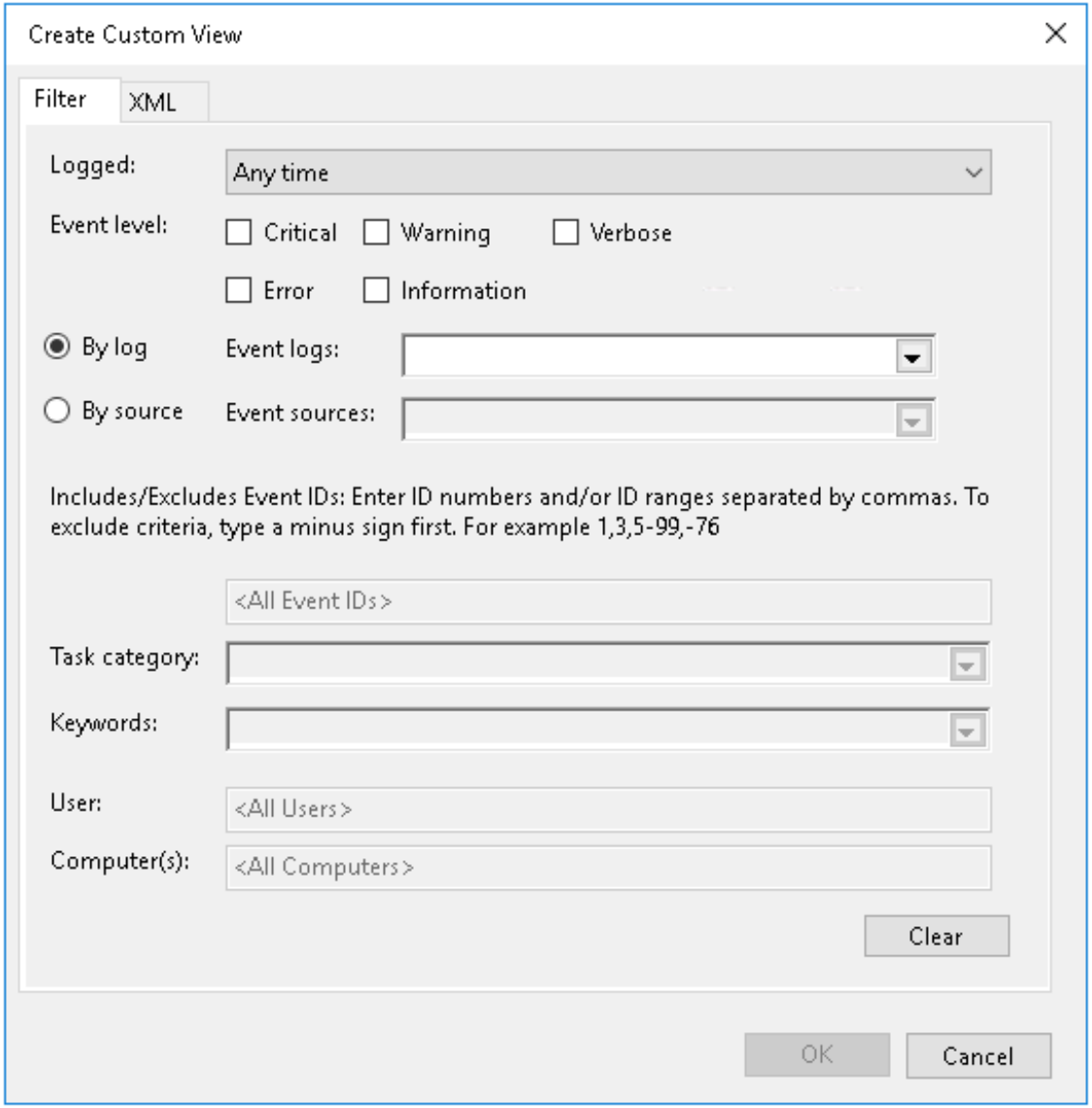
- Using Server Manager to view event logs
- What is a custom view?
- What are event log subscriptions?

Using Server Manager to view event logs

- Server Manager provides a centralized location for event logs from remote servers
- Event logging
  - Enabled by default
  - Categorized by technology: AD DS, DNS, and Remote Access
- Customized views
  - Create queries for specific types of events that need to be displayed
  - Configure event data that needs to be displayed

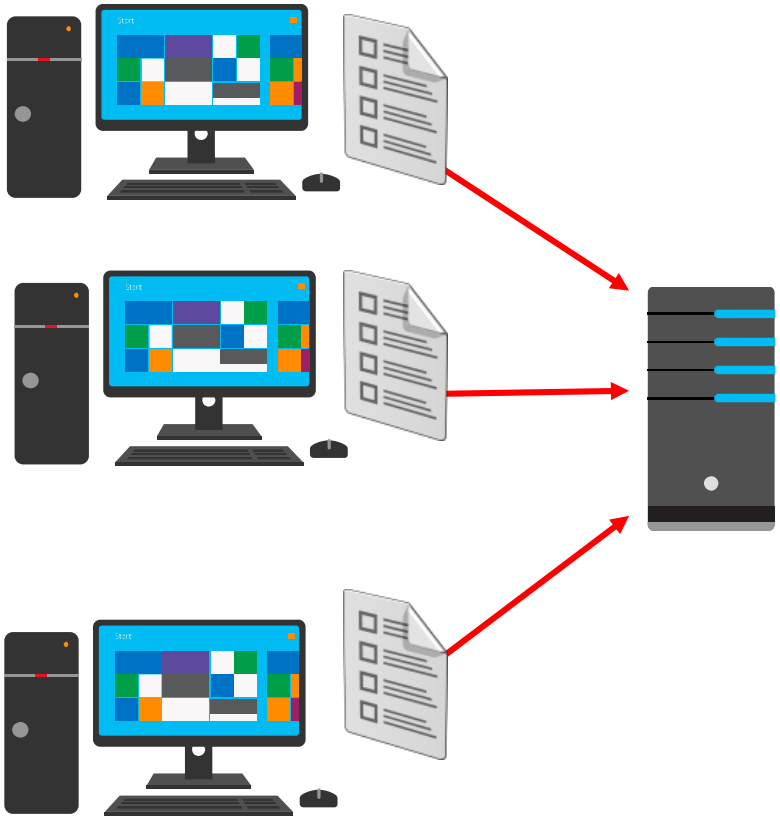
What is a custom view?

Custom views allow you to query and sort just the events that you want to analyze



What are event log subscriptions?

Event subscriptions allow you to collect event logs from multiple servers, and then store them locally



Module 4

Installing and configuring domain controllers

Module Overview

- Overview of AD DS
- Overview of AD DS domain controllers
- Deploying a domain controller

Lesson 1: Overview of AD DS

- AD DS components
- What is the AD DS schema?
- What is an AD DS forest?
- What is an AD DS domain?
- What are OUs?
- What is new in AD DS in Windows Server 2016?
- What is Azure AD?
- Overview of AD DS administration tools
- Administrative Center to administer and manage AD DS

AD DS components

AD DS is composed of both logical and physical components

Logical components	Physical components
• Partitions • Schema • Domains • Domain trees • Forests • Sites • OUs • Containers	• Domain controllers • Data stores • Global catalog servers • RODCs

What is the AD DS schema?

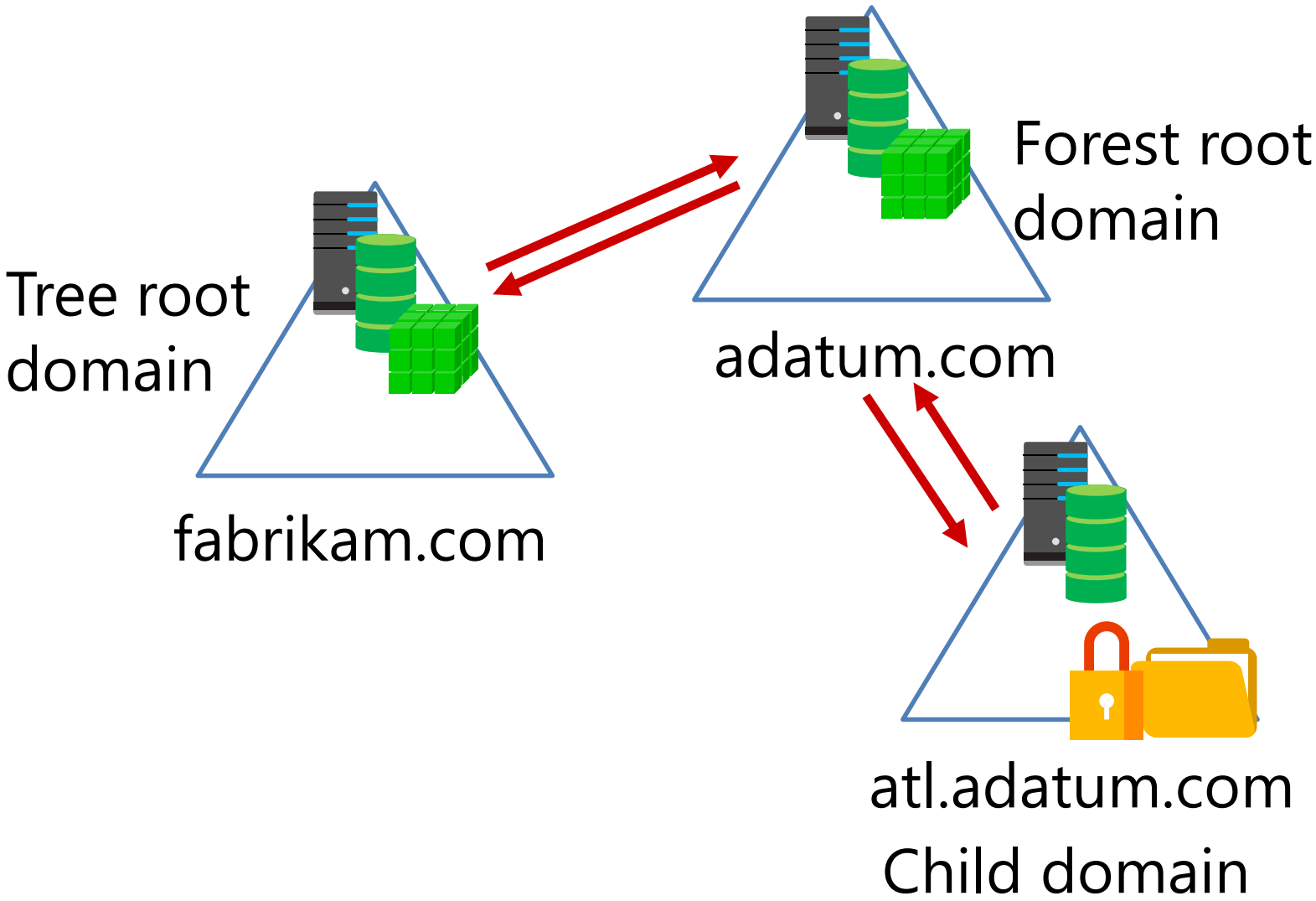
Console1 - [Console Root\Active Directory Schema [LON-DC1.Adatum.com]\Classes\user]

File Action View Favorites Window Help

- rpcProfileElement
- rpcServer
- rpcServerElement
- rRASAdministrationConnection
- rRASAdministrationDictionary
- samDomain
- samDomainBase
- samServer
- secret
- securityObject
- securityPrincipal
- server
- serversContainer
- serviceAdministrationPoint
- serviceClass
- serviceConnectionPoint
- serviceInstance
- shadowAccount
- simpleSecurityObject
- site
- siteLink
- siteLinkBridge
- sitesContainer
- storage
- subnet
- subnetContainer
- subSchema
- top
- trustedDomain
- typeLibrary
- user
- volume
- Attributes

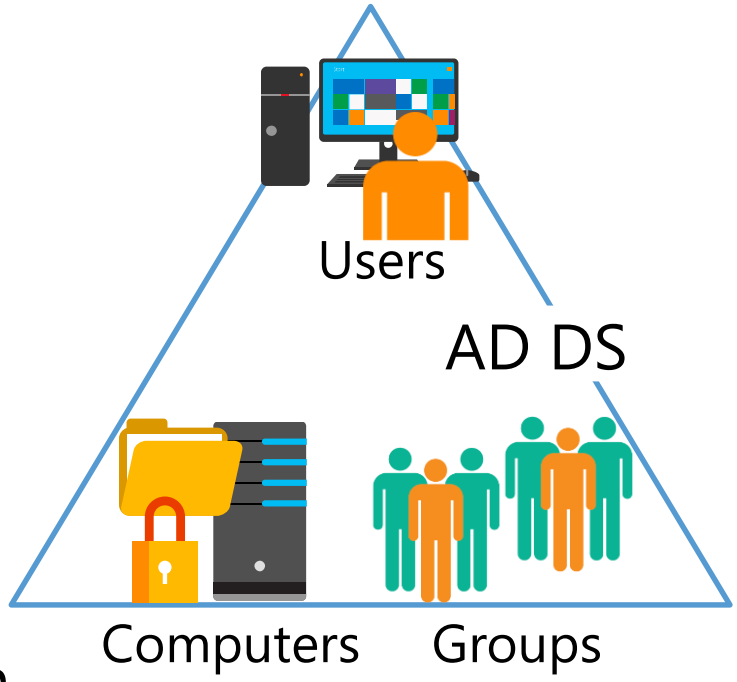
Name	Type	System	Description	Source Class
userPassword	Optional	No	User-Password	posixAccount
homeDirectory	Optional	No	Home-Directory	posixAccount
unixHomeDirectory	Optional	No	The absolute path to the...	posixAccount
gidNumber	Optional	No	An integer uniquely ide...	posixAccount
uidNumber	Optional	No	An integer uniquely ide...	posixAccount
cn	Optional	No	Common-Name	posixAccount
uid	Optional	No	A user ID.	posixAccount
userPassword	Optional	Yes	User-Password	person
telephoneNumber	Optional	Yes	Telephone-Number	person
sn	Optional	Yes	Surname	person
serialNumber	Optional	Yes	Serial-Number	person
seeAlso	Optional	Yes	See-Also	person
attributeCertificateAtt...	Optional	No	A digitally signed or cert...	person
cn	Mandatory	Yes	Common-Name	person
msDS-AllowedToAct...	Optional	Yes	This attribute is used for...	organizationalPerson
x121Address	Optional	Yes	X121-Address	organizationalPerson
comment	Optional	Yes	User-Comment	organizationalPerson
title	Optional	Yes	Title	organizationalPerson
co	Optional	Yes	Text-Country	organizationalPerson
primaryTelexNumber	Optional	Yes	Telex-Primary	organizationalPerson
telexNumber	Optional	Yes	Telex-Number	organizationalPerson
teletexTerminalIdentif...	Optional	Yes	Teletex-Terminal-Identifi...	organizationalPerson
street	Optional	Yes	Street-Address	organizationalPerson
st	Optional	Yes	State-Or-Province-Name	organizationalPerson
registeredAddress	Optional	Yes	Registered-Address	organizationalPerson
preferredDeliveryMet...	Optional	Yes	Preferred-Delivery-Meth...	organizationalPerson
postalCode	Optional	Yes	Postal-Code	organizationalPerson
postalAddress	Optional	Yes	Postal-Address	organizationalPerson
postOfficeBox	Optional	Yes	Post-Office-Box	organizationalPerson
thumbnailPhoto	Optional	Yes	Picture	organizationalPerson
physicalDeliveryOffic...	Optional	Yes	Physical-Delivery-Office...	organizationalPerson

What is an AD DS forest?



What is an AD DS domain?

- AD DS requires one or more domain controllers
- All domain controllers hold a copy of the domain database, which is continually synchronized
- The domain is the context within which user accounts, computer accounts, and groups are created
- The domain is a replication boundary
- The domain is an administrative center for configuring and managing objects
- Any domain controller can authenticate any sign-in anywhere in the domain
- The domain provides authorization



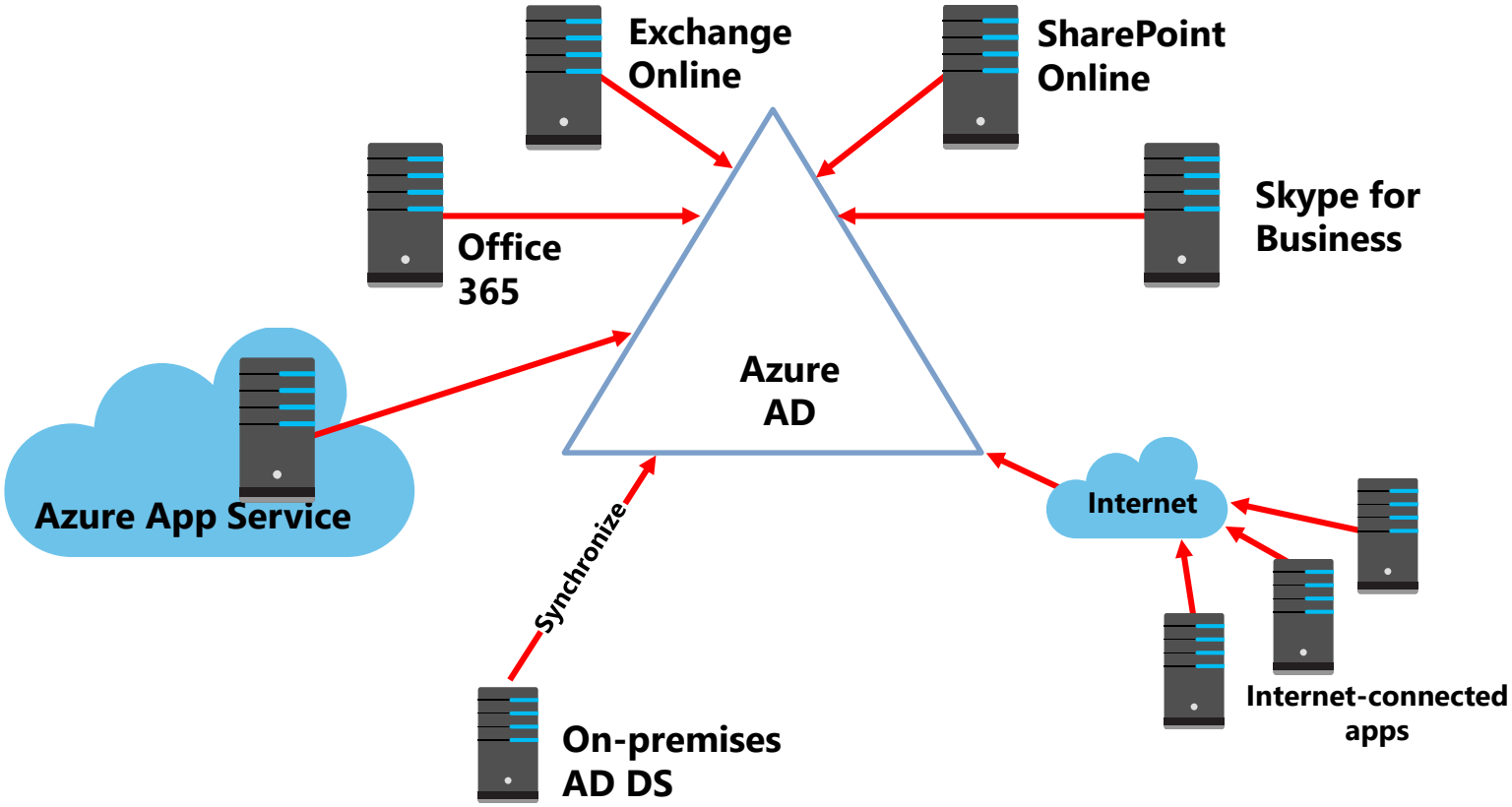
What are OUs?

- Use containers to group objects within a domain:
  - You cannot apply GPOs to containers
  - Containers are used for system objects and as the default location for new objects
- Create OUs to:
  - Configure objects by assigning GPOs to them
  - Delegate administrative permissions

What is new in AD DS in Windows Server 2016?

- PAM
- Azure AD Join
- Microsoft Passport

What is Azure AD?



Overview of AD DS administration tools

You typically perform AD DS management by using the following tools:

- Active Directory Administrative Center
- Active Directory Users and Computers
- Active Directory Sites and Services
- Active Directory Domains and Trusts
- Active Directory Schema snap-in
- Active Directory module for Windows PowerShell

Lesson 2: Overview of AD DS domain controllers

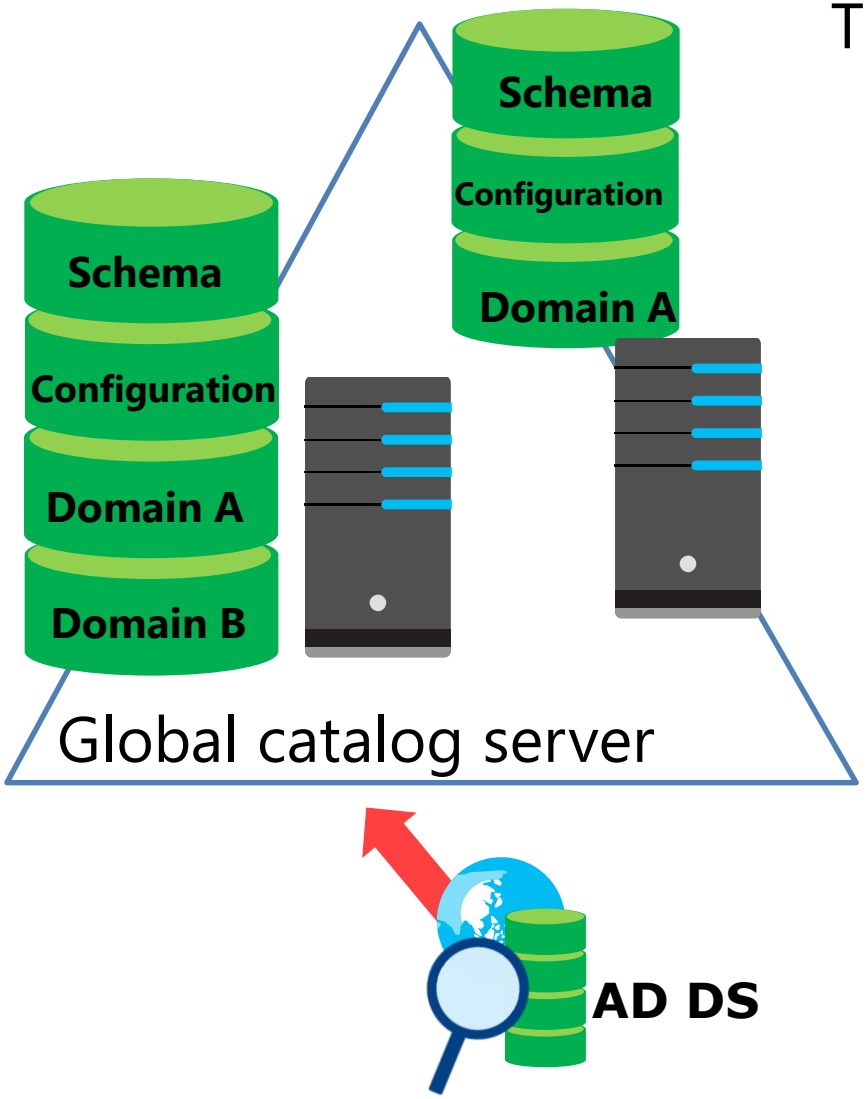
- What is a domain controller?
- What is a global catalog?
- Overview of domain controller SRV records
- AD DS sign-in process
- What are operations masters?
- Transferring and seizing roles

What is a domain controller?

Domain controllers:

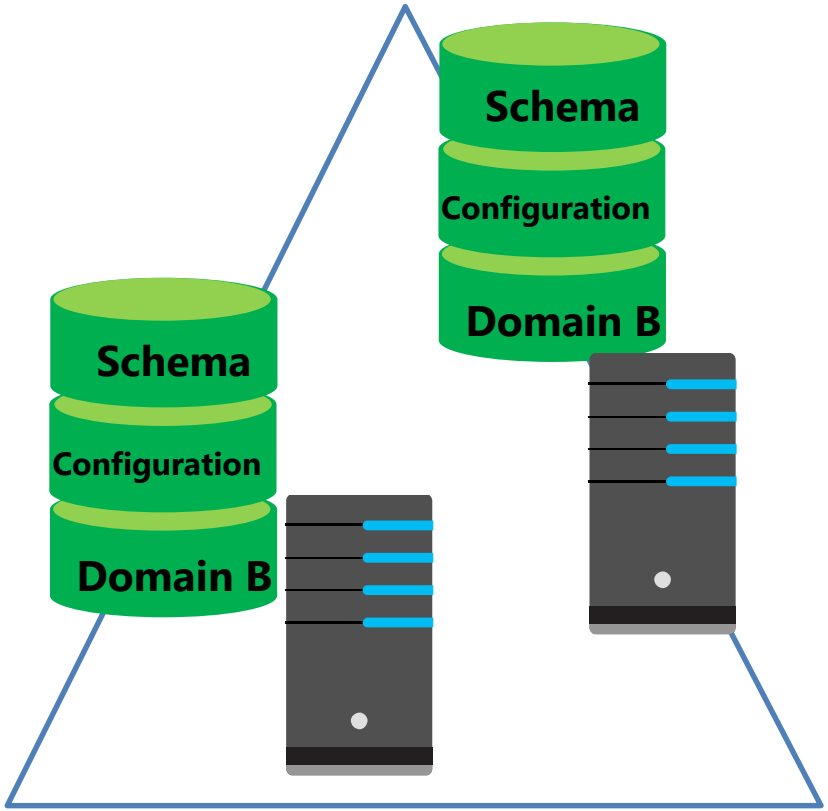
- Are servers that host the AD DS database (**Ntds.dit**) and **SYSVOL**
- Host the Kerberos authentication service and KDC services to perform authentication
- Have best practices for:
  - Availability:
    - Use at least two domain controllers in a domain
  - Security:
    - Use an RODC or BitLocker

What is a global catalog?



The global catalog:

- Hosts a partial attribute set for other domains in the forest
- Supports queries for objects throughout the forest

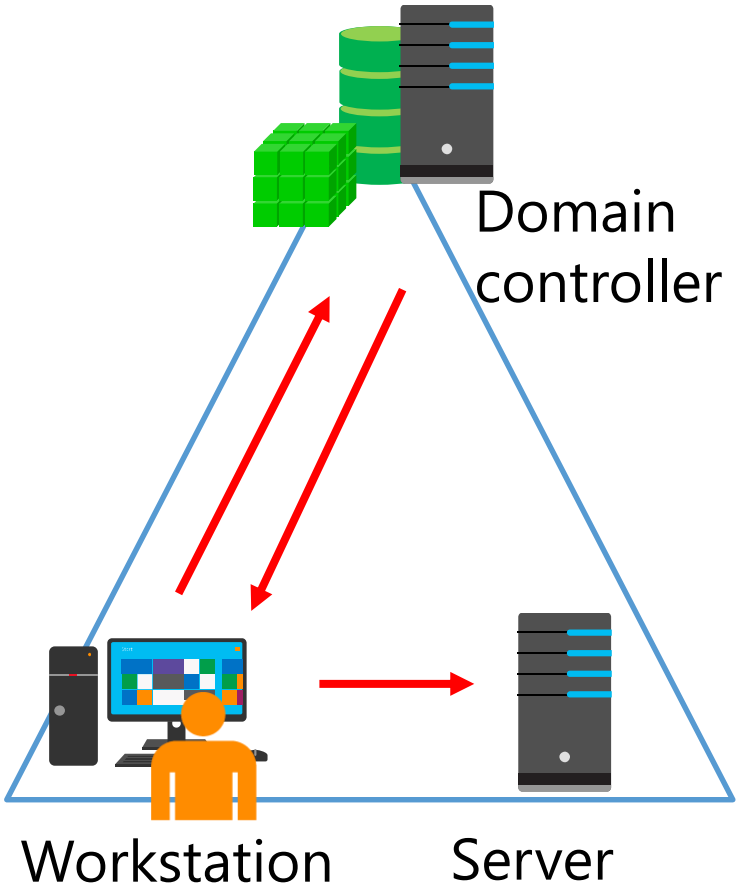


Overview of domain controller SRV records

- Clients find domain controllers through DNS lookup
- Domain controllers dynamically register their addresses with DNS
- The results of DNS queries for domain controllers are returned in this order:
  1. A list of domain controllers in the same site as the client
  2. A list of domain controllers in the next closest site, if none are available in the same site
  3. A random list of domain controllers in other sites, if no domain controller is available in the next closest site

AD DS sign-in process

1. The user account is authenticated to the domain controller
2. The domain controller returns a TGT back to client
3. The client uses the TGT to apply for access to the workstation
4. The domain controller grants access to the workstation
5. The client uses the TGT to apply for access to the server
6. The domain controller returns access to the server



What are operations masters?

- In the multimaster replication model, some operations must be single master operations
- Many terms are used for single master operations in AD DS, including:
  - Operations master (or operations master role)
  - Single master role
  - Flexible single master operations (FSMO)

The five FSMOs	
Forest: • Domain naming master • Schema master	Domain: • RID master • Infrastructure master • PDC emulator master

Transferring and seizing roles

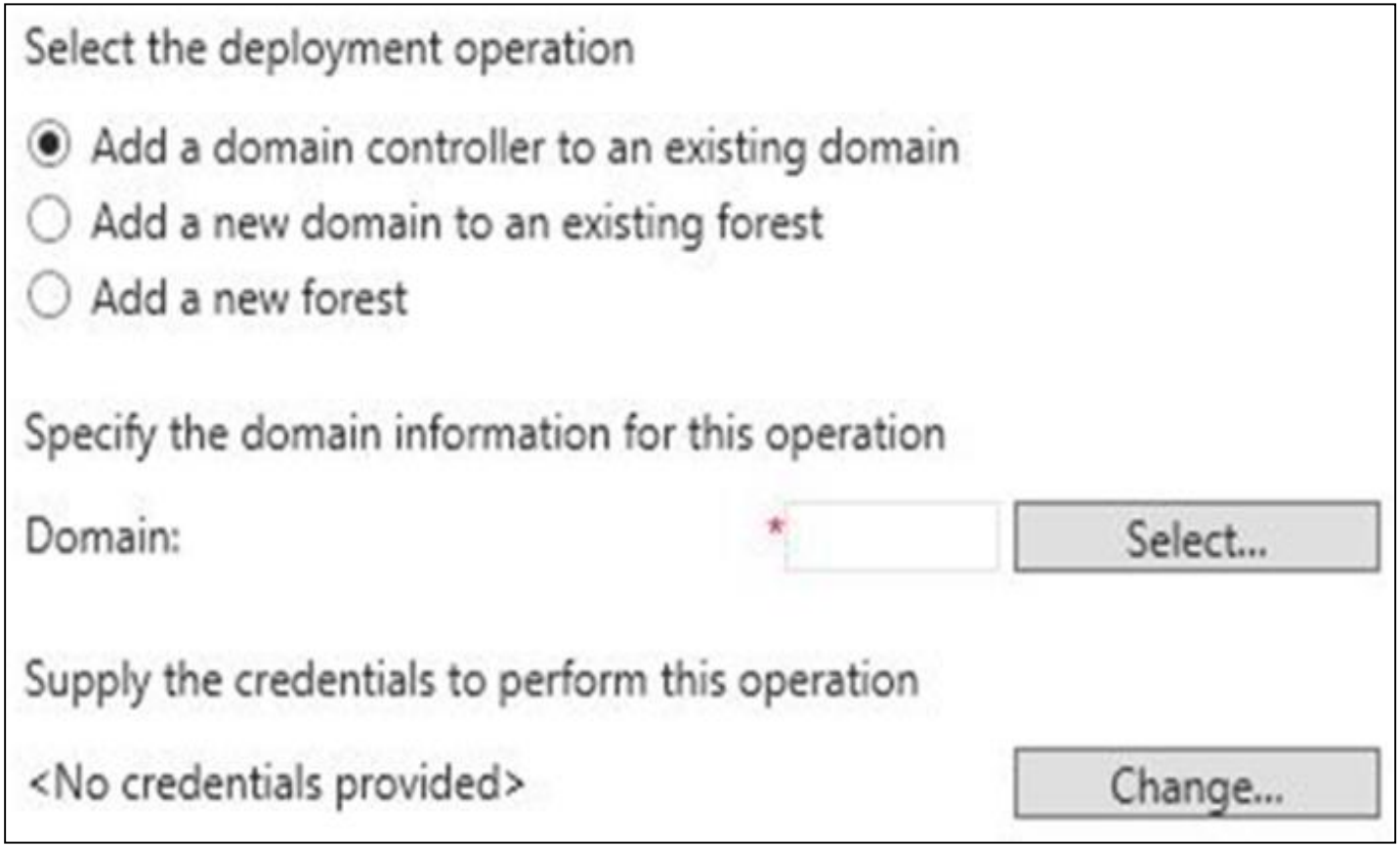
- Transferring is:
  - Planned
  - Done with the latest data
  - Done through snap-ins, Windows PowerShell, or ntdsutil.exe
- Seizing is:
  - Unplanned and a last resort
  - Done with incomplete or out-of-date data
  - Done through Windows PowerShell or ntdsutil.exe

Lesson 3: Deploying a domain controller

- Installing a domain controller from Server Manager
- Installing a domain controller on a Server Core installation of Windows Server 2016
- Upgrading a domain controller
- Installing a domain controller by installing from media
- Cloning domain controllers
- Best practices for domain controller virtualization

Installing a domain controller from Server Manager

The **Deployment Configuration** section of the **Active Directory Domain Services Configuration Wizard**



Installing a domain controller on a Server Core installation of Windows Server 2016

- Using Server Manager:
  1. Install the AD DS role
  2. Run the **Active Directory Domain Services Configuration Wizard**
- Using Windows PowerShell:
  1. Install the files by running the command **Install-WindowsFeature AD-Domain-Services**
  2. Install the domain controller role by running the command **Install-ADDSDomainController**

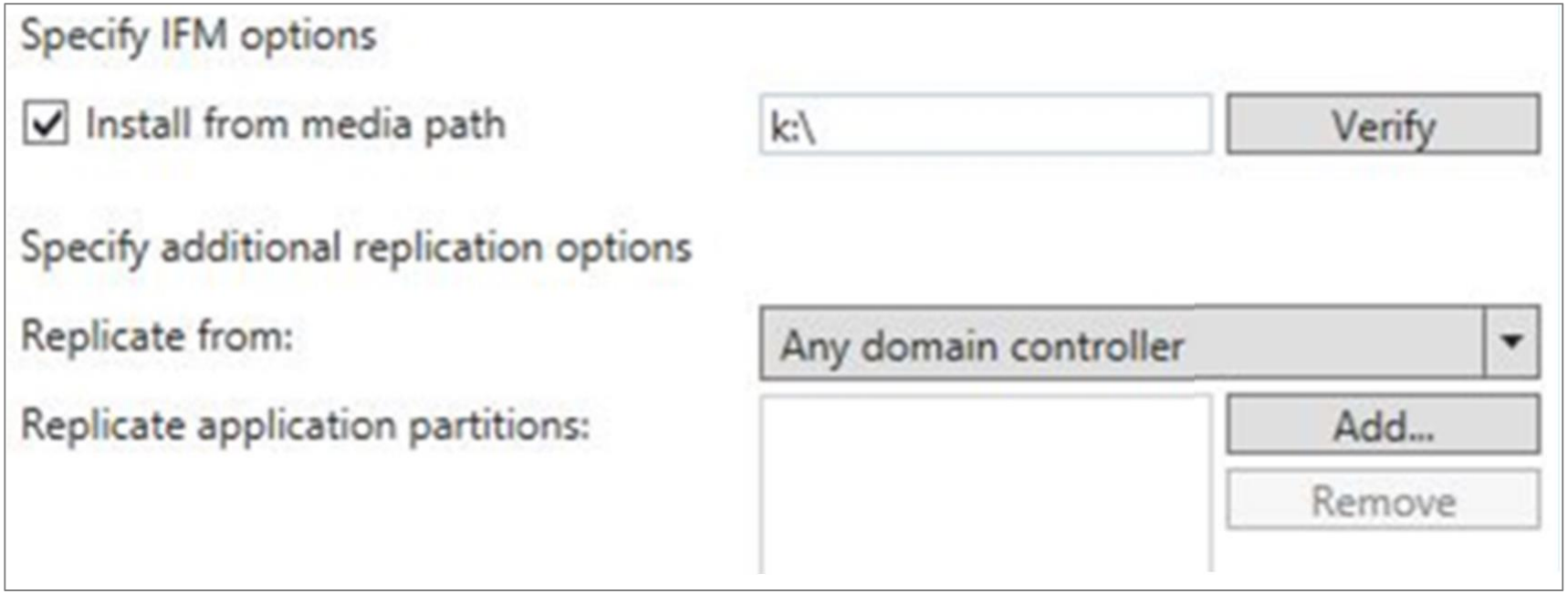
Upgrading a domain controller

You have two options for upgrading AD DS to Windows Server 2016:

- Perform an in-place upgrade from Windows Server 2008 or later to Windows Server 2016:
  - Benefit: Except for the prerequisite checks, all the files and programs stay in place, and no additional work is required
  - Risk: It might leave obsolete files and dynamic-link libraries
- Introduce a new server running Windows Server 2016 into the domain, and then promote it to be a domain controller (this option is usually preferred):
  - Benefit: The new server has no obsolete files and settings
  - Risk: It might require additional work to migrate administrators' files and settings

Installing a domain controller by installing from media

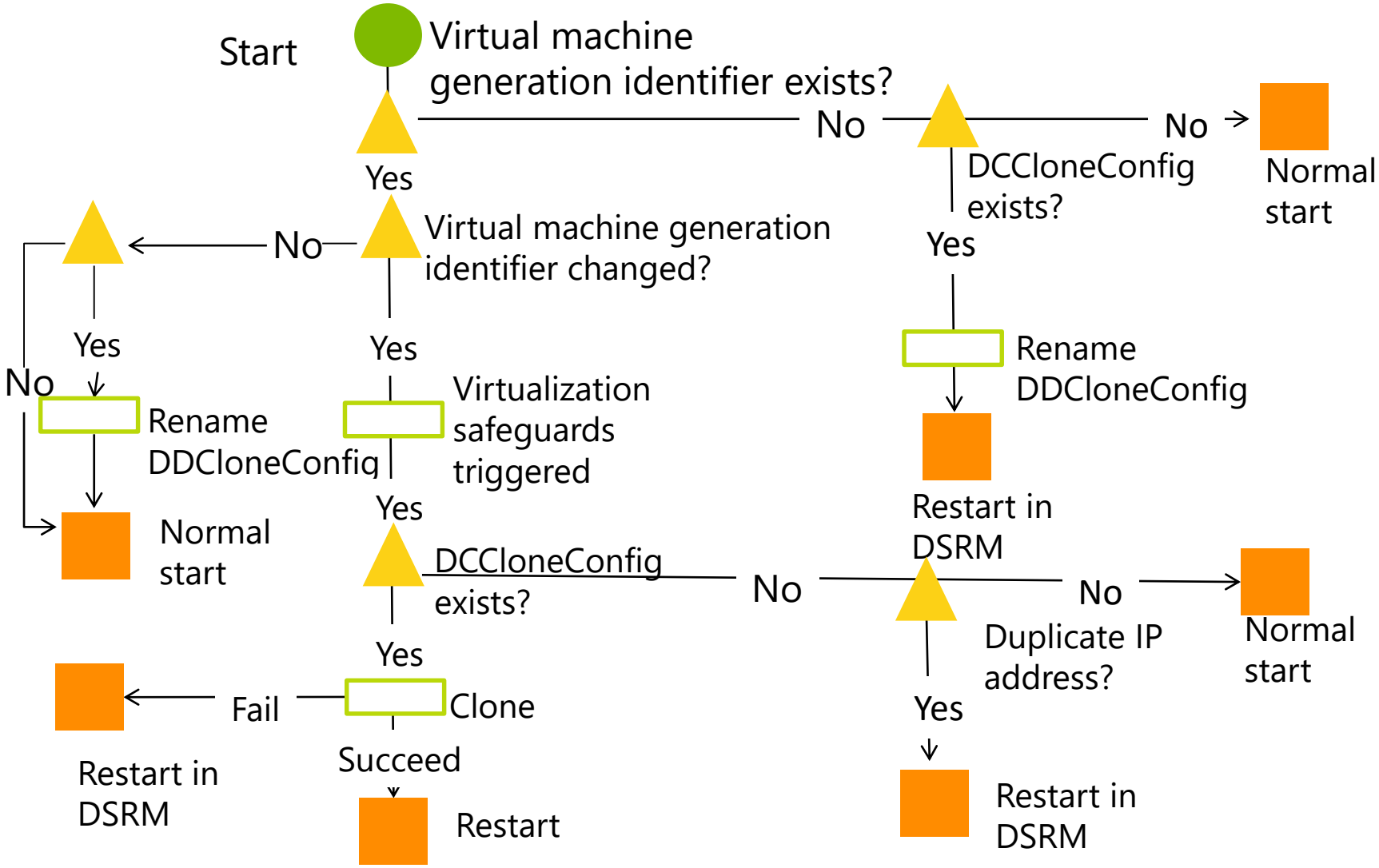
The **Install from media** section on the **Additional Options** page of the **Active Directory Domain Services Configuration Wizard**



Cloning domain controllers

- You might clone domain controllers for:
  - Rapid deployment
  - Private clouds
  - Recovery strategies
- To clone a source domain controller:
  - Add the domain controller to the **Cloneable Domain Controllers** group
  - Verify app and service compatibility
  - Create a **DCCloneConfig.xml** file
  - Export it once, and then create as many clones as needed
  - Start the clones

Cloning domain controllers



Best practices for domain controller virtualization

- Avoid single points of failure
- Use the time services
- Use virtualization technology with the virtual machine generation identifier feature
- Use Windows Server 2012 or later as virtualization guests
- Avoid or disable checkpoints
- Strive to improve security
- Consider taking advantage of cloning in your deployment or recovery strategy
- Start a maximum number of 10 new clones at the same time
- Consider using virtualization technologies that allow virtual machine guests to move between sites
- Adjust your naming strategy to allow for domain controller clones

Module 5

Implementing Group Policy

Module Overview

- Introducing Group Policy
- Implementing and administering GPOs
- Group Policy scope and Group Policy processing

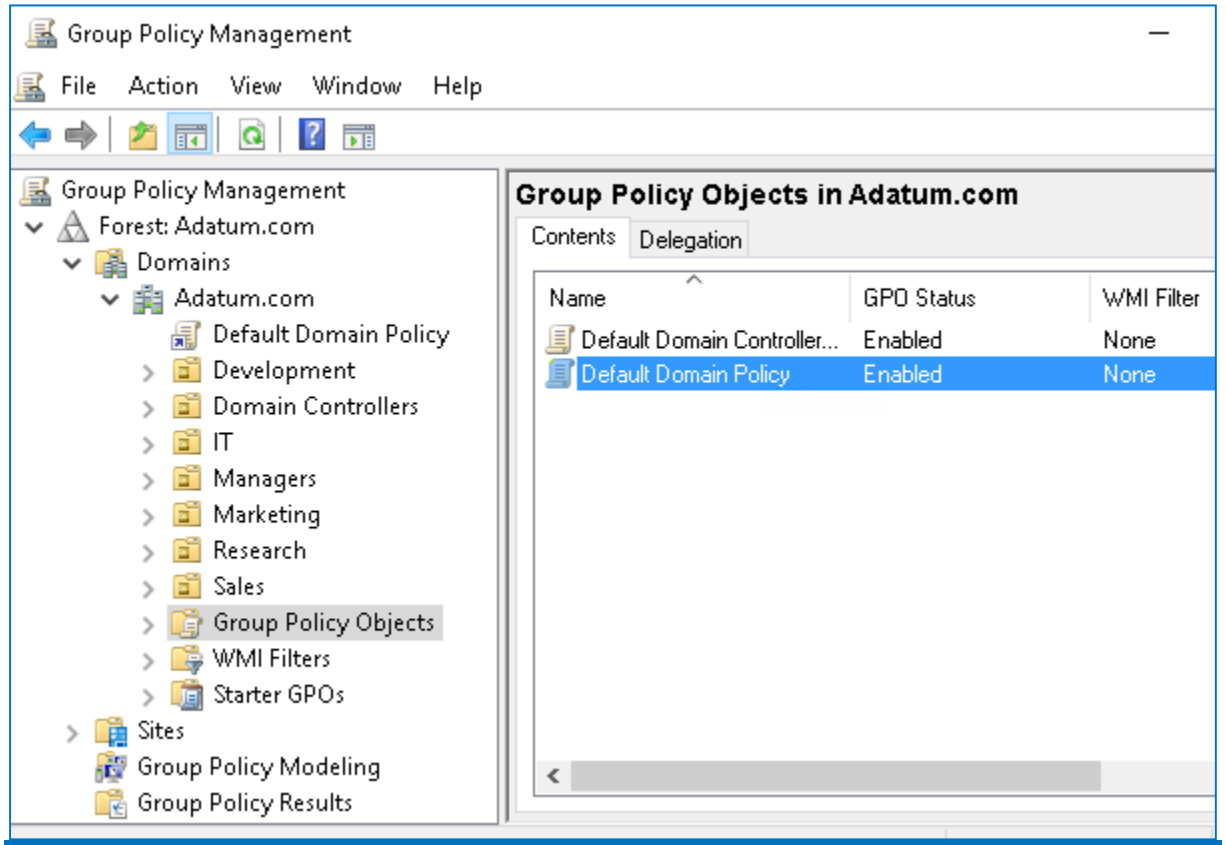
Lesson 1: Introducing Group Policy

- What is configuration management?
- Overview of Group Policy tools and consoles
- Benefits of using Group Policy
- Group Policy Objects
- Overview of GPO scope
- Overview of GPO inheritance
- The Group Policy Client service and client-side extensions
- New features in Group Policy in Windows Server 2016

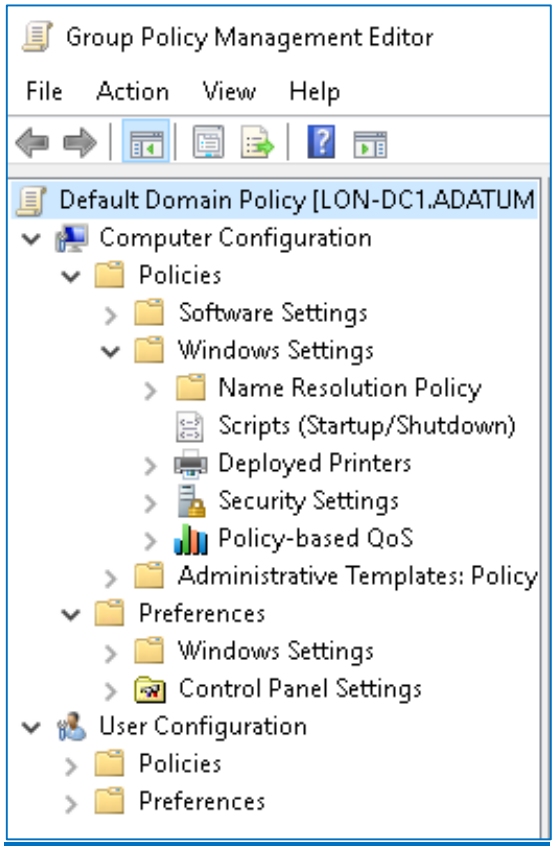
What is configuration management?

- *Configuration management* is a centralized approach to applying one or more changes to more than one user or computer
- The key elements of configuration management are:
  - Setting
  - Scope
  - Application

Overview of Group Policy tools and consoles



Group Policy Management Console



Group Policy Management Editor

Command-line utilities: **GPUpdate** and **GPResult**

Benefits of using Group Policy

- Group Policy is a very powerful administrative tool
- You can use it to enforce various types of settings to a large number of users and computers
- Typically, you use GPOs to:
  - Apply security settings
  - Manage desktop application settings
  - Deploy application software
  - Manage Folder Redirection
  - Configure network settings

Group Policy Objects

A GPO is:

- A container for one or more policy settings
- Managed with the GPMC
- Stored in the GPOs container
- Edited with Group Policy Management Editor
- Applied to a specific level in the AD DS hierarchy

Overview of GPO scope

- The *scope* of a GPO is the collection of users and computers that will apply the settings in the GPO
- You can use several methods to scope a GPO:
  - Link the GPO to a container, such as an OU
  - Filter by using security settings
  - Filter by using WMI filters
- For Group Policy preferences:
  - You can filter or target the settings that you configure by Group Policy preferences within a GPO based on several criteria

Overview of GPO inheritance

GPOs are processed on a client computer in the following order:

1. Local GPOs
2. Site-level GPOs
3. Domain-level GPOs
4. OU GPOs, including any nested OUs

The Group Policy Client service and client-side extensions

- Group Policy application process:
  1. Group Policy Client retrieves GPOs
  2. Client downloads and caches GPOs
  3. Client-side extensions process the settings
- Policy settings in the **Computer Configuration** node apply at system startup and every 90–120 minutes thereafter
- Policy settings in the **User Configuration** node apply at sign-in and every 90–120 minutes thereafter

New features in Group Policy in Windows Server 2016

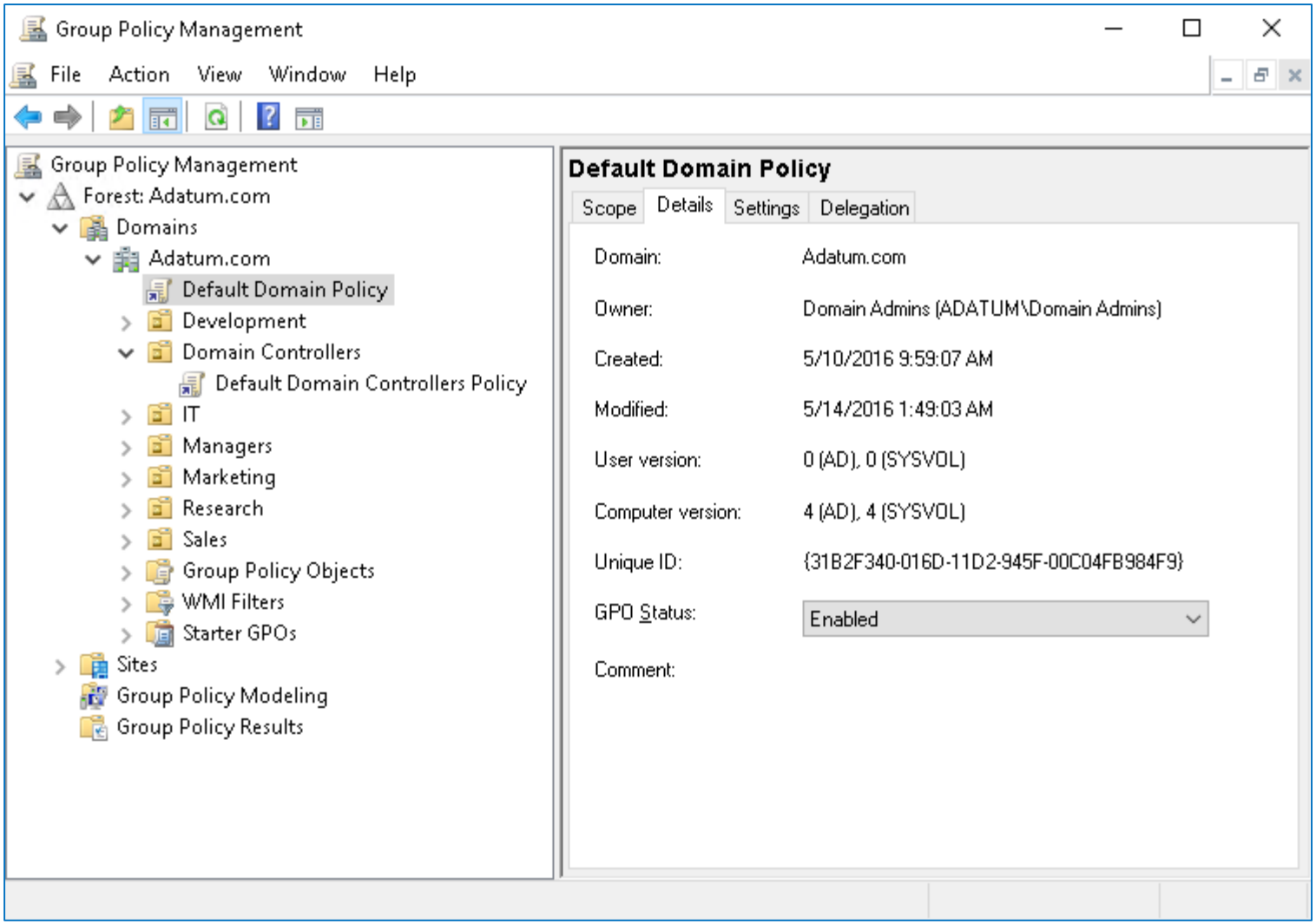
Windows Server 2016 introduces a few changes and improvements to Group Policy, including:

- Importing the following types of policy settings on Nano Server:
  - Registry settings
  - Security settings
  - Audit settings
- Including Windows 10 administrative templates

Lesson 2: Implementing and administering GPOs

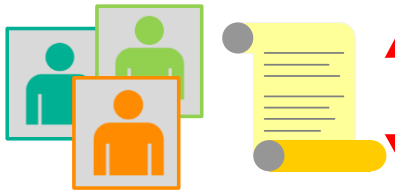
- What are domain-based GPOs?
- GPO storage
- What are starter GPOs?
- Common GPO management tasks
- Delegating administration of Group Policy

What are domain-based GPOs?



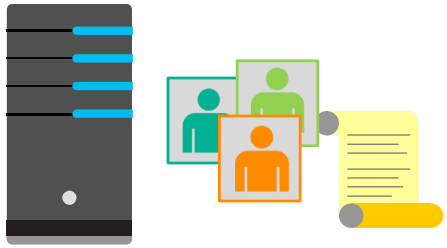
GPO storage

GPO



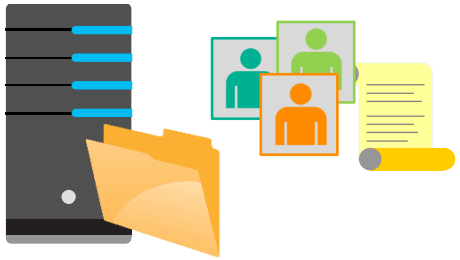
- Contains Group Policy settings
- Stores content in two locations

Group Policy container



- Stored in AD DS
- Provides version information

Group Policy template



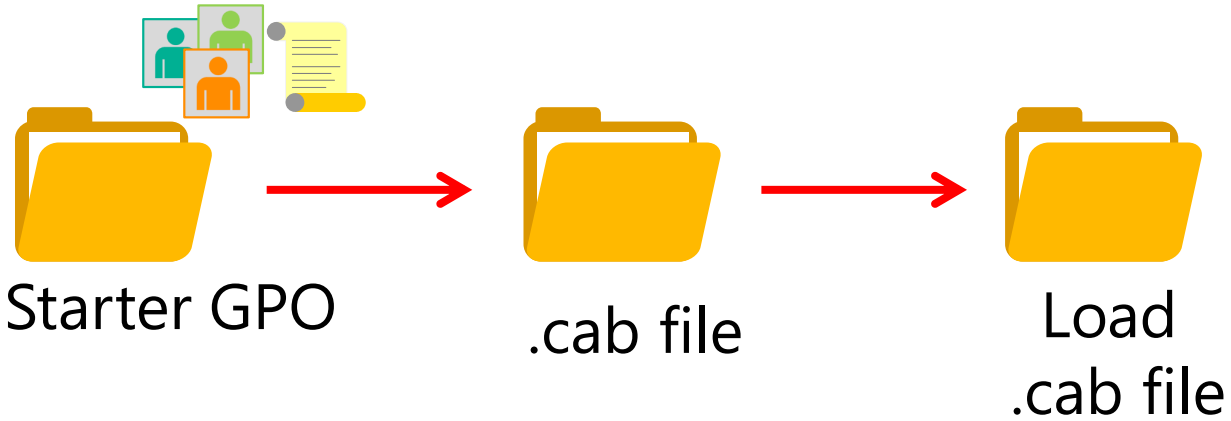
- Stored in shared SYSVOL folder
- Provides Group Policy settings

What are starter GPOs?

A starter GPO:

- Stores administrative template settings on which new GPOs will be based
- Can be exported to .cab files
- Can be imported into other areas of an organization

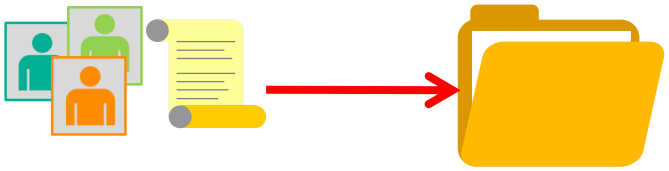
Exported to .cab file **Imported to the GPMC**



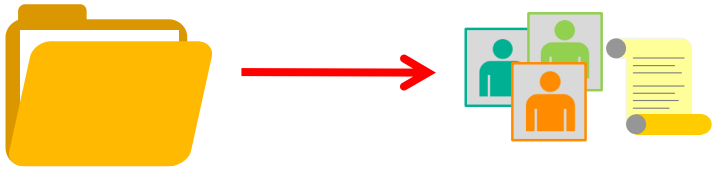
Common GPO management tasks

You can manage GPOs by using GPMC or Windows PowerShell. These are some of the options for managing the state of GPOs:

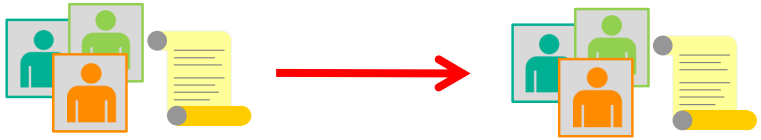
Back up GPOs



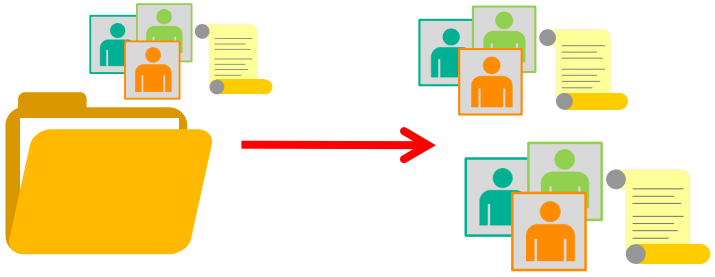
Restore GPOs



Copy GPOs



Import GPOs



Delegating administration of Group Policy

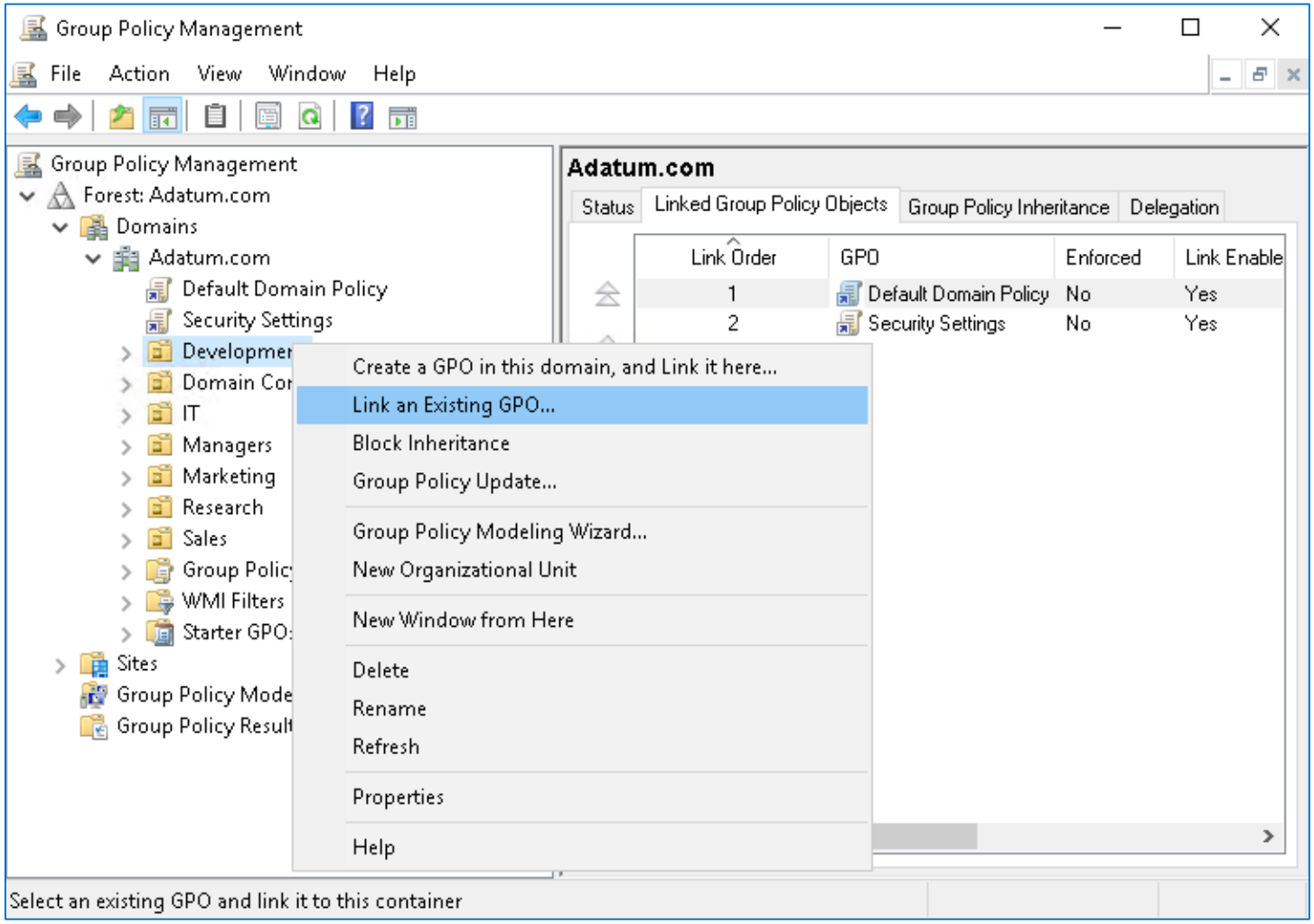
- Delegation of GPO-related tasks allows the administrative workload to be distributed across the enterprise
- You can delegate the following Group Policy tasks independently:
  - Creating GPOs
  - Editing GPOs
  - Managing Group Policy links for a site, domain, or OU
  - Performing Group Policy modeling analysis in a domain or OU
  - Reading Group Policy results data in a domain or OU
  - Creating WMI filters in a domain

Lesson 3: Group Policy scope and Group Policy processing

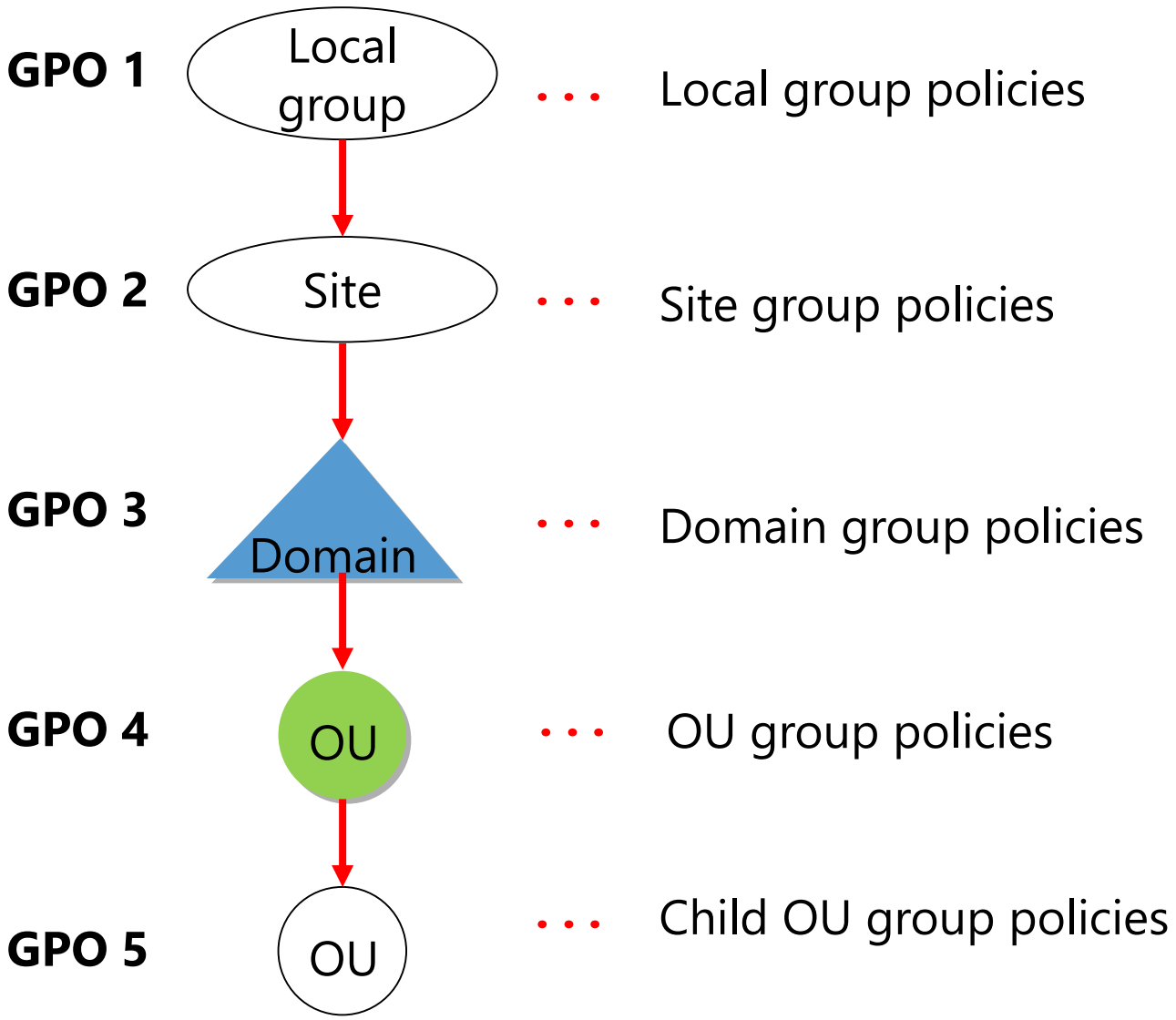
- What are GPO links?
- Demonstration: Linking GPOs
- Group Policy processing order
- Configuring GPO inheritance and precedence
- Using security filtering to modify Group Policy scope
- What are WMI filters?
- How to enable or disable GPOs and GPO nodes
- Loopback policy processing
- Considerations for slow links and disconnected systems
- Identifying when settings become effective

What are GPO links?

After you have linked a GPO, the users or computers in that container are within the scope of the GPO, including computers and users in child OUs



Group Policy processing order



Configuring GPO inheritance and precedence

- The application of GPOs linked to each container results in a cumulative effect called *policy inheritance:*
  - Default precedence: Local → Site → Domain → OU → Child OU… (LSDOU)
  - Visible on the **Group Policy Inheritance** tab
- Link order (attribute of GPO link):
  - Lower number → Higher on list → Precedence
- Block Inheritance (attribute of OU):
  - Blocks the processing of GPOs from a higher level
- Enforced (attribute of GPO link):
  - Enforced GPOs override Block Inheritance
  - Enforced GPO settings win over conflicting settings in lower GPOs

Using security filtering to modify Group Policy scope

- Apply Group Policy permission:
  - GPO has an ACL (**Delegation** tab → **Advanced**)
  - Members of the Authenticated Users group have Allow Apply Group Policy permissions by default
- To scope only to users in selected global groups:
  - Remove the Authenticated Users group
  - Add appropriate global groups: Must be global groups (GPOs do not scope to domain local)
- To scope to users except for those in selected groups:
  - On the **Delegation** tab, click **Advanced**
  - Add appropriate global groups
  - Deny the Apply Group Policy permission

What are WMI filters?

- WMI queries can filter GPOs based on system characteristics, including:
  - RAM
  - Processor speed
  - Disk capacity
  - IP address
  - Operating system version
- WMI queries are written by using WQL, for example

  select * from Win32_OperatingSystem where Version like "10.%"
- WMI filters can be expensive in terms of Group Policy processing performance

What are WMI filters?

Group Policy Management

File Action View Window Help

Group Policy Manage
Forest: Adatum.co
Domains
Adatum.co
Default
Security
Develop
Domain
IT
Manag
Market
Researc
Sales
Group
WMI Fi
Starter
Sites
Group Policy M
Group Policy F

Linked GPO

New WMI Filter

Name:
Windows 10 or Windows Server 2016

Description:

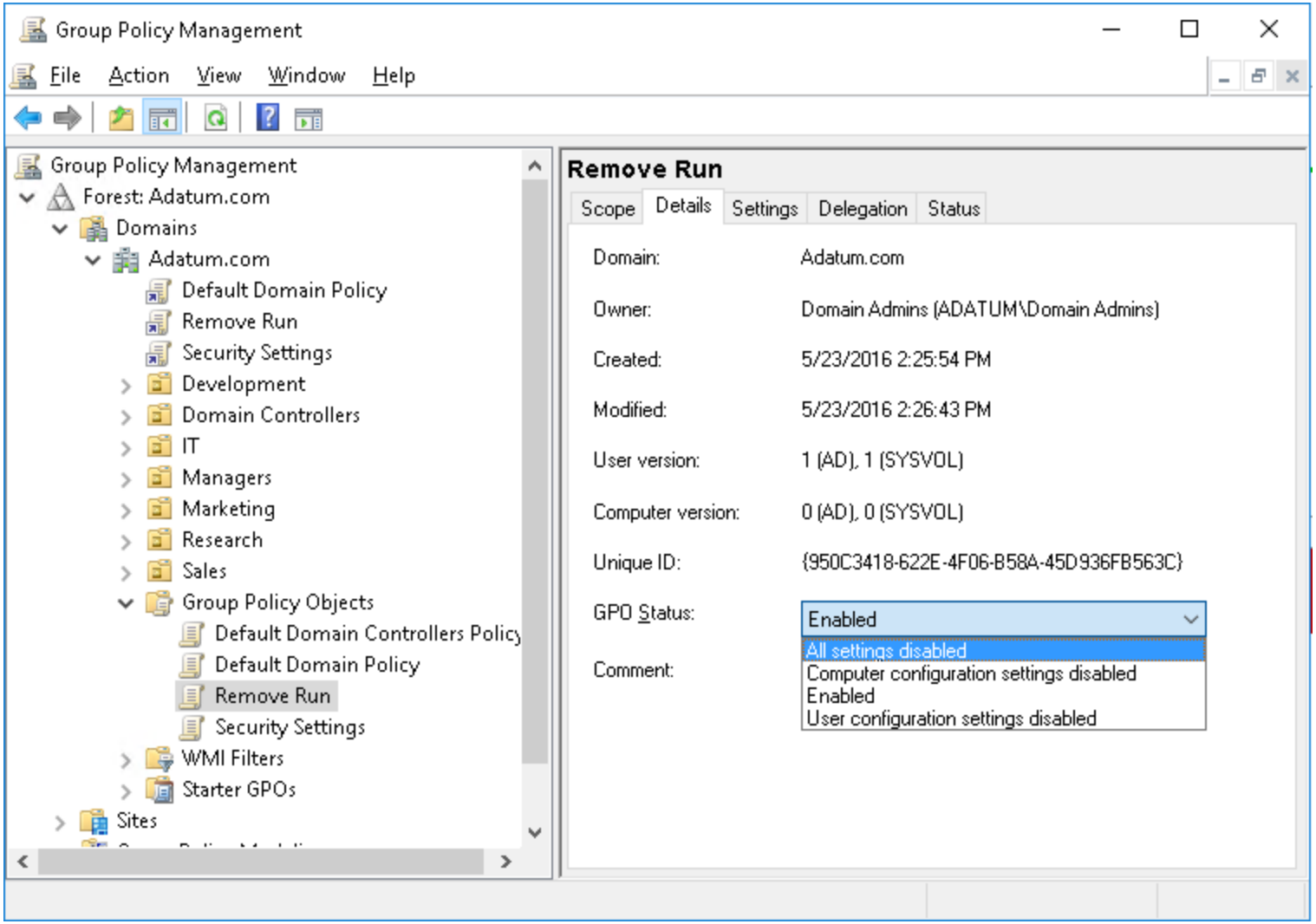
Queries:

Namespace	Query
root\CIMv2	Select * From Win32_OperatingSystem Where Version Like "10.%"

Add
Remove
Edit

Save
Cancel

How to enable or disable GPOs and GPO nodes



Loopback policy processing

- Provides the ability to apply user Group Policy settings based on the computer to which the user is signing in
- Replace mode:
  - Only the list of GPOs based on the computer object is used
- Merge mode:
  - The list of the GPOs based on the computer have higher precedence than the list of GPOs based on the user
- Useful in closely managed environments and special-use computers, such as:
  - Terminal servers, public-use computers, and classrooms

Loopback policy processing

Group Policy Management Editor

File Action View Help

- System
  - Access-Denied Ass
  - Audit Process Crea
  - Credentials Delega
  - Device Guard
  - Device Installation
  - Device Redirection
  - Disk NV Cache
  - Disk Quotas
  - Distributed COM
  - Driver Installation
  - Early Launch Antir
  - Enhanced Storage
  - File Classification I
  - File Share Shadow
  - Filesystem
  - Folder Redirection
  - Group Policy
  - Internet Communi
  - iSCSI
  - KDC
  - Kerberos
  - Locale Services
  - Logon

53 setting(s)

Configure user Group Policy loopback processing mode

Configure user Group Policy loopback processing mode

Previous Setting | Next Setting

- Not Configured
- Enabled
- Disabled

Comment:

Supported on: At least Windows 2000

Options:

Mode: Replace

Help:

This policy setting directs the system to apply the set of Group Policy objects for the computer to any user who logs on to a computer affected by this setting. It is intended for special-use computers, such as those in public places, laboratories, and classrooms, where you must modify the user setting based on the computer that is being used.

By default, the user's Group Policy Objects determine which user settings apply. If this setting is enabled, then, when a user logs on to this computer, the computer's Group Policy Objects determine which set of Group Policy Objects applies.

If you enable this setting, you can select one of the following modes from the Mode box:

"Replace" indicates that the user settings defined in the computer's Group Policy Objects replace the user settings normally applied to the user.

"Merge" indicates that the user settings defined in the computer's Group Policy Objects and the user settings normally

OK | Cancel | Apply

Considerations for slow links and disconnected systems

- Slow link detection:
  - By default, connection speeds below 500 kbps
  - The following CSEs apply by default:
    - Security Settings - security policy
    - Administrative Templates - Registry policy
- Disconnected computers:
  - Cache Group Policy so that settings still apply
  - Perform Group Policy refresh when reconnecting with the domain network if a background refresh has been missed

Identifying when settings become effective

- GPO replication must occur
- Group changes must replicate
- Group Policy refresh must occur
- User must sign out and sign in or the computer must restart
- You must perform a manual refresh
- Most CSEs do not reapply unchanged GPO settings

Module 6

Securing Active Directory Domain Services

Module Overview

- Securing domain controllers
- Implementing account security
- Implementing audit authentication
- Configuring managed service accounts
- Integrate additional service to Windows Server

Lesson 1: Securing domain controllers

- Security risks that can affect domain controllers
- Modifying the security settings of domain controllers
- Implementing secure authentication
- Securing physical access to domain controllers
- What are RODCs?
- Deploying an RODC
- Planning and configuring an RODC password replication policy
- Separating RODC local administration

Security risks that can affect domain controllers

- Domain controllers are prime targets for attacks and the most important resources to secure
- Security risks include:
  - Network security
  - Authentication attacks
  - Elevation of privilege
  - DoS attack
  - Operating system, service, or application attacks
  - Operational risks
  - Physical security threats

Modifying the security settings of domain controllers

- Use a GPO to apply the same security settings to all domain controllers
- Consider custom GPOs that link to the Domain Controllers OU
- Security options include:
  - Account policies, such as passwords and account lockout
  - Local policies, such as auditing, user rights, and security options
  - Event log configuration
  - Restricted groups
  - Secure system services
  - Windows Firewall with advanced security
  - Public key policies
  - Advanced auditing

Implementing secure authentication

Consider the following factors when implementing secure authentication:

- Secure user accounts and passwords
- Secure groups with elevated permissions
- Audit critical object changes
- Deploy secure authentication, such as smart cards or multi-factor authenication
- Secure network activity
- Establish deprovisioning and cleanup processes
- Secure client computers

Securing physical access to domain controllers

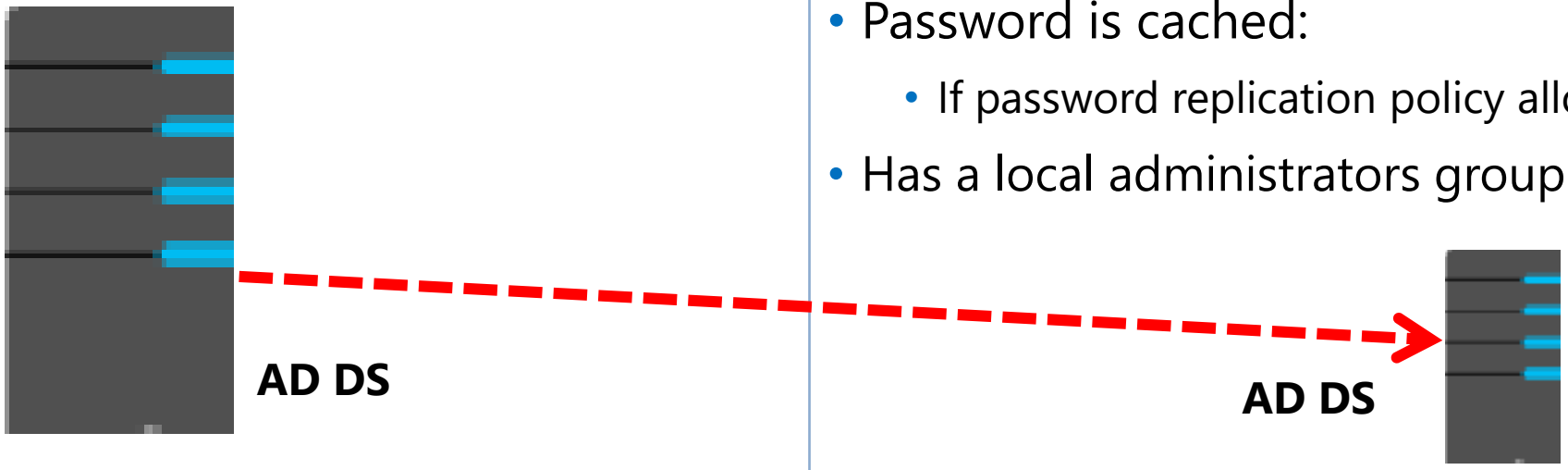
When securing physical access to your domain controllers, consider the following:

- Only deploy domain controllers where physical security is ensured
- Use RODCs
- Use BitLocker on domain controller disk volumes
- Monitor hot-swap disk systems because they can lead to domain controller theft
- Protect virtual disks; virtual machine admins must be highly trusted
- Store backups in secure locations

What are RODCs?

Datacenter	Branch office

• Writable Windows Server 2008 or newer domain controller
• Password replication policy:
  • Specifies which user and computer passwords can be cached by the RODC
	• RODC:
	  • All objects
	  • Subset of attributes:
	  • No secrets
	• Not writable
	• Users sign in:
	  • RODC forwards authentication
	• Password is cached:
	  • If password replication policy allows
	• Has a local administrators group



What are RODCs?

Consider the following limitations when deploying RODCs:

- RODCs cannot be operations master role holders
- RODCs cannot be bridgehead servers
- You should have only one RODC per site, per domain
- RODCs cannot authenticate across trusts when a WAN connection is not available
- No replication changes originate at an RODC
- RODCs cannot support any app properly that needs to update AD DS interactively

Deploying an RODC

- Prerequisites:
  - **ADPrep /RODCPrep**
  - Sufficient Windows Server 2008 or newer replication partners for the RODCs
- For a one-step deployment, perform either of the following steps:
  - In Server Manager, open Add Roles and Features, and then use **Active Directory Domain Services Configuration Wizard**
  - Windows PowerShell: **Install-ADDSDomainController –ReadOnlyReplica**
- For a two-step deployment, perform the following steps:
  1. Prestaging: Create the account by using Active Directory Administrative Center or **Add-ADDSReadOnlyDomainControllerAccount**
  2. Delegated promotion: Join the RODC as delegated admin: Server Manager or **Install-ADDSDomainController -ReadOnlyReplica**

Planning and configuring an RODC password replication policy

- A password replication policy determines which users' or computers' credentials that a specific RODC caches
- You can configure these credentials by using a:
  - Domain-wide password replication policy
  - RODC-specific password replication policy
  - RODC filtered attribute set

Separating RODC local administration

- Administrator role separation allows performance of local administrative tasks on the RODC for nondomain administrators
- Each RODC maintains a local Security Accounts Manager database of groups for specific administrative purposes
- Configure the local administrator by:
  - Adding the user or group when precreating or installing the RODC
  - Adding a user or group on the **Managed By** tab on the RODC account properties

Lesson 2: Implementing account security

- Account security in Windows Server 2016
- Password policies
- Account lockout policies
- Kerberos policies
- Protecting groups in AD DS
- Fine-grained password and lockout policies
- Tools for creating PSOs
- PSO precedence and resultant PSO
- Account-security options in Windows Server 2016
- Configuring user account policies
- Enhancing password authentication with Windows Hello and MFA

Account security in Windows Server 2016

Account security features in Windows Server 2016 include:

- Password policies
- Account lockout policies
- Fine-grained password policies
- Protected users
- Authentication policies
- Authentication policy silos

Password policies

Set password requirements by using the following settings:

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password complexity requirements:
  - Does not contain name or user name
  - Must have at least six characters
  - Contains characters from three of the following four groups groups: uppercase, lowercase, numeric, and special characters

Account lockout policies

- Account lockout policies define whether accounts should be locked automatically after several failed attempts to sign in
- To configure these policy settings, you must consider:
  - Account lockout duration
  - Account lockout threshold
  - Reset account lockout counter after
- Account lockout policies provide a level of security but also provide an opportunity for DoS attacks

Kerberos policies

- Kerberos policy settings determine timing for Kerberos tickets and other events

Setting	Default
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

- Kerberos claims and compound authentication for DAC requires Windows Server 2012 or newer domain controllers

Protecting groups in AD DS

- Restricted groups:
  - You can control membership for local groups on workstations and servers by using the following attributes:
    - Members
    - Member of
  - You cannot use these with domain groups
- Protected Users group:
  - Provides additional protection against the compromise of credentials during authentication processes
  - Members of this group automatically have nonconfigurable protection applied to their accounts

Fine-grained password and lockout policies

- You can use fine-grained password policies to specify multiple password policies within a single domain
- Fine-grained password policies:
  - Apply only to user objects, **InetOrgPerson** objects, or global security groups
  - Do not apply directly to an OU
  - Do not interfere with custom password filters that you might use in the same domain

Tools for creating PSOs

Windows Server 2012 and newer operating systems provide two tools for configuring PSOs:

- Windows PowerShell cmdlets:
  - **New-ADFineGrainedPasswordPolicy**
  - **Add-FineGrainedPasswordPolicySubject**
- Active Directory Administrative Center

PSO precedence and resultant PSO

- If multiple PSOs apply to a user:
  - The PSOs that you directly apply take precedence rather than the PSOs that you apply by using group memberships
  - The PSO with the lowest precedence wins
  - If two PSOs have the same precedence, the smallest objectGUID wins
- To evaluate a user object to see which PSO has been applied, you can use the **msDS-ResultantPSO** Active Directory attribute
- To view the effective PSO that AD DS applies to a user:
  1. Open Active Directory Users and Computers, and on the **View** menu, ensure that Advanced Features is enabled
  2. Open the properties of a user account
  3. On the **Attribute Editor** tab, view the **msDS-ResultantPSO** attribute if you have configured the **Show Constructed Attributes** option under the **Filter** options

Account-security options in Windows Server 2016

- Protected Users group:
  - Protects users in the Protected Users group
  - Prevents locally cached user profiles and credentials
  - Requires Kerberos authentication, limits TGT to four hours
  - No offline sign in
  - Windows 8.1, Windows 10, Windows Server 2012 R2 and Windows Server 2016 domain members only
- Authentication policies:
  - Configured as authentication policy object in AD DS, applied to user, service, or computer accounts
  - Custom TGT
  - Uses claims (DAC) for custom conditions
- Authentication policy silos:
  - AD DS object
  - Centrally apply authentication policies to multiple objects
  - Additional claim allows administrators to configure file access per silo

Configuring user account policies

- Local Security Policy account settings:
  - Configure with **secpol.msc**
  - Apply to local user accounts
- Group Policy account settings:
  - Configure with the Group Policy Management console
  - Apply to all accounts in AD DS and local accounts on computers joined to the domain
  - Can apply only once in a domain and in only one GPO
  - Take precedence over Local Security Policy settings

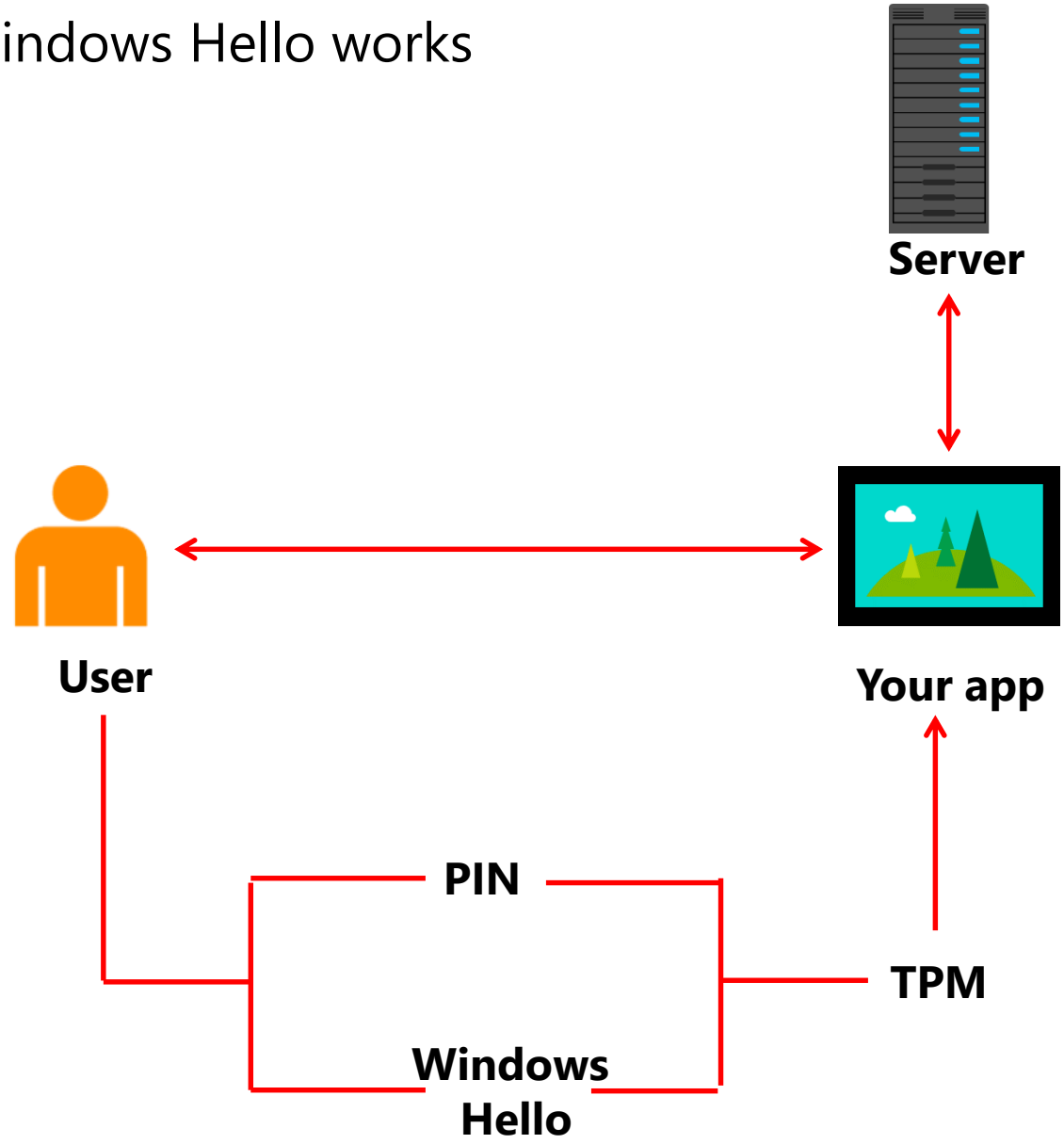
Enhancing password authentication with Windows Hello and MFA

To enhance security of the authentication process, you can use:

- Windows Hello:
  - For biometric-based sign in to Windows
- Microsoft Passport:
  - To leverage Windows Hello and TPM
- Azure Multi-Factor Authentication:
  - To enhance account security by adding second factor of verification
  - Can be used in cloud or for on-premises applications

Enhancing password authentication with Windows Hello and MFA

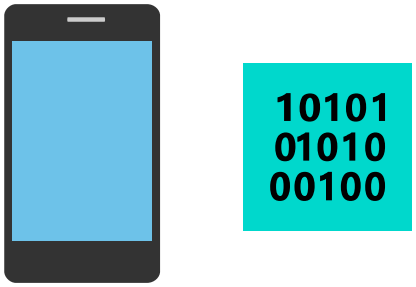
How Windows Hello works



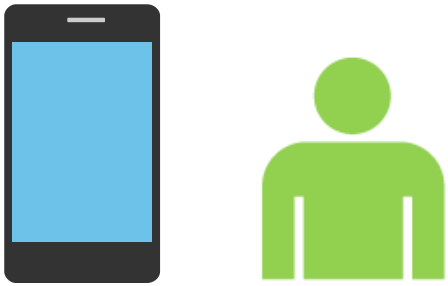
Enhancing password authentication with Windows Hello and MFA

Multi-Factor Authentication adds a second level of authentication:

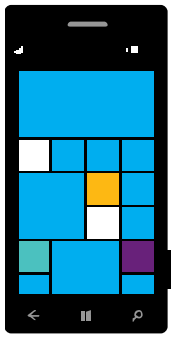
- Text message



- Phone call



- Mobile app

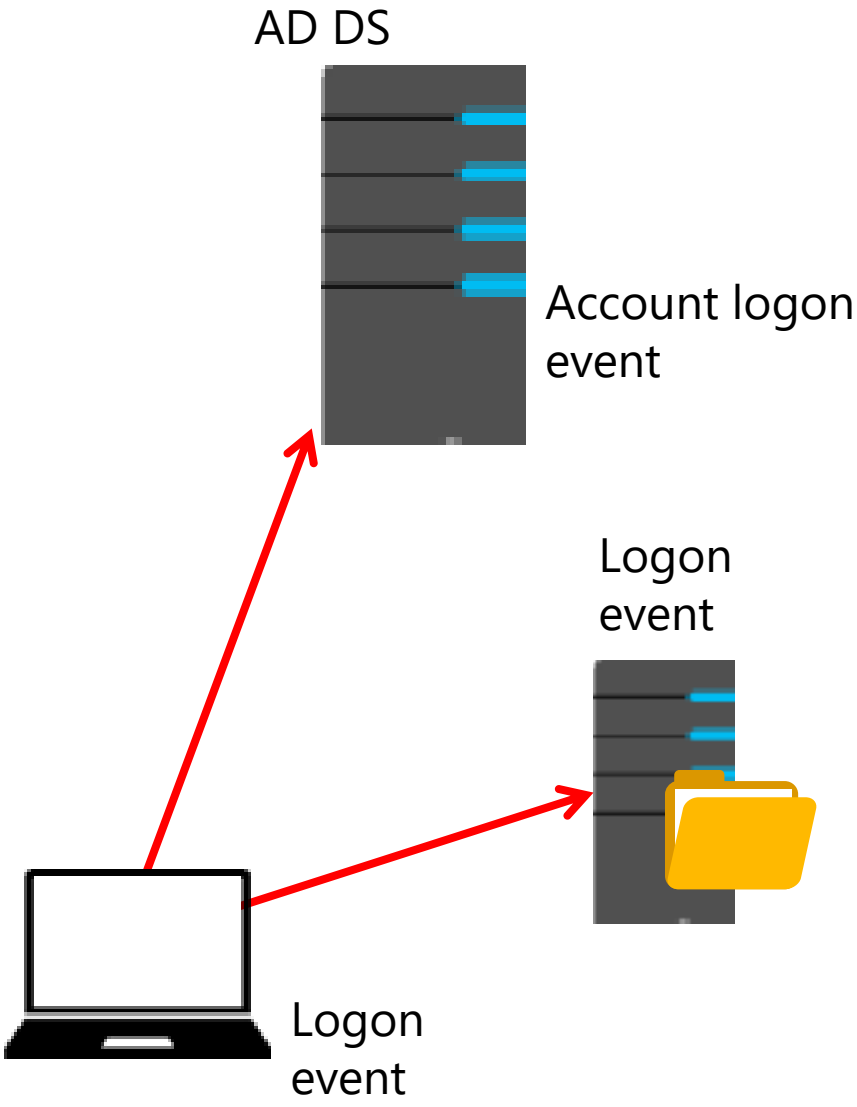


Lesson 3: Implementing audit authentication

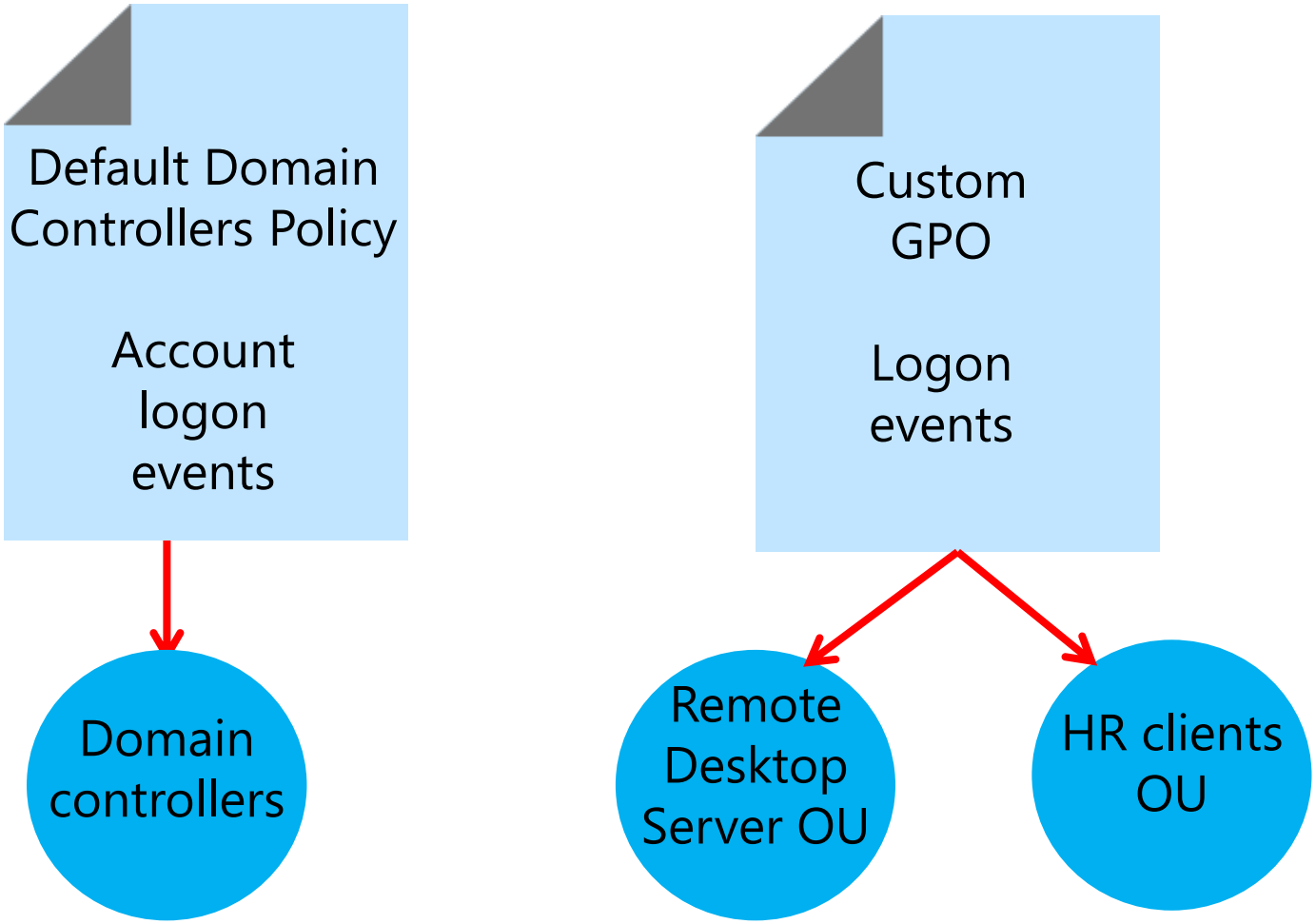
- Account logon and logon events
- Scoping audit policies

Account logon and logon events

- Account logon events:
  - The system that authenticates the account registers these events
  - For domain accounts: domain controllers
  - For local accounts: local computer
- Logon events:
  - The machine at or to which a user logged on registers these events
  - Interactive logon: user's system
  - Network logon: server



Scoping audit policies



Lesson 4: Configuring managed service accounts

- Overview of service accounts
- Challenges of using service accounts
- Overview of managed service accounts
- What are group MSAs?
- SPNs and Kerberos delegation

Overview of service accounts

- Sometimes, applications require resource access:
  - For this purpose, you can create domain or local accounts to manage such access. However, this might compromise security
- Use the following service accounts instead:
  - Local System:
    - Most privileged, still vulnerable if compromised
  - Local Service:
    - Least privileged, may not have enough permissions to access all required resources
  - Network Service:
    - Can access network resources with proper credentials

Challenges of using service accounts

- Extra administration effort to manage the service account password
- Difficulty in determining where a domain-based account is used as a service account
- Extra administration effort to mange the SPN

Overview of managed service accounts

- Use MSAs to automate password and SPN management for service accounts that services and applications use
- Requires a Windows Server 2008 R2 or newer installed with:
  - .NET Framework 3.5.x
  - Active Directory module for Windows PowerShell
- Recommended to run with AD DS configured at the Windows Server 2008 R2 functional level or higher

What are group MSAs?

- Group MSAs extend the capability of standard MSAs by:
  - Enabling MSAs for use on more than one computer in the domain
  - Storing MSA authentication information on domain controllers
- To support group MSA, your environment:
  - Must have at least one Windows Server 2012 or newer domain controller
  - Must have a KDS root key created for the domain

SPNs and Kerberos delegation

- Kerberos delegation of authentication:
  - Services can delegate service tickets issued to them by the KDC to another service
- Constrained delegation:
  - Allows administrators to define which services can use service tickets issued to other services
- SPNs help identify services uniquely
- Windows Server 2016 allows:
  - Constrained delegation across domains
  - Service administrators to configure constrained delegation

Lesson 5: Integrate additional service to Windows Server

- Hardware and license requirement
- Network and architecture requirement
- Prerequisite Software
- System account
- Compatibility

Example SQL Server 2017

Hardware and software requirements

The following requirements apply to all installations:

Component	Requirement
Operating system	Windows 10 TH1 1507 or greater Windows Server 2016 or greater
.NET Framework	Minimum operating systems includes minimum .NET framework.
Network Software	Supported operating systems for SQL Server have built-in network software. Named and default instances of a stand-alone installation support the following network protocols: Shared memory, Named Pipes, and TCP/IP.
Hard Disk	SQL Server requires a minimum of 6 GB of available hard-disk space. Disk space requirements will vary with the SQL Server components you install. For more information, see Hard Disk Space Requirements later in this article. For information on supported storage types for data files, see Storage Types for Data Files.
Monitor	SQL Server requires Super-VGA (800x600) or higher resolution monitor.
Internet	Internet functionality requires Internet access (fees may apply).

Example SQL Server 2017

Processor, memory, and operating system requirements

The following memory and processor requirements apply to all editions of SQL Server:

Component	Requirement
Memory *	**Minimum:** Express Editions: 512 MB All other editions: 1 GB **Recommended:** Express Editions: 1 GB All other editions: At least 4 GB and should be increased as database size increases to ensure optimal performance.
Processor Speed	**Minimum:** x64 Processor: 1.4 GHz **Recommended:** 2.0 GHz or faster
Processor Type	x64 Processor: AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support

Example SQL Server 2017

OS compatibility

The following table shows which editions of SQL Server 2019 are compatible with which versions of Windows:

SQL Server edition:	Enterprise	Developer	Standard	Web	Express
Windows Server 2019 Datacenter	Yes	Yes	Yes	Yes	Yes
Windows Server 2019 Standard	Yes	Yes	Yes	Yes	Yes
Windows Server 2019 Essentials	Yes	Yes	Yes	Yes	Yes
Windows Server 2016 Datacenter	Yes	Yes	Yes	Yes	Yes
Windows Server 2016 Standard	Yes	Yes	Yes	Yes	Yes
Windows Server 2016 Essentials	Yes	Yes	Yes	Yes	Yes
Windows 10 Enterprise	No	Yes	Yes	No	Yes
Windows 10 Professional	No	Yes	Yes	No	Yes
Windows 10 Home	No	Yes	Yes	No	Yes