elev8

Active Directory

Module 04

About this Module

- This course provides to the students the information they need to know to get started with Active Directory (AD DS) and its key concepts.

- In this module is to provide coverage of AD DS objects, AD DS deployments, how to deploy an AD DS environment, configure AD DS trusts, implementing Group policies and much more.

- The goal of this course is to help learning Active Directory and to be more efficiently in a future job.

Agenda

- **Unit 01** – Installing and configuring domain controllers
- **Unit 02** – Managing objects in AD DS
- **Unit 03** – Advanced AD DS infrastructure management
- **Unit 04** – Implementing and administering AD DS sites and replication
- **Unit 05** – Implementing Group Policy
- **Unit 06** – Managing user settings with Group Policy
- **Unit 07** – Securing Active Directory Domain Services

Agenda

- **Unit 08** – Deploying and managing AD CS
- **Unit 09** – Deploying and managing certificates
- **Unit 10** – Implementing and administering AD FS
- **Unit 11** – Implementing AD DS synchronization with Microsoft Azure AD
- **Unit 12** – Monitoring, managing, and recovering AD DS

Unit 01

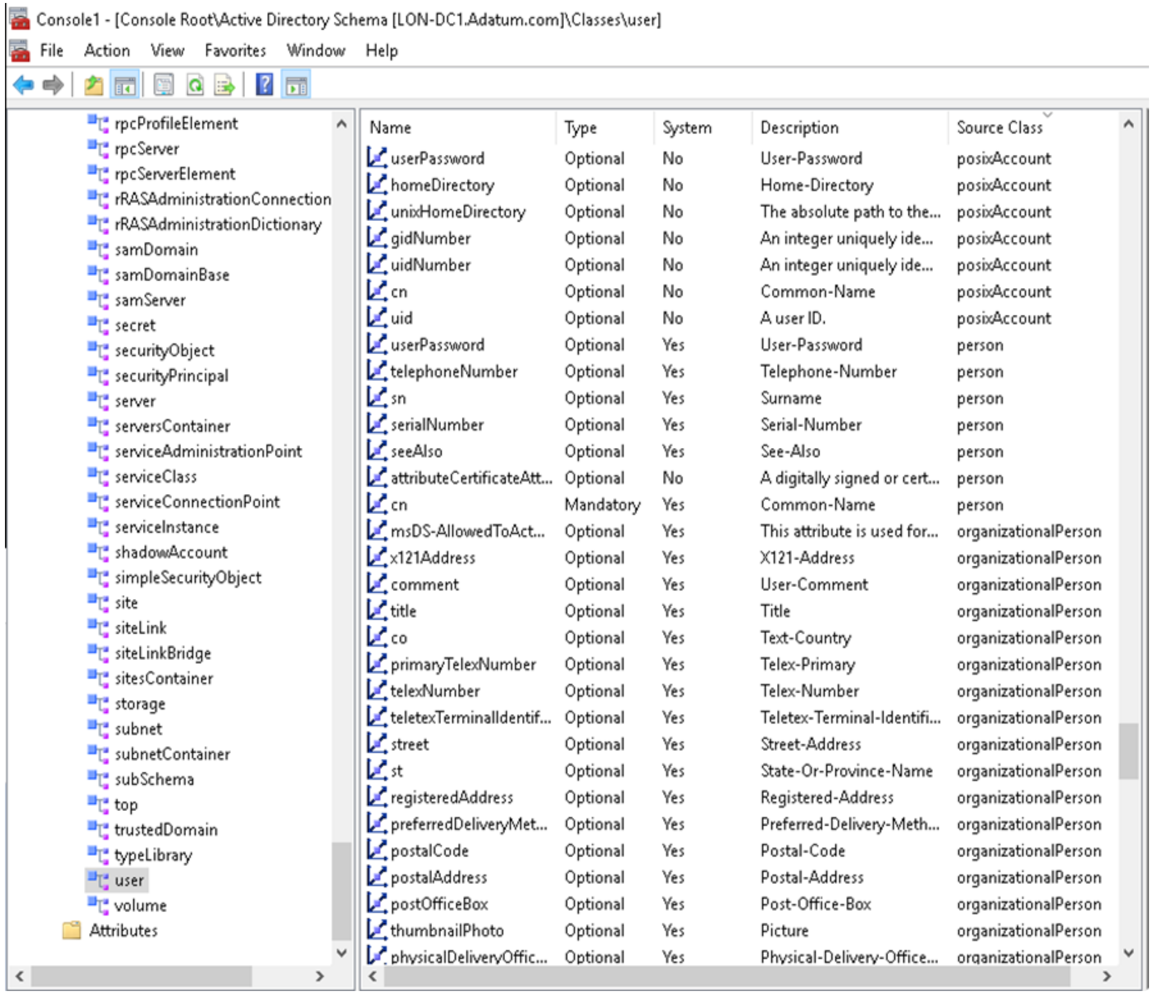
Installing and configuring domain controllers

elev8 LEARNING SOLUTIONS

AD DS 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?

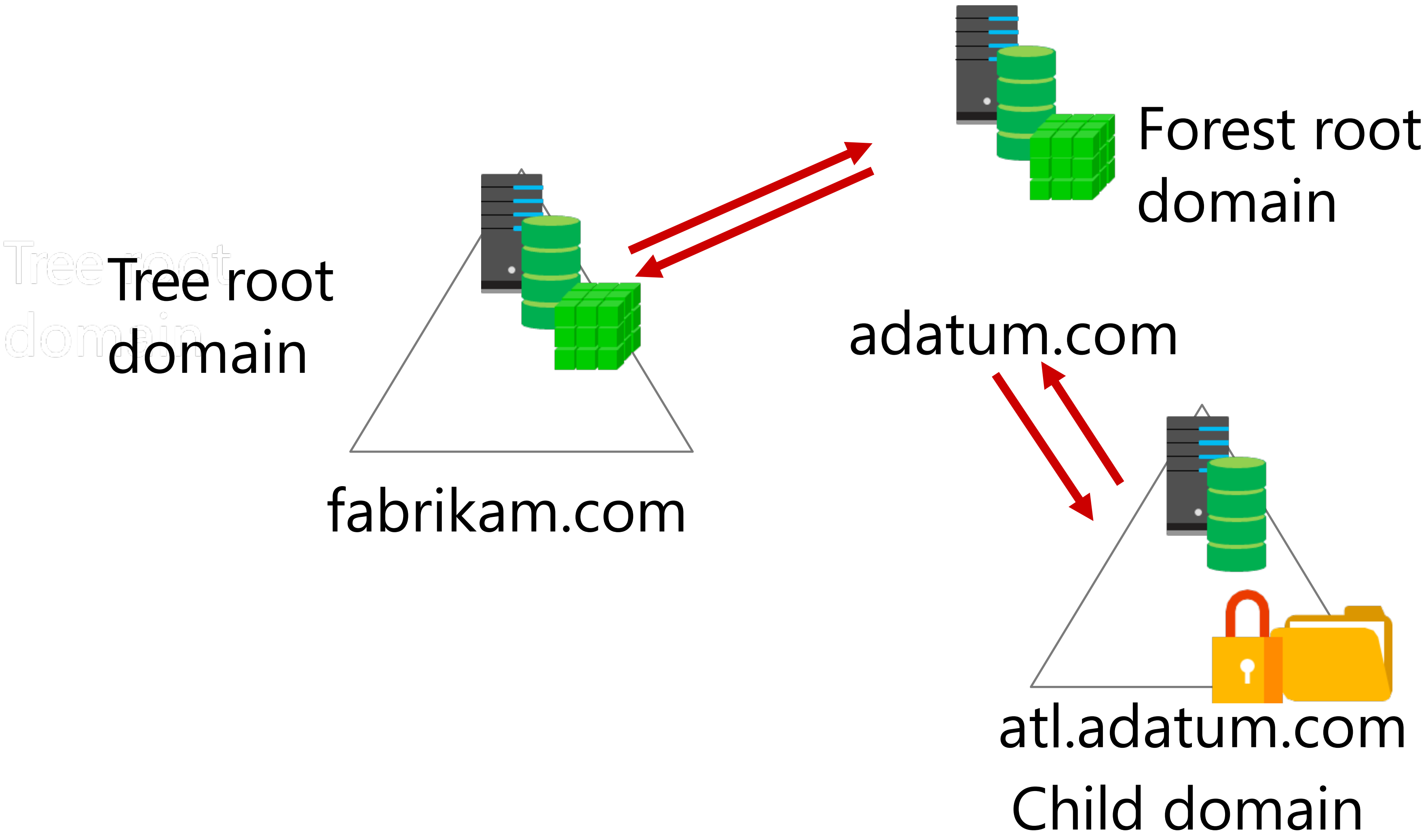


Console1 - [Console Root\Active Directory Schema [LON-DC1.Adatum.com]\Classes\user]

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?



Forest root domain

adatum.com

Tree root domain

Tree root domain

fabrikam.com

atl.adatum.com

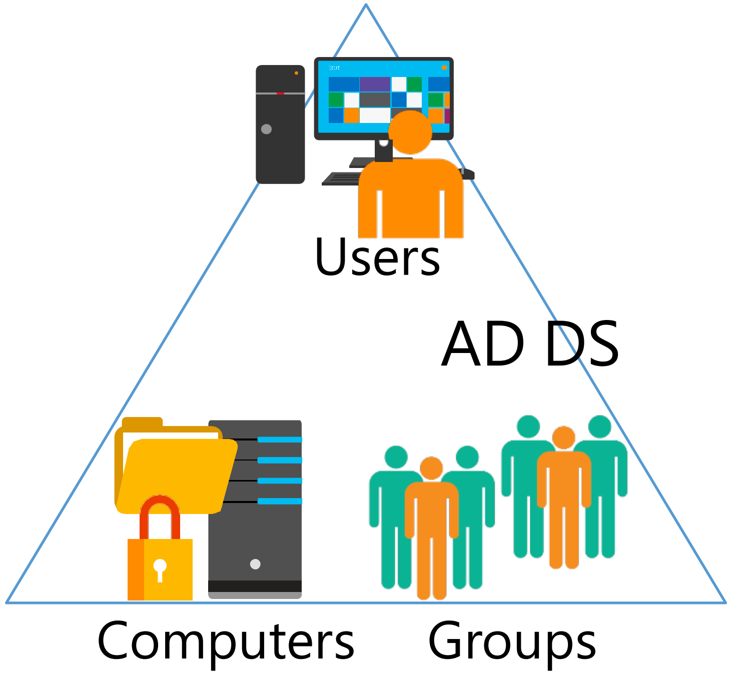
Child domain

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

What is an AD DS domain?

- 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?

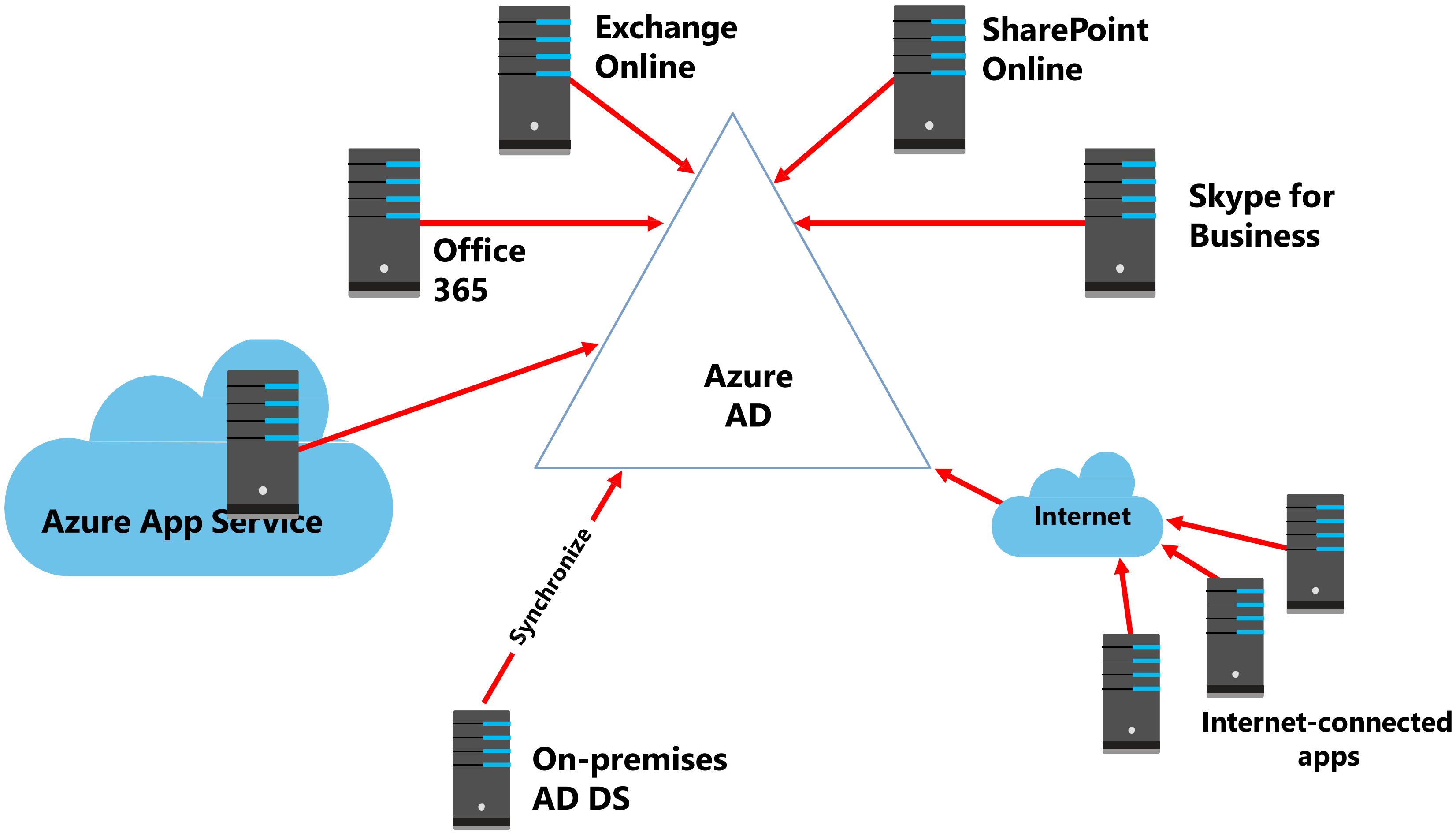
Use containers to group objects within a domain:

- 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

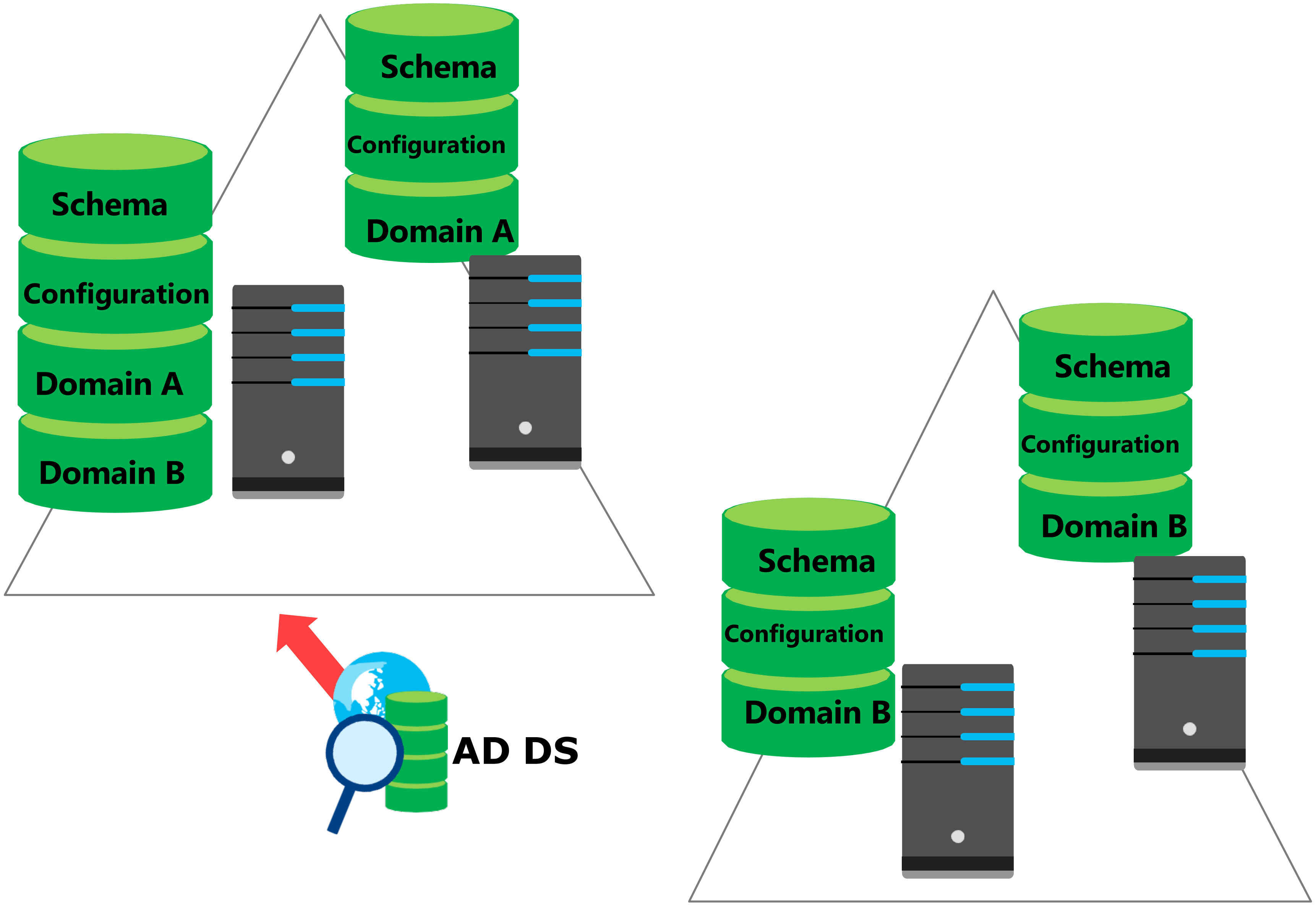
What is Azure AD?



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?

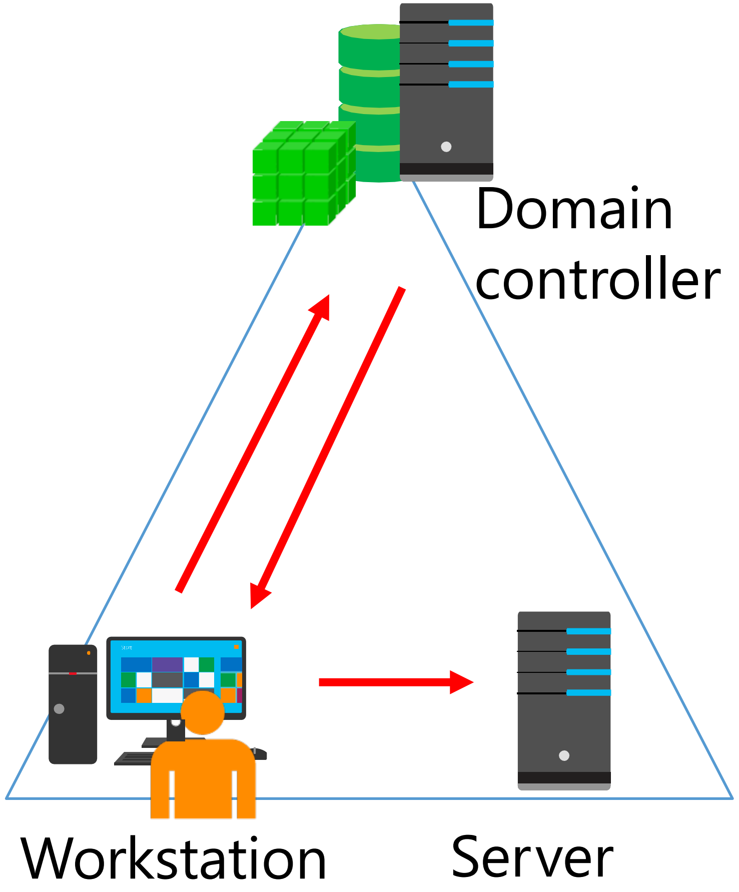


Overview of domain controller SRV records

- 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:
    - A list of domain controllers in the same site as the client
    - A list of domain controllers in the next closest site, if none are available in the same site
    - 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)

What are operations masters?

The five FSMOs

Forest:

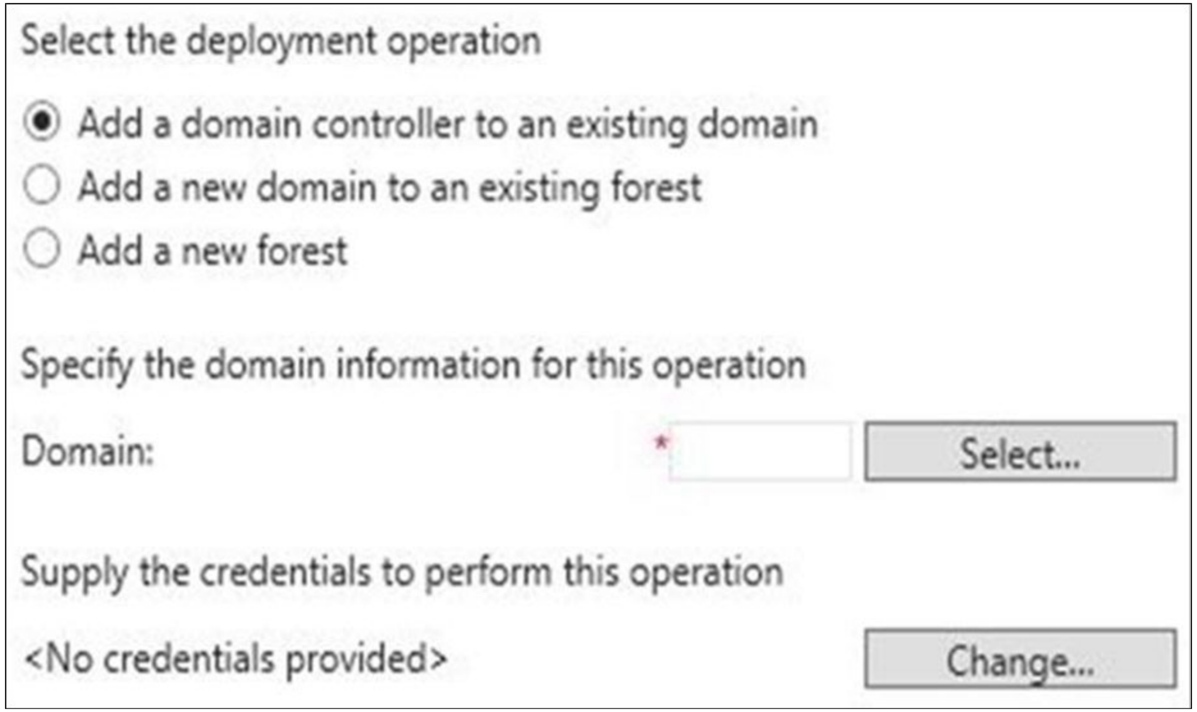
- Domain naming master
- Schema master

Domain:

- RID master
- Infrastructure master
- PDC emulator master

Installing a domain controller from Server Manager

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



Select the deployment operation

● Add a domain controller to an existing domain

○ Add a new domain to an existing forest

○ Add a new forest

Specify the domain information for this operation

Domain: *

Supply the credentials to perform this operation

<No credentials provided>

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

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

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

Best practices for domain controller virtualization

- 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

Unit 02

Managing objects in AD DS

Creating user accounts

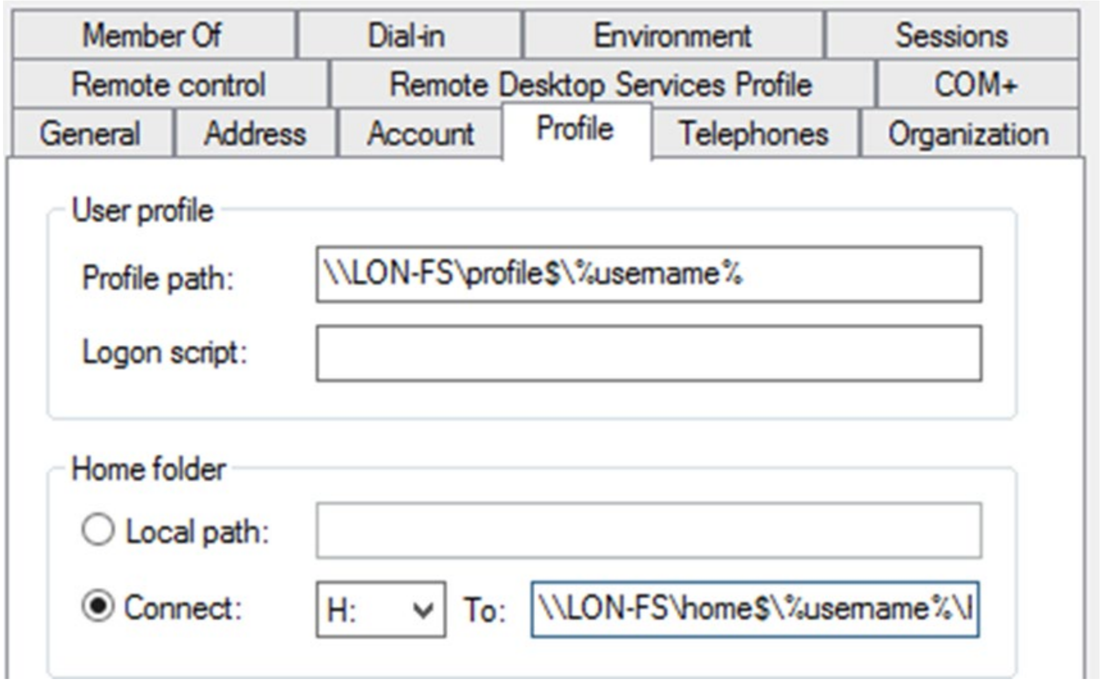
- Users accounts:
  - Allow or deny access to sign into computers
  - Grant access to processes and services
  - Manage access to network resources
- User accounts can be created by using:
  - Active Directory Users and Computers
  - Active Directory Administrative Center
  - Windows PowerShell
  - Directory command line tool dsadd
- Considerations for naming users include:
  - Naming formats
  - UPN suffixes

Configuring user account attributes

- User properties include the following categories:
  - Account
  - Organization
  - Member of
  - Password Settings
  - Profile
  - Policy
  - Silo
  - Extensions

Creating user profiles

- The Profile section of the User Properties window



User profile

Profile path: \\LON-FS\profile$\%username%

Logon script:

Home folder

○ Local path:

● Connect: H: To: \\LON-FS\home$\%username%\l

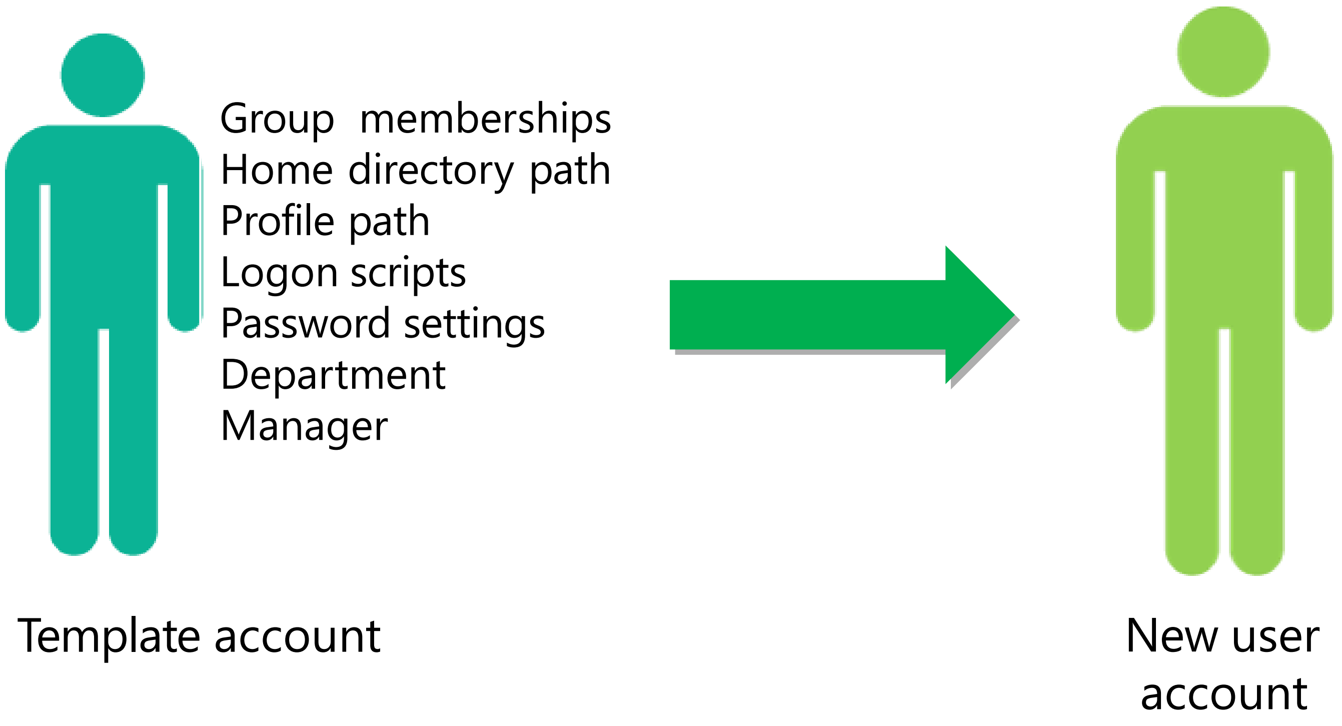
Managing inactive and disabled user accounts

- Users accounts that will be inactive for a period of time should be disabled rather than deleted
- To disable an account in Active Directory Users and Computers, right-click the account and click Disable Account from the menu

User account templates

- User templates simplify the creation of new user accounts

User templates simplify the creation of new user accounts



Group types

- **Distribution groups**
  - Used only with email applications
  - Not security enabled (no SID)
  - Cannot be given permissions

- **Security groups**
  - Security principal with a SID
  - Can be given permissions
  - Can also be email-enabled

- You can convert security groups to distribution groups and distribution groups to security groups

Group scopes

- Local groups can contain users, computers, global groups, domain- local groups and universal groups from the same domain, domains in the same forest and other trusted domain and can be given permissions to resources on the local computer only

- Domain-local groups have the same membership possibilities but can be given permission to resources anywhere in the domain

Group scopes

- Universal groups can contain users, computers, global groups and other universal groups from the same domain or domains in the same forest and can be given permissions to any resource in the forest

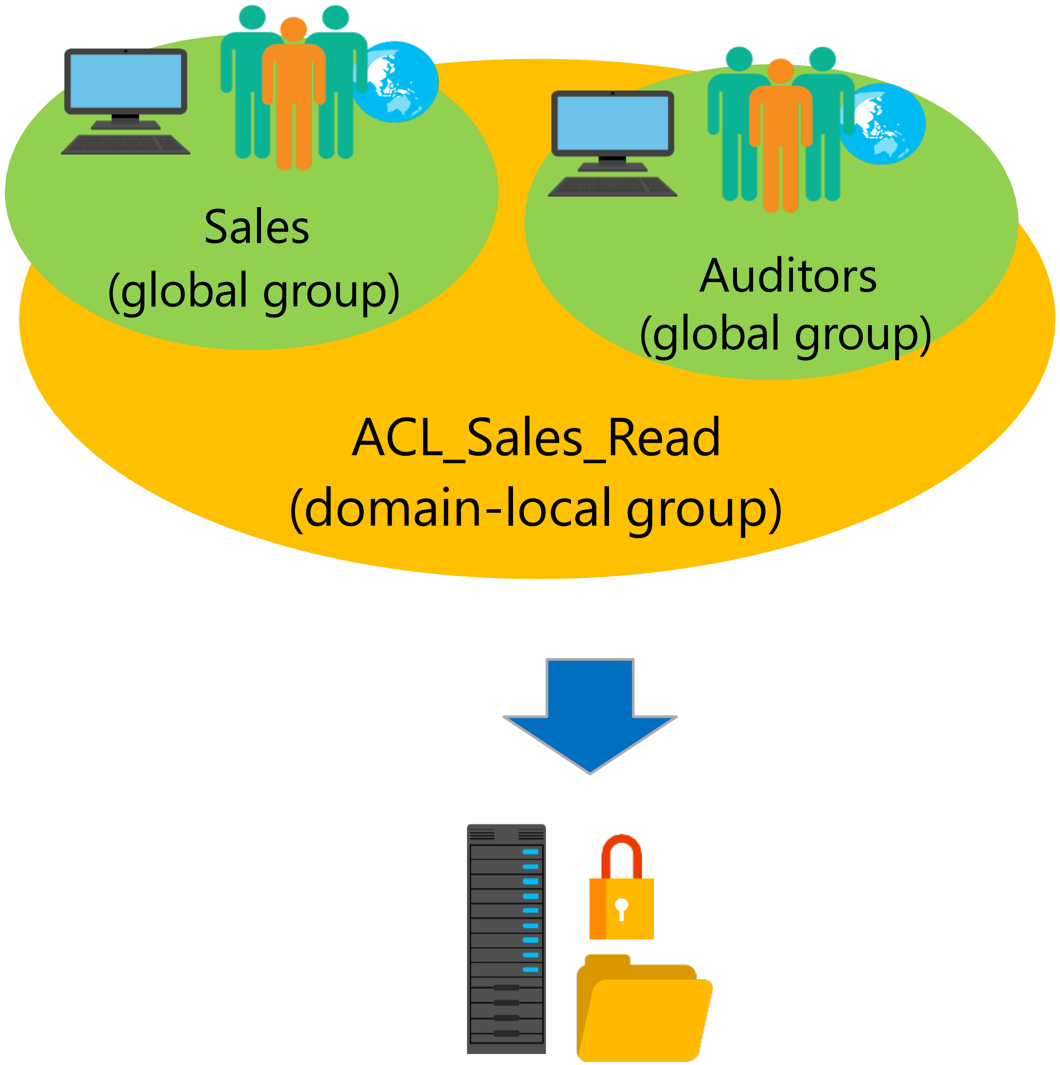
- Global groups can only contain users, computers and other global groups from the same domain and can be given permission to resources in the domain or any trusted domain

Implementing group management

I: Identities, users, or computers, which are members of

G: Global groups, which collect members based on members' roles, which are members of

DL: Domain-local groups, which provide management such as resource access A: Assigned access to a resource



Implementing group management

I: Identities, users, or computers, which are members of

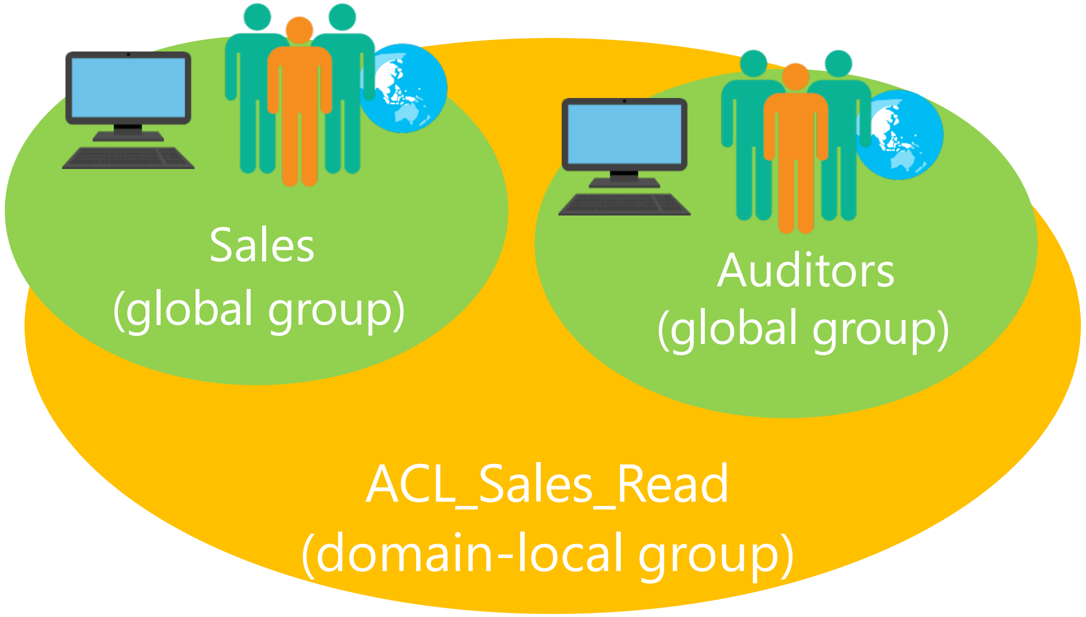
Implementing group management

I: Identities, users, or computers, which are members of

G: Global groups, which collect members based on members' roles, which are members of

Implementing group management

- I:Identities, users, or computers, which are members of
- G: Global groups, which collect members based on members' roles, which are members of
- DL: Domain-local groups, which provide management such as resource access which are



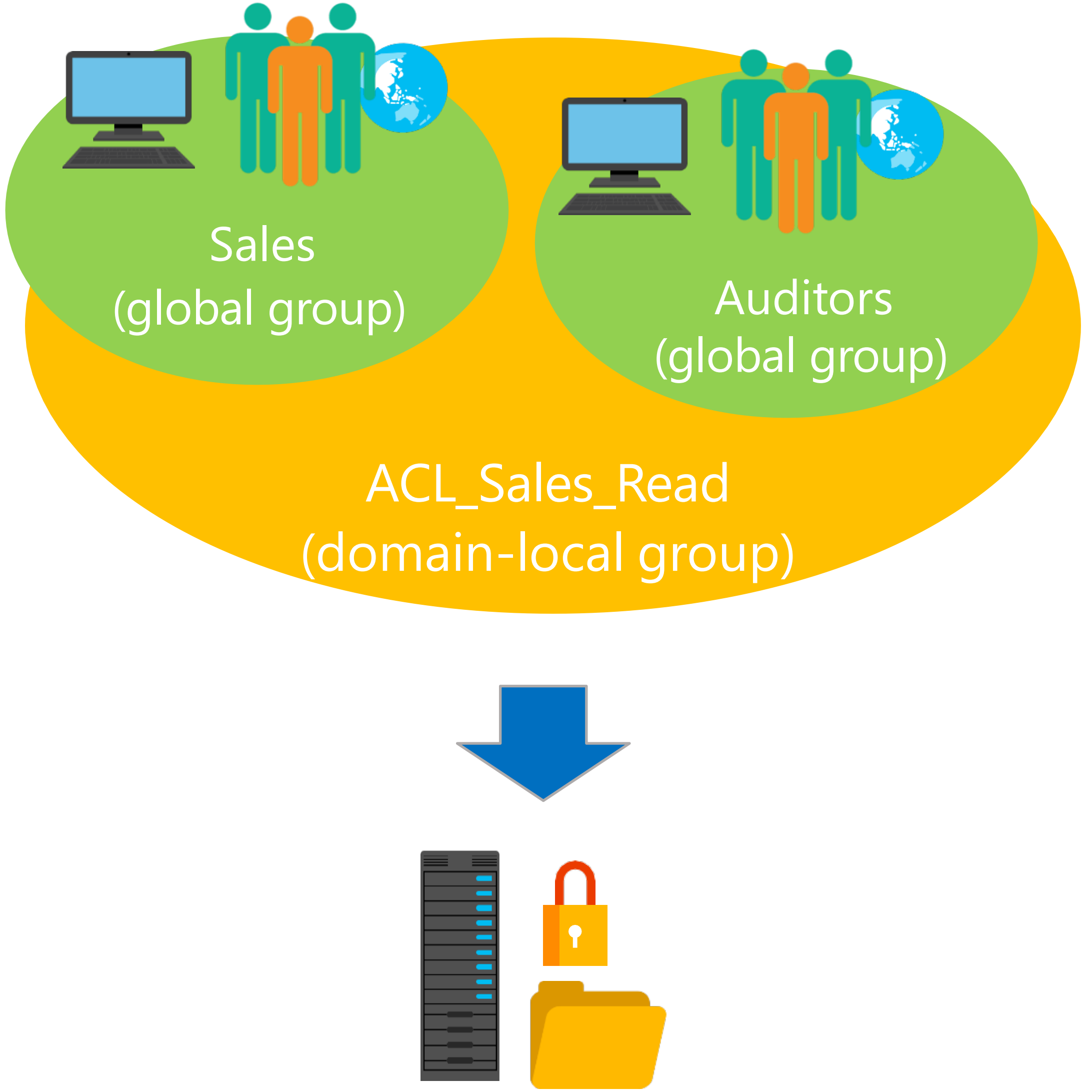
Implementing group management

I: Identities, users, or computers, which are members of

G: Global groups, which collect members based on members’ roles, which are members of

DL: Domain-local groups, which provide management such as resource access which are

A: Assigned access to a resource



Implementing group management

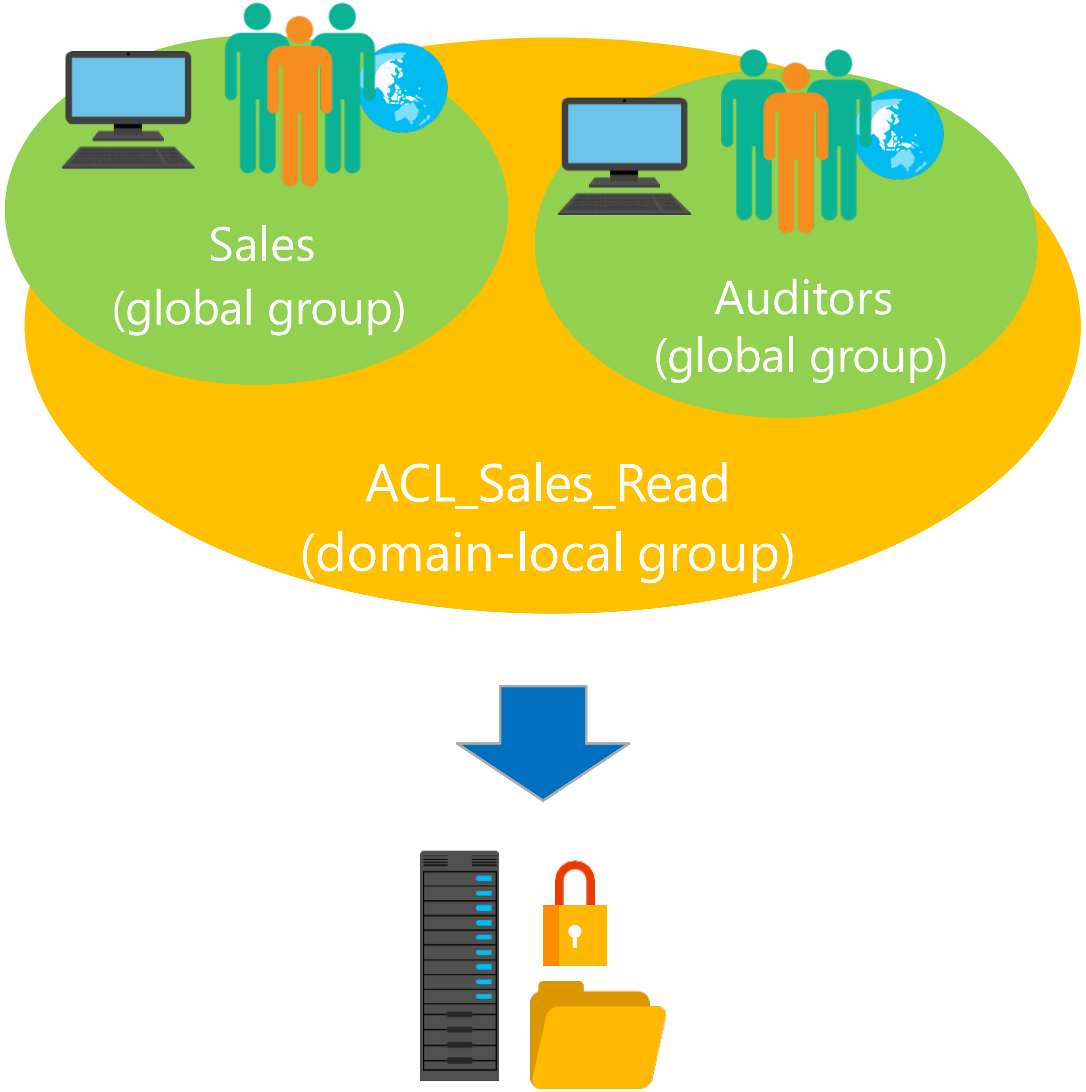
This best practice for nesting groups is known as IGDLA

I: Identities, users, or computers, which are members of

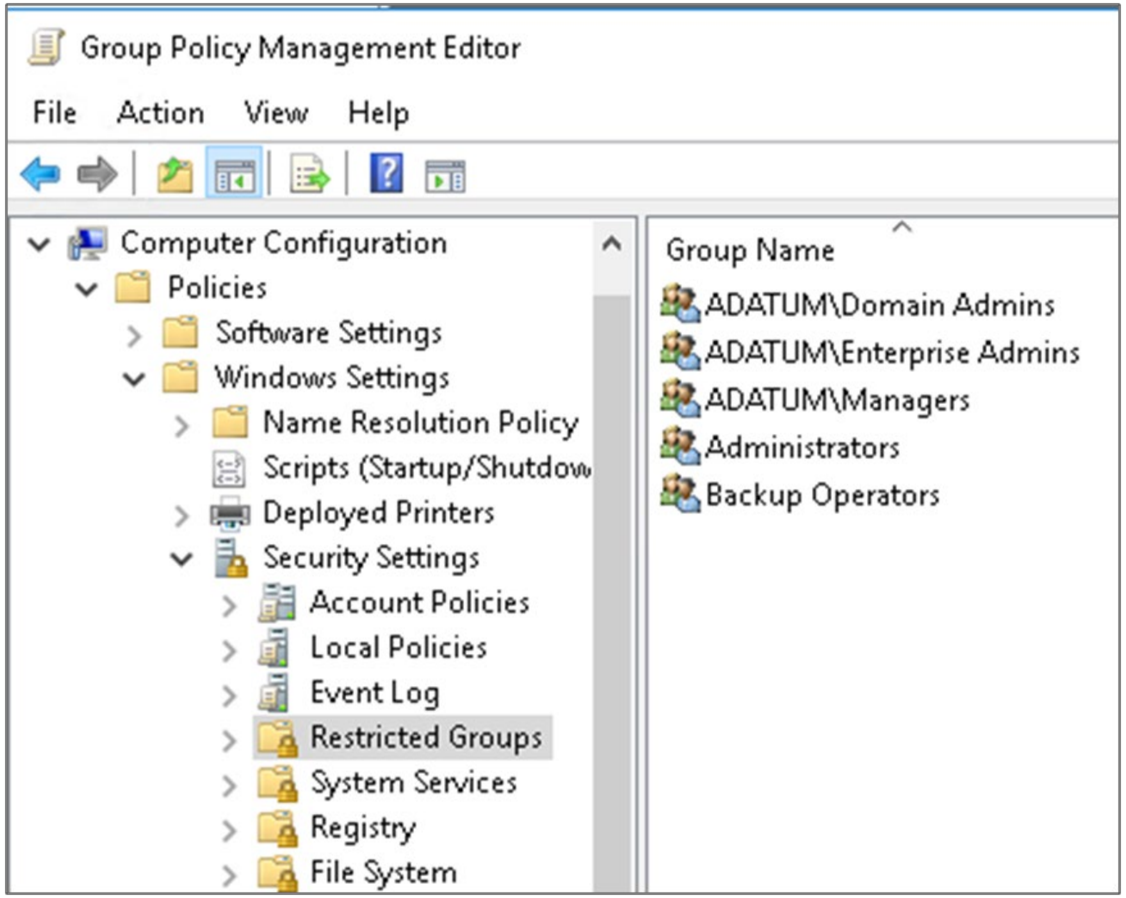
G: Global groups, which collect members based on members' roles, which are members of

DL: Domain-local groups, which provide management such as resource access which are

A: Assigned access to a resource



Managing group membership by using Group Policy



Group Policy Management Editor

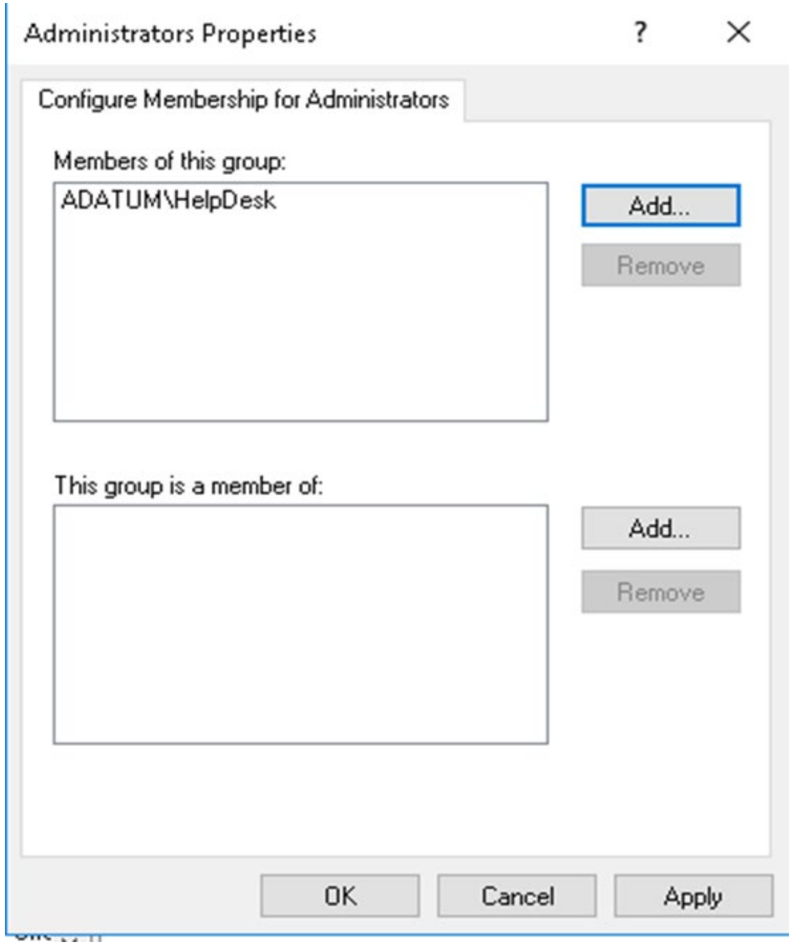
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdow
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System

Group Name
ADATUM\Domain Admins
ADATUM\Enterprise Admins
ADATUM\Managers
Administrators
Backup Operators

- Restricted Groups can simplify group management
- You use it to manage local and AD DS groups

Managing group membership by using Group Policy

- Members can be added to the group and the group can be nested into other groups



Administrators Properties

Configure Membership for Administrators

Members of this group:

ADATUM\HelpDesk

This group is a member of:

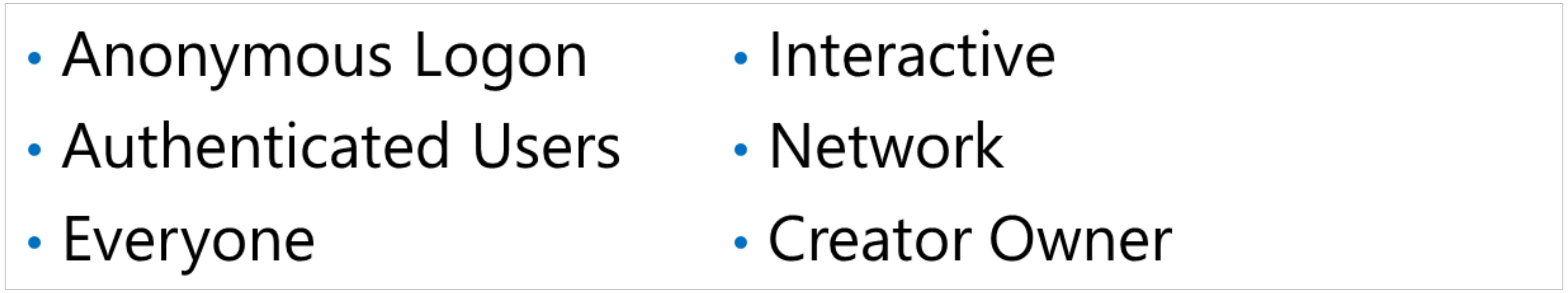
Default groups

- Carefully manage the default groups that provide administrative privileges, because these groups:
- Typically have broader privileges than are necessary for most delegated environments
- Often apply protection to their members

Group	Location
Enterprise Admins	Users container of the forest root domain
Schema Admins	Users container of the forest root domain
Administrators	Built-in container of each domain
Domain Admins	Users container of each domain
Server Operators	Built-in container of each domain
Account Operators	Built-in container of each domain
Backup Operators	Built-in container of each domain
Print Operators	Built-in container of each domain
Cert Publishers	Users container of each domain

Special identities

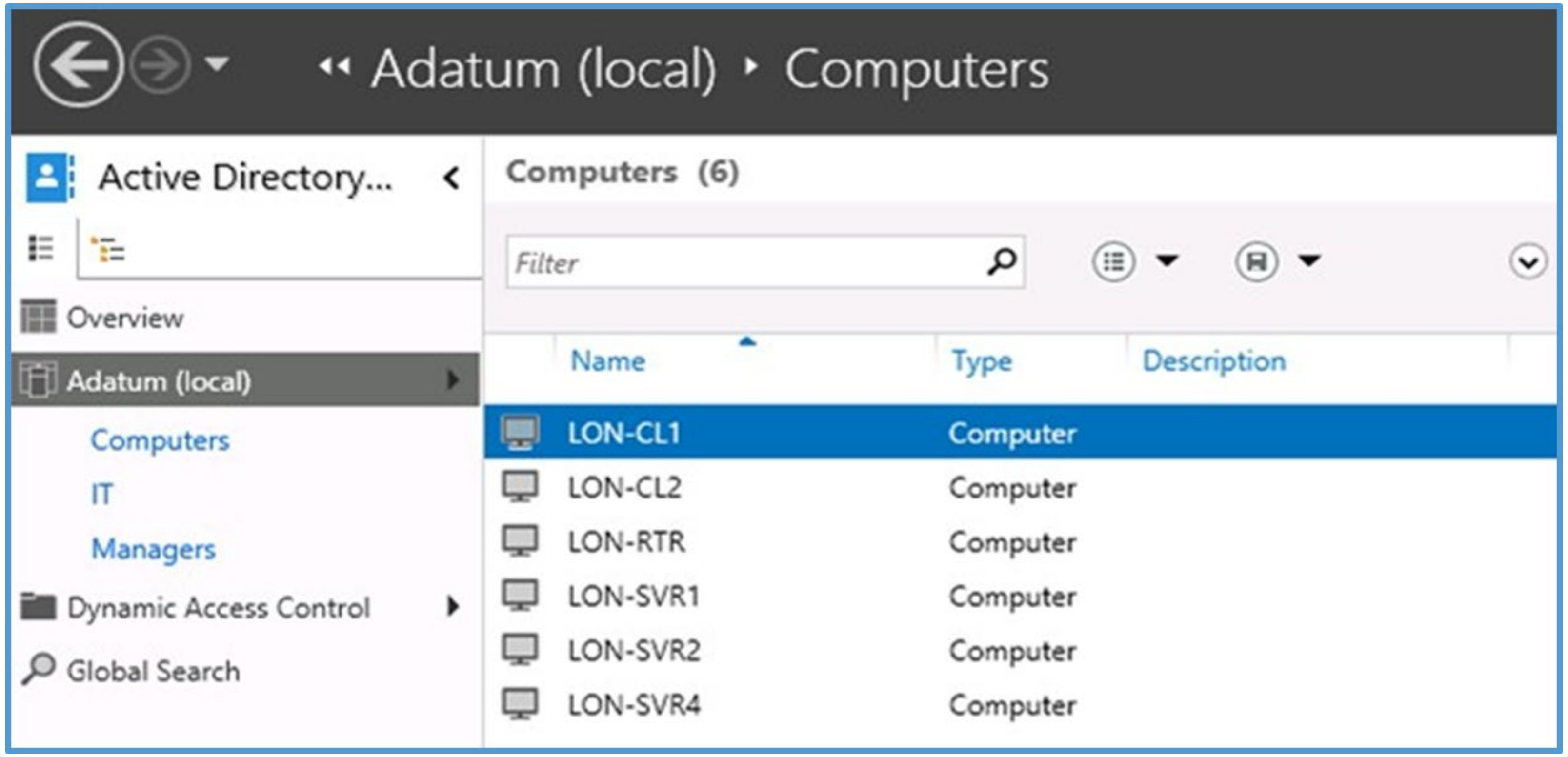
- Special identities:
  - Are groups for which the operating system controls membership
  - Can be used by the Windows Server operating system to provide access to resources based on the type of authentication or connection, not on the user account.
- Important special identities include:



- Anonymous Logon
- Authenticated Users
- Everyone
- Interactive
- Network
- Creator Owner

What is the Computers container?

- Active Directory Administrative Center is opened to the Adatum (local)\Computers container
  - Distinguished Name is CN=Computers,DC=Adatum,DC=com

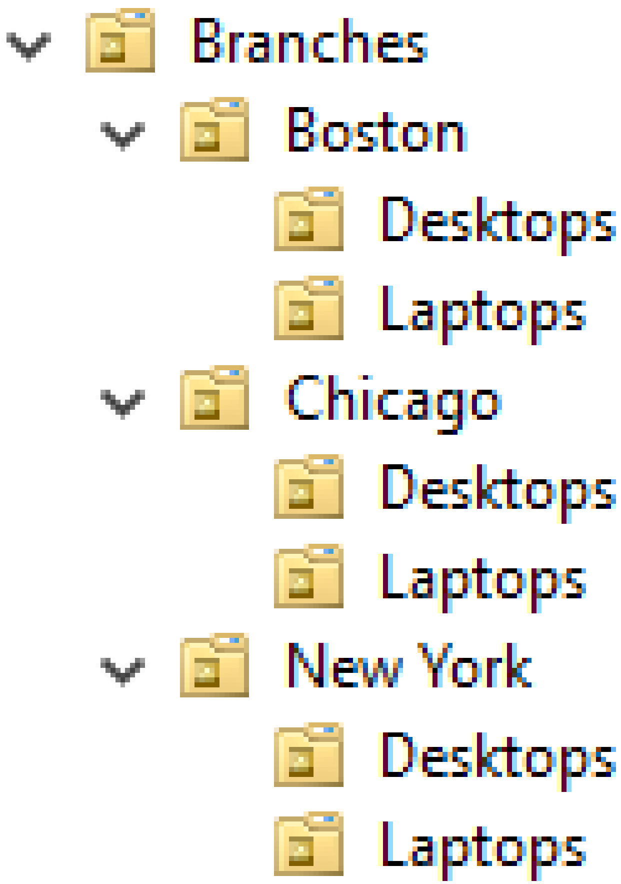


Computers (6)

Name	Type	Description
LON-CL1	Computer	
LON-CL2	Computer	
LON-RTR	Computer	
LON-SVR1	Computer	
LON-SVR2	Computer	
LON-SVR4	Computer	

Specifying the location of computer accounts

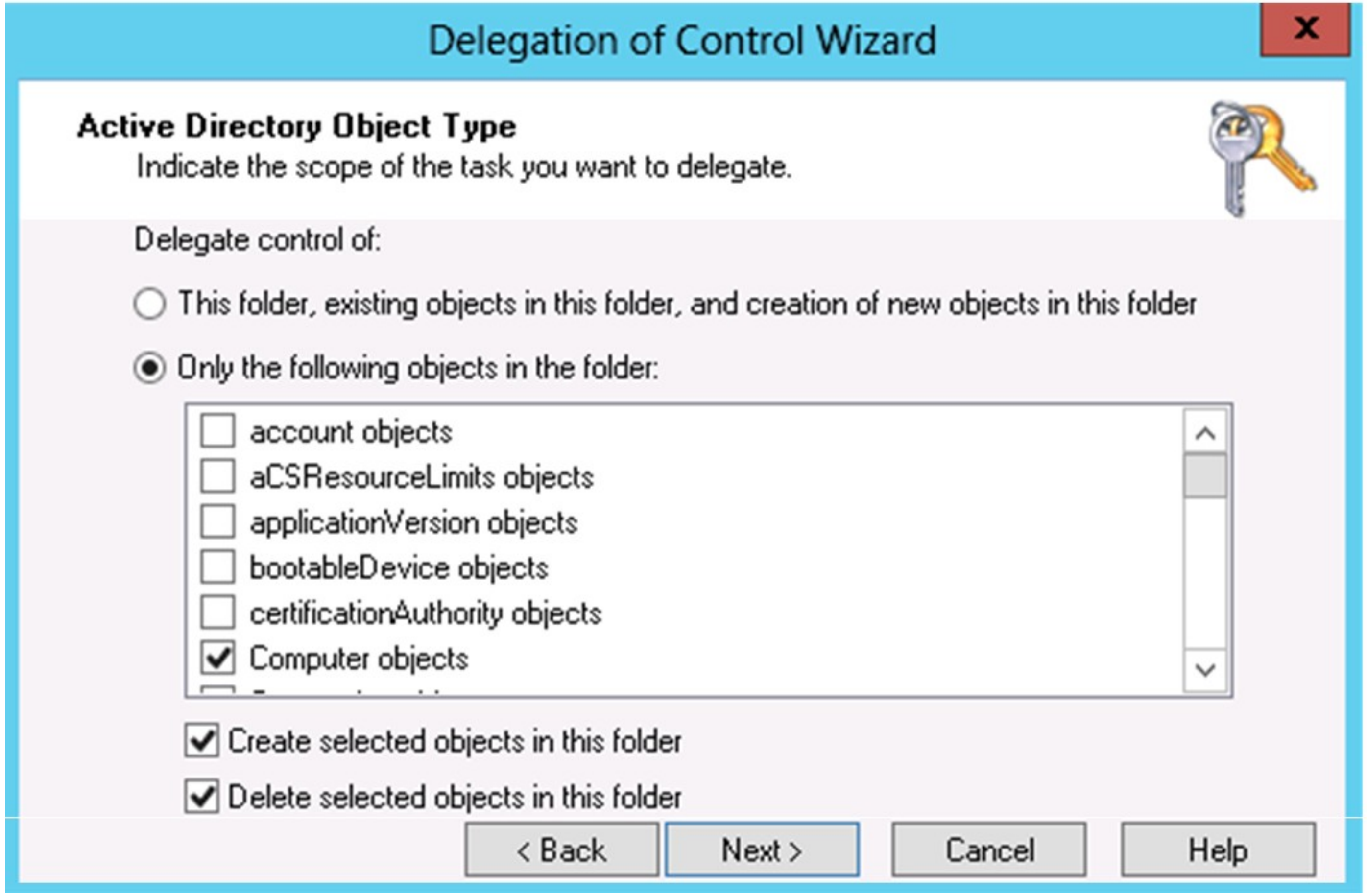
- Best practice is to create OUs for computer objects
  - Servers are typically subdivided by server role
  - Client computers are typically subdivided by region
- Divide OUs:
  - By administration
  - To facilitate configuration with Group Policy



- Branches
  - Boston
    - Desktops
    - Laptops
  - Chicago
    - Desktops
    - Laptops
  - New York
    - Desktops
    - Laptops

Controlling permissions to create computer accounts

- In the Delegation of Control Wizard window, the administrator is creating a custom delegation for computer objects



Delegation of Control Wizard

Active Directory Object Type

Indicate the scope of the task you want to delegate.

Delegate control of:

○ This folder, existing objects in this folder, and creation of new objects in this folder

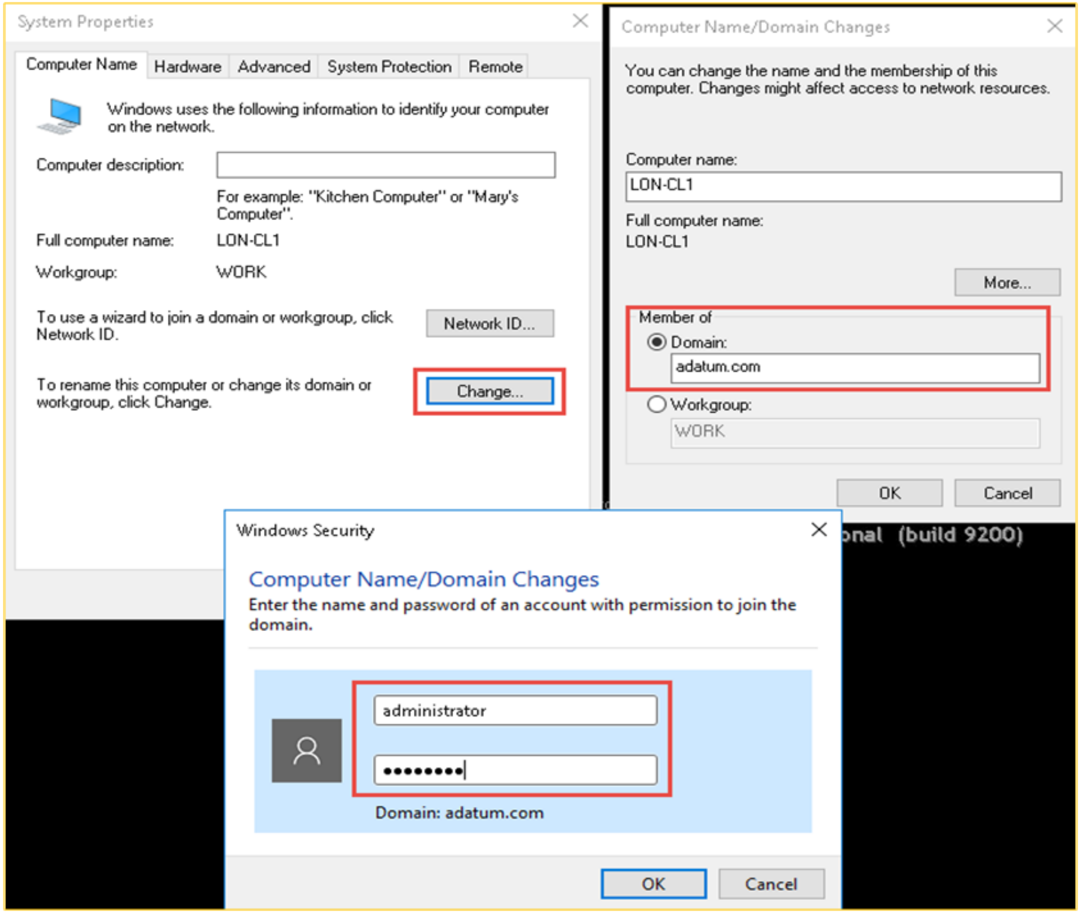
● Only the following objects in the folder:

- □ account objects
- □ aCSResourceLimits objects
- □ applicationVersion objects
- □ bootableDevice objects
- □ certificationAuthority objects
- ☑ Computer objects

☑ Create selected objects in this folder

☑ Delete selected objects in this folder

Joining a computer to a domain



System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: LON-CL1

Workgroup: WORK

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: LON-CL1

Full computer name:
LON-CL1

Member of

● Domain: adatum.com

○ Workgroup: WORK

Windows Security

Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

administrator

••••••••

Domain: adatum.com

Computer accounts and secure channels

- Computers have accounts:
  - SAMAccountName and password
  - Used to create a secure channel between the computer and a domain controller
- Scenarios in which a secure channel might be broken:
  - Reinstalling a computer, even with same name, generates a new SID and password
  - Restoring a computer from an old backup or rolling back a computer to an old snapshot
  - The computer and domain disagreeing about what the password is

Resetting the secure channel

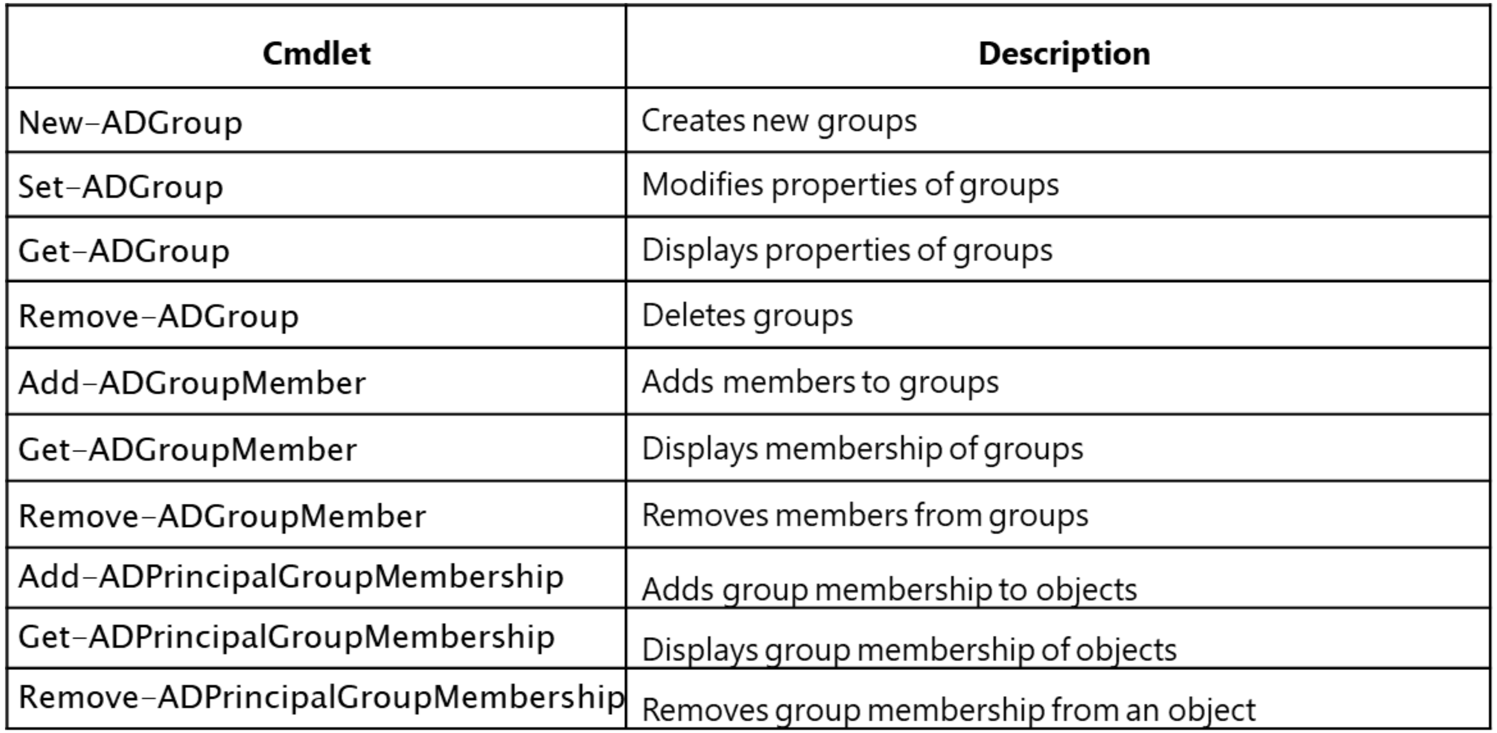
- Do not delete a computer from the domain and then rejoin it; this creates a new account, resulting in a new SID and lost group memberships
- Options for resetting the secure channel:
    - nltest
    - netdom
    - Active Directory Users and Computers
    - Active Directory Administrative Center
    - Windows PowerShell
    - dsmod

Using Windows PowerShell cmdlets to manage user accounts

Cmdlet	Description
New-ADUser	Creates user accounts
Set-ADUser	Modifies properties of user accounts
Remove-ADUser	Deletes user accounts
Set-ADAccountPassword	Resets the password of a user account
Set-ADAccountExpiration	Modifies the expiration date of a user account
Unlock-ADAccount	Unlocks a user account after it has become locked after too many incorrect sign in attempts
Enable-ADAccount	Enables a user account
Disable-ADAccount	Disables a user account

```
New-ADUser "Sterling Smith" –AccountPassword (Read-Host
–AsSecureString "Enter password") -Department IT
```

Using Windows PowerShell cmdlets to manage groups



Cmdlet	Description
New-ADGroup	Creates new groups
Set-ADGroup	Modifies properties of groups
Get-ADGroup	Displays properties of groups
Remove-ADGroup	Deletes groups
Add-ADGroupMember	Adds members to groups
Get-ADGroupMember	Displays membership of groups
Remove-ADGroupMember	Removes members from groups
Add-ADPrincipalGroupMembership	Adds group membership to objects
Get-ADPrincipalGroupMembership	Displays group membership of objects
Remove-ADPrincipalGroupMembership	Removes group membership from an object

```
New-ADGroup -Name "CustomerManagement" -Path
"ou=managers,dc=adatum,dc=com" -GroupScope Global
-GroupCategory Security
```

```
Add-ADGroupMember -Name “CustomerManagement” -Members "Joe"
```

Using Windows PowerShell cmdlets to manage computer accounts

Cmdlet	Description
New-ADComputer	Creates new computer accounts
Set-ADComputer	Modifies properties of computer accounts
Get-ADComputer	Displays properties of computer accounts
Remove-ADComputer	Deletes computer accounts
Test-ComputerSecureChannel	Verifies or repairs the trust relationship between a computer and the domain
Reset- ComputerMachinePassword	Resets the password for a computer account

```
New-ADComputer –Name “LON-SVR8” -Path
"ou=marketing,dc=adatum,dc=com" -Enabled $true
```

```
Test-ComputerSecureChannel -Repair
```

Using Windows PowerShell cmdlets to manage OUs

Cmdlet	Description
New-ADOrganizationalUnit	Creates OUs
Set-ADOrganizationalUnit	Modifies properties of OUs
Get-ADOrganizationalUnit	Views properties of OUs
Remove-ADOrganizationalUnit	Deletes OUs

```
New-ADOrganizationalUnit -Name “Sales”
-Path "ou=marketing,dc=adatum,dc=com"
-ProtectedFromAccidentalDeletion $true
```

What are bulk operations?

- A bulk operation is a single action that changes multiple objects
- Sample bulk operations:
  - Create user accounts based on data in a spreadsheet
  - Disable all accounts not used in six months
  - Rename the department for many users
- You can perform bulk operations by using:
  - Graphical tools
  - Command-line tools
  - Scripts

Planning OUs

Location-based strategy	- Static - Delegation can be complicated
Organization-based strategy	- Not static - Easy to categorize
Resource-based strategy	- Not static - Easy to delegate administration
Multitenancy-based strategy	- Static - Easy to delegate administration - Easy to include and separate new tenants
Hybrid strategy	

OU hierarchy considerations

Align OU strategy to administrative requirements, not the organizational chart, because organizational charts are more subject to change than your IT administration model

AD DS inheritance behavior can simplify Group Policy administration because it allows group polices to be set on an OU and flow down to lower OUs in the hierarchy

Plan to accommodate changes in the IT administration model

Considerations for using OUs

- OUs can be created using AD DS graphical tools or command-line tools
- New OUs are protected from accidental deletion by default
- When objects are moved between OUs:
  - Directly assigned permissions remain in place
  - Inherited permissions will change
- Appropriate permissions are required to move objects between OUs

AD DS permissions

- Users receive their token (list of SIDs) during sign in
- Objects have a security descriptor that describes:
  - Who (SID) has been granted or denied access
  - Which permissions (Read, Write, Create or Delete child)
  - What kind of objects
  - Which sublevels
- When users browse the Active Directory structure, their token is compared to the security descriptor to evaluate their access rights

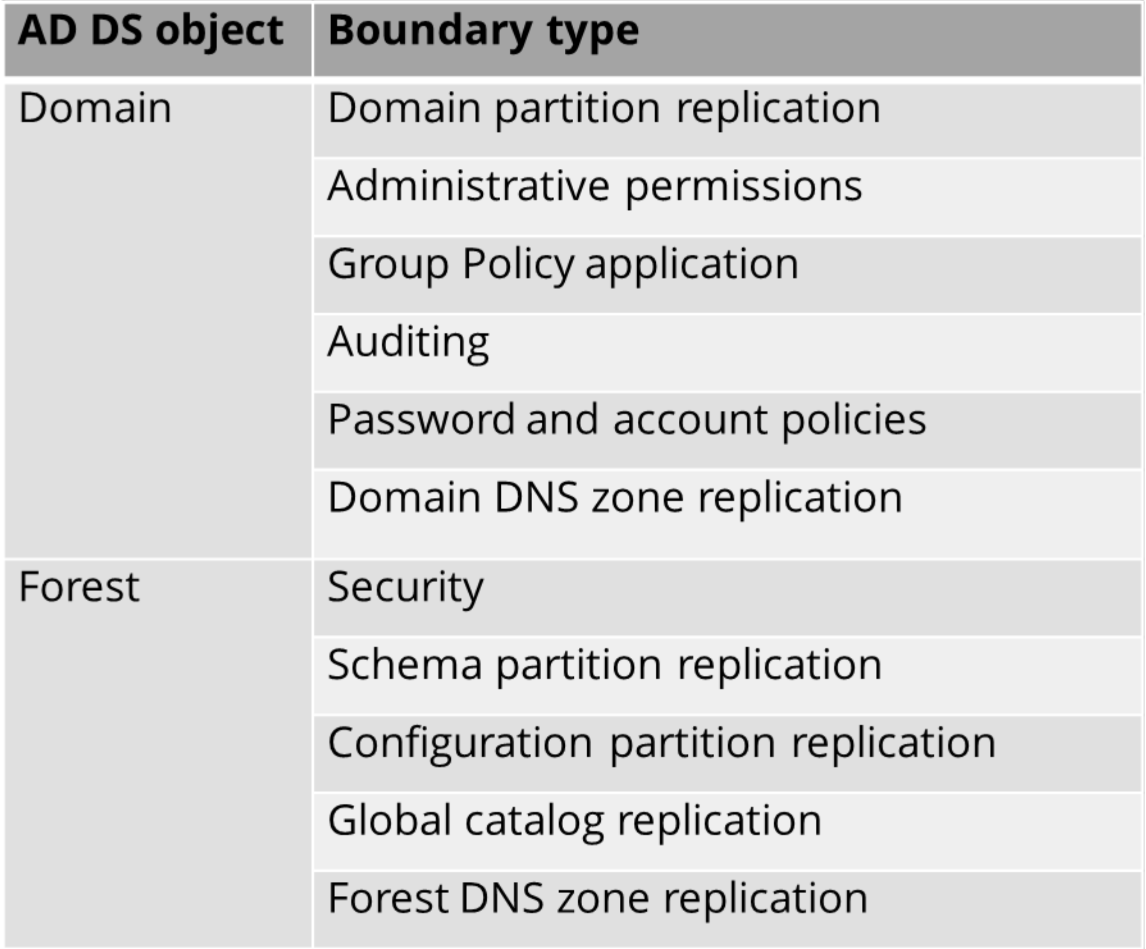
Delegating AD DS permissions

- Permissions on AD DS objects can be granted to users or groups
- Permission models are usually object-based or role-based
- The Delegation of Control Wizard can simplify assigning common administrative tasks
- The OU advanced security properties allow you to grant granular permissions

Unit 03

Advanced AD DS infrastructure management

Overview of domain and forest boundaries in an AD DS structure



AD DS object	Boundary type
Domain	Domain partition replication
	Administrative permissions
	Group Policy application
	Auditing
	Password and account policies
	Domain DNS zone replication
Forest	Security
	Schema partition replication
	Configuration partition replication
	Global catalog replication
	Forest DNS zone replication

Why implement multiple domains?

- Organizations might choose to deploy multiple domains to meet:
  - Domain replication requirements
  - DNS namespace requirements
  - Distributed administration requirements
  - Forest administrative group security requirements
  - Resource domain requirements

Why implement multiple forests?

- Organizations might choose to deploy multiple forests to meet:
- Security isolation requirements:
  - PAM in Windows Server 2016 AD DS uses a separate bastion forest to isolate privileged accounts in order to protect against credential theft techniques
- Incompatible schema requirements
- Multinational requirements
- Extranet security requirements
- Business merger or divestiture

Deploying a domain controller in Azure IaaS

- Scenarios in which you might deploy AD DS on an Azure virtual machine:
  - Disaster recovery
  - Geo-distributed domain controllers
  - Isolated applications
- Considerations during deployment include:
  - Network topology
  - Site topology
  - Service healing
  - IP addressing
  - DNS
  - Hard disk read/write caching

Managing objects in complex AD DS deployments

- Potential issues include:
  - User and group management
  - User self-service
  - Certificate management
  - Identity syncing
- MIM 2016 provides:
  - Cloud-ready identities for Azure Active Directory
  - Powerful user self-service features with multi-factor authentication
  - PAM

AD DS domain functional levels

- New functionality requires that domain controllers are running a particular version of the Windows operating system:
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016

- You cannot raise the functional level while domain controllers are running previous Windows Server versions

- You cannot add domain controllers that are running previous Windows Server versions after raising the functional level

Deploying new AD DS domains

- **Forest root domain:**
  - Is automatically created with a new forest
  - Is the base of an AD DS infrastructure
  - Can be the only domain in an AD DS deployment

- **Child domain:**
  - Is a child of a parent domain
  - Shares the same namespace with the parent domain

- **Tree domain:**
  - Creates a new domain tree and a new namespace
  - Are commonly used in merger and acquisition scenarios

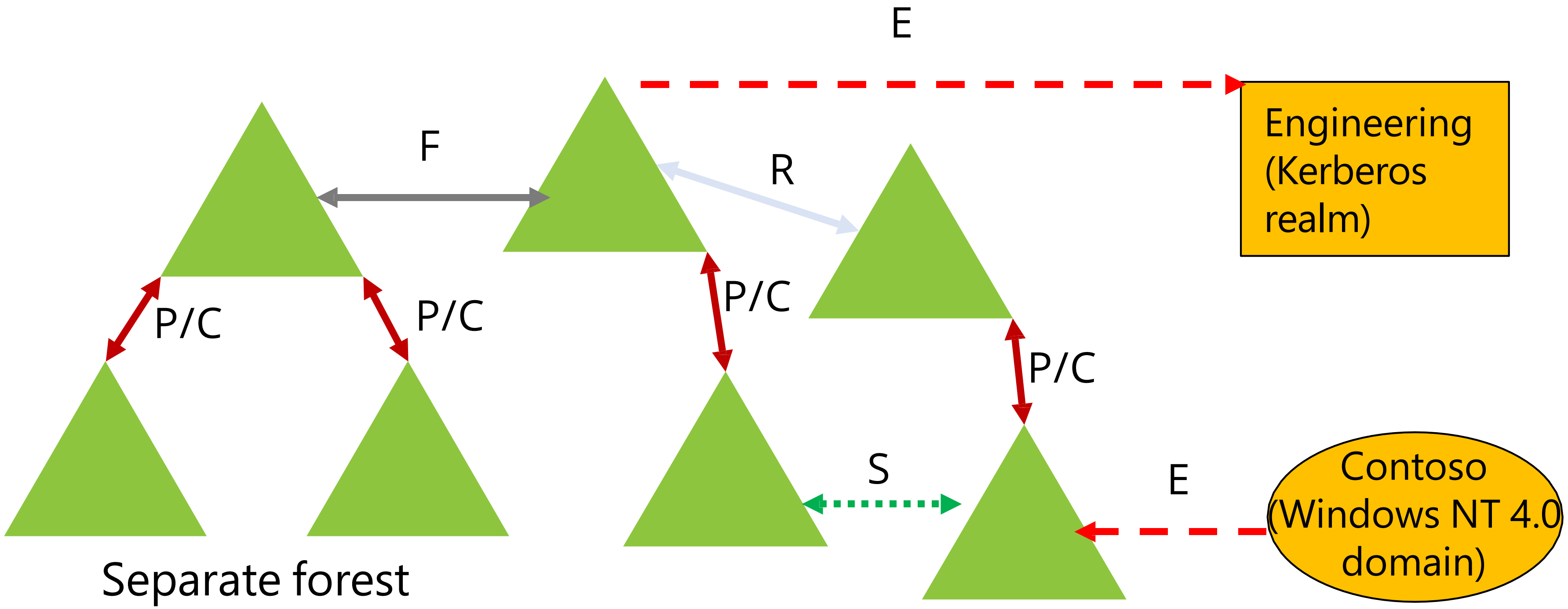
Considerations for implementing complex AD DS environments

- DNS considerations:
  - Centralized versus decentralized
  - Verify the DNS client configuration and name resolution
  - Optimize DNS name resolution:
    - Conditional forwarders and stub zones
    - DNS name devolution and DNS suffix search order
  - Deploy a GlobalNames zone
  - Use Active Directory-integrated zones
  - Extending AD DS to Azure

Considerations for implementing complex AD DS environments

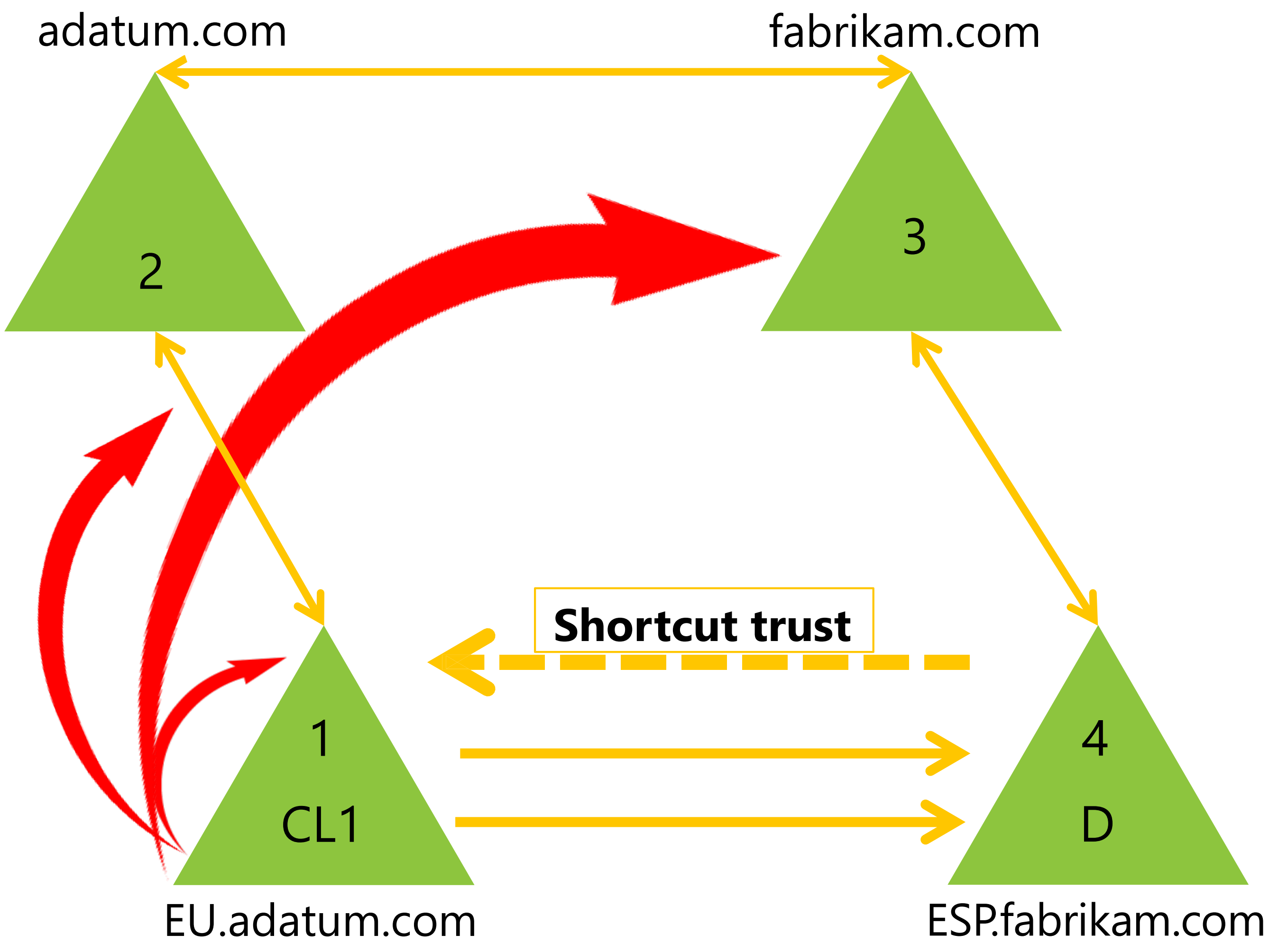
- UPN considerations:
  - UPN suffixes
  - Global catalog
  - Federated authentication scenarios

Overview of different AD DS trust types



Trust type	Transitive?	Color
P/C - Parent-child	Yes	Purple
R - Tree root	Yes	Black
E - External (domain or Kerberos realm)	No	Red/Dashed
S - Shortcut	Yes	Green/Dotted
F - Forest (complete or selective)	Yes	Blue

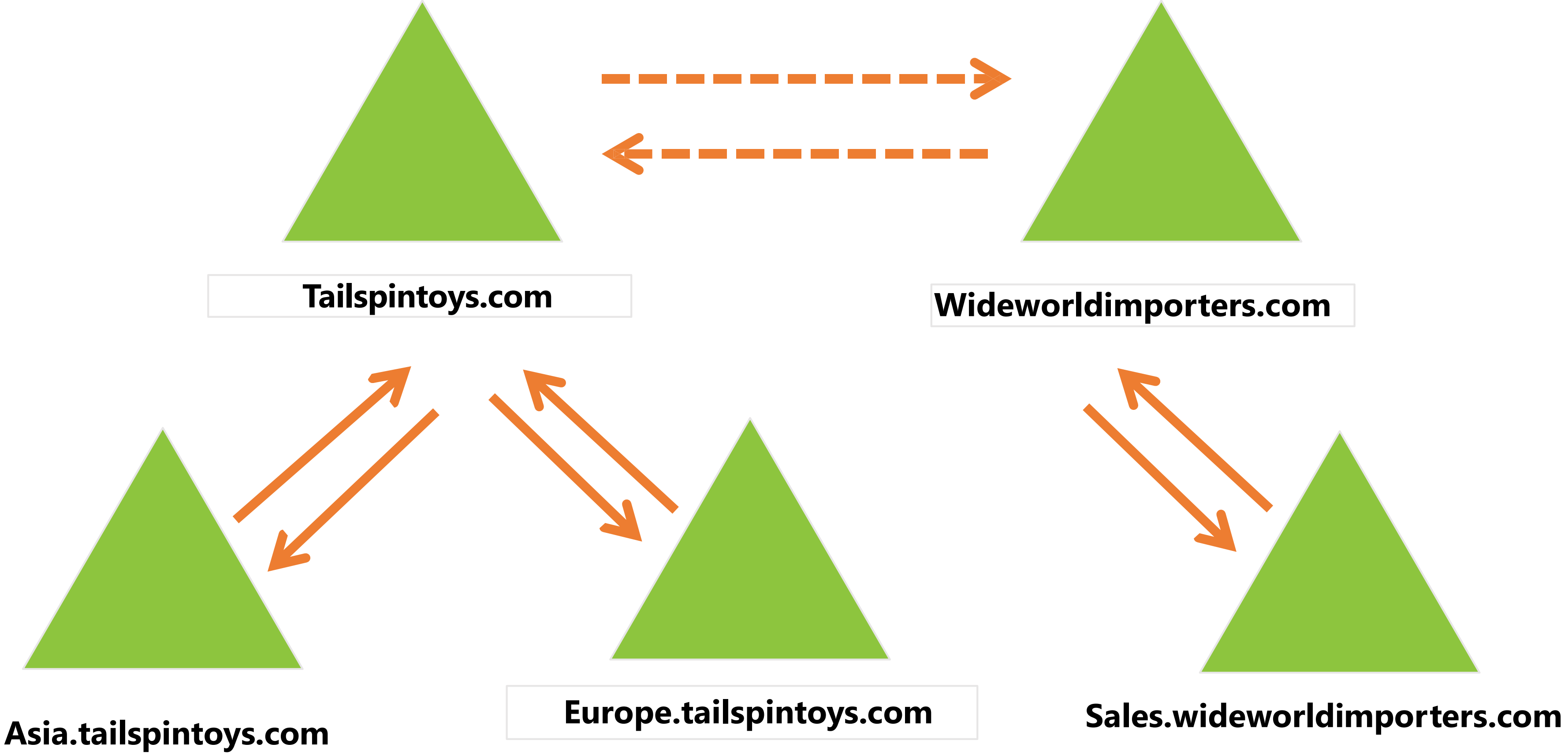
How trusts work in a forest



Client computer CL1 requests access to a file on file server D

How trusts work between forests

A forest trust is a one-way or two-way trust relationship between the forest root domains of two forests



Configuring advanced AD DS trust settings

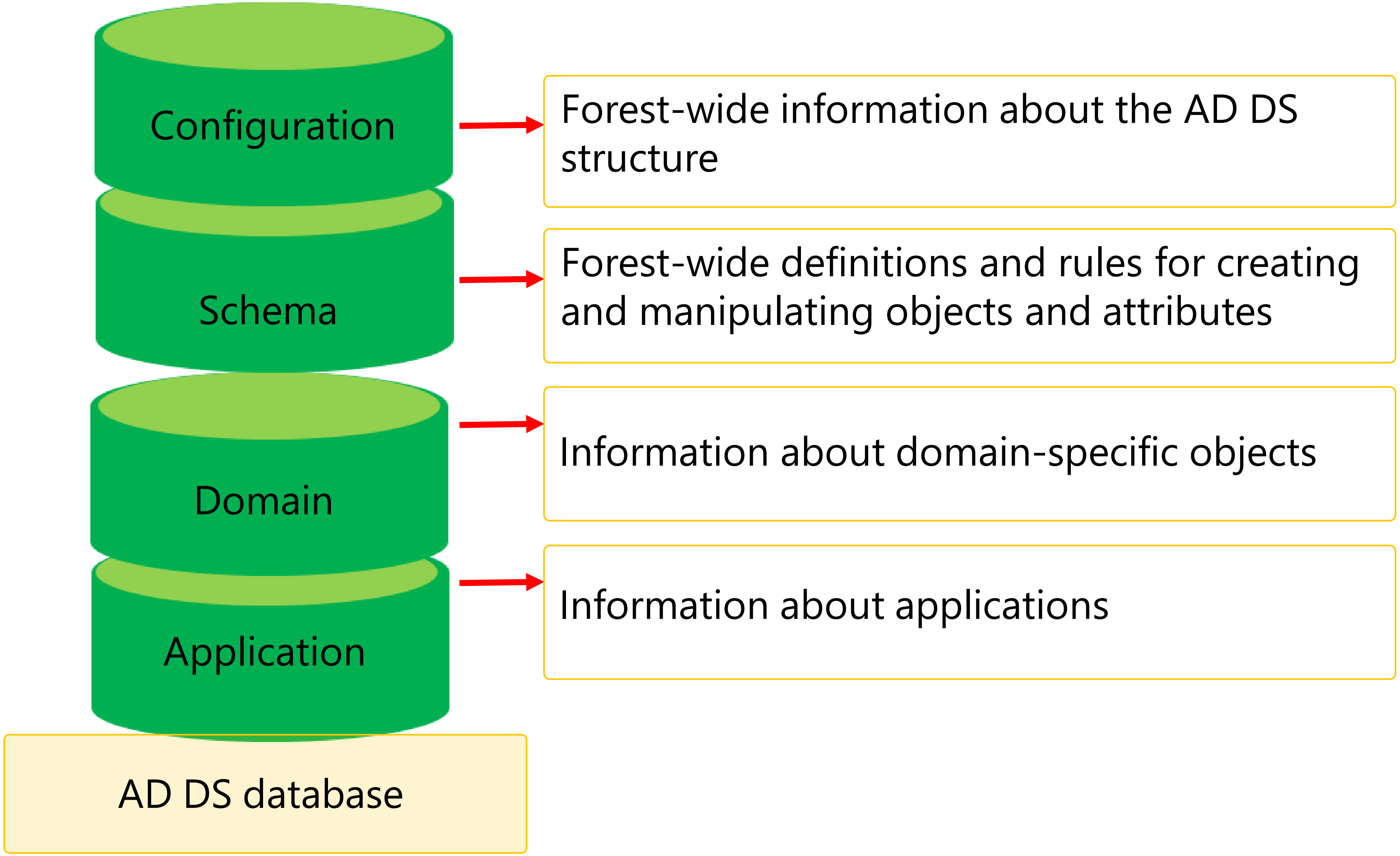
- Security considerations in forest trusts include:
- SID filtering
- Selective authentication
- Name suffix routing
- An incorrectly configured trust can allow unauthorized access to resources

Unit 04

Implementing and administering AD DS sites and replication

elev8 LEARNING SOLUTIONS

What are AD DS partitions?



Configuration → Forest-wide information about the AD DS structure

Schema → Forest-wide definitions and rules for creating and manipulating objects and attributes

Domain → Information about domain-specific objects

Application → Information about applications

AD DS database

Characteristics of AD DS replication

- Multi-master replication ensures:
  - Accuracy (integrity)
  - Consistency (convergence)
  - Performance (keeping replication traffic to a reasonable level)

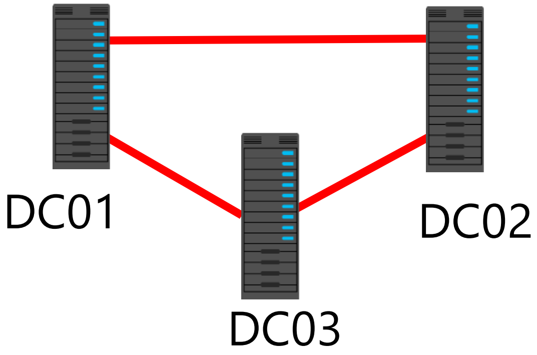
Characteristics of AD DS replication

- Multi-master replication
- Pull replication
- Store-and-forward replication
- Partitions
- Automatic generation of an efficient, robust replication topology
- Attribute-level and multivalue replication
- Distinct control of intersite replication
- Collision detection and management

How AD DS replication works within a site

Intrasite replication uses:

- Connection objects for inbound replication to a domain controller
- Knowledge Consistency Checker to automatically create a topology that is efficient (maximum three-hop) and robust
- (two-way)
- Notifications in which the domain controller tells its downstream partners that a change is available



How AD DS replication works within a site

- Polling, in which the domain controller checks with its upstream partners for changes:
  - Downstream domain controller directory replication agent replicates changes
  - Changes to all partitions held by
  - both domain controllers are replicated

Resolving replication conflicts

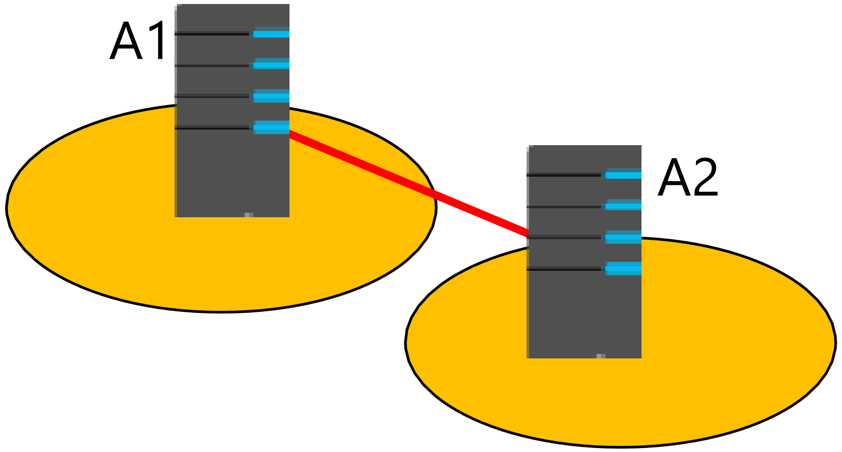
- In multi-master replication models, replication conflicts arise when:
  - The same attribute is changed on two domain controllers simultaneously
  - An object is moved or added to a deleted container on another domain controller
  - Two objects with the same relative distinguished name are added to the same container on two different domain controllers
- To resolve replication conflicts, AD DS uses:
  - Version number
  - Time stamp
  - Server GUID

How SYSVOL replication works

- SYSVOL contains logon scripts, Group Policy templates, and GPOs with their content
- SYSVOL replication can take place by using:
  - FRS, which is primarily used in Windows Server 2003 and older domain
  - structures
  - DFS Replication, which is used in Windows Server 2008 and newer domains
- To migrate SYSVOL replication from FRS to DFS Replication:
  - The domain functional level must be at least Windows Server 2008
  - Use the **Dfsrmig.exe** tool to perform the migration

What are AD DS sites?

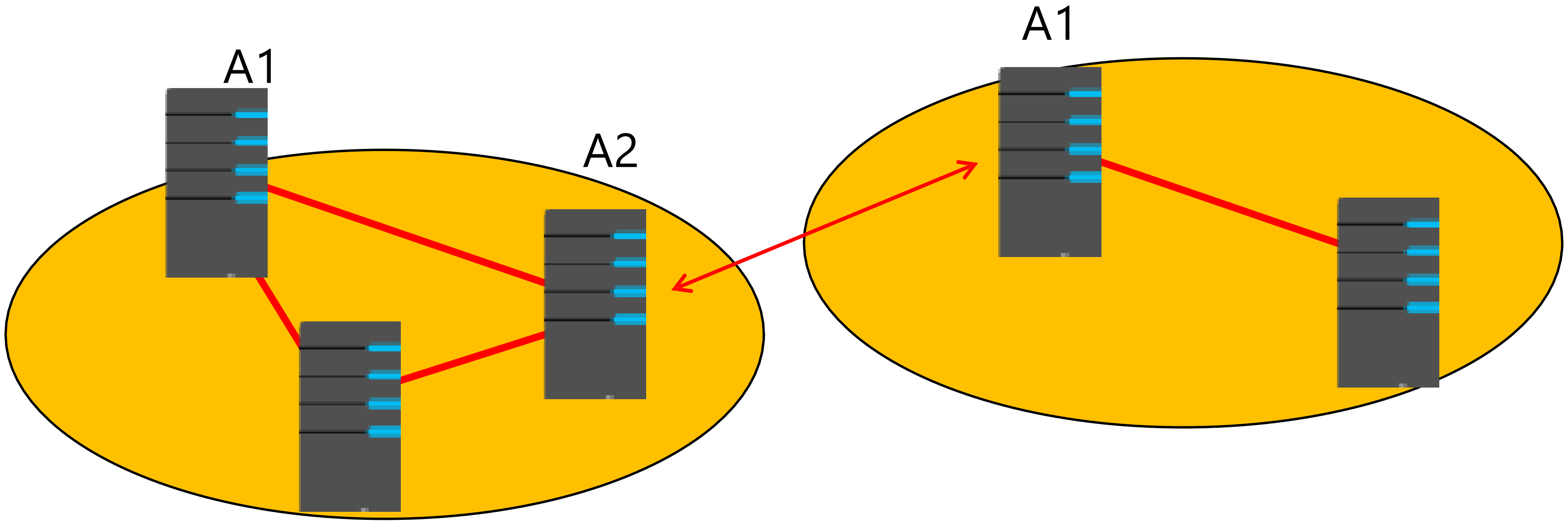
- Sites identify network locations with fast, reliable network connections
- Sites are associated with subnet objects
- Sites are used to manage:
  - Replication when domain controllers are separated by slow, expensive links
  - Service localization:
    - Domain controller authentication
    - AD DS–aware (site-aware) services or aplications



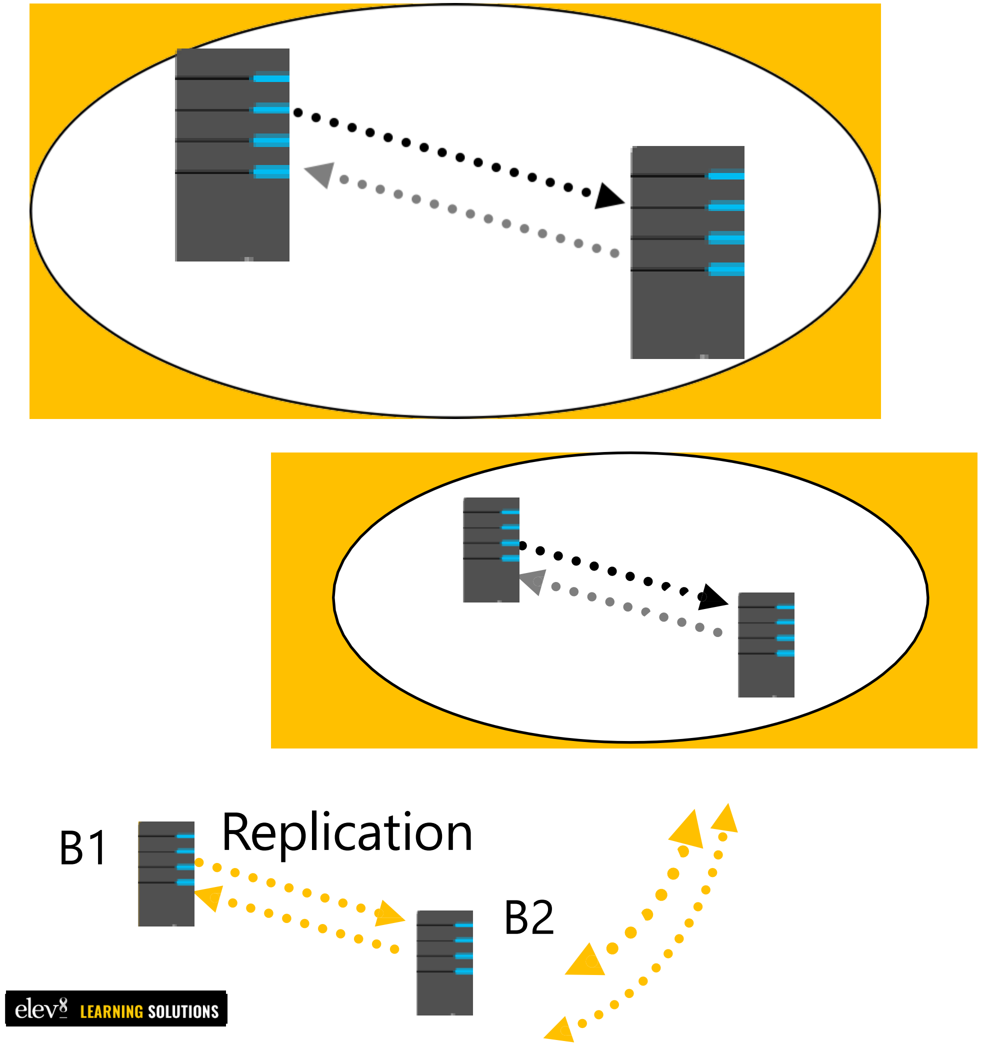
Why implement additional sites?

Create additional sites when:

- A slow link separates a part of the network
- A part of the network has enough users to warrant hosting domain controllers or other services in that location
- You want to control service localization
- You want to control replication between domain controllers



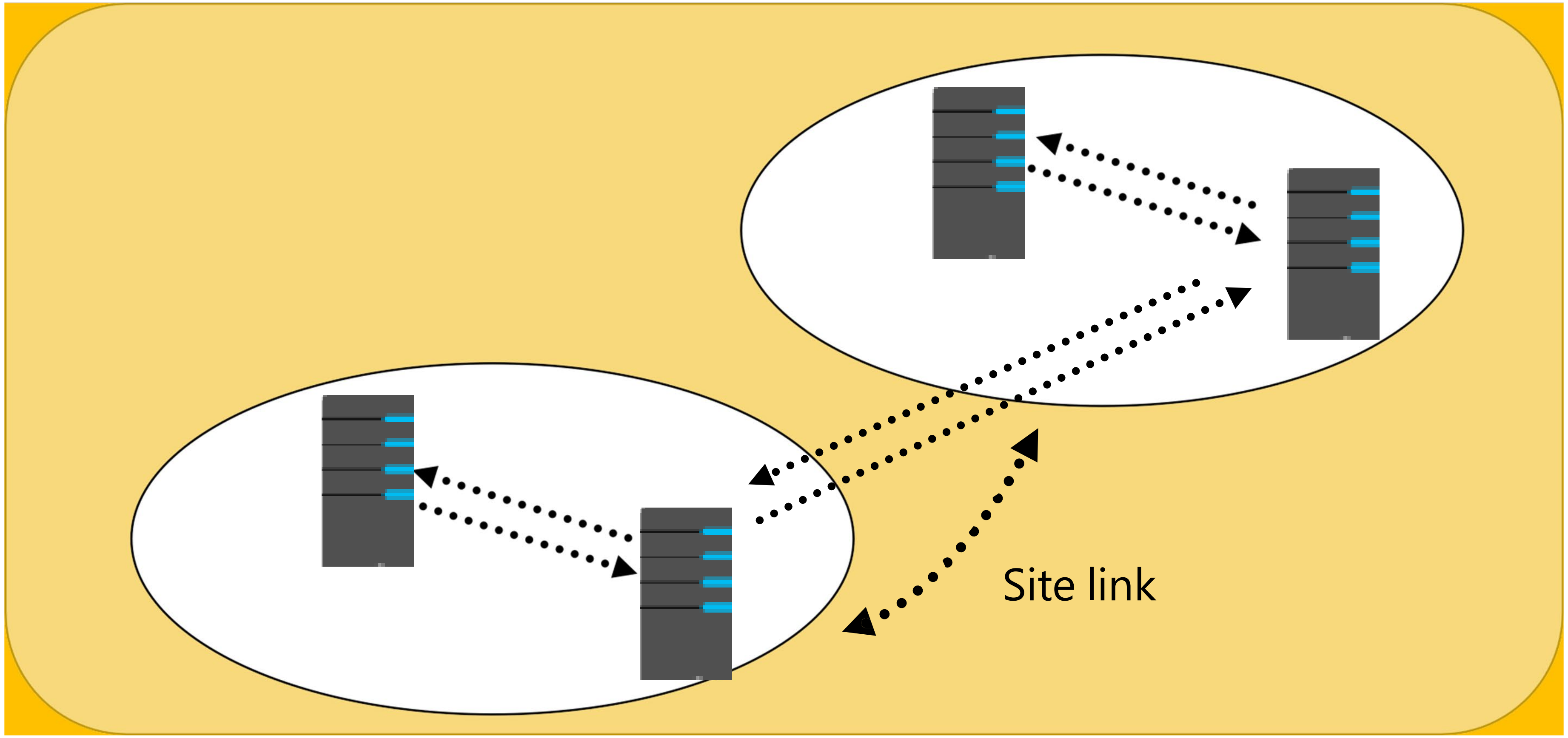
How replication works between sites



- Replication within sites:
  - Assumes fast, inexpensive, and highly reliable network links
  - Does not compress traffic
  - Uses a change notification mechanism
- Replication between sites:
  - Assumes higher cost, limited bandwidth, and unreliable network links
  - Has the ability to compress replication
  - Occurs on a configured schedule

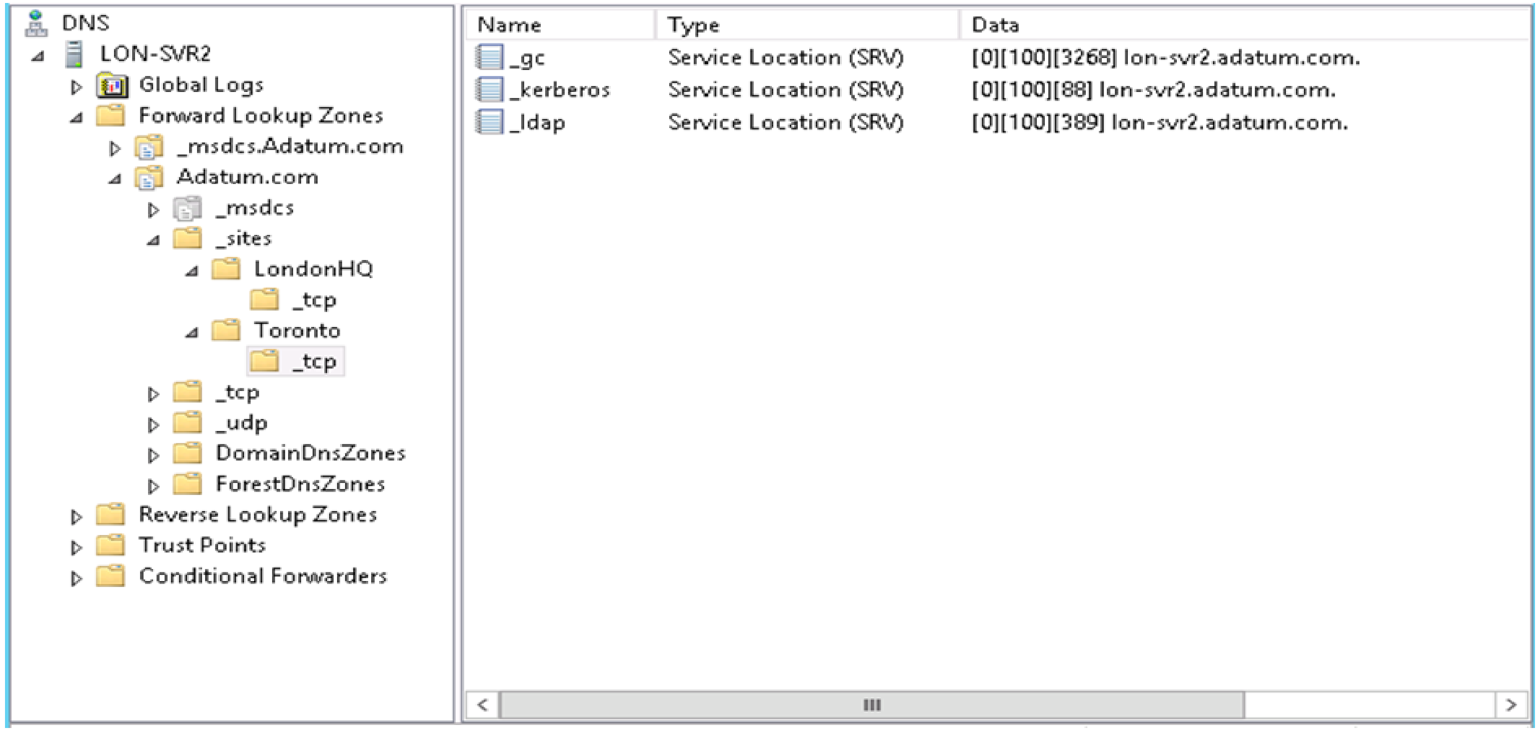
What is the ISTG?

ISTG defines the replication between AD DS sites on a network



Overview of SRV records

- Domain controllers register SRV records as follows:
  - **_tcp.adatum.com**: All domain controllers in the domain
  - **_tcp.*sitename*._sites.adatum.com**: All services in a specific site
- Clients query DNS to locate services in specific sites



```
DNS
  LON-SVR2
    Global Logs
    Forward Lookup Zones
      _msdcs.Adatum.com
      Adatum.com
        _msdcs
        _sites
          LondonHQ
            _tcp
          Toronto
            _tcp
        _tcp
        _udp
        DomainDnsZones
        ForestDnsZones
    Reverse Lookup Zones
    Trust Points
    Conditional Forwarders
```

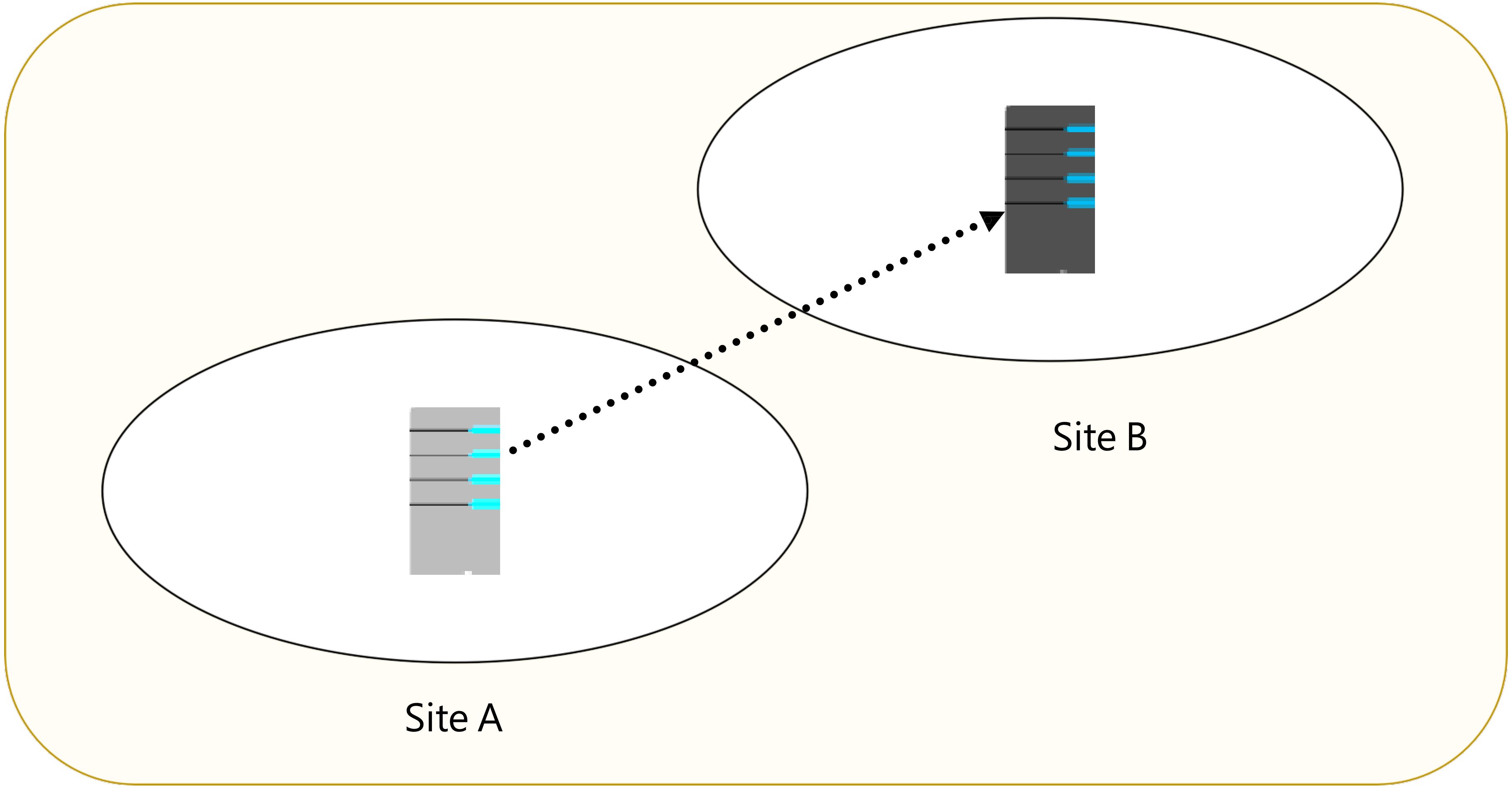
Name	Type	Data
_gc	Service Location (SRV)	[0][100][3268] lon-svr2.adatum.com.
_kerberos	Service Location (SRV)	[0][100][88] lon-svr2.adatum.com.
_ldap	Service Location (SRV)	[0][100][389] lon-svr2.adatum.com.

How client computers locate domain controllers within sites

The process for locating a domain controller is as follows:

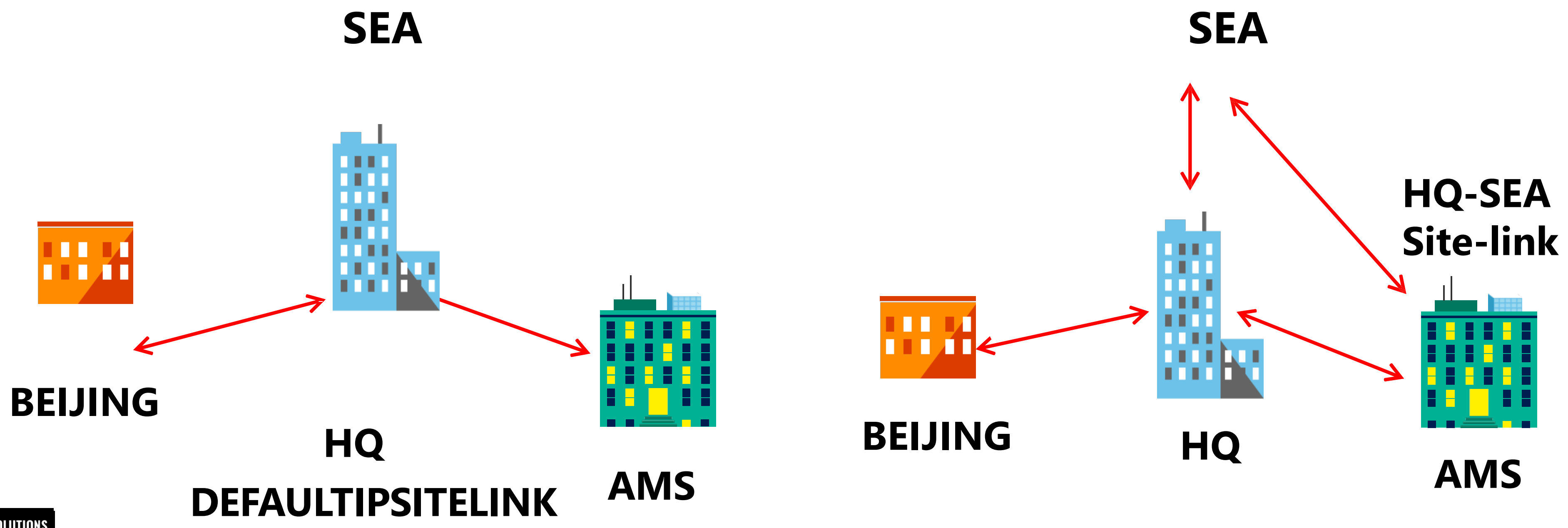
1. The new client queries for all domain controllers in the domain
2. The client attempts an LDAP ping to find all domain controllers
3. First domain controller responds
4. The client queries for all domain controllers in the site
5. The client attempts an LDAP ping to find all domain controllers in the site
6. The client forms an affinity

Moving domain controllers between sites



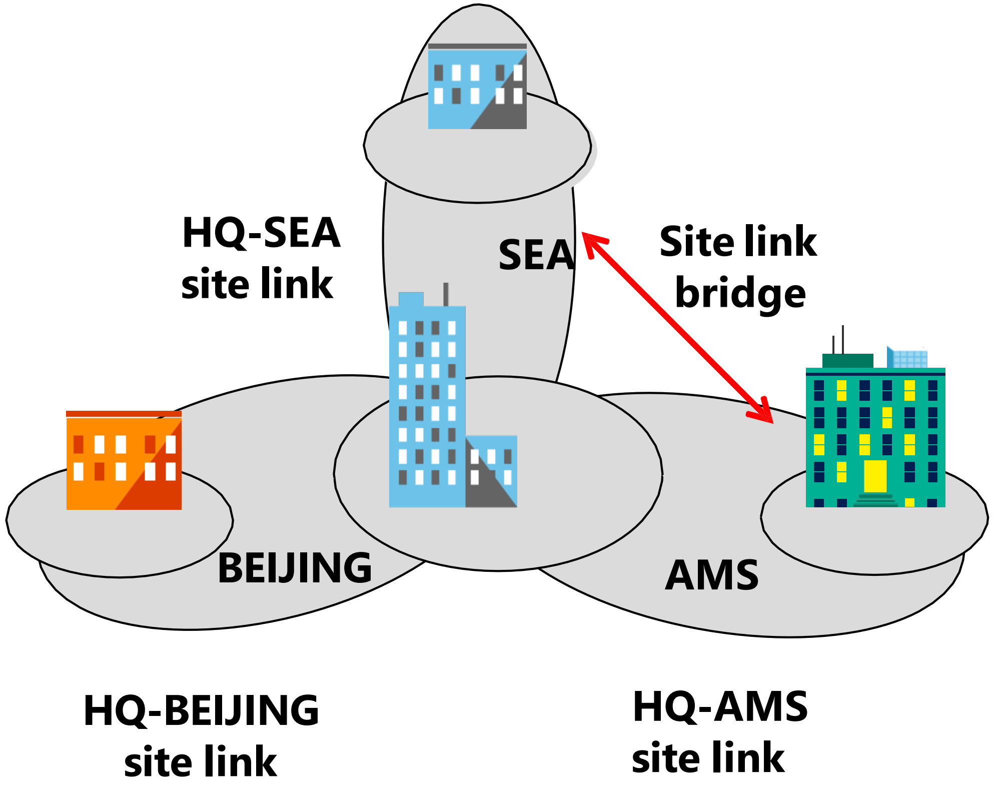
What are AD DS site links?

- Site links contain sites:
  - Within a site link, a connection object can be created between any two domain controllers
  - The default site link, DEFAULTIPSITELINK, is not always appropriate
  - with your network topology



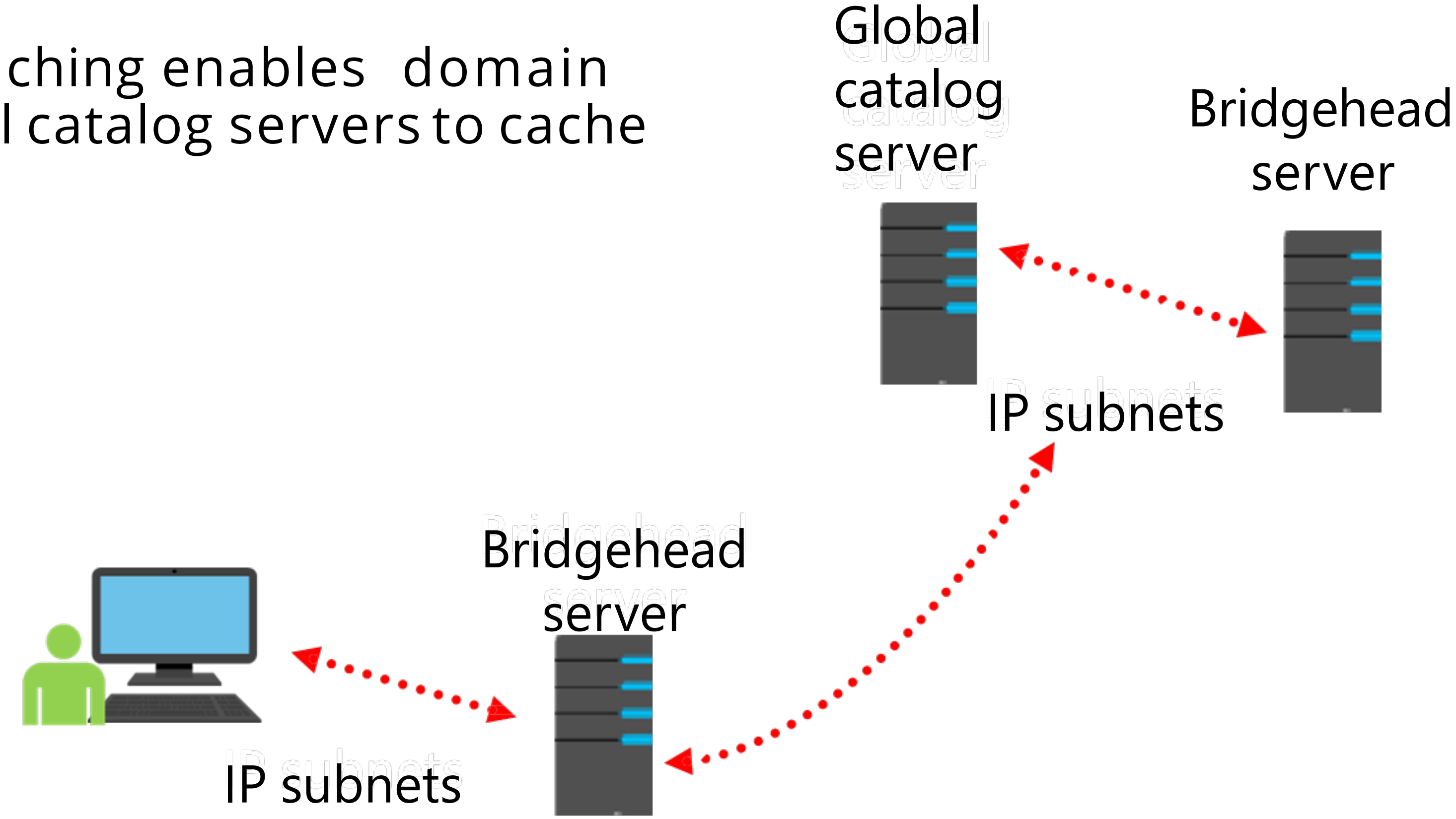
What is site link bridging?

- By default, automatic site link bridging:
  - Enables ISTG to create connection objects between site links
  - Allows disabling of transitivity in the properties of the IP transport
- Site link bridges:
  - Enable you to create transitive site links manually
  - Are useful only when transitivity is disabled



What is universal group membership caching?

Universal group membership caching enables domain controllers in a site with no global catalog servers to cache universal group membership



Managing intersite replication

- Site link costs:
  - Replication uses connections with the lowest cost
- Replication:
  - During polling, the downstream bridgehead polls its upstream partners:
    - Default is 3 hours
    - Minimum is 15 minutes
    - Recommended is 15 minutes
  - Replication schedules:
    - 24 hours a day
    - Can be scheduled

Tools for monitoring and managing replication

- **Repadmin.exe**
- **Dcdiag.exe**
- Monitor replication with Operations Manager
- Use Windows PowerShell cmdlets

Unit 05

Implementing Group Policy

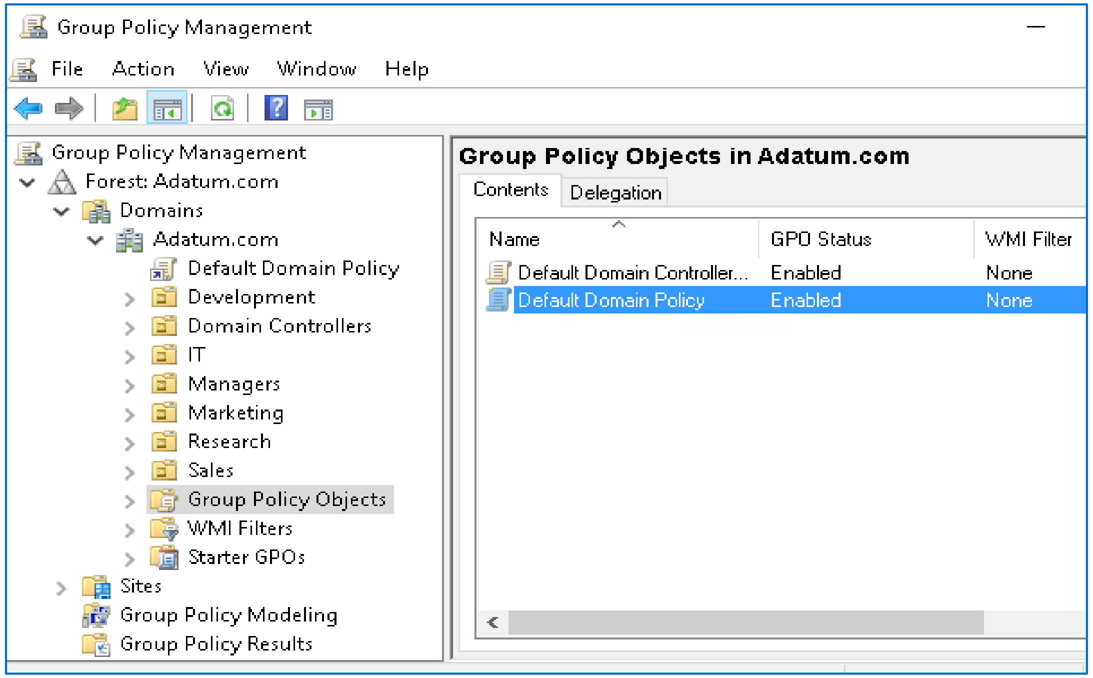
elev8 LEARNING SOLUTIONS

What is configuration management?

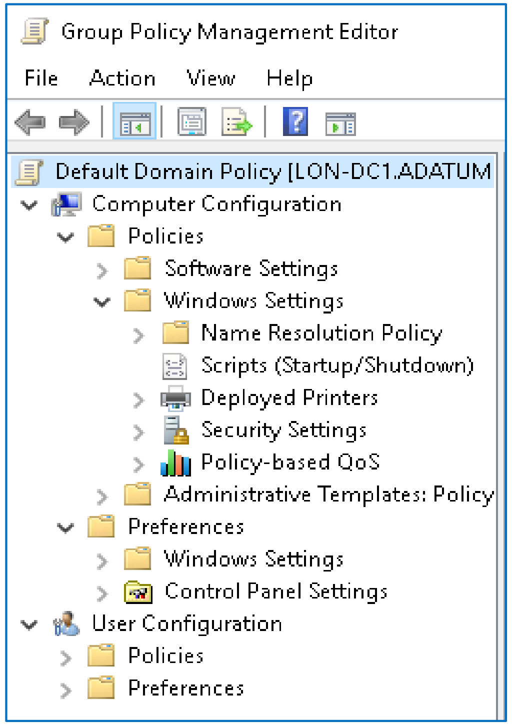
Configuration management is a centralized approach to applying one or more changes to more than one user or computer

- The key elements of configuration management are:
  - Setting
  - Scope
  - Application

Overview of Group Policy tools and consoles



Name	GPO Status	WMI Filter
Default Domain Controller...	Enabled	None
Default Domain Policy	Enabled	None



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

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

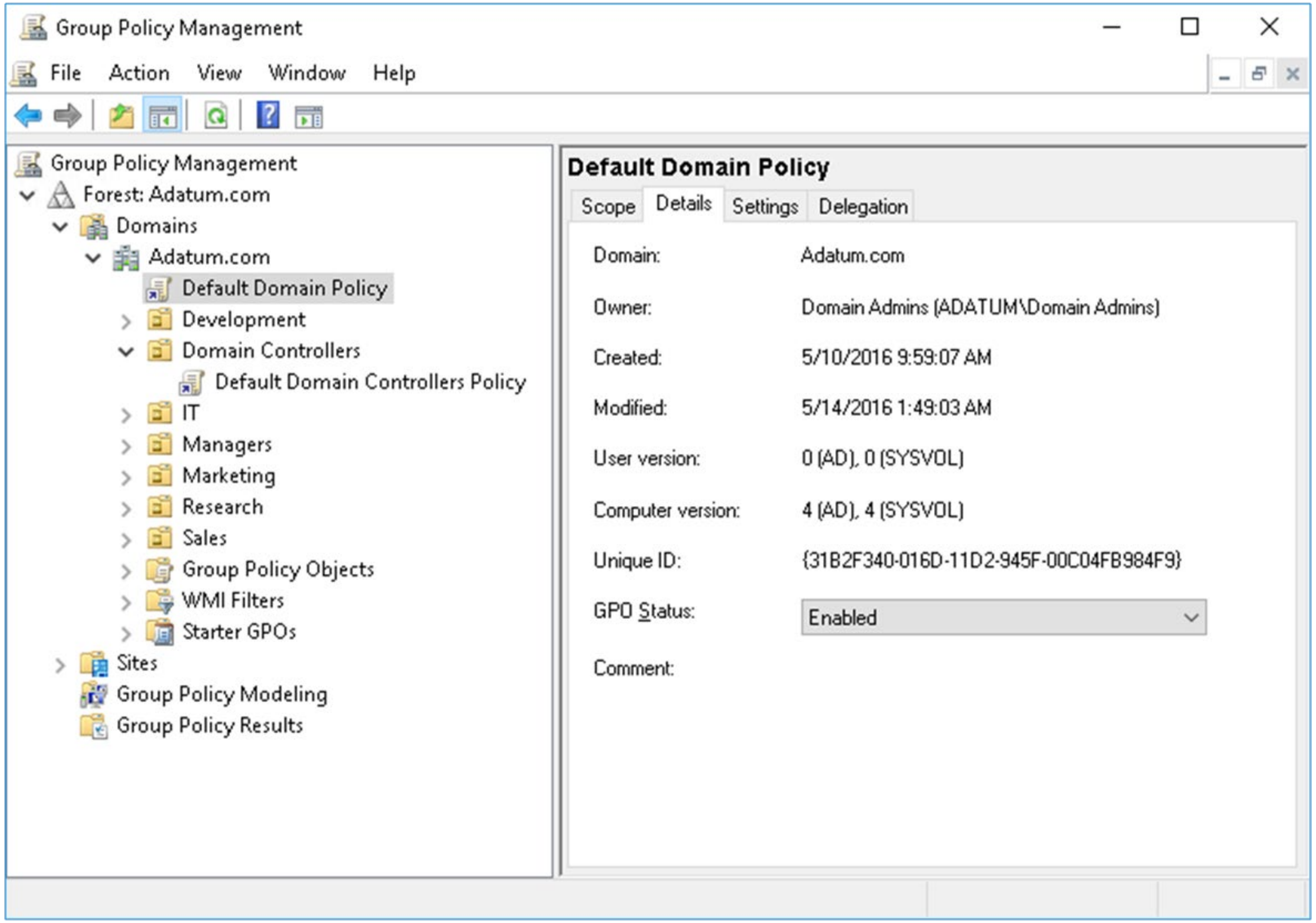
- Group Policy application process:

  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

What are domain-based GPOs?



Default Domain Policy

Domain: Adatum.com

Owner: Domain Admins (ADATUM\Domain Admins)

Created: 5/10/2016 9:59:07 AM

Modified: 5/14/2016 1:49:03 AM

User version: 0 (AD), 0 (SYSVOL)

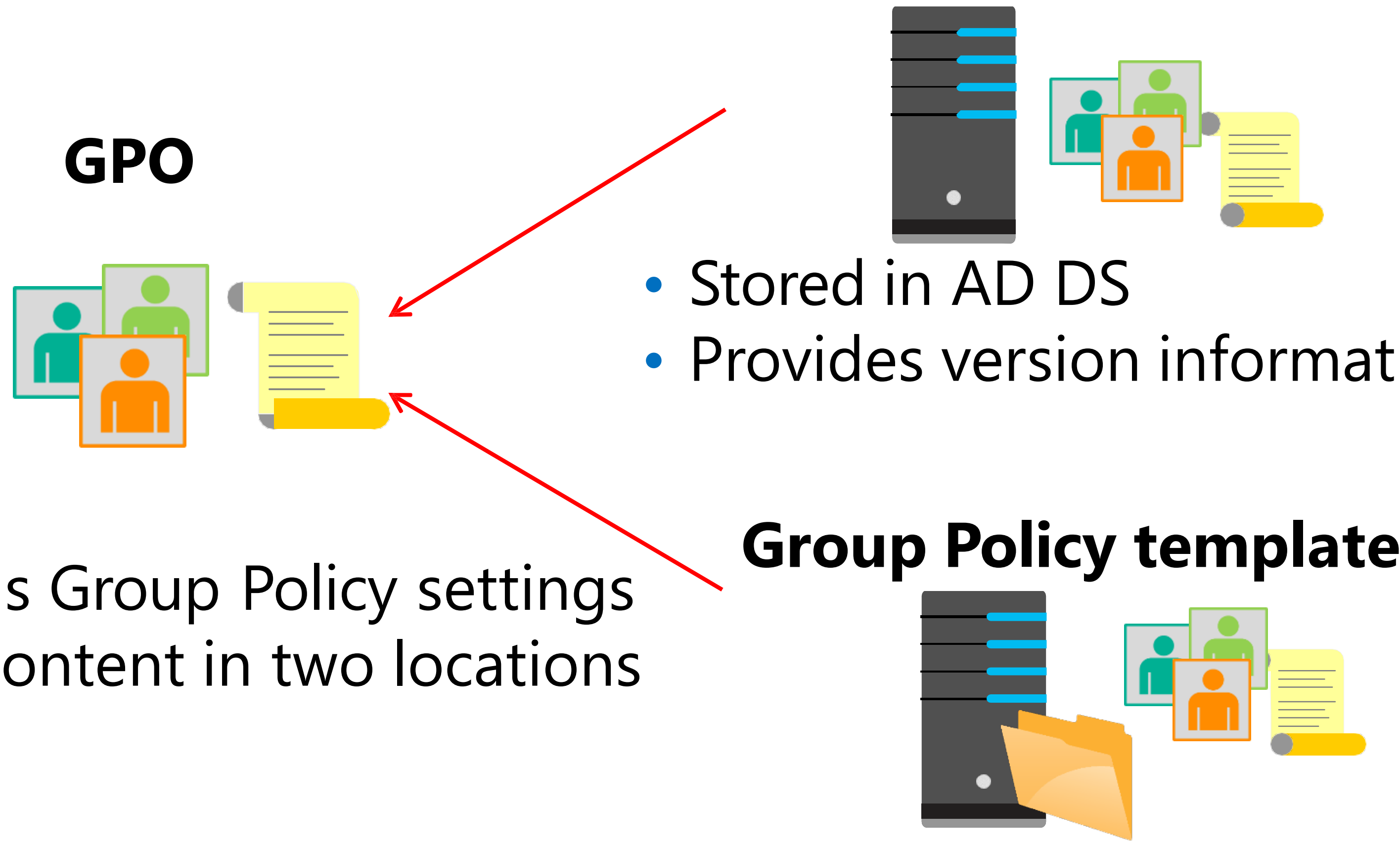
Computer version: 4 (AD), 4 (SYSVOL)

Unique ID: {31B2F340-016D-11D2-945F-00C04FB984F9}

GPO Status: Enabled

Comment:

GPO storage



GPO

- Contains Group Policy settings
- Stores content in two locations

- Stored in AD DS
- Provides version information

Group Policy template

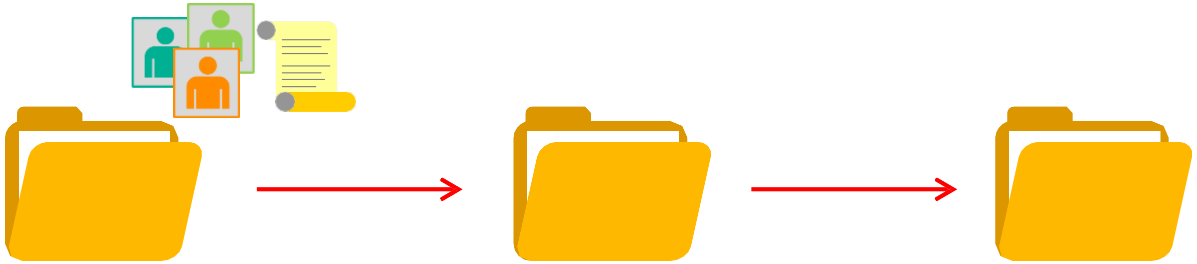
- Stored in shared SYSVOL folder
- Provides Group Policy settings

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**



Starter GPO

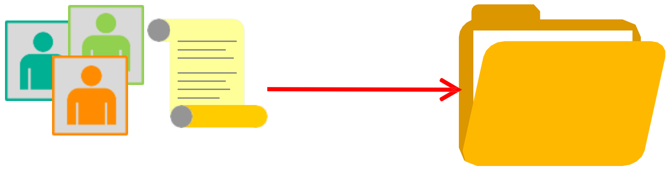
.cab file

Load
.cab file

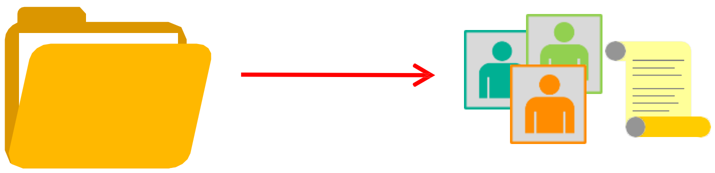
Common GPO management tasks

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

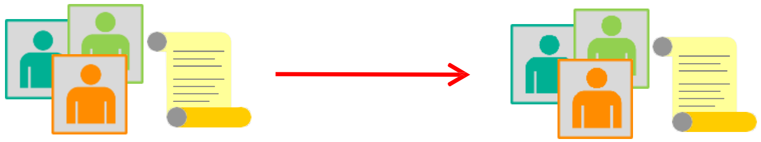
Back up GPOs



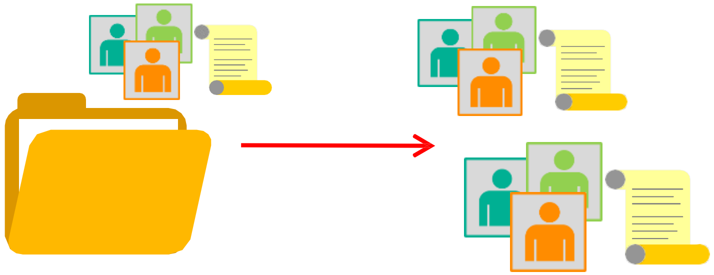
Restore GPOs



Copy GPOs



Import GPOs



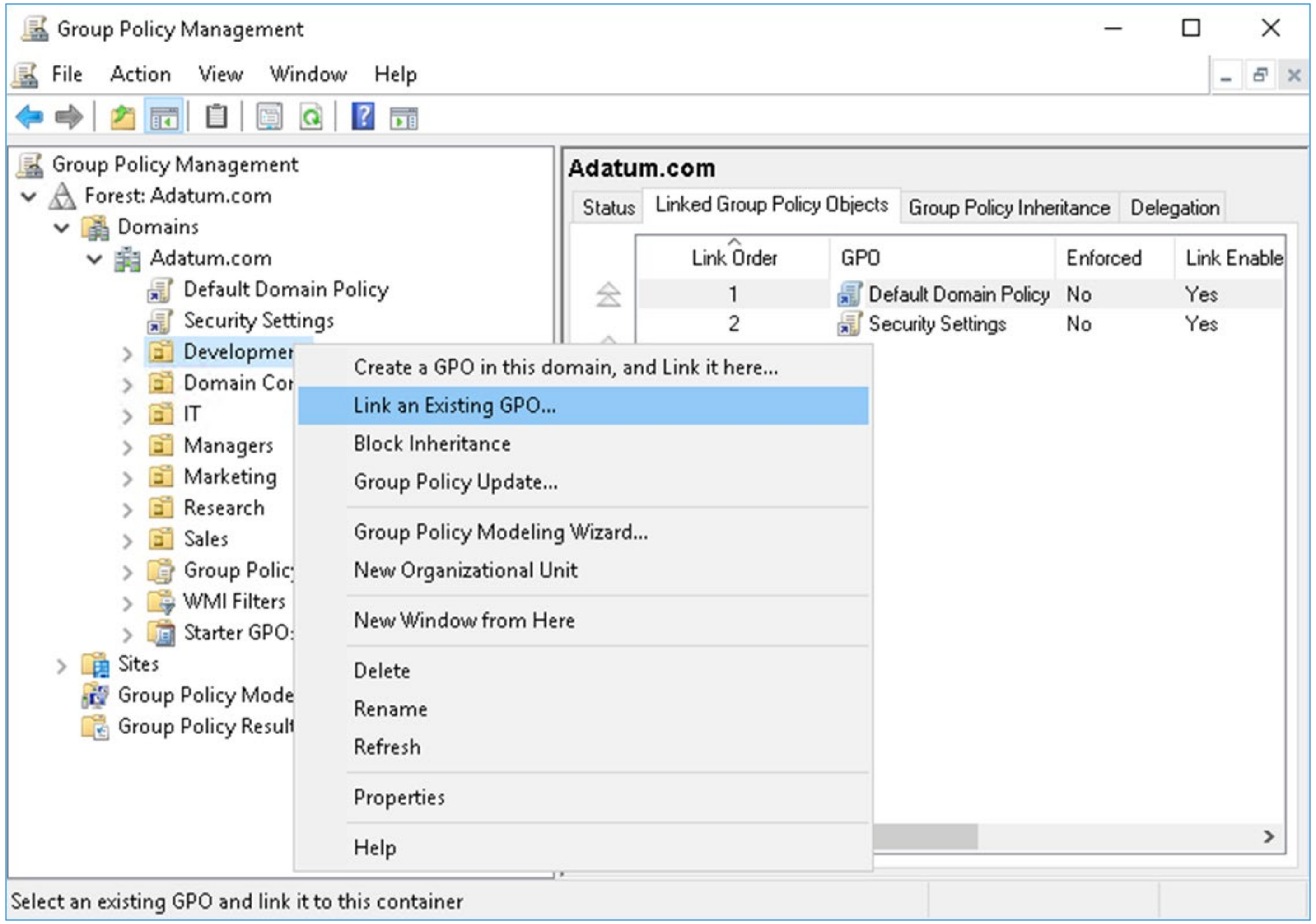
Delegating administration of Group Policy

- 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

What are GPO links?

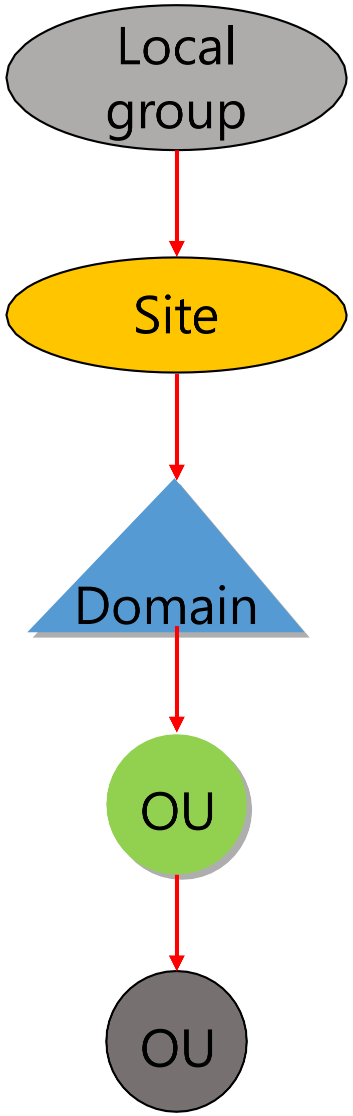
- After you have linked a GPO, the users or computers in that container are within the scope of the GPO, including computers and users in child OUs



Link Order	GPO	Enforced	Link Enable
1	Default Domain Policy	No	Yes
2	Security Settings	No	Yes

Select an existing GPO and link it to this container

Group Policy processing order



GPO 1 Local group . . . Local group policies

GPO 2 Site . . . Site group policies

GPO 3 Domain . . . Domain group policies

GPO 4 OU . . . OU group policies

GPO 5 OU . . . Child OU group policies

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

Configuring GPO inheritance and 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

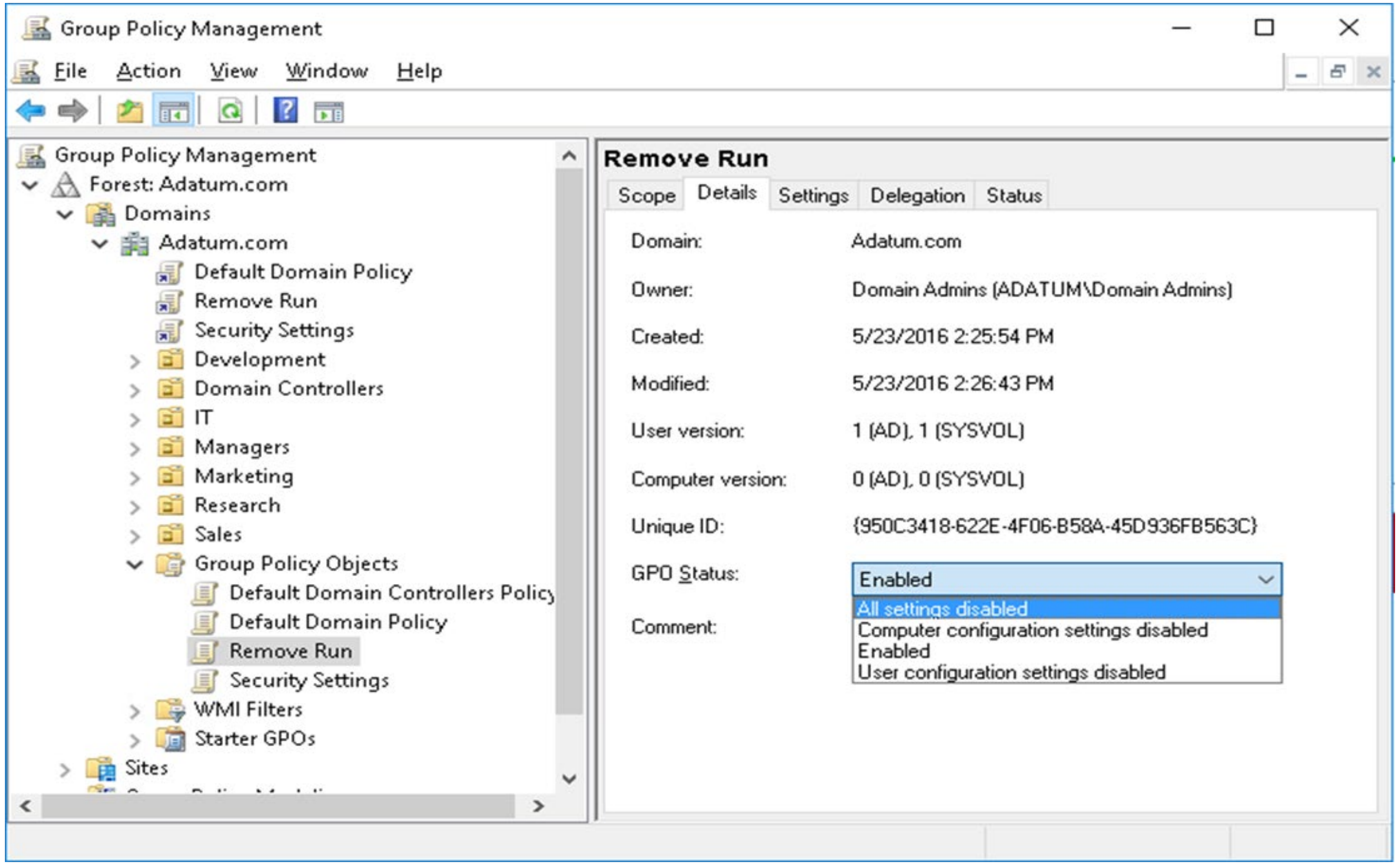
To scope only to users in selected global groups:

- 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

How to enable or disable GPOs and GPO nodes



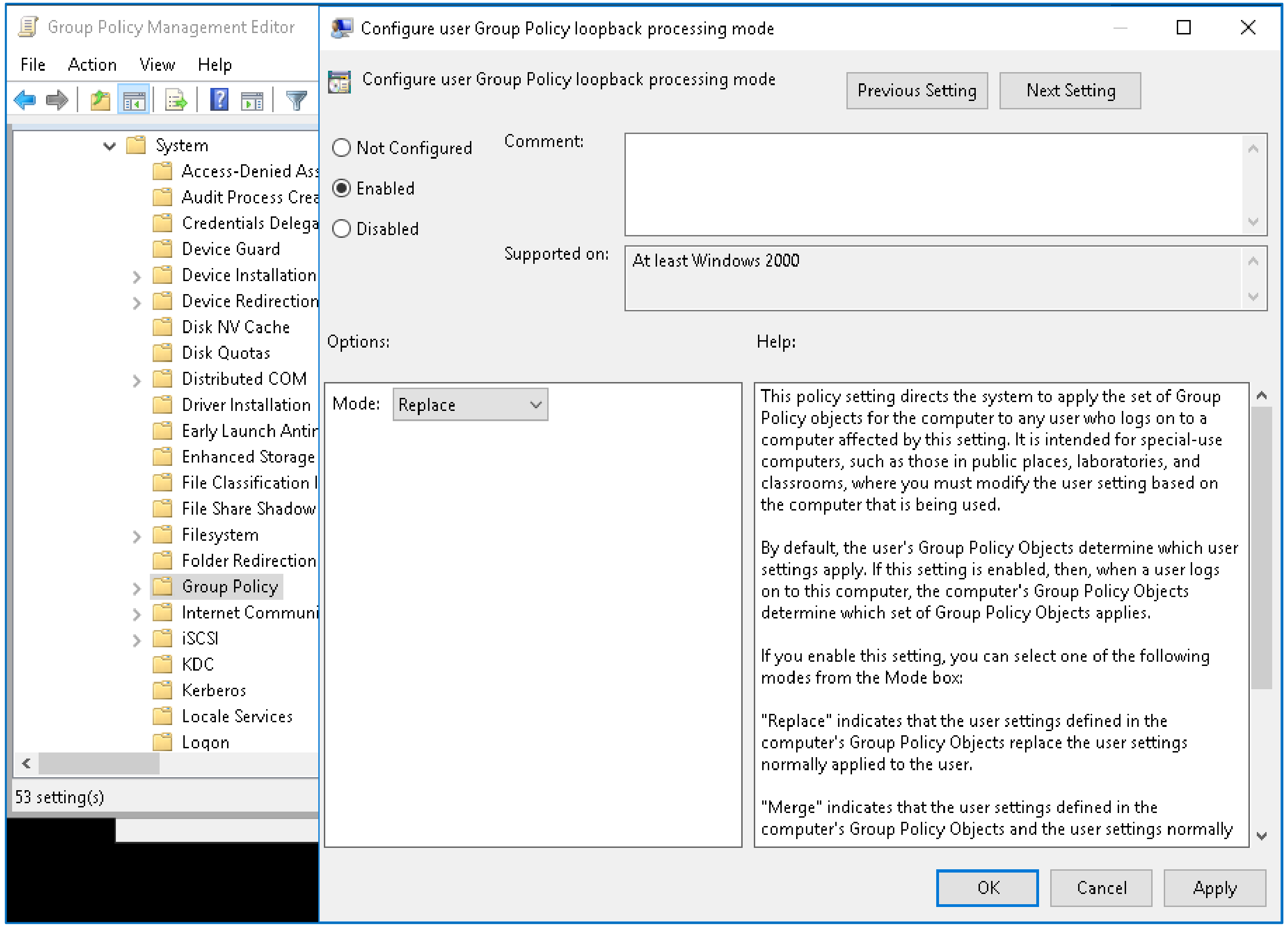
Remove Run

Domain:	Adatum.com
Owner:	Domain Admins (ADATUM\Domain Admins)
Created:	5/23/2016 2:25:54 PM
Modified:	5/23/2016 2:26:43 PM
User version:	1 (AD), 1 (SYSVOL)
Computer version:	0 (AD), 0 (SYSVOL)
Unique ID:	{950C3418-622E-4F06-B58A-45D936FB563C}
GPO Status:	Enabled
Comment:	

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



Configure user Group Policy loopback processing mode

Configure user Group Policy loopback processing mode

○ 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

| 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
  - Administrative Templates

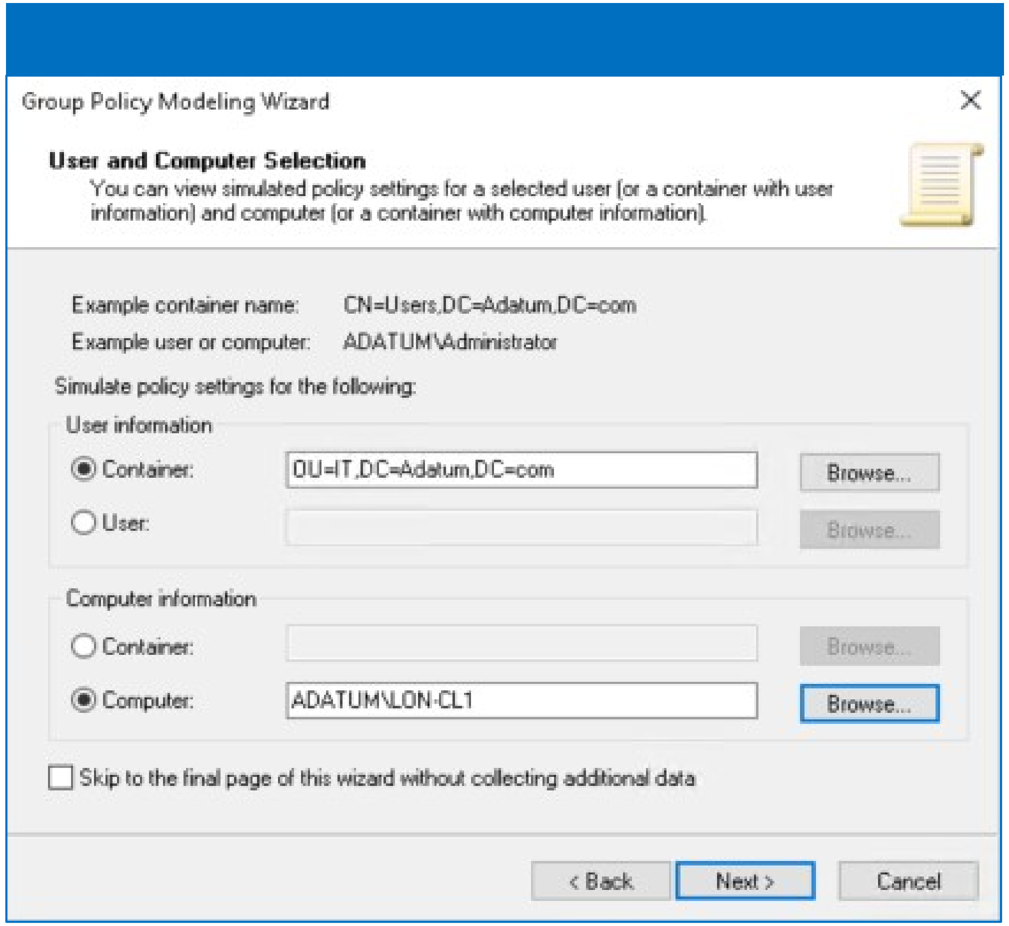
Disconnected computers:

- 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

What is RSoP?



Group Policy Modeling Wizard

User and Computer Selection

You can view simulated policy settings for a selected user (or a container with user information) and computer (or a container with computer information).

Example container name: CN=Users,DC=Adatum,DC=com

Example user or computer: ADATUM\Administrator

Simulate policy settings for the following:

User information

● Container: OU=IT,DC=Adatum,DC=com

○ User:

Computer information

○ Container:

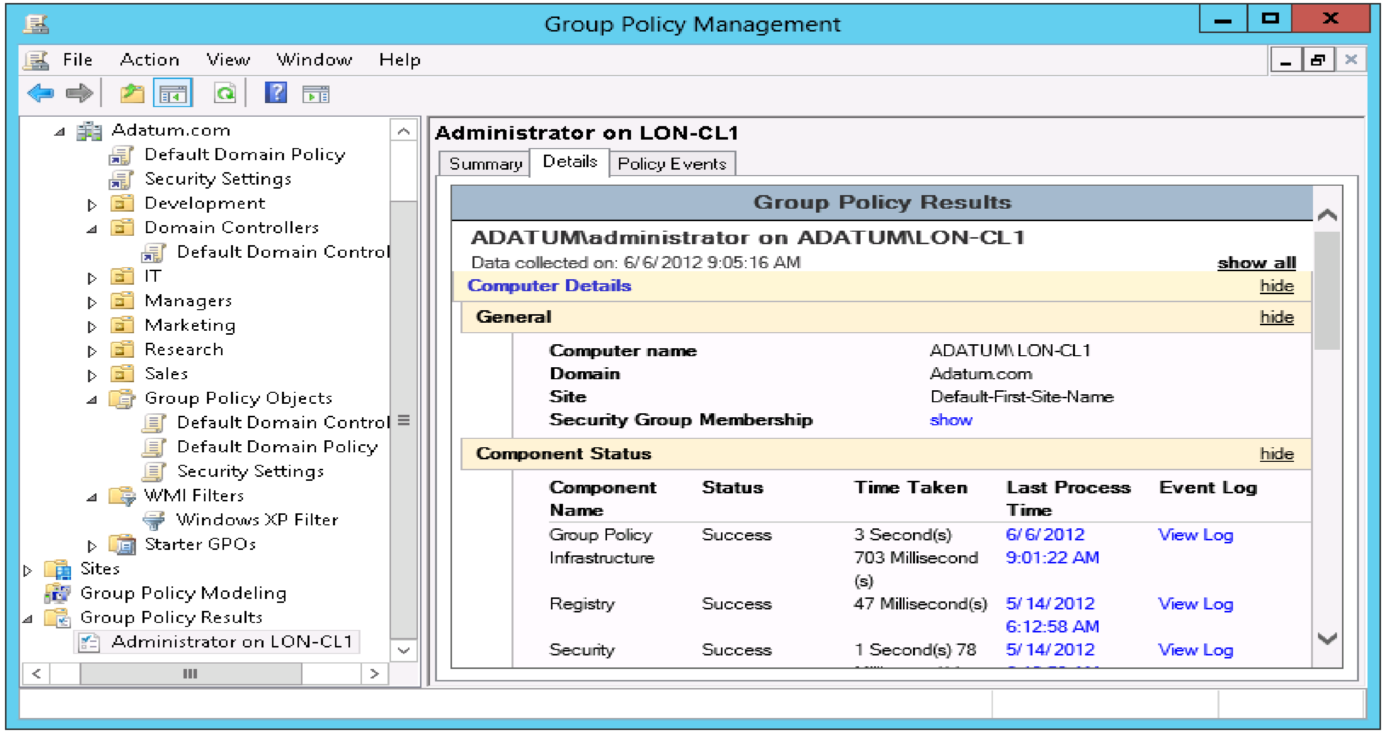
● Computer: ADATUM\LON-CL1

□ Skip to the final page of this wizard without collecting additional data

Generating RSoP reports

- RSoP reports show the actual settings being applied to the user and computer
- Might show the time taken to apply Group Policy
- You can generate RSoP reports by using:
  - **Group Policy Results Wizard**
  - **GPResults**
  - **Get-GPResultantSetOfPolicy**
- Target computer must be online
- Remote WMI must be enabled

Generating RSoP reports



Administrator on LON-CL1

Group Policy Results

ADATUM\administrator on ADATUM\LON-CL1

Data collected on: 6/6/2012 9:05:16 AM **show all**

Computer Details hide

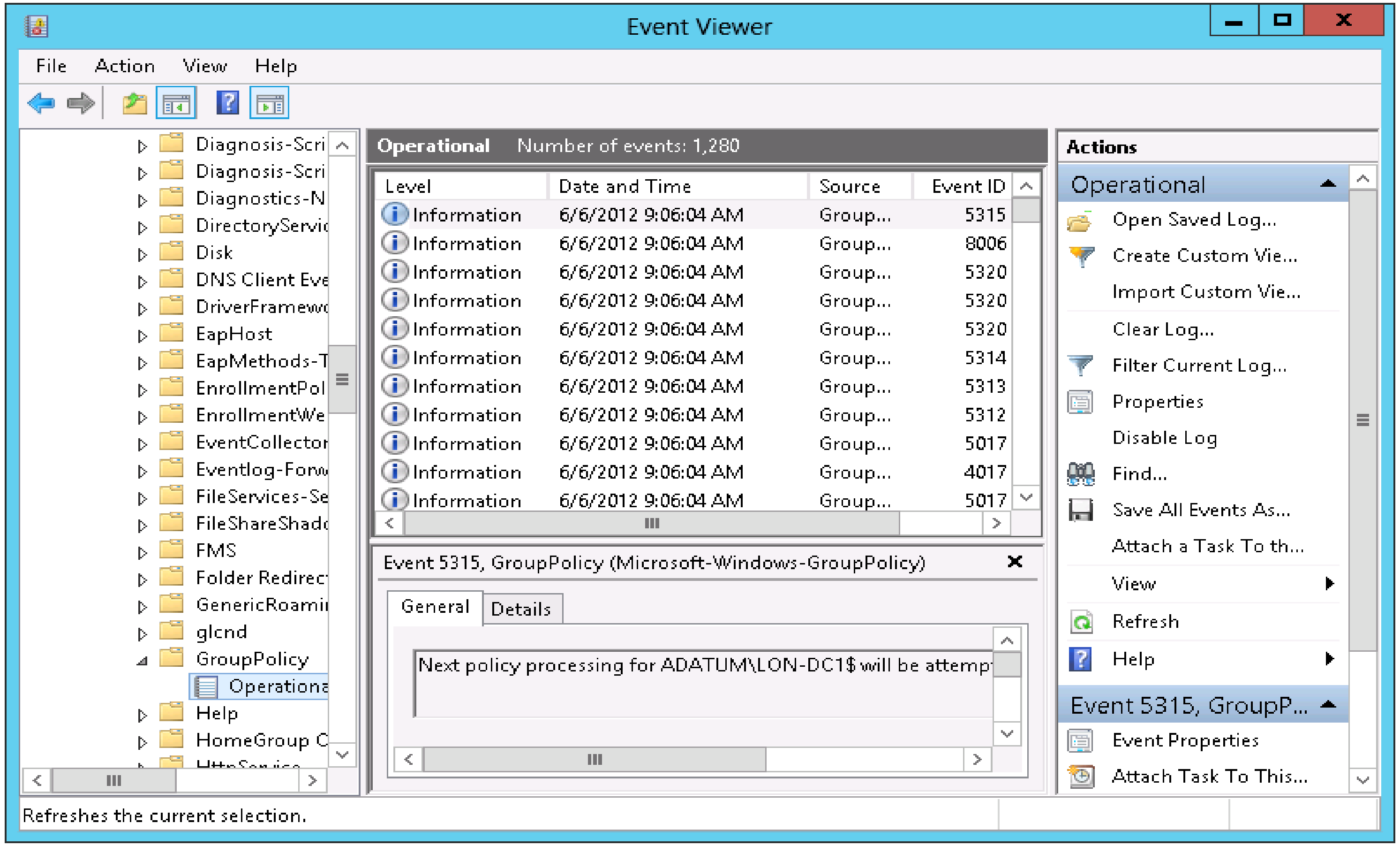
General hide

Computer name	ADATUM\ LON-CL1
Domain	Adatum.com
Site	Default-First-Site-Name
Security Group Membership	show

Component Status hide

Component Name	Status	Time Taken	Last Process Time	Event Log
Group Policy Infrastructure	Success	3 Second(s) 703 Millisecond (s)	6/6/2012 9:01:22 AM	View Log
Registry	Success	47 Millisecond(s)	5/14/2012 6:12:58 AM	View Log
Security	Success	1 Second(s) 78	5/14/2012	View Log

Examining Group Policy event logs



Operational Number of events: 1,280

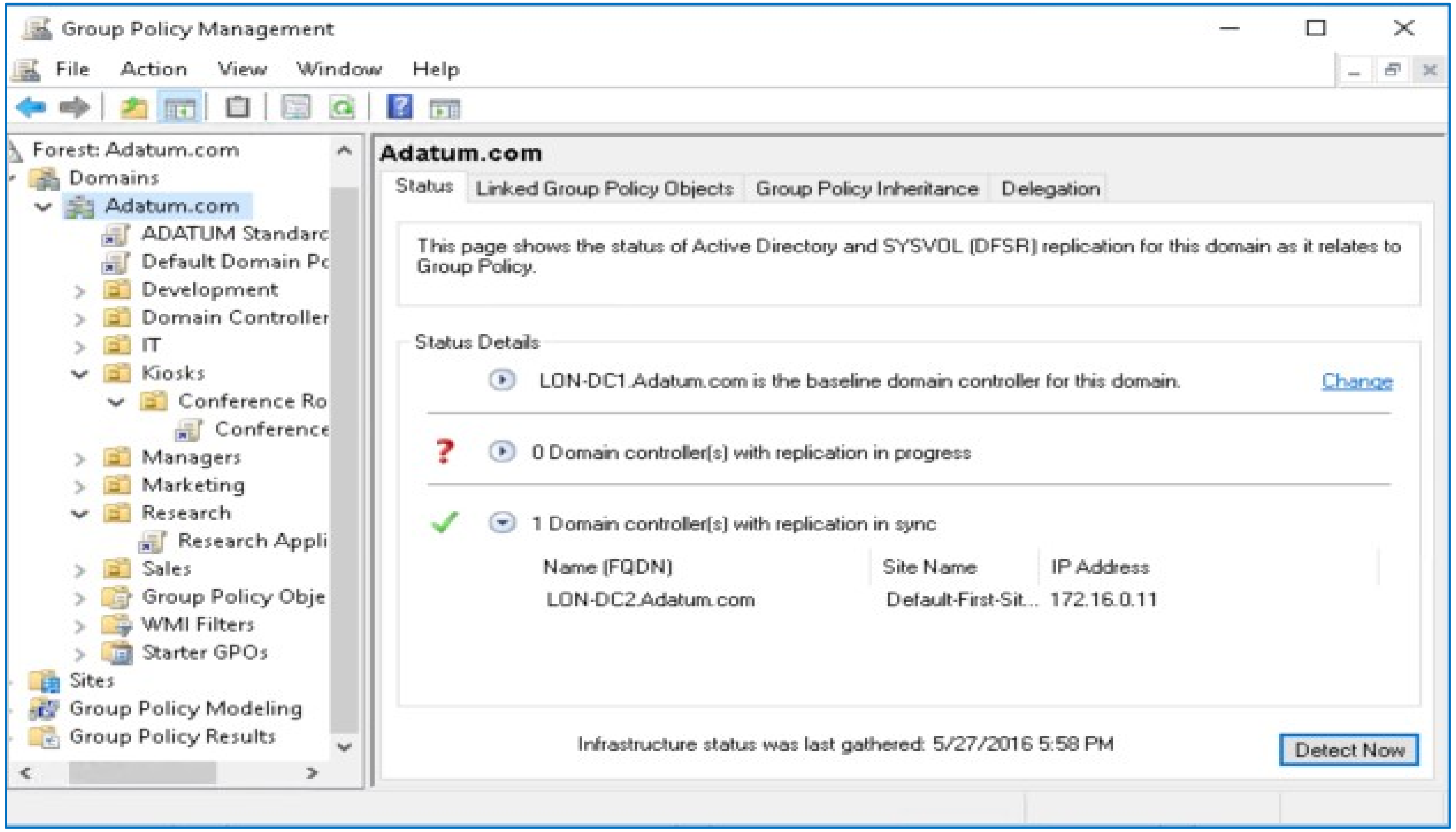
Level	Date and Time	Source	Event ID
Information	6/6/2012 9:06:04 AM	Group...	5315
Information	6/6/2012 9:06:04 AM	Group...	8006
Information	6/6/2012 9:06:04 AM	Group...	5320
Information	6/6/2012 9:06:04 AM	Group...	5320
Information	6/6/2012 9:06:04 AM	Group...	5320
Information	6/6/2012 9:06:04 AM	Group...	5314
Information	6/6/2012 9:06:04 AM	Group...	5313
Information	6/6/2012 9:06:04 AM	Group...	5312
Information	6/6/2012 9:06:04 AM	Group...	5017
Information	6/6/2012 9:06:04 AM	Group...	4017
Information	6/6/2012 9:06:04 AM	Group...	5017

Event 5315, GroupPolicy (Microsoft-Windows-GroupPolicy)

Next policy processing for ADATUM\LON-DC1$ will be attemp

Refreshes the current selection.

Detecting Group Policy health issues



Adatum.com

This page shows the status of Active Directory and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.

Status Details

LON-DC1.Adatum.com is the baseline domain controller for this domain.

? 0 Domain controller(s) with replication in progress

✓ 1 Domain controller(s) with replication in sync

Name (FQDN)	Site Name	IP Address
LON-DC2.Adatum.com	Default-First-Sit...	172.16.0.11

Infrastructure status was last gathered: 5/27/2016 5:58 PM

Detecting Group Policy health issues

In Group Policy Management Console:

- The **Status** tab displays information that indicates the health of the Group Policy infrastructure:
  - Domain
  - GPO

- Information displayed includes:
  - Domain controllers
  - Permissions on the Group Policy container and the Group Policy template
  - GPO replication
  - GPO versioning

- Domain controllers not reachable or inconsistent with the baseline domain controller are added to the **Domain controller(s) with replication in progress** list

Unit 06

Managing user settings with Group Policy

elev8 LEARNING SOLUTIONS

What are administrative templates?

- Administrative templates give you the ability to control the environment of the operating system and the user experience:
- Administrative template section for computers:
  - Control Panel
  - Network
  - Printers
  - System
  - Windows-based components

What are administrative templates?

- Administrative template section for users:
  - Control Panel
  - Desktop
  - Network
  - Start menu and taskbar
  - System
  - Windows-based components
- Each of these main sections contain many subfolders to further organize settings

What are .adm and .admx files?

.adm files:

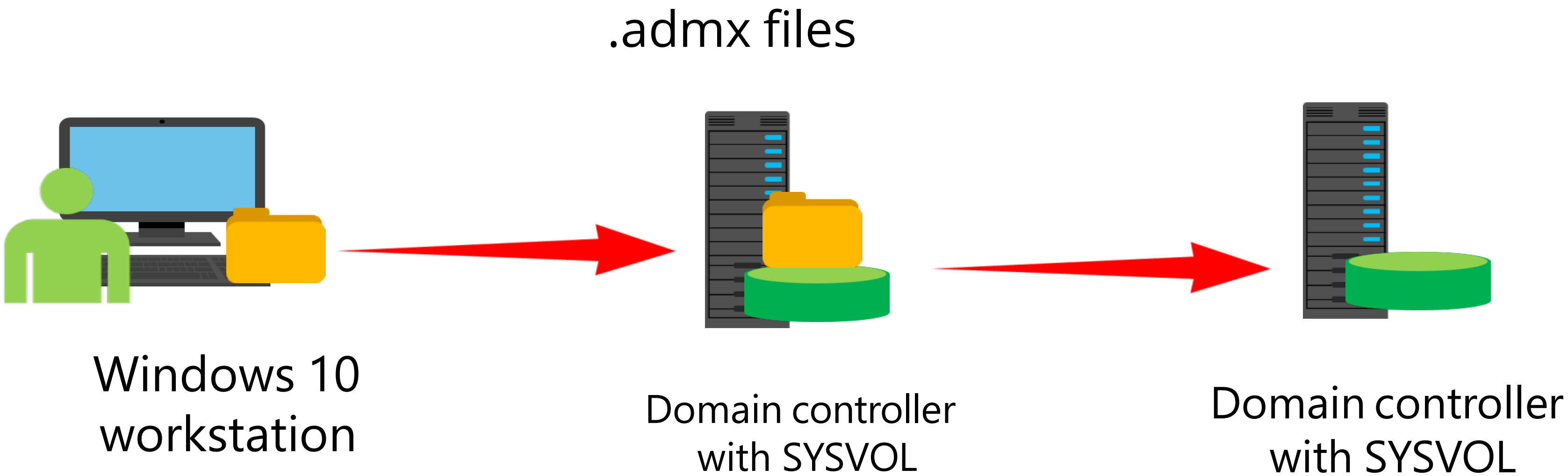
- Are copied into every GPO in SYSVOL
- Are difficult to customize
- Are not language-neutral
- Could cause SYSVOL bloat if there are many GPOs

.admx files:

- Are language-neutral
- .adml files provide the localized language
- Are not stored in the GPO
- Are extensible through XML

Overview of the central store

- **The central store:**
  - Is a central repository for .admx and .adml files
  - Is stored in SYSVOL
  - Must be created manually
  - Is detected automatically by Windows Vista, Windows Server 2008, and newer operating systems



Importing security templates

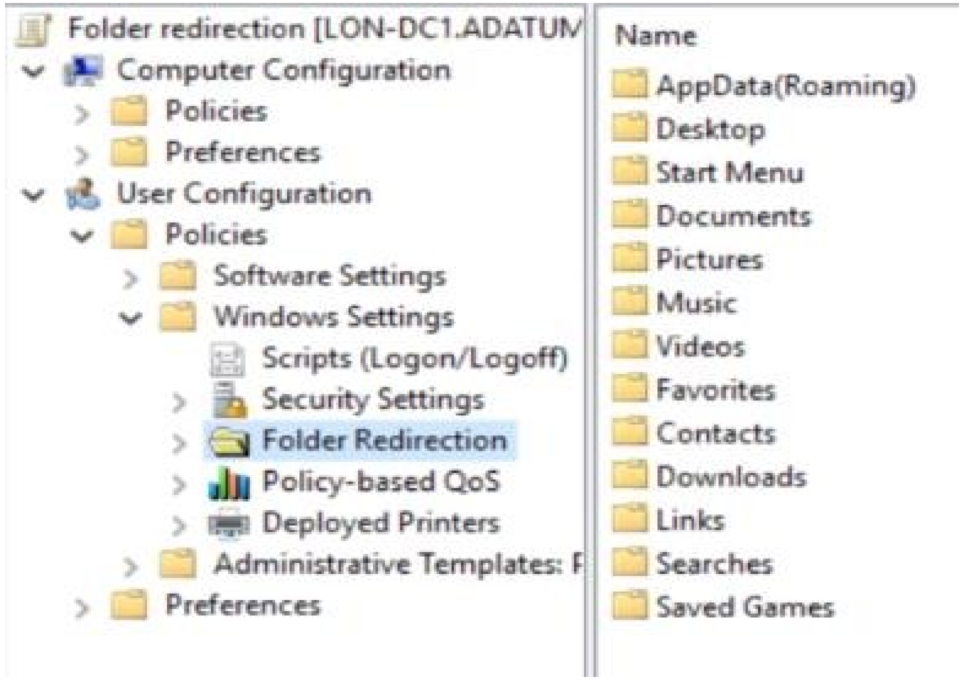
- Security Templates contain settings for:
  - Account policies
  - Local policies
  - Event log
  - Restricted groups
  - System services
  - Registry
  - File system
- More security settings are available in a GPO
- Security templates created in the Security Templates snap-in can be imported into a GPO
- The Security Compliance Manager can export security baselines in a GPO backup format

Managing administrative templates

- Extend the set of administrative templates by:
  1. Creating new templates or downloading available templates
  2. Adding the templates to the central store so the settings become available in all GPOs
  3. Configuring the settings in a GPO
  4. Deploying the GPO
- .admx files are available for both Microsoft and third-party applications
- Import legacy .adm files to the Administrative Templates section of a GPO

What is Folder Redirection?

- Folder Redirection allows folders to be located on a network server, but appear as if they are located on a local drive
- Folders that can be redirected in Windows Vista and later are:

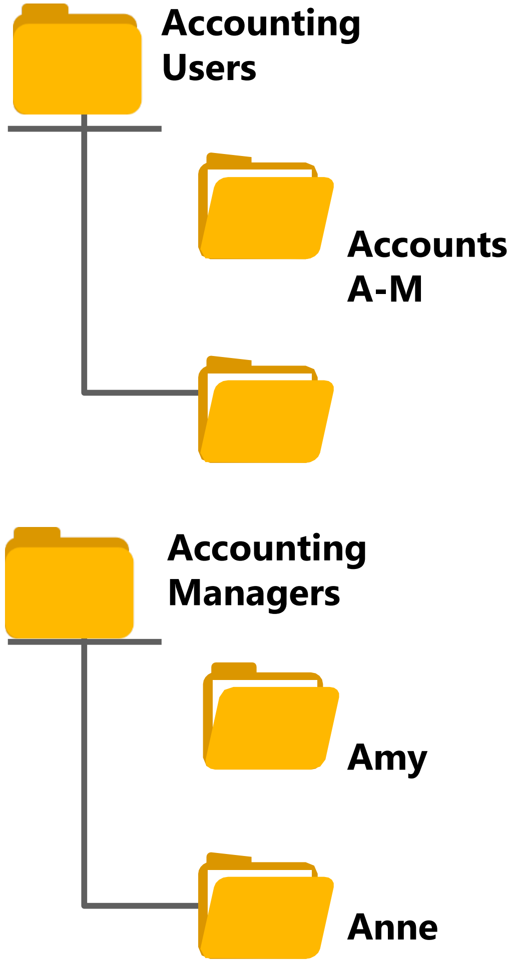


Name

- AppData(Roaming)
- Desktop
- Start Menu
- Documents
- Pictures
- Music
- Videos
- Favorites
- Contacts
- Downloads
- Links
- Searches
- Saved Games

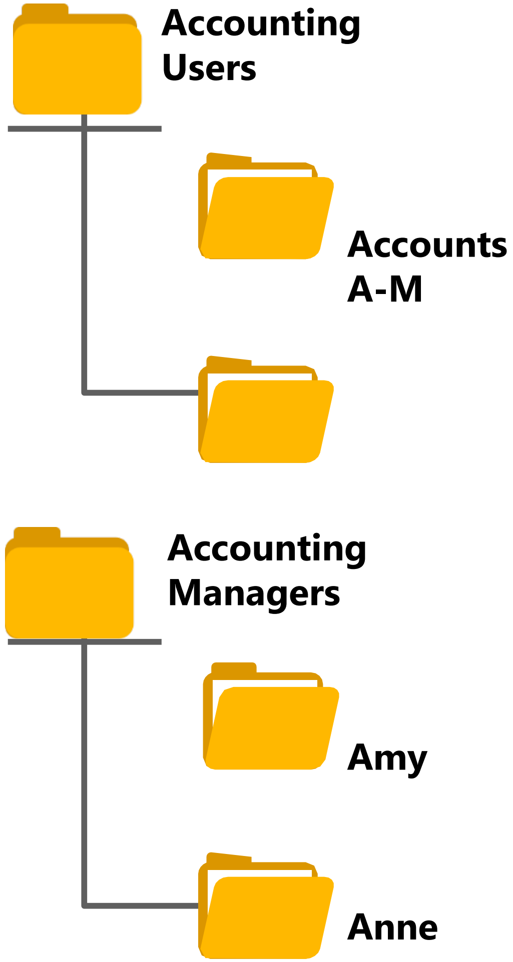
Settings for configuring Folder Redirection

- Folder Redirection configuration options:
  - Use Basic Folder Redirection when all users
  - save their files to the same location
  - Use Advanced Folder Redirection when the server hosting the folder location is based on group membership
  - Use the Follow the Documents folder to force certain folders to become subfolders of Documents



Settings for configuring Folder Redirection

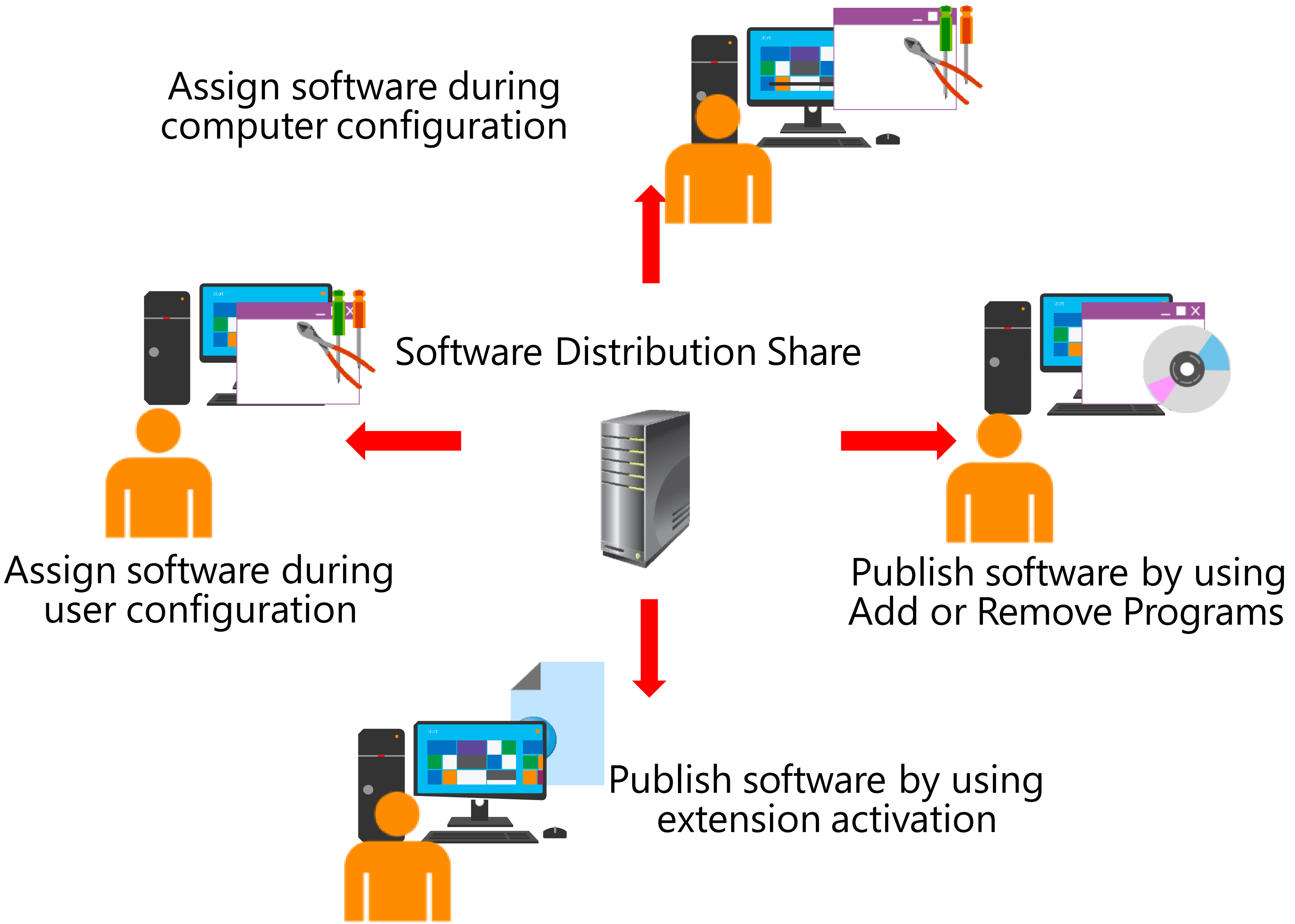
- Target folder location options:
  - Create a folder for each user under the root path
  - Redirect to the following location
  - Redirect to the local user profile location
  - Redirect to the user's home directory (Documents folder only)



Security settings for redirected folders

NTFS permissions for root folder	
Creator/Owner	**Full control – subfolders and files only**
Administrator	None
Security group of users that save data on the share	List Folder/Read Data, Create Folders/Append Data-This Folder Only
Local System	Full control
Share permissions for root folder	
Creator/Owner	**Full control – subfolders and files only**
Security group of users that save data on the share	Full control
NTFS permissions for each user’s redirected folder	
Creator/Owner	**Full control – subfolders and files only**
%Username%	Full control, owner of folder
Administrators	None
Local System	Full control

Managing software with Group Policy



Assign software during computer configuration

Software Distribution Share

Assign software during user configuration

Publish software by using Add or Remove Programs

Publish software by using extension activation

Group Policy settings for applying scripts

- You can use scripts to perform many tasks, such as clearing page files, mapping drives, and clearing temp folders for users
- Scripts languages include VBScript, Jscript, Windows PowerShell, and
- command/batch files
- You can assign Group Policy script settings to assign:
  - For computers:
    - Startup scripts
    - Shutdown scripts
  - For users:
    - Logon scripts
    - Logoff scripts

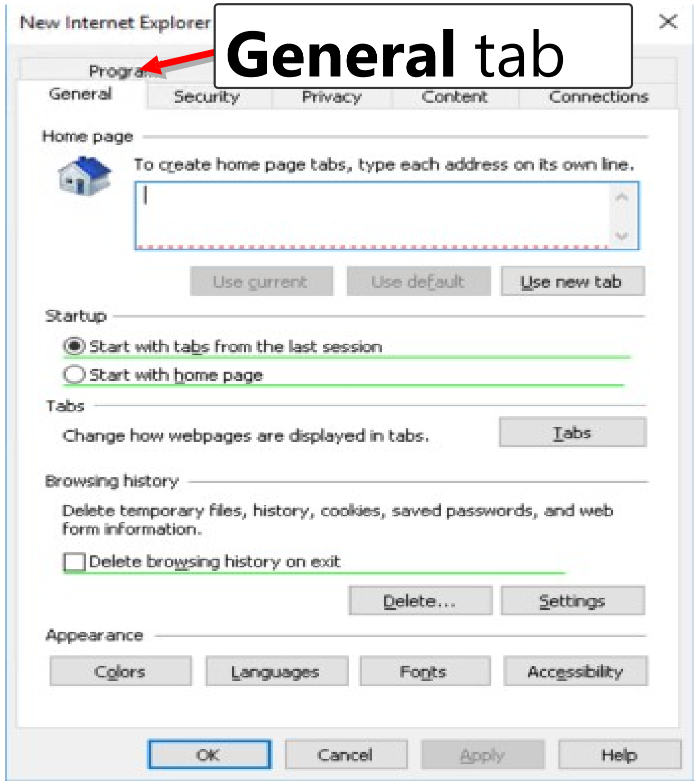
What are Group Policy preferences?

- Group Policy preferences extensions expand the range of configurable settings within a GPO:
- Enables you to manage settings that were previously not manageable by using Group Policy
- Are supported natively on Windows Server 2008 and newer and Windows Vista SP2 and newer
- Can be created, deleted, replaced, or updated
- Categories include mapped drives, shortcuts, registry changes, power options, schedules tasks, and Internet Explorer settings

Comparing Group Policy preferences and Group Policy settings

Group Policy settings	Group Policy preferences
Strictly enforce policy settings by writing the settings to areas of the registry that standard users cannot modify	Are written to the normal locations in the registry that the application or operating system feature uses to store the setting
Typically disable the user interface for settings that Group Policy is managing	Do not cause the application or operating system feature to disable the user interface for settings they configure
Refresh policy settings at a regular interval	Refresh preferences by using the same interval as Group Policy settings by default, but can be configured to apply only once

Features of Group Policy preferences



New Internet Explorer

General tab

Home page

To create home page tabs, type each address on its own line.

Startup

● Start with tabs from the last session

○ Start with home page

Tabs

Change how webpages are displayed in tabs.

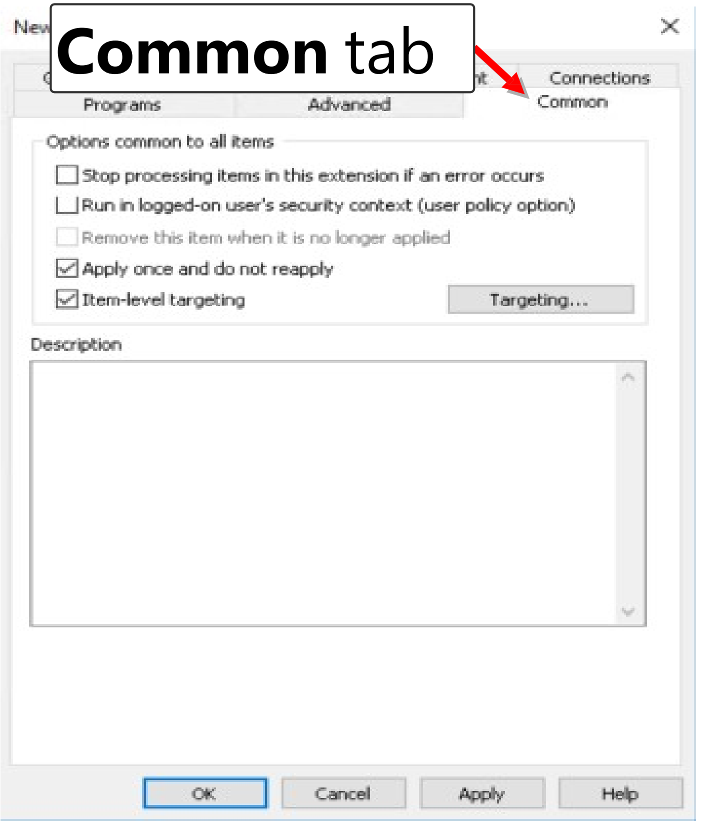
Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit

Appearance

- Configure most settings
- Look out for red dotted-lines
- The setting is not enabled; use F6 to enable it



Common tab

Options common to all items

□ Stop processing items in this extension if an error occurs

□ Run in logged-on user's security context (user policy option)

□ Remove this item when it is no longer applied

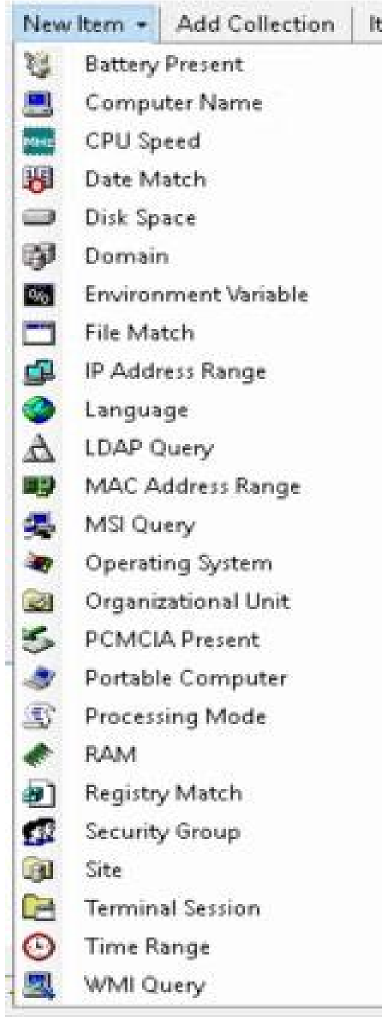
☑ Apply once and do not reapply

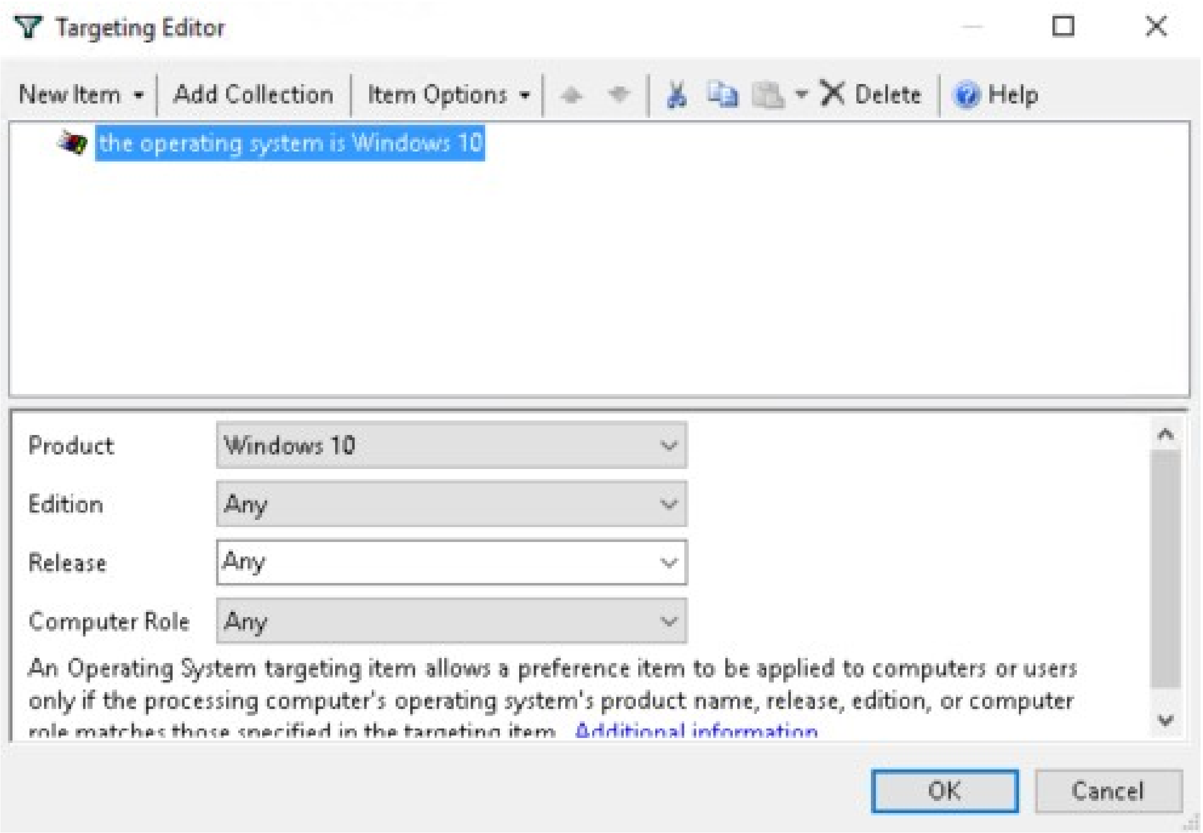
☑ Item-level targeting

Description

Configure additional options that control the behavior of a Group Policy preference item

Item-level targeting options





the operating system is Windows 10

Product: Windows 10

Edition: Any

Release: Any

Computer Role: Any

An Operating System targeting item allows a preference item to be applied to computers or users only if the processing computer's operating system's product name, release, edition, or computer role matches those specified in the targeting item. Additional information

Item-level targeting options

- Restrict drive mappings to an Active Directory security group
- Configure different power plans to portable and desktop computers
- Deploy printers only to computers that meet specific criteria, and to users that are members of a specific group
- Copy Microsoft Office templates based on the language of the operating system installed on the computer

Unit 07

Securing Active Directory Domain Services

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
- Secure client computers

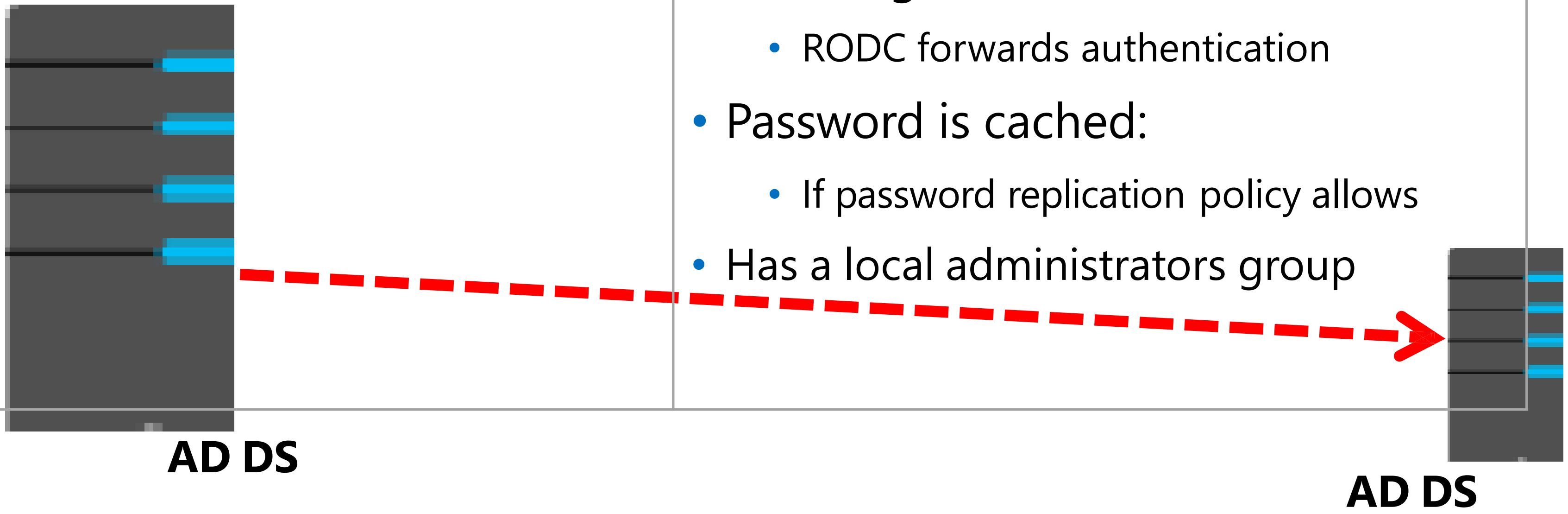
Securing physical access to domain controllers

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

  - **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**

Deploying an RODC

- 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

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

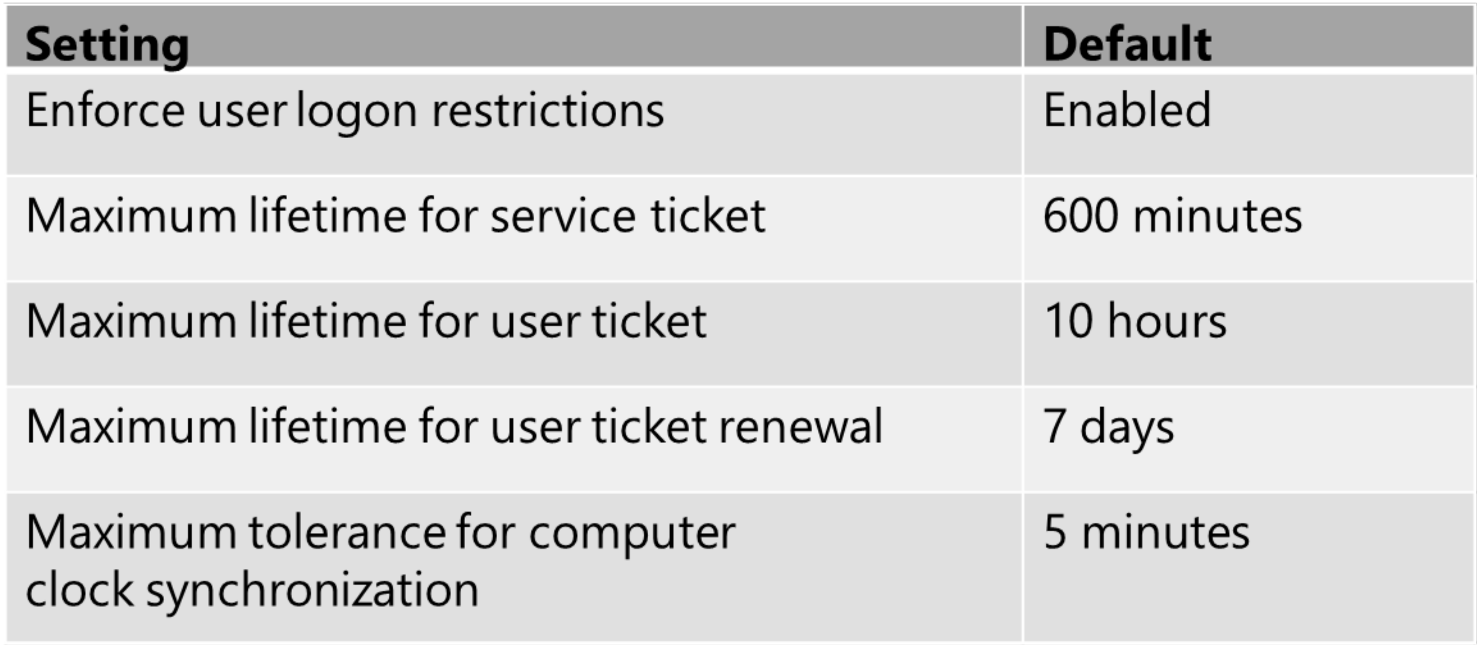
- Account lockout policies define whether accounts should be locked automatically after several failed attempts to sign in

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

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:

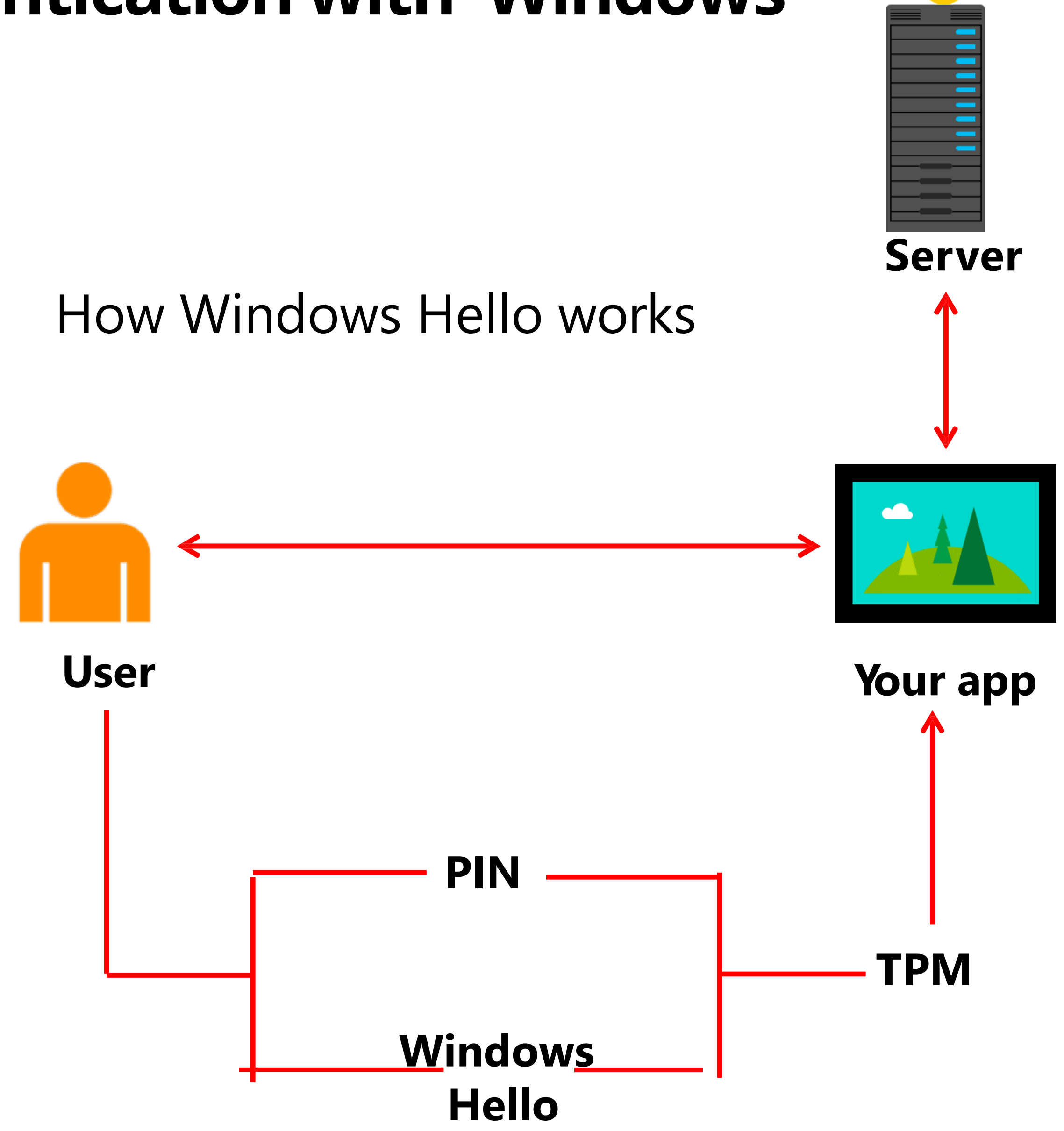
- Configure with the Group Policy Management console
- Apply to all accounts in AD DS and local accounts on computers joined to the domain
- Can apply only once in a domain and in only one GPO
- Take precedence over Local Security Policy settings

- 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

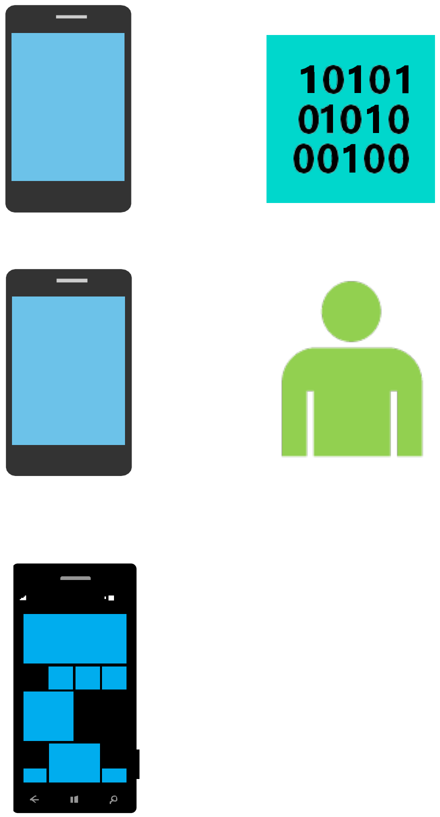


Enhancing password authentication with Windows Hello and MFA

Text message

Phone call

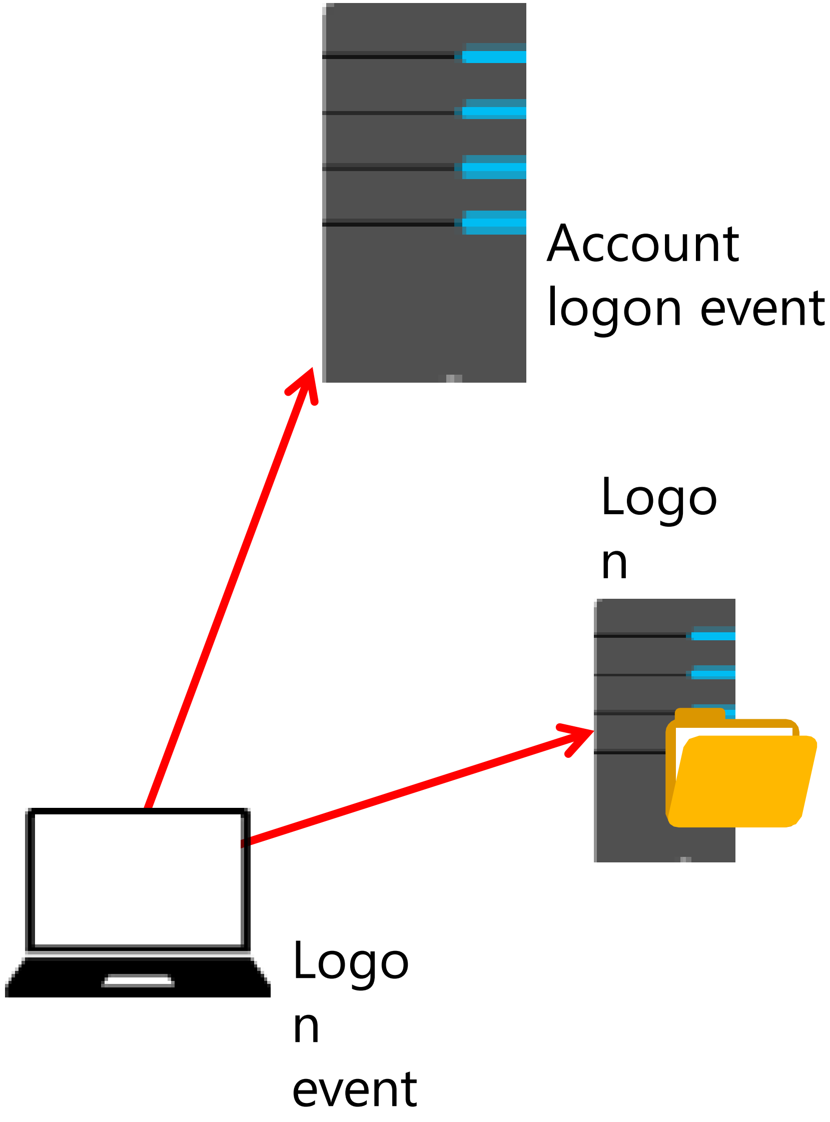
Mobile app



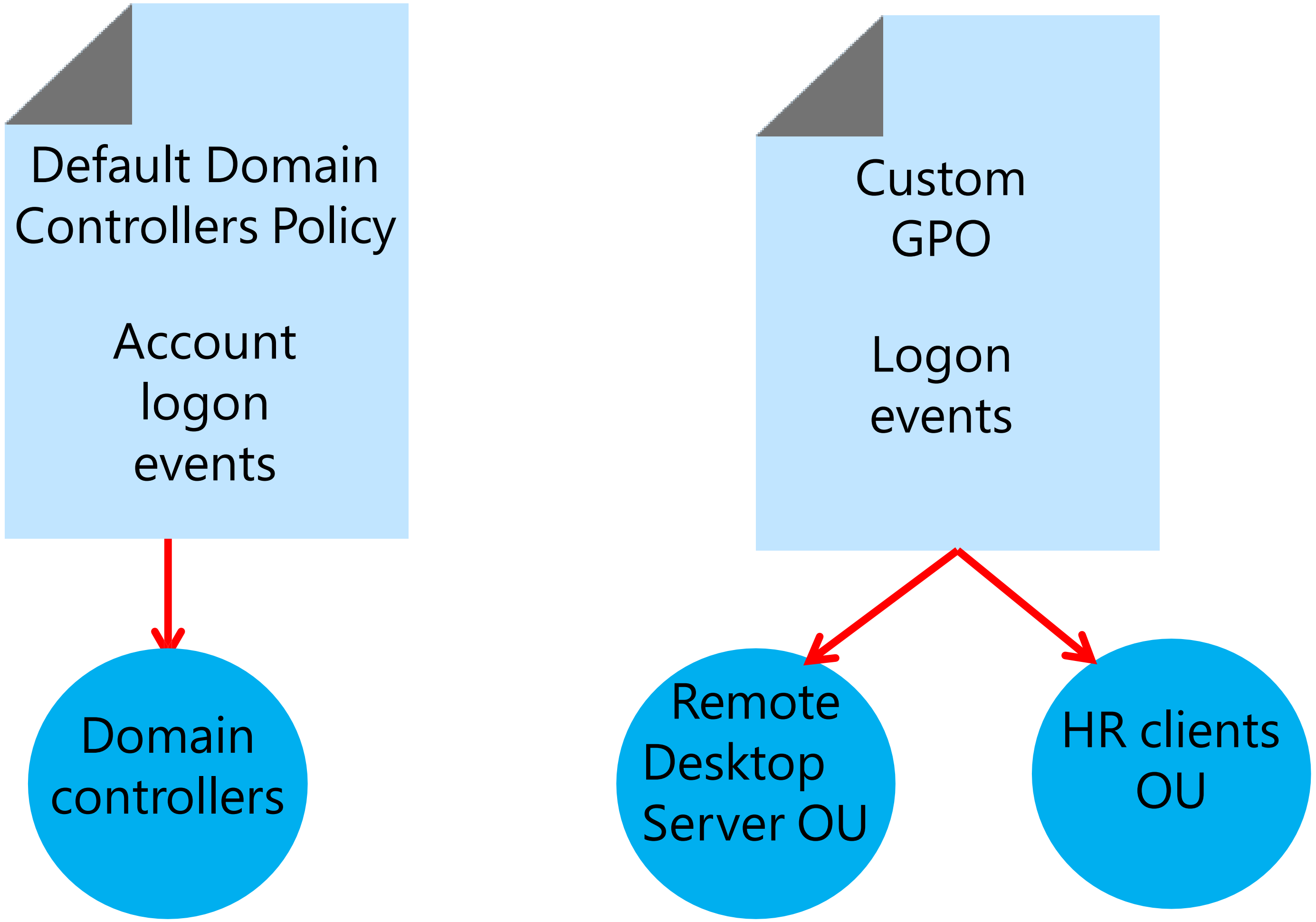
Account logon and logon events

- 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



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

Unit 08

Deploying and managing AD CS

What is AD CS?

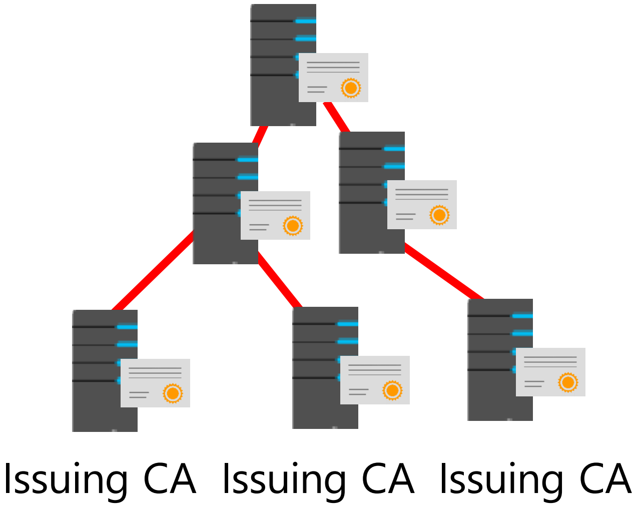
Allows you to implement a PKI for your organization:

- Issue and manage certificates

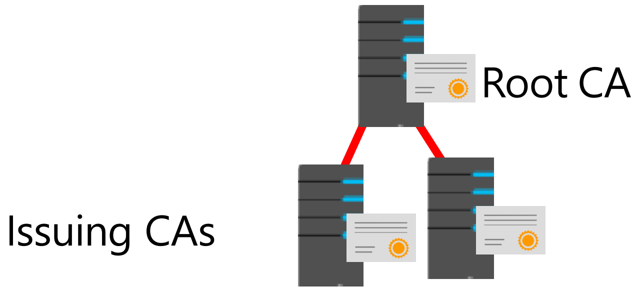
AD CS role services in Windows Server 2016:

- Certification Authority
- Certification Authority Web Enrollment
- Online Responder
- Network Device Enrollment Service
- Certificate Enrollment Web Service
- Certificate Enrollment Policy Web Service

Options for implementing CA hierarchies

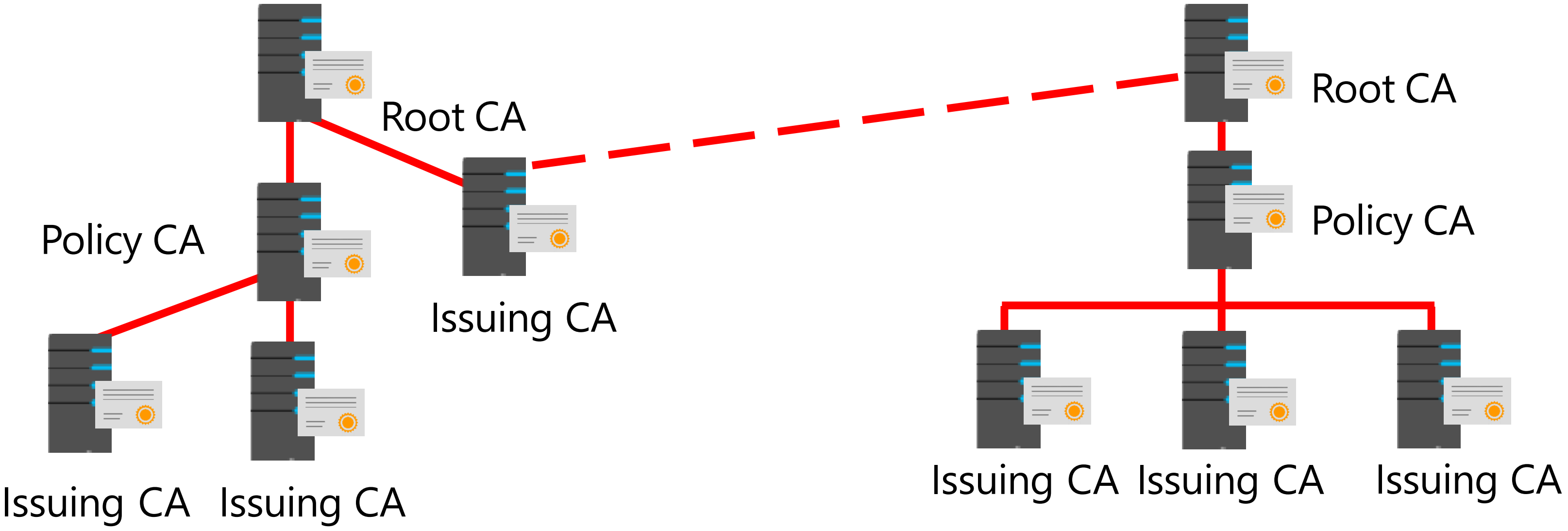


Issuing CA Issuing CA Issuing CA



Root CA

Issuing CAs



Root CA

Policy CA

Issuing CA

Issuing CA Issuing CA

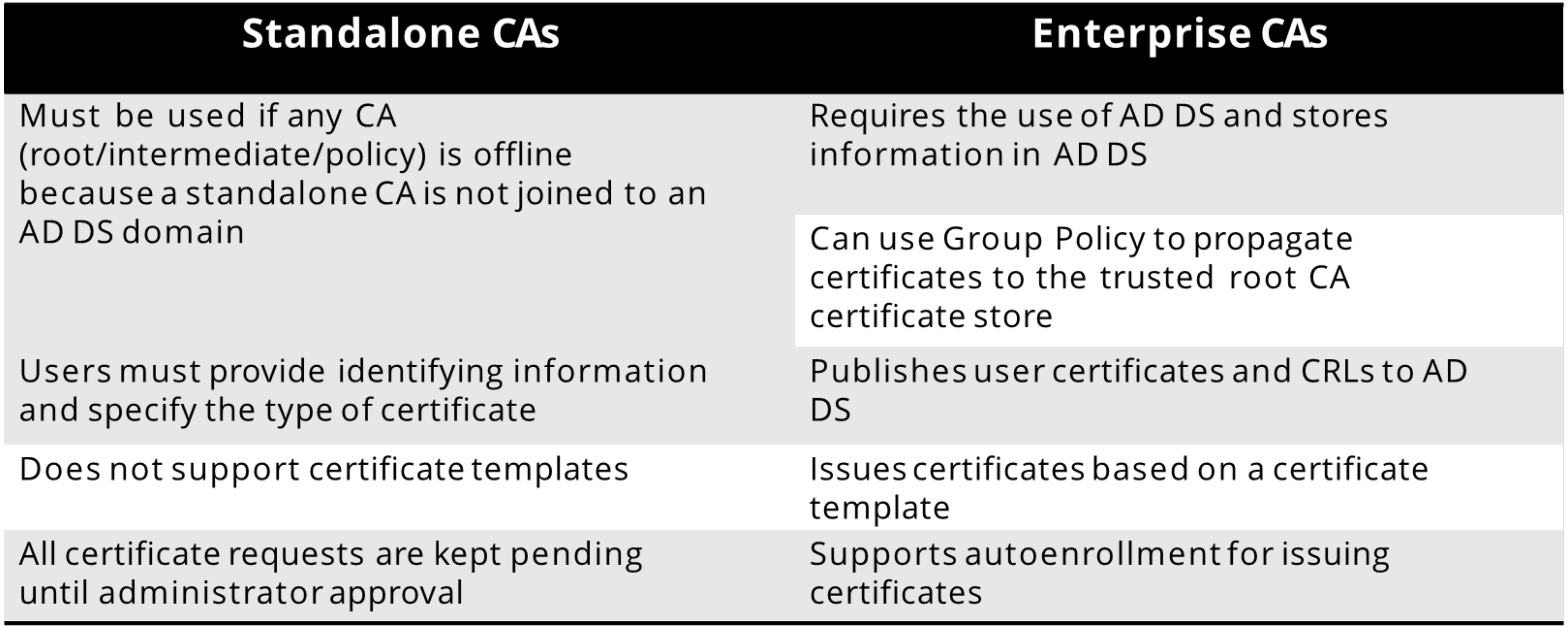
Root CA

Policy CA

Issuing CA Issuing CA Issuing CA

Cross-certification trust

Standalone vs. enterprise CAs

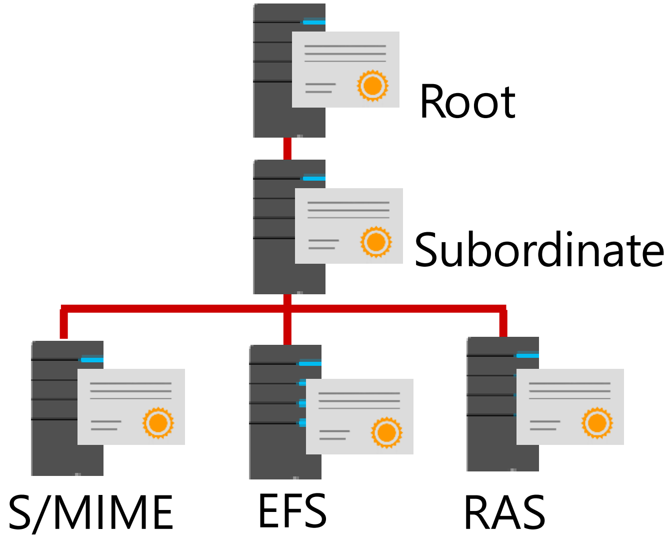


Standalone CAs	Enterprise CAs
Must be used if any CA (root/intermediate/policy) is offline because a standalone CA is not joined to an AD DS domain	Requires the use of AD DS and stores information in AD DS
	Can use Group Policy to propagate certificates to the trusted root CA certificate store
Users must provide identifying information and specify the type of certificate	Publishes user certificates and CRLs to AD DS
Does not support certificate templates	Issues certificates based on a certificate template
All certificate requests are kept pending until administrator approval	Supports autoenrollment for issuing certificates

Considerations for deploying a root CA

- Computer name and domain membership cannot change
- When you plan private key configuration, consider the following:
  - CSP
  - Key character length, with a default of 2,048
  - The hash algorithm that is used to sign certificates issued by a CA
- When you plan a root CA, consider the following:
  - Name and configuration
  - Certificate database and log location
  - Validity period

Considerations for deploying a subordinate CA



Root

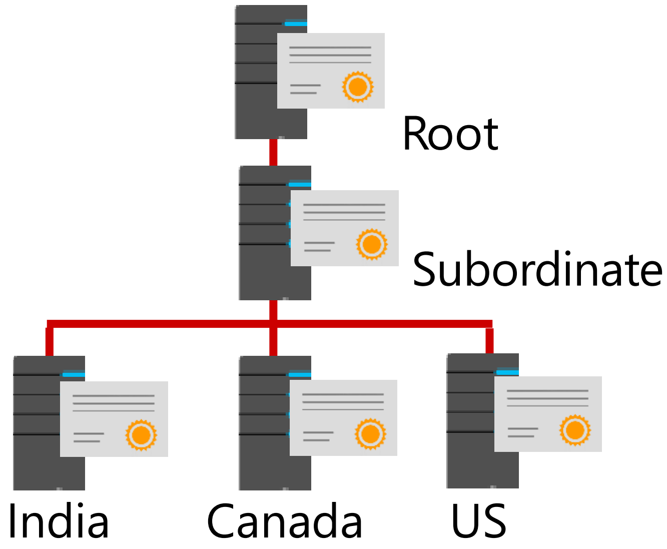
Subordinate

S/MIME

EFS

RAS

Certificate uses



Root

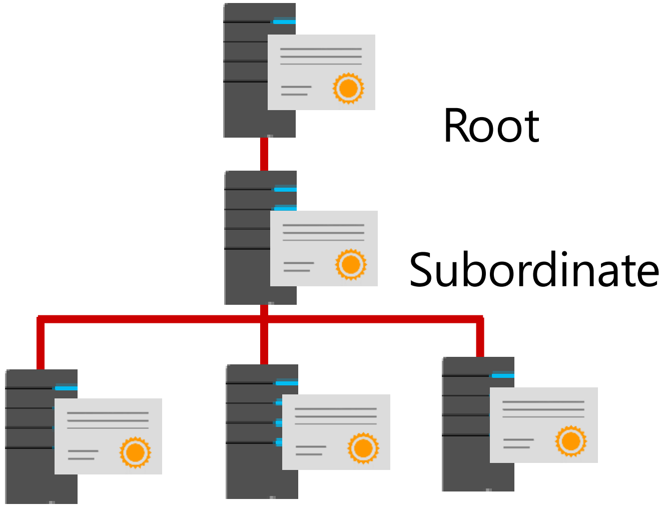
Subordinate

India

Canada

US

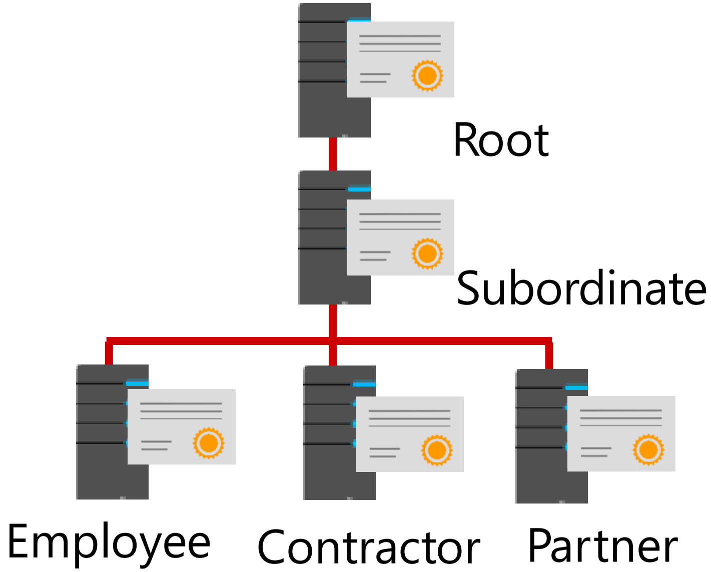
Locations



Root

Subordinate

Load Balancing



Root

Subordinate

Employee

Contractor

Partner

Organizational divisions

Managing CAs

- For managing CA hierarchy, you can use:
  - CA management console
  - Windows PowerShell
  - Certutil command-line tool
- Certutil provides an interface for advanced CA and PKI configuration and management
- PKI options are manageable through Group Policy, if you use the
- following:
  - Credential roaming
  - Autoenrollment of certificates
  - Certificate path validation
  - Certificate distribution

Configuring CA security

- You can assign the following permissions on a CA object:
  - Read
  - Issue and Manage Certificates
  - Manage CA
  - Request Certificates

- Security principals with the Issue and Manage Certificates permission can be restricted to a specific template
  - The Certificate Managers tab on the CA object properties

Security roles for CA administration

- Role-based administration:
    - Grant predefined CA permissions to a security group
    - Must be manually configured; roles are not automatically created
- Typical roles for AD CS might be:
    - CA Administrator
    - Certificate Manager
    - Backup Operator
    - Auditor
    - Enrollee
- Roles might be unique to each AD CS deployment

Configuring CA policy and exit modules

- The *policy module* determines the action that is performed after the certificate request is received
- The *exit module* determines what happens with a certificate after it is issued
- Each CA is configured with default policy and exit modules
- MIM 2016 Certificate Management deploys custom policy and exit modules
- The exit module can send email or publish a certificate to a file system
- You have to use certutil to specify these settings, because they are not available in the CA administrator console

Configuring CDPs and AIA locations

- The AIA specifies where to retrieve the CA's certificate
- The CDP specifies from where the CRL for a CA can be retrieved
- Publication locations for AIA and CDP:
  - AD DS (LDAP)
  - Web servers (HTTP)
  - FTP servers
  - File servers
- Ensure that you properly configure CRL and AIA locations for offline and standalone CAs
- Ensure that the CRL for an offline root CA does not expire

Renewing a CA certificate

- The CA certificate needs to be renewed when the validity period of the CA certificate is close to its expiration date
- The CA will never issue a certificate that has a longer validity time than its own certificate
- Considerations for renewing a root CA certificate:
  - Key length
  - Validity period
- Considerations for renewing a certificate for an issuing CA:
  - New key pair
  - Smaller CRLs
- Procedure for renewing a CA certificate

Unit 09

Deploying and managing certificates

elev8 LEARNING SOLUTIONS

What are certificates and certificate templates?

- A certificate contains information about users, devices, usage, validity, and a key pair
- A certificate template defines:
  - The format and contents of a certificate
  - The process for creating and submitting a valid certificate request
  - The security principals that are allowed to read, enroll, or use autoenrollment for a certificate that will be based on the template
  - The permissions that are required to modify a certificate template

Configuring certificate template permissions

Permission	Description
Full Control	Allows a designated user, group, or computer to modify all attributes—including ownership and permissions
Read	Allows a designated user, group, or computer to read the certificate in AD DS when enrolling
Write	Allows a designated user, group, or computer to modify all attributes except permissions
Enroll	Allows a designated user, group, or computer to enroll for the certificate template
Autoenroll	Allows a designated user, group, or computer to receive a certificate through the autoenrollment process

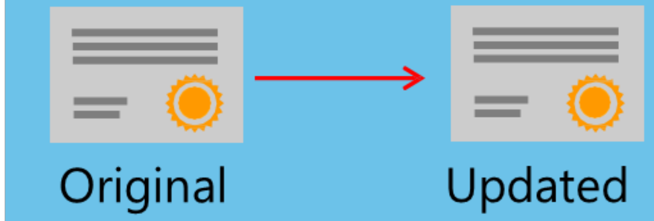
Configuring certificate template settings

- For each certificate template, you can customize several settings, such as validity time, purpose, CSP, private key exportability, and issuance requirements

Category	Example of single purpose	Example of multipurpose
Users	• Basic EFS • Authenticated session • Smart card sign-in	• Administrator • User • Smart card user
Computers	• Web server • IPsec	• Computer • Domain controller

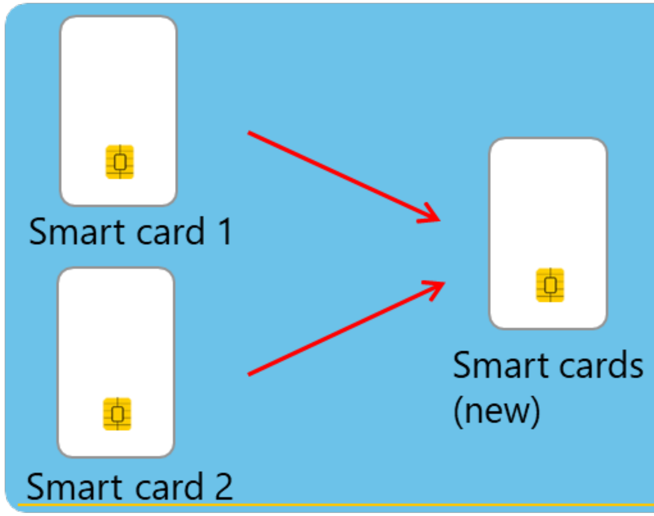
Options for updating a certificate template

Modifying



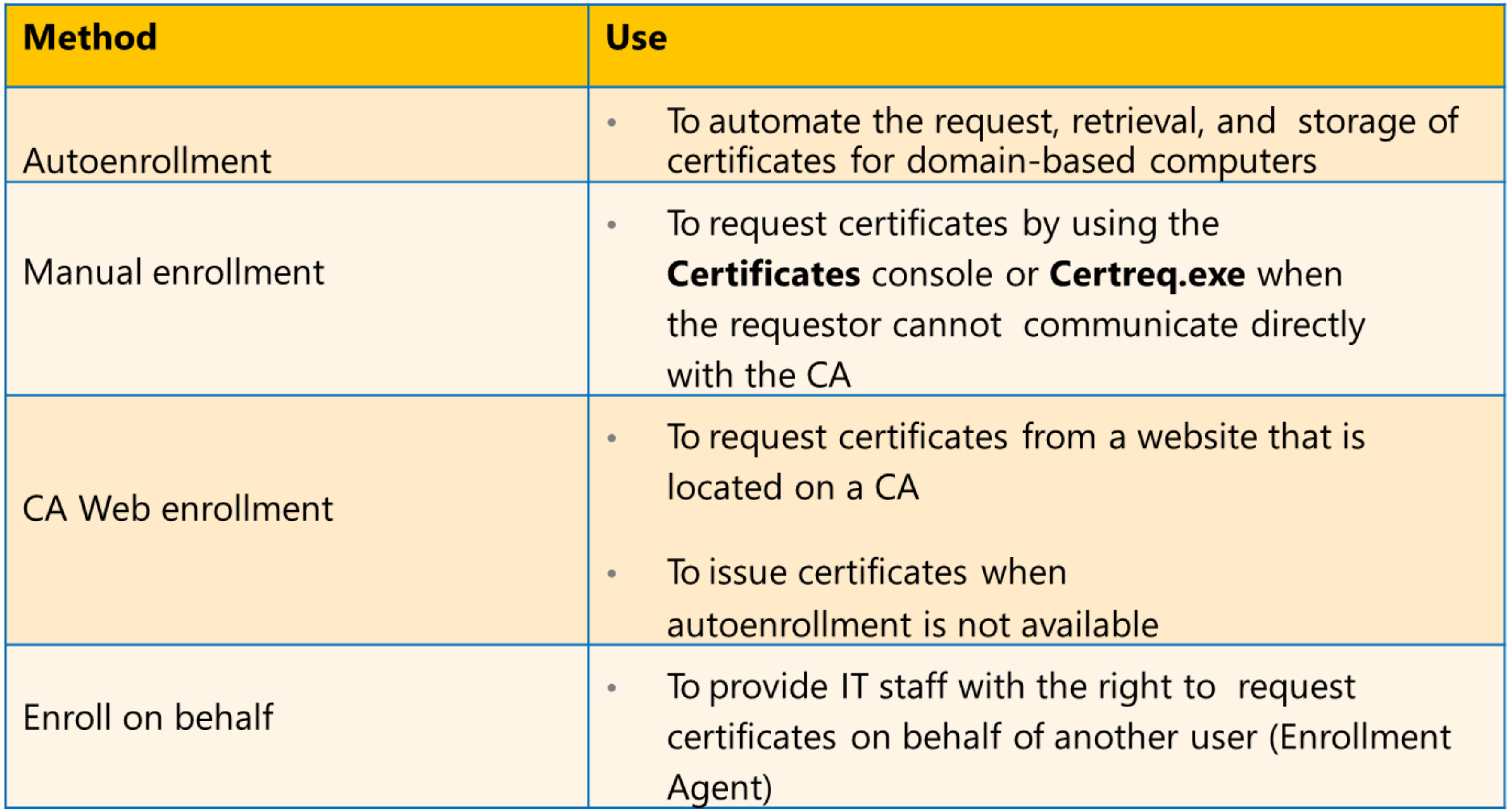
Modify the original certificate template to incorporate the new settings

Superseding



Replace one or more certificate templates with an upZdated certificate template

Certificate enrollment methods



Method	Use
Autoenrollment	- To automate the request, retrieval, and storage of certificates for domain-based computers
Manual enrollment	- To request certificates by using the **Certificates** console or **Certreq.exe** when the requestor cannot communicate directly with the CA
CA Web enrollment	- To request certificates from a website that is located on a CA - To issue certificates when autoenrollment is not available
Enroll on behalf	- To provide IT staff with the right to request certificates on behalf of another user (Enrollment Agent)

What is an enrollment agent?

- An Enrollment Agent is a user account used to request certificates on behalf of another user account
- An Enrollment Agent must possess a certificate based on the Enrollment Agent template
- Enrollment Agents are typically members of corporate or IT security departments
- You can limit the scope of an Enrollment Agent to:
- Specific users or security groups
- Specific certificate templates

How does certificate revocation work?

The following are steps in the certificate revocation lifecycle:

- A certificate is revoked
- A CRL is published
- A client computer verifies certificate validity and revocation

Using certificates for SSL

- The purpose of securing a connection with SSL is to protect data during communication
- For SSL, a certificate must be installed on the server
- Be aware of trust issues

SSL works in the following steps:

- The user types an HTTPS URL
- The web server sends its SSL certificate
- The client performs a check of the server certificate
- The client generates a symmetric encryption key
- The client encrypts this key with the server’s public key
- The server uses its private key to decrypt the encrypted symmetric key

Using certificates for digital signatures

Digital signatures ensure that:

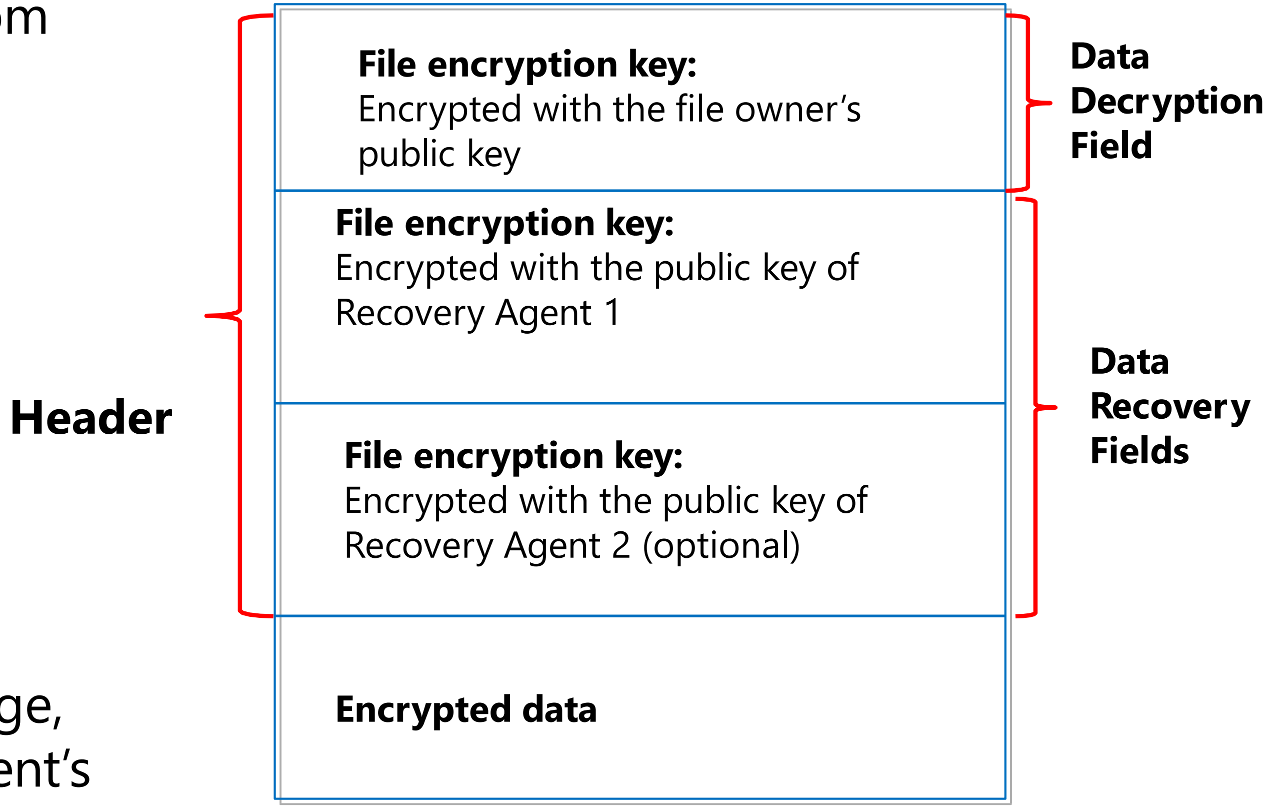
- Content is not modified during transport
- The identity of the author is verifiable

Digital signatures work in the following way:

- When an author digitally signs a document or a message, the operating system on his or her computer creates a message cryptographic digest
- The cryptographic digest is then encrypted by using the author’s
- private key and added to the end of the document or message
- The recipient uses the author’s public key to decrypt the cryptographic digest and compare it to the cryptographic digest created on the recipient’s computer
- Users need to have a certificate that is based on a User template to use digital signatures

Using certificates for content encryption

- Encryption protects data from unauthorized access
- EFS uses certificates for file encryption



Header

File encryption key:
Encrypted with the file owner's public key

File encryption key:
Encrypted with the public key of Recovery Agent 1

File encryption key:
Encrypted with the public key of Recovery Agent 2 (optional)

Encrypted data

Data Decryption Field

Data Recovery Fields

- To send an encrypted message, you must possess the recipient's public key

Using certificates for authentication

- You can use certificates for user and device authentication
- You can also use certificates in network and application access scenarios such as:
  - L2TP/IPsec VPN
  - EAP-TLS
  - PEAP
  - NAP with IPsec
  - Outlook Web App
  - Mobile device authentication

What is a smart card?

- A smart card is a miniature computer, with limited storage and processing capabilities, embedded in a plastic card about the size of a credit card

- Smart cards:
  - Provide options for multifactor authentication
  - Provide enhanced security over passwords

- You must use a valid smart card and PIN together

How does smart card authentication work?

Smart cards can be used for:

- Interactive sign in to AD DS
- Client authentication
- Remote sign-in
- Offline sign-in

What is a virtual smart card?

- A smart card infrastructure might be expensive
- Windows Server 2012 AD CS introduced virtual smart cards
- Virtual smart cards use the capabilities of the
- TPM chip
- No cost for buying smart cards and smart card readers
- The computer acts like a smart card
- The cryptographic capabilities of the TPM protect the private keys

Enrolling certificates for smart cards

- Before you issue smart cards, define the method of enrolling smart card certificates
- Smart card certificate enrollment requires some manual intervention
- For smart card enrollment:
- Define the certificate template for the smart cards
- Enroll one or more users for the Enrollment Agent certificate
- Configure the enrollment station
- Start the Enroll On Behalf Of wizard

- Ensure that users change their personal PINs

Smart card management

Smart card management tasks:

- Issuance
- Revocation
- Renewal
- Blocking and unblocking
- Duplication
- Suspension

Smart card management

Use MIM to:

- Issue smart cards to users
- Store information in a SQL database
- Manage revocation, renewal, unblocking, suspension, and reinstatement procedures
- Provide users and administrators with a web-based, self-service smart card management interface
- Manage smart card printing with appropriate hardware
- Implement workflows for each management task

Moving a root CA to another computer

To move a CA from one computer to another, you have to perform backup and restore:

  - To back up a computer, follow this procedure:

- Record the names of the certificate templates
- Back up a CA in the CA admin console
- Export the registry subkey
- Uninstall the CA role
- Confirm the %SystemRoot% folder locations
- Remove the old CA from the domain

Moving a root CA to another computer

To restore, follow this procedure:

- Install AD CS
- Use the existing private key
- Restore the registry file
- Restore the CA database and settings
- Restore the certificate templates

Monitoring CA operations

- For monitoring and maintenance of a CA hierarchy, you can use PKIView and CA auditing

With PKIView, you can:

- Access and manage PKI-related AD DS containers
- Monitor CAs and their health state
- Check the status of CA certificates
- Check the status of AIA locations
- Check the status of CRLs
- Check the status of CDPs
- Evaluate the state of the Online Responder
- CA auditing provides logging for various events that occur on the CA

Unit 10

Implementing and administering AD FS

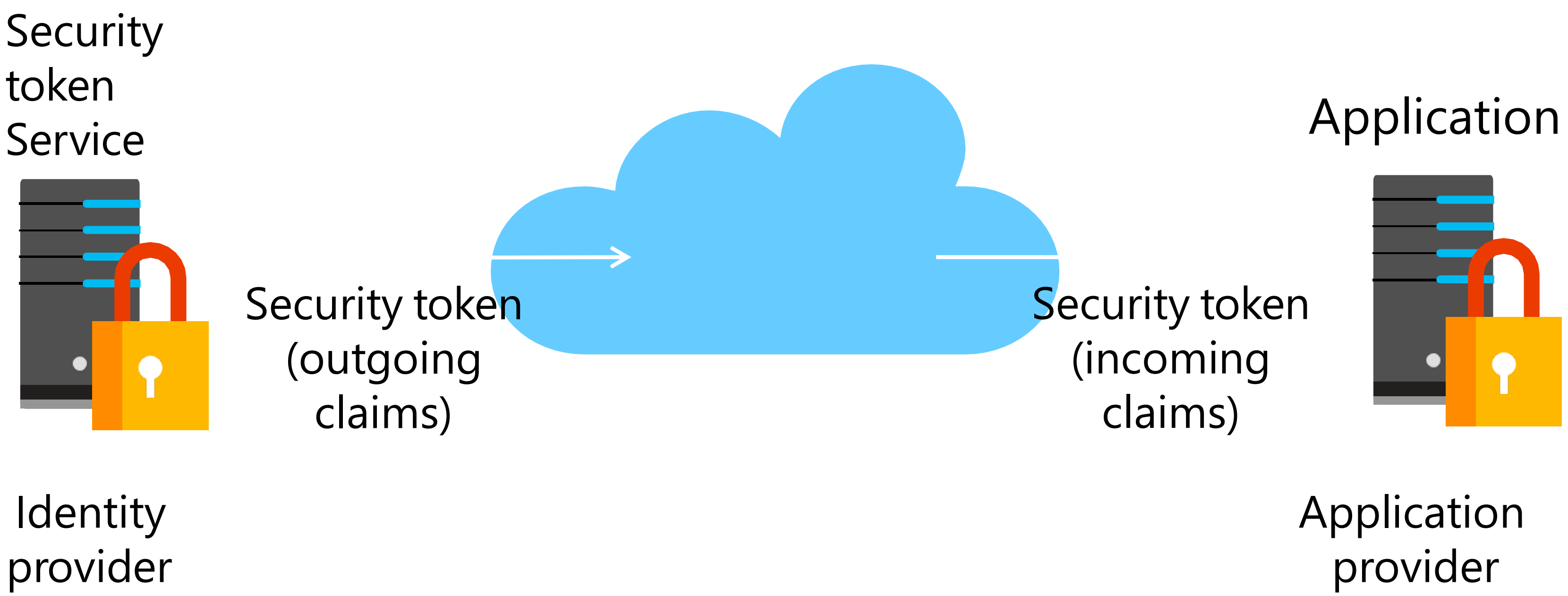
elev8 LEARNING SOLUTIONS

What is identity federation?

- Allows identification, authentication, and authorization across organizational and platform boundaries
- Requires a federated trust relationship between two organizations or entities
- Allows organizations to retain control over who can access resources
- Allows organizations to retain control of their user and group accounts

What are claims-based identity and claims-based authentication?

- Claims provide information about the users
- The users' identity provider supplies information that the application provider accepts



Overview of web services

Web services comprise a standardized set of specifications used to build applications and services

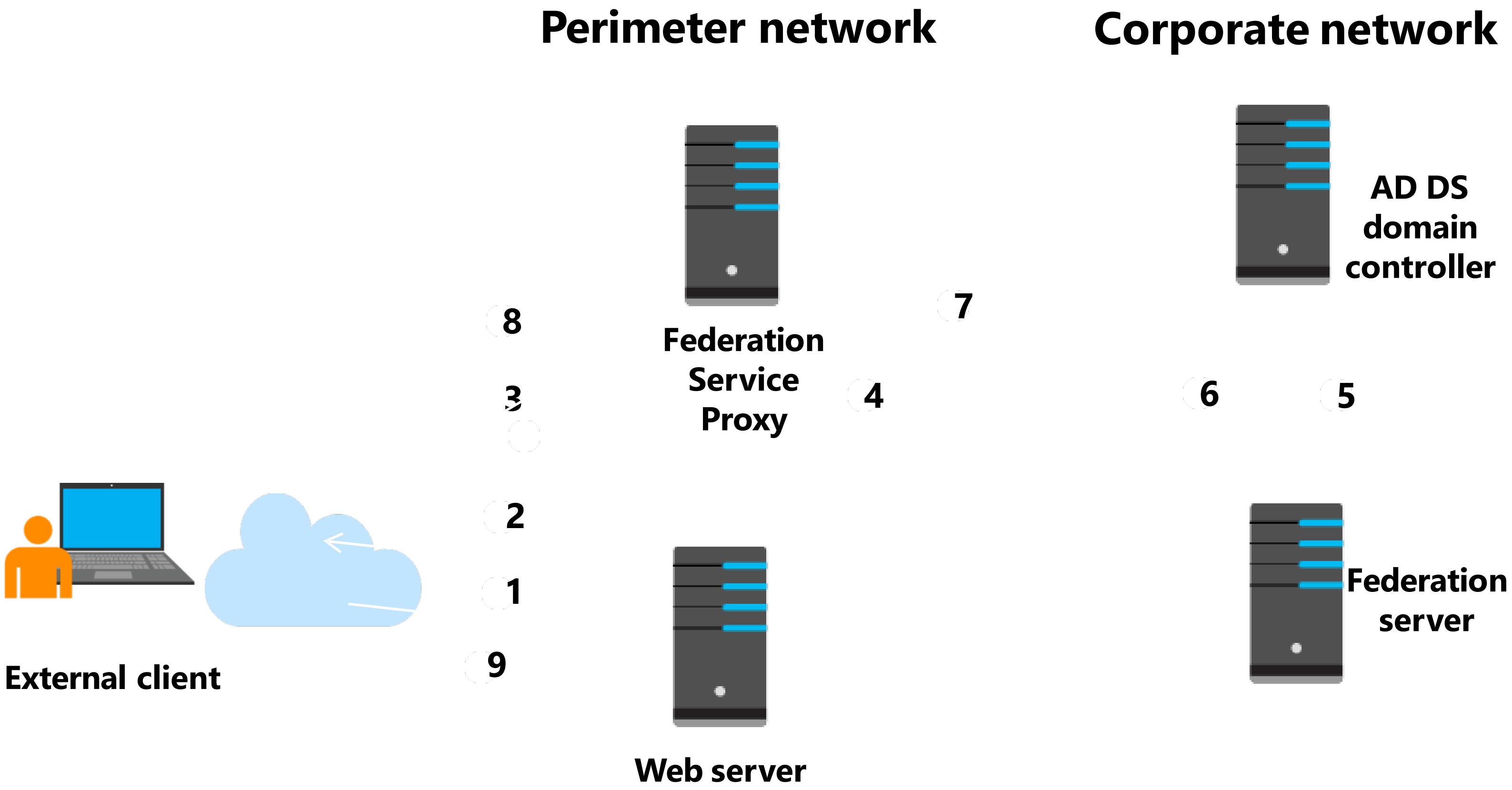
Web services typically:

- Transmit data as XML
- Use SOAP to define the XML message format
- Use WSDL to define valid SOAP messages
- Use UDDI to describe available web services
- SAML is a standard for exchanging identity claims

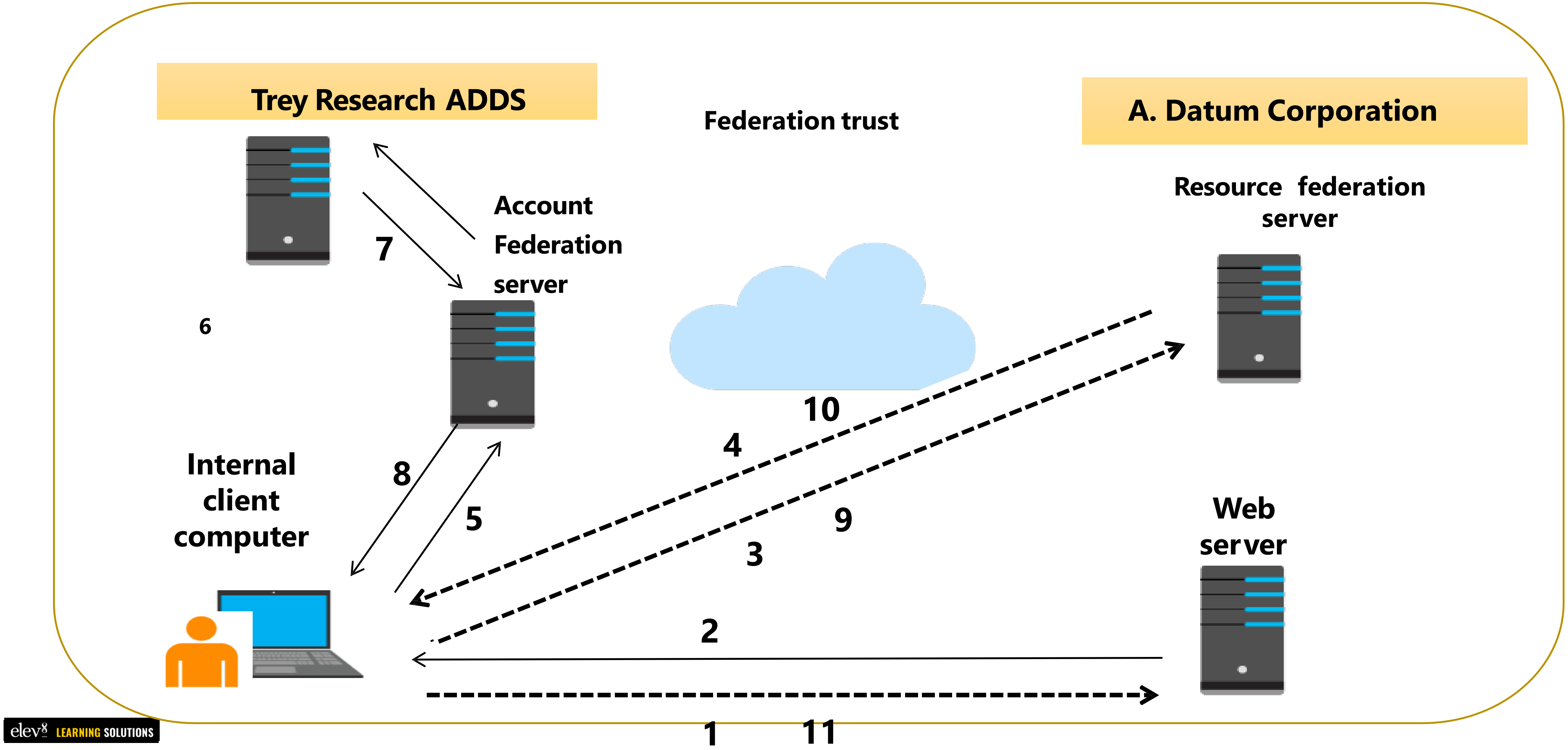
What is AD FS?

- AD FS is the Microsoft identity federation product that can use claims-based authentication
- AD FS has the following features:
- SSO for web-based apps
- Interoperability with web services on multiple platforms
- Support for many clients, such as web browsers, mobile devices, and applications
- Extensibility to support customized claims from third-
- party applications
- The Delegation of account management to the user’s
- organization

How AD FS enables SSO in a single organization



How AD FS enables SSO in a business-to-business federation



AD FS components

Federation server	Relying parties
Federation server proxy and Web Application Proxy	Claims provider trust
Claims	Relying party trust
Claim rules	Certificates
Attribute store	Endpoints
Claims providers	

AD FS requirements

A successful AD FS deployment includes the following critical infrastructure:

- TCP/IP network connectivity
- AD DS
- Attribute stores
- DNS

PKI and certificate requirements

AD FS uses the following certificates:

- Service communication certificates
- Token-signing certificates
- Token-decrypting certificates
- When choosing certificates, ensure that all federation partners and clients trust the service communication certificate

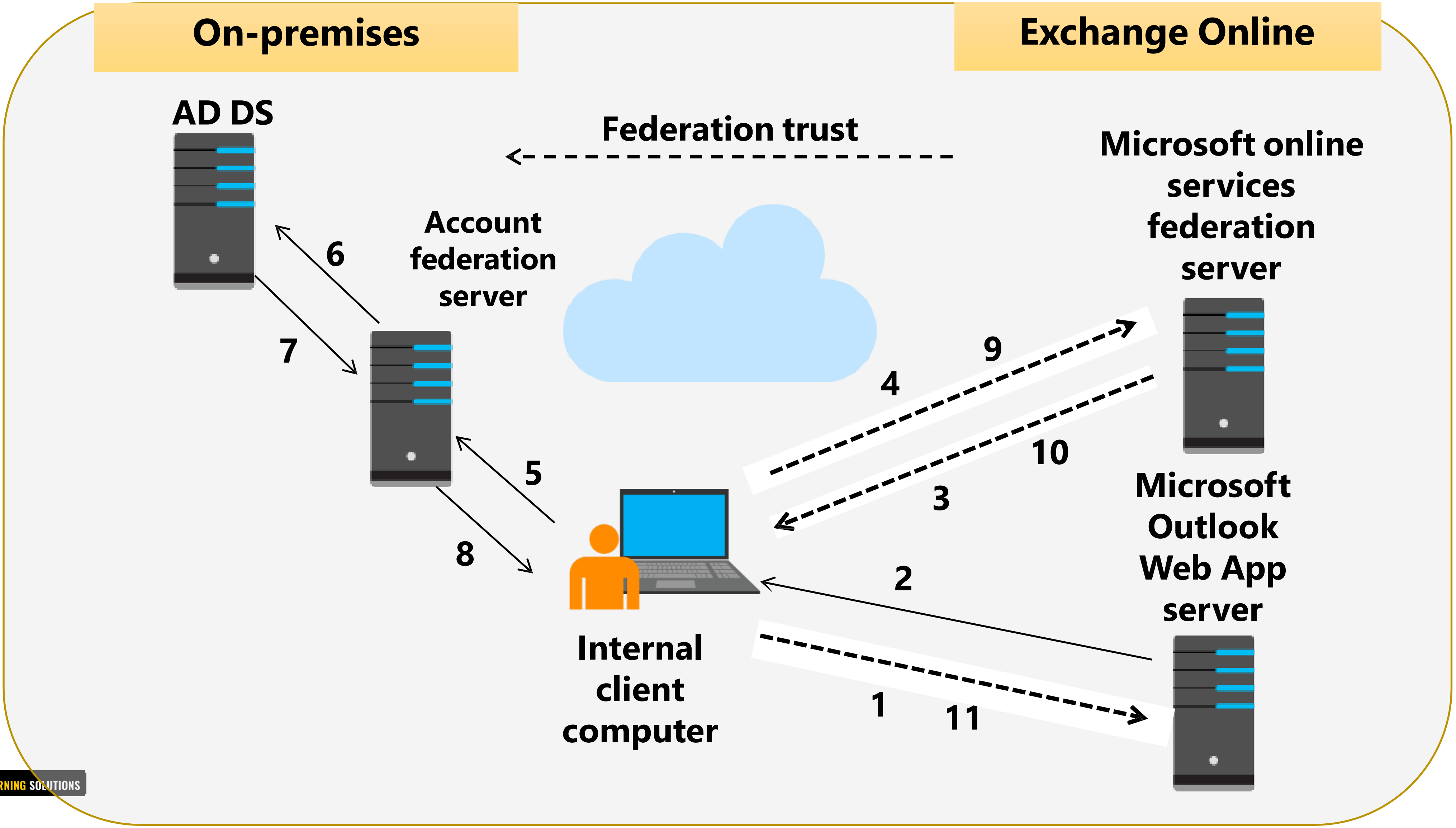
Federation server roles

- A claims provider federation server:
  - Authenticates internal users
  - Issues signed tokens containing user claims

- A relying party federation server:
  - Consumes tokens from the claims provider
  - Issues tokens for application access

- A Federation Service Proxy:
  - Gets deployed in a perimeter network
  - Provides a layer of security enhancement for internal federation servers

Planning an AD FS deployment for online services


On-premises
Exchange Online
AD DS
Federation trust
Microsoft online services federation server
Account federation server
6
7
4
9
10
3
5
8
2
1
11
Microsoft Outlook Web App server
Internal client computer

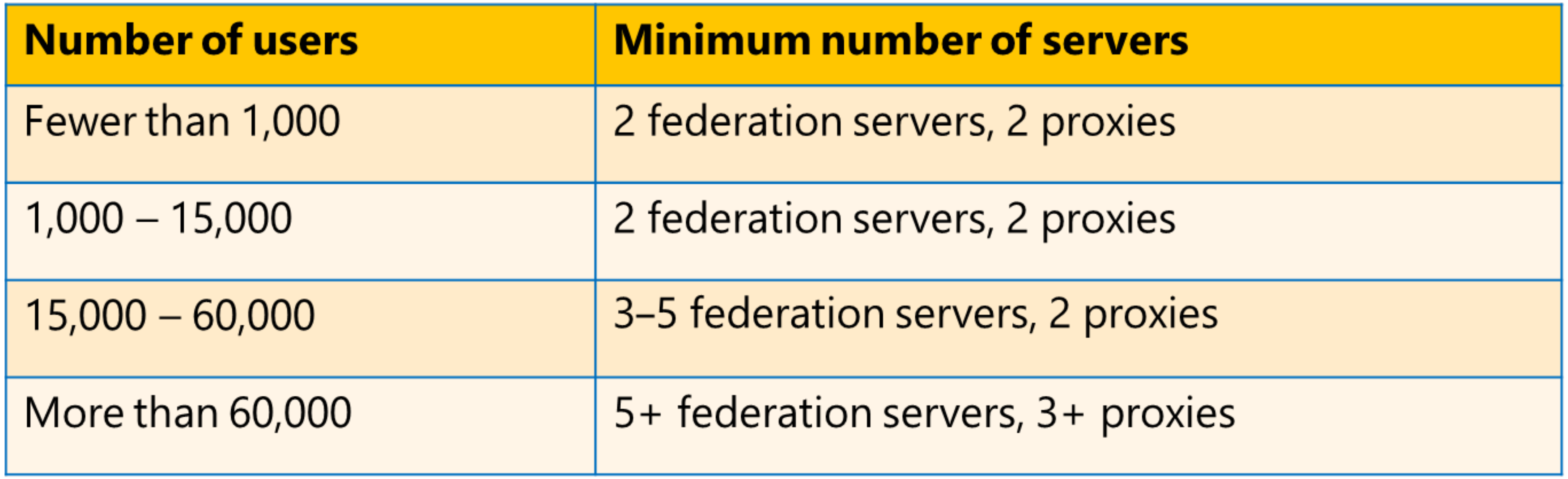
Deploying SSO integration with Microsoft online services

To configure SSO for integration with online services, you must:

- Prepare your environment for SSO
- Deploy federation services
- Deploy directory synchronization
- Verify SSO

Capacity planning

- Estimation table:



Number of users	Minimum number of servers
Fewer than 1,000	2 federation servers, 2 proxies
1,000 – 15,000	2 federation servers, 2 proxies
15,000 – 60,000	3–5 federation servers, 2 proxies
More than 60,000	5+ federation servers, 3+ proxies

What are AD FS claims and claim rules?

Claims provide information about users from the claims provider to the relying party

AD FS:

- Provides a default set of built- in claims
- Enables the creation of custom claims
- Requires each claim have a unique URI

Claims can be:

- Retrieved from an attribute store
- Calculated based on retrieved values
- Transformed into alternate values

What are AD FS claims and claim rules?

- Claim rules define how claims are sent and consumed by AD FS servers
- Claims provider rules are acceptance transform rules

Relying party rules can be:

- Issuance transform rules
- Issuance authorization rules
- Delegation authorization rules
- AD FS servers provide default claim rules, templates, and a syntax for creating custom claim rules

What is a claims provider trust?

- Claims provider trusts:
  - Are configured on the relying party federation server
  - Identify the claims provider
  - Configure the claim rules for the claims provider

- In a single-organization scenario, a claims provider trust called Active Directory defines how AD DS user credentials are processed

- You can configure claims provider trusts by:
  - Importing the federation metadata
  - Importing a configuration file
  - Configuring the trust manually

What is a relying party trust?

- Relying party trusts:
  - Are configured on the claims provider federation server
  - Identify the relying party
  - Configure the claim rules for the relying party

- In a single-organization scenario, a relying party trust defines the connection to internal applications

- You can configure relying party trusts by:
  - Importing the federation metadata
  - Importing a configuration file
  - Manually configuring the trust

Configuring an account partner and a resource partner

An account partner is a claims provider in a business-to-business federation scenario. To configure an account partner:

- Implement the physical topology
- Add an attribute store
- Configure a relying party trust
- Add a claim description
- Prepare the client computers for federation

A resource partner is a relying party in a business-to-business federation scenario. To configure a relying partner:

- Implement the physical topology
- Add an attribute store
- Configure a claims provider trust
- Create claim rule sets for the claims provider trust

Managing an AD FS deployment

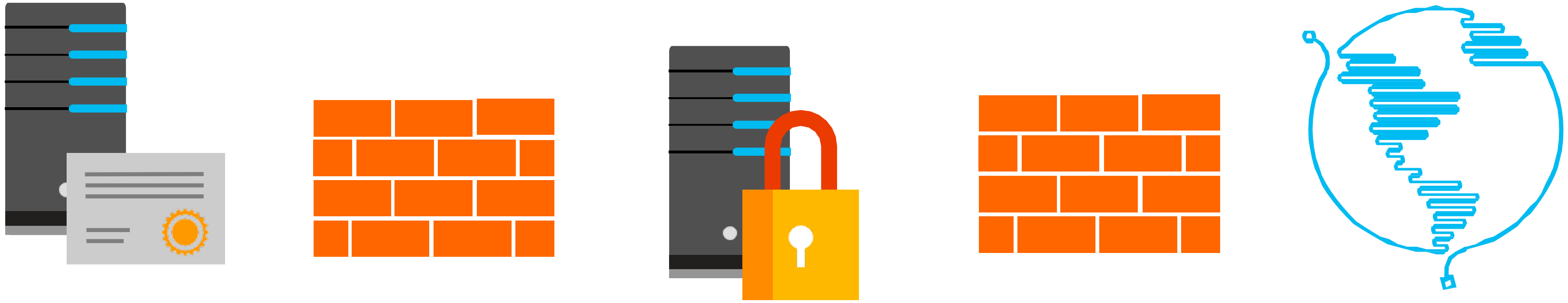
- After the installation, you might need to perform periodic AD FS management tasks, including:
- Managing the certificate life cycle
- Using automatic certificate rollover, which renews AD FS certificates once a year
- Using the Get-ADFSCertificate cmdlet to view certificate expiration dates
- Using the Update-MsolFederatedDomain cmdlet to manage certificate rollover when the AD FS token-signing certificate renews on an annual basis
- Using the Set-AdfsSyncProperties cmdlet to change the primary and secondary AD FS federation servers

What is the Web Application Proxy?

- Windows Server 2016 includes several improvements to the Web Application Proxy role, including:
- Preauthentication for HTTP Basic app publishing
- Wildcard domain publishing of apps
- HTTP to HTTPS redirection
- HTTP publishing

Web Application Proxy and AD FS proxy

- The Web Application Proxy is an AD FS proxy
- The same certificate is used on the AD FS server and the Web Application Proxy
- Split DNS allows the same name to resolve to different IP addresses



AD FS server
adfs.adatum.com
172.16.0.21

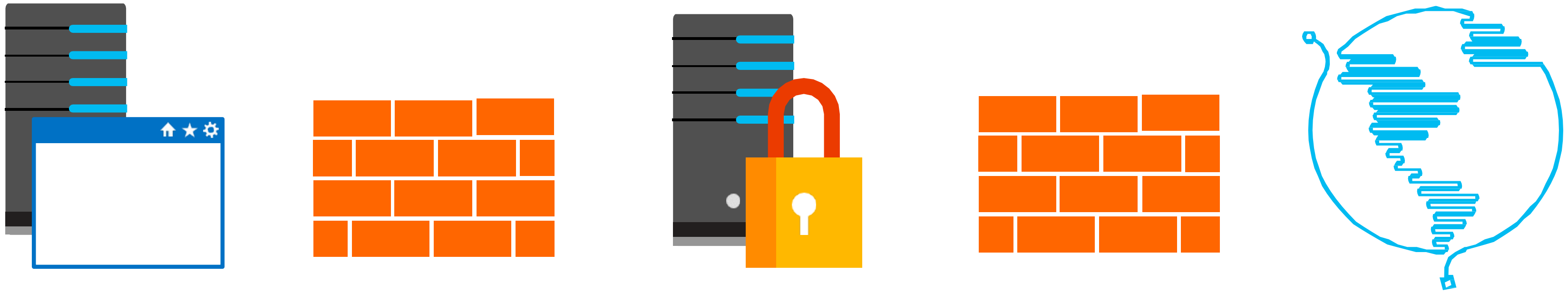
Web Application Proxy
adfs.adatum.com
10.10.0.100

Internet

Web Application Proxy authentication methods

Preauthentication types:

- AD FS
- Pass-through



Intranet application

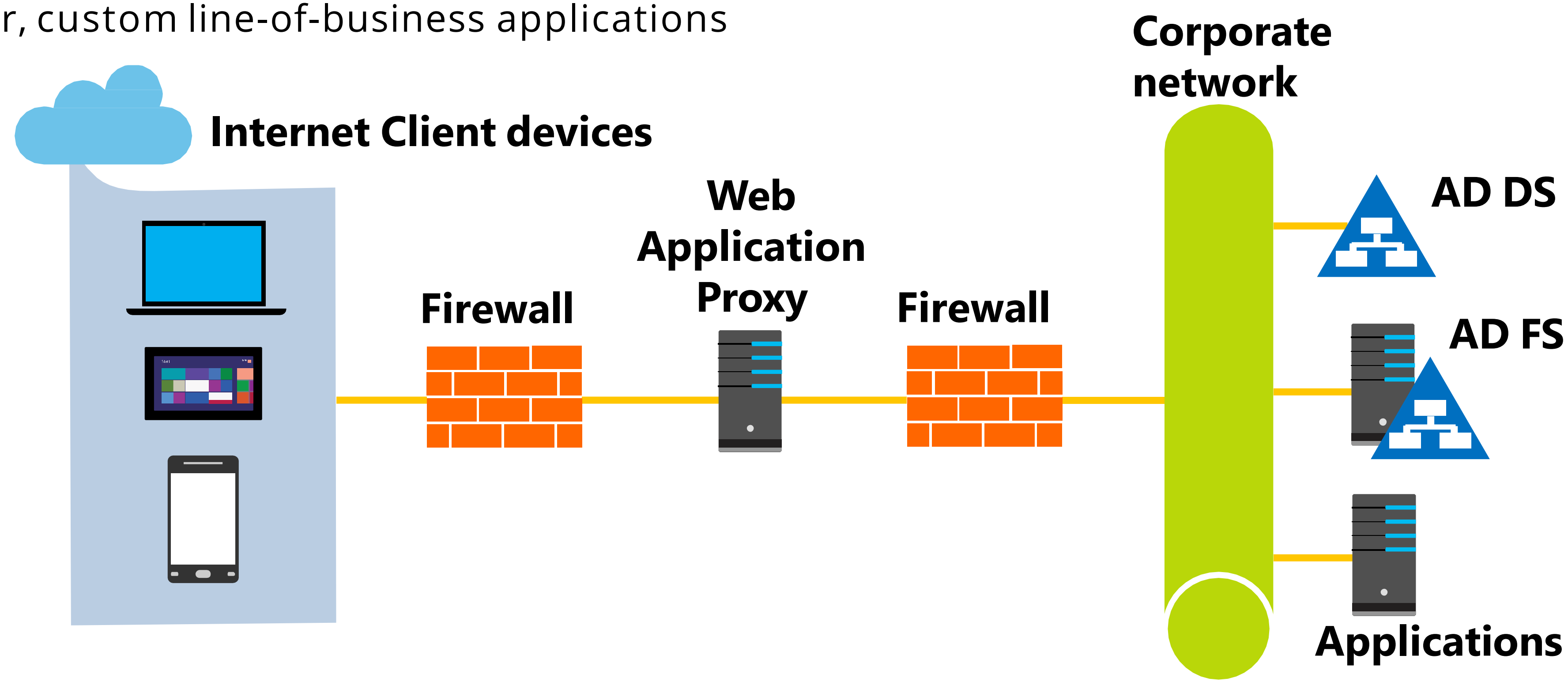
Web Application Proxy

Internet

Scenarios for using the Web Application Proxy

You can use the Web Application Proxy to publish:

- SharePoint services
- Exchange services
- Remote Desktop Gateway services
- Other, custom line-of-business applications



Installing and configuring the Web Application Proxy

You might need to prepare the following items before installing the Web Application Proxy

- Load balancing
- DNS

During the deployment of the Web Application Proxy, you will:

- Install the Web Application Proxy
    - Configure the Web Application Proxy
    - Update the Web Application Proxy

Unit 11

Implementing AD DS synchronization with Microsoft Azure AD

elev8 LEARNING SOLUTIONS

Extending the scope of AD DS

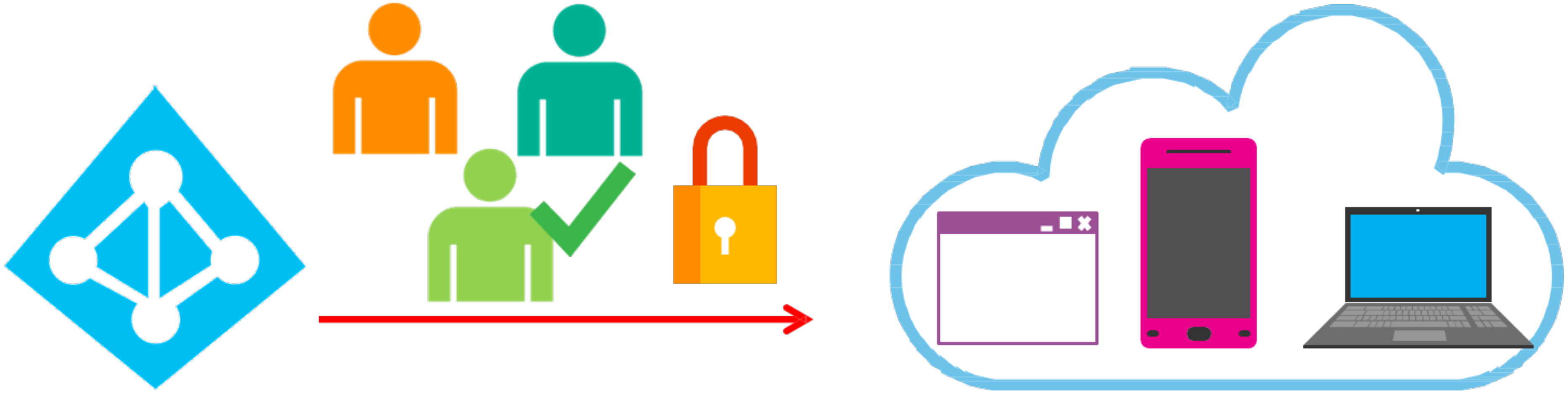
AD DS was designed primarily for on-premises deployments, so its limitations are that it:

- Has a single tenant by design
- Employs protocols not suited for Internet communication
- Requires domain-joined computers to deliver full functionality
- You can install AD DS domain controllers on Azure virtual machines

Extending the scope of AD DS

You can use AD DS to provide authentication and authorization for cloud-based services and mobile devices by using:

- AD FS and Web Application Proxy
- Azure AD Device Registration
- Federation support



Azure AD as an authentication system

Key differences between Azure AD and AD DS:

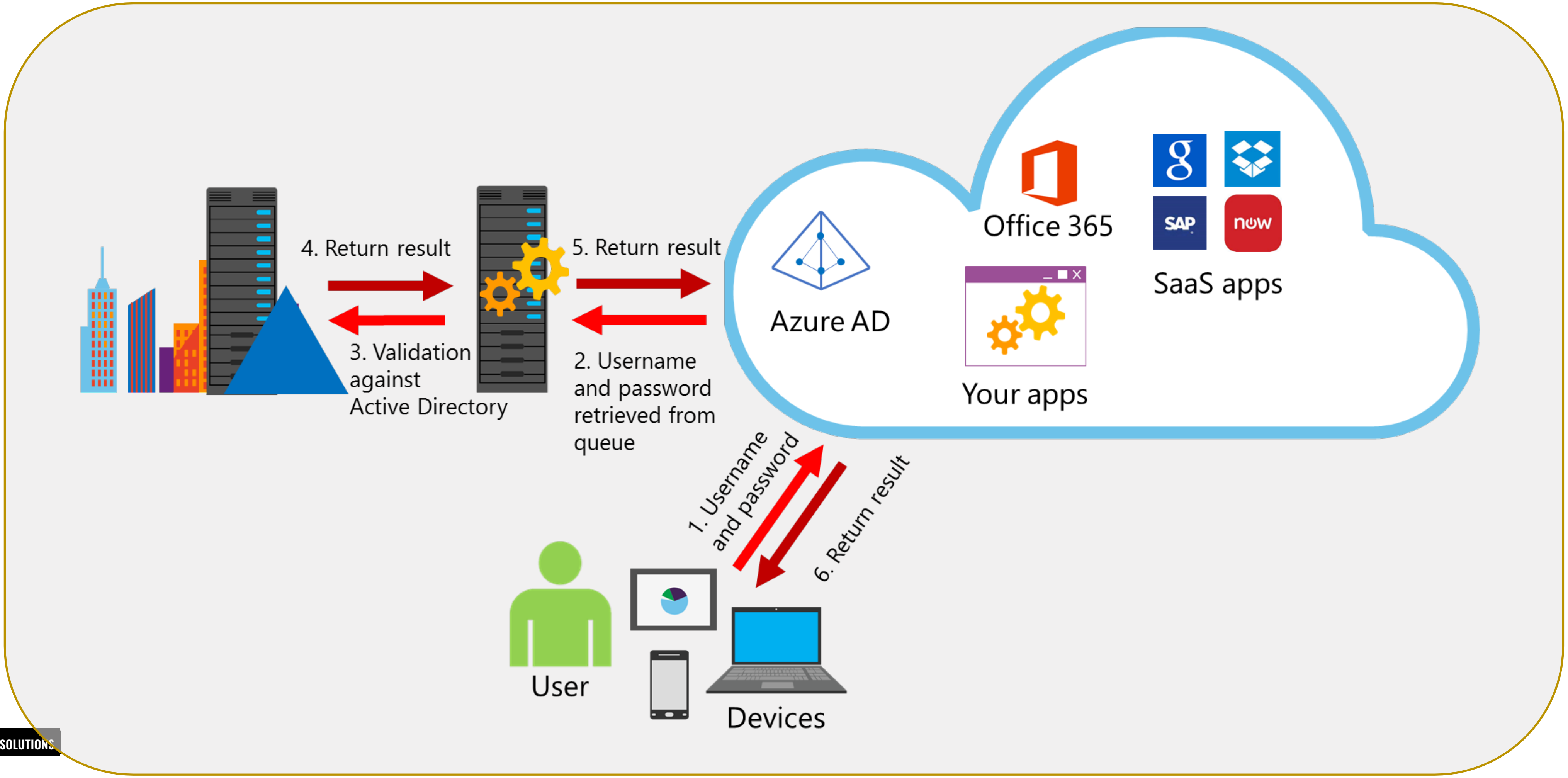
- Azure AD is designed for Internet-based applications
- In Azure AD, there are no OUs or GPOs
- Azure AD cannot be queried through LDAP
- Azure AD does not use Kerberos authentication
- Azure AD includes federation services

Azure AD authentication options

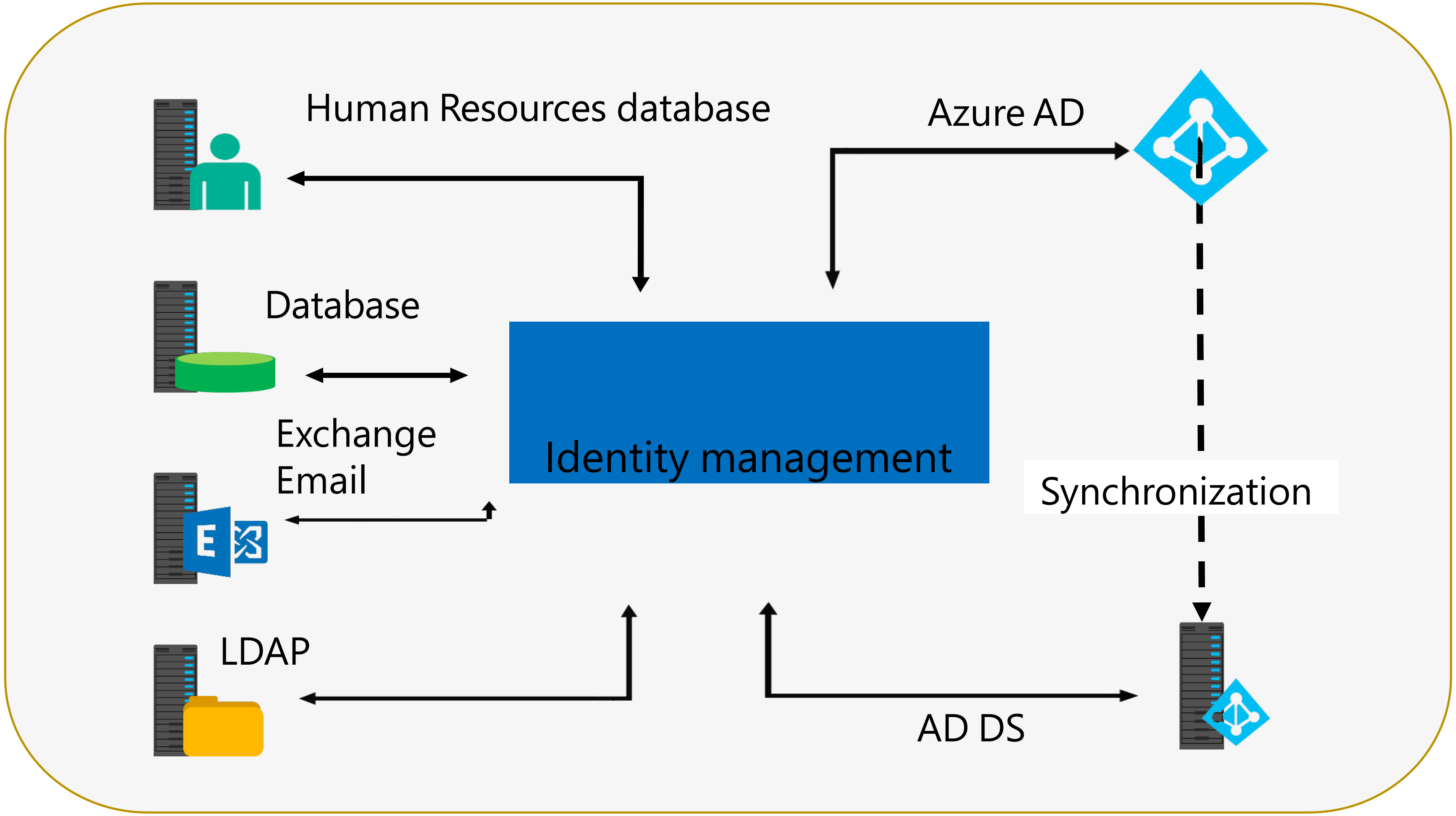
Cloud identity	Synchronized identity	Federated identity
Azure AD	Azure AD	Azure AD
	Azure AD Connect and password sync	Azure AD Connect Federation
	AD DS	AD DS
Independent cloud identity	Single identity, enabling the same sign-on experience with password hash synchronization	Single federated identity, enabling SSO in some scenarios and additional flexibility

Azure AD pass-through authentication

- Azure AD pass-through authentication enables you to centralize authentication for both on-premises and cloud resources without deploying AD FS



Overview of directory synchronization



Planning directory synchronization

- Best practices for deploying directory synchronization:
- Have a proper project plan
- If AD DS filtering is used, configure it before synchronizing objects to Azure AD
- Work with a Microsoft certified cloud solution provider
- Perform thorough capacity planning
- Remediate AD DS before deploying directory synchronization
- Add all SMTP domains as verified domains before synchronizing

Prerequisites and preparation for directory synchronization

When reviewing the prerequisites for directory synchronization, your tasks should include:

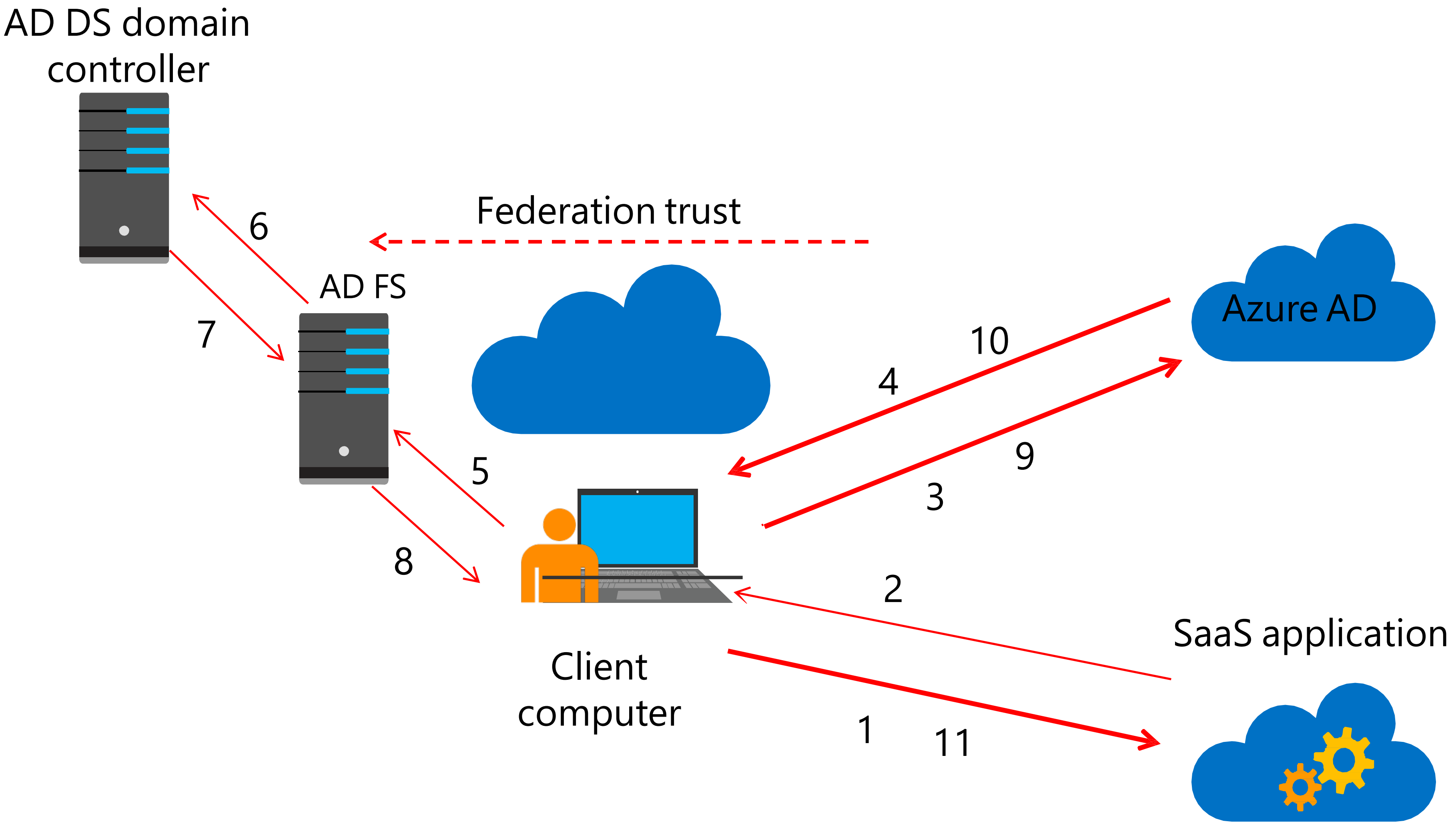
- Capacity planning for your directory synchronization database server
- Identifying the hardware requirements for your directory synchronization computer
- Identifying whether your environment exceeds the Azure AD object quota
- Reviewing the network ports required by directory synchronization
- Determining if any schema extensions to AD DS are required

Configuring a tenant for directory synchronization

To enable Active Directory synchronization by using the Azure portal:

- In the Azure portal, click Azure Active Directory.
- In the list of options, click Azure AD Connect.
- Select desired authentication option.

AD FS and Azure AD



Overview of Azure AD Connect

When you use Azure AD Connect for directory synchronization:

- New user, group, and contact objects in on-premises
- AD DS are added to Azure AD
- Attributes of existing user, group, or contact objects that are modified in on-premises AD DS are modified in Azure AD
- Existing user, group, and contact objects that are deleted from on-premises AD DS are deleted from Azure AD
- Existing user objects that are disabled on-premises are disabled in Azure AD

Azure AD Connect requirements

When you identify the Azure AD Connect requirements, you should review:

- Azure AD requirements
- Domain and forest requirements
- Operating system and supporting software requirements
- Permissions and accounts
- Database requirements

Azure AD Connect express synchronization

Scenarios for using the express settings include:

- You have a single AD DS forest
- Users sign in with the same password by using passwords synchronization

Installing Azure AD Connect with express settings:

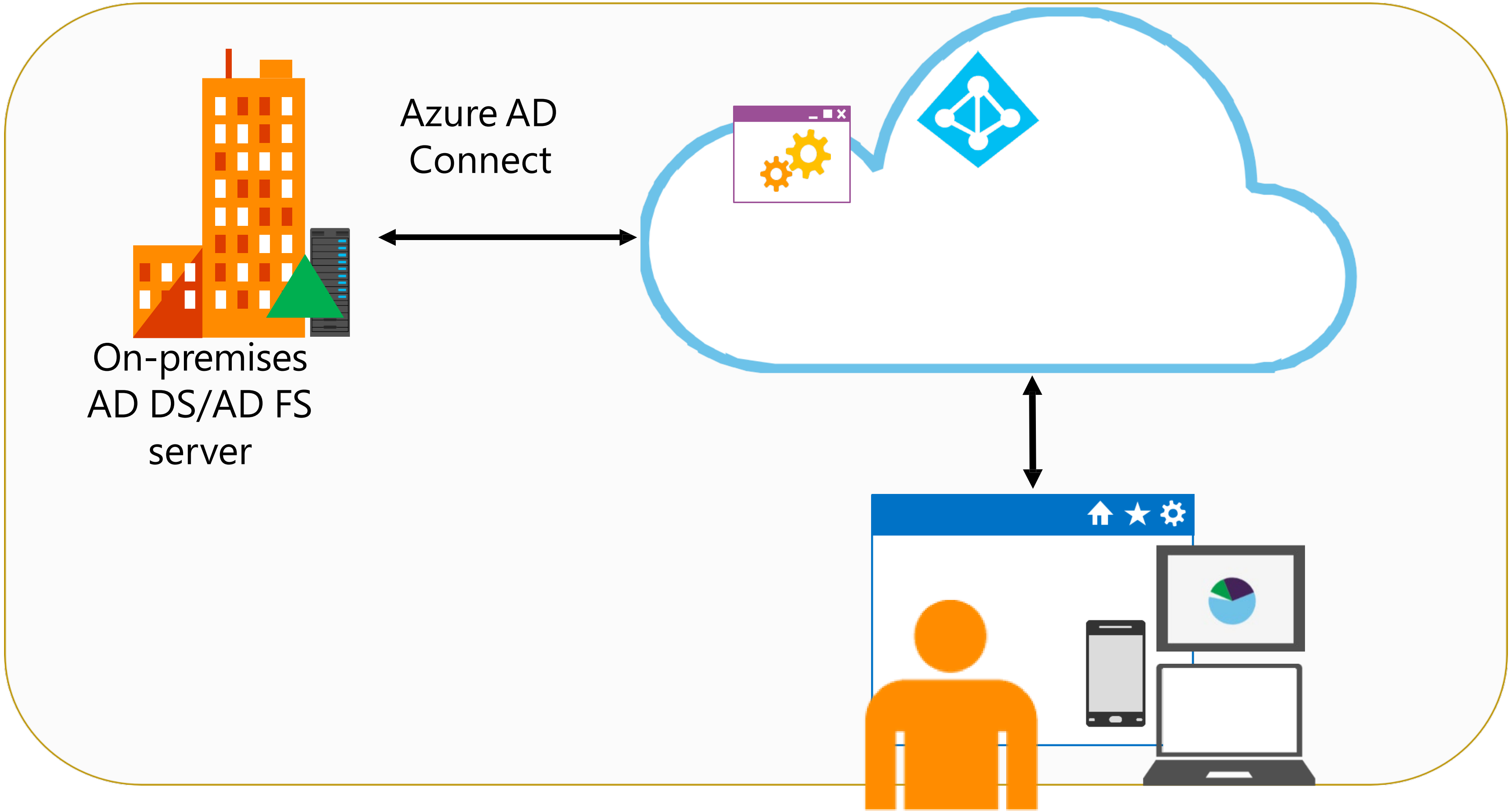
- Installs the synchronization engine
- Configures Azure AD Connector
- Configures the on-premises AD DS connector
- Enables password synchronization
- Configures synchronization

Azure AD Connect customized synchronization

You can select customized settings for the following scenarios:

- When you have multiple forests
- When you customize your sign-in option, such as AD FS for federation, or use a non-Microsoft identity provider
- When you customize synchronization features, such as filtering and writeback

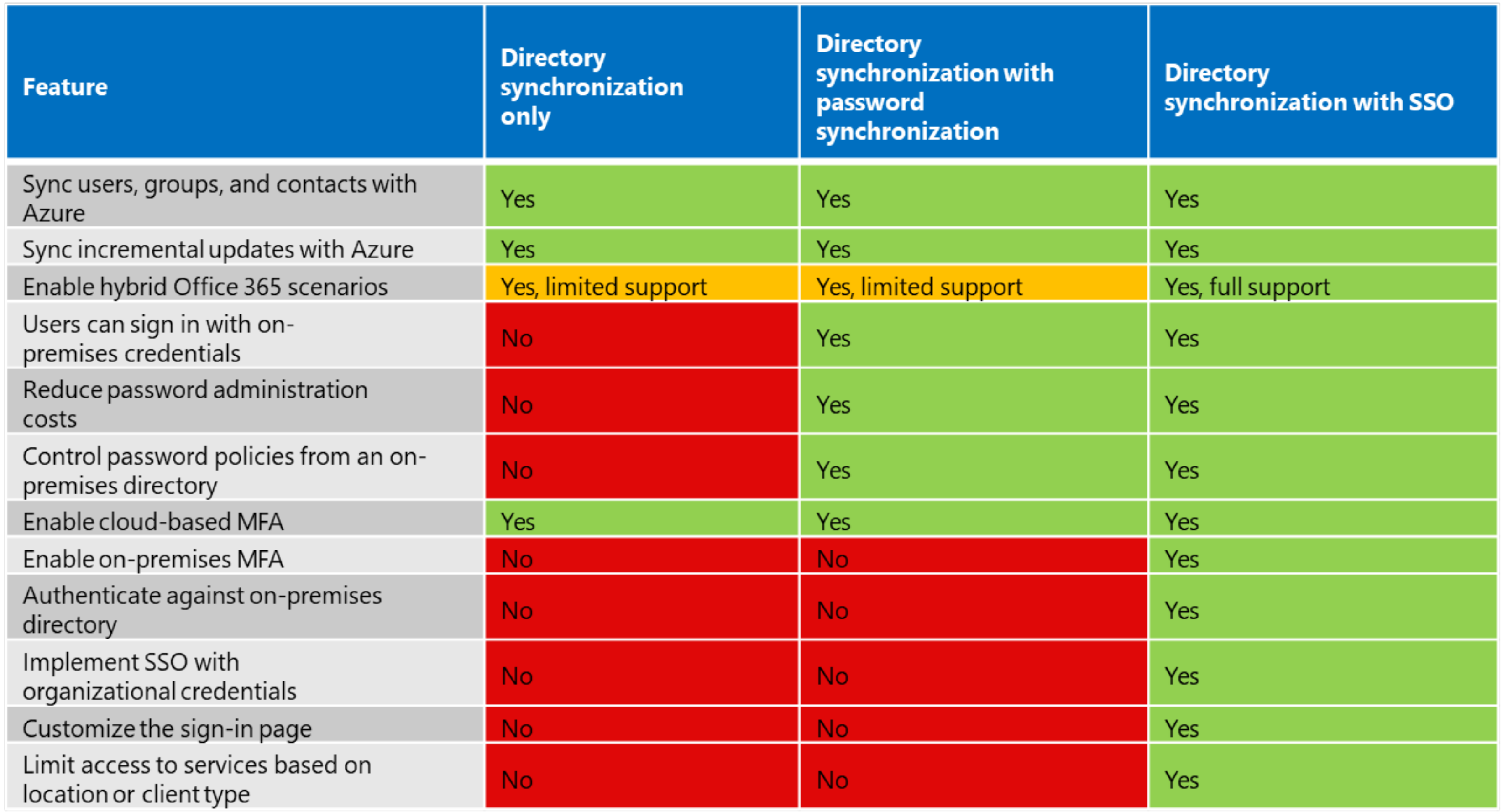
Azure AD Connect monitoring features



Azure AD Privileged Identity Management

- Azure AD Privileged Identity Management allows you to:
- Discover which users are the Azure AD administrators
- Enable on-demand, just-in-time administrative access to directory resources
- Get reports about administrator access history and the changes in administrator assignments
- Get alerts about access to a privileged role

Comparing options for identity synchronization



Feature	Directory synchronization only	Directory synchronization with password synchronization	Directory synchronization with SSO
Sync users, groups, and contacts with Azure	Yes	Yes	Yes
Sync incremental updates with Azure	Yes	Yes	Yes
Enable hybrid Office 365 scenarios	Yes, limited support	Yes, limited support	Yes, full support
Users can sign in with on-premises credentials	No	Yes	Yes
Reduce password administration costs	No	Yes	Yes
Control password policies from an on-premises directory	No	Yes	Yes
Enable cloud-based MFA	Yes	Yes	Yes
Enable on-premises MFA	No	No	Yes
Authenticate against on-premises directory	No	No	Yes
Implement SSO with organizational credentials	No	No	Yes
Customize the sign-in page	No	No	Yes
Limit access to services based on location or client type	No	No	Yes

Managing users with directory synchronization

- After you deploy Azure AD Connect successfully and enable scheduled synchronization, perform these required management tasks to ensure users synchronize efficiently:
- User writeback
- Password writeback
- Device writeback
- Primary SMTP address management
- Recovery from accidental deletions
- Recovery from unsynchronized deletions
- Accidental account deletion
- Bulk activation of new accounts

Managing groups with directory synchronization

- The group writeback feature writes groups from Azure AD to on- premises AD DS
- The cmdlet Initialize-ADSyncGroupWriteBack prepares AD DS automatically for group writeback
- The OU where on-premises AD DS stores the cloud groups is $groupOU
- Groups from Azure AD are represented as distribution groups in on-premises AD DS
- An Azure AD Premium license is required if you enable a group writeback without the Exchange Server hybrid writeback feature

Modifying directory synchronization

- Filtering configuration types that you apply to Azure AD Connect include:

Domain:

- Allows you to select which AD DS domains are allowed to synchronize to Azure AD
- Uses Azure AD Connect or Synchronization Service Manager

OU:

- Allows you to select which OUs in AD DS are allowed to synchronize to Azure AD
- Uses Azure AD Connect or Synchronization Service Manager

Attribute:

- Allows you to control which objects in AD DS should synchronize to the Azure AD based on criteria of the objects' attributes
- Uses Synchronization Rules Editor

Monitoring directory synchronization

Tools to monitor directory synchronization:

- Operations Manager—use the System Center Management Pack for Azure
- The Azure portal
- Windows PowerShell
- Synchronization Service Manager
- Event logs

Troubleshooting directory synchronization

Troubleshooting tasks for directory synchronization include:

- Analyzing logs for errors
- Remediating synchronization errors with the tool

Typical issues that can lead to problems include:

- Installation errors, such as using incorrect on-premises or Azure AD credentials
- Inadvertently deactivating directory synchronization in the Azure
- portal or through Windows PowerShell
- Unexpected changes in AD DS that affect OU scoping or attribute filtering
- Corrupted AD DS requiring directory recovery

Unit 12

Monitoring, managing, and recovering AD DS

Understanding performance and bottlenecks

A bottleneck is a resource that is currently at peak utilization Key system resources:

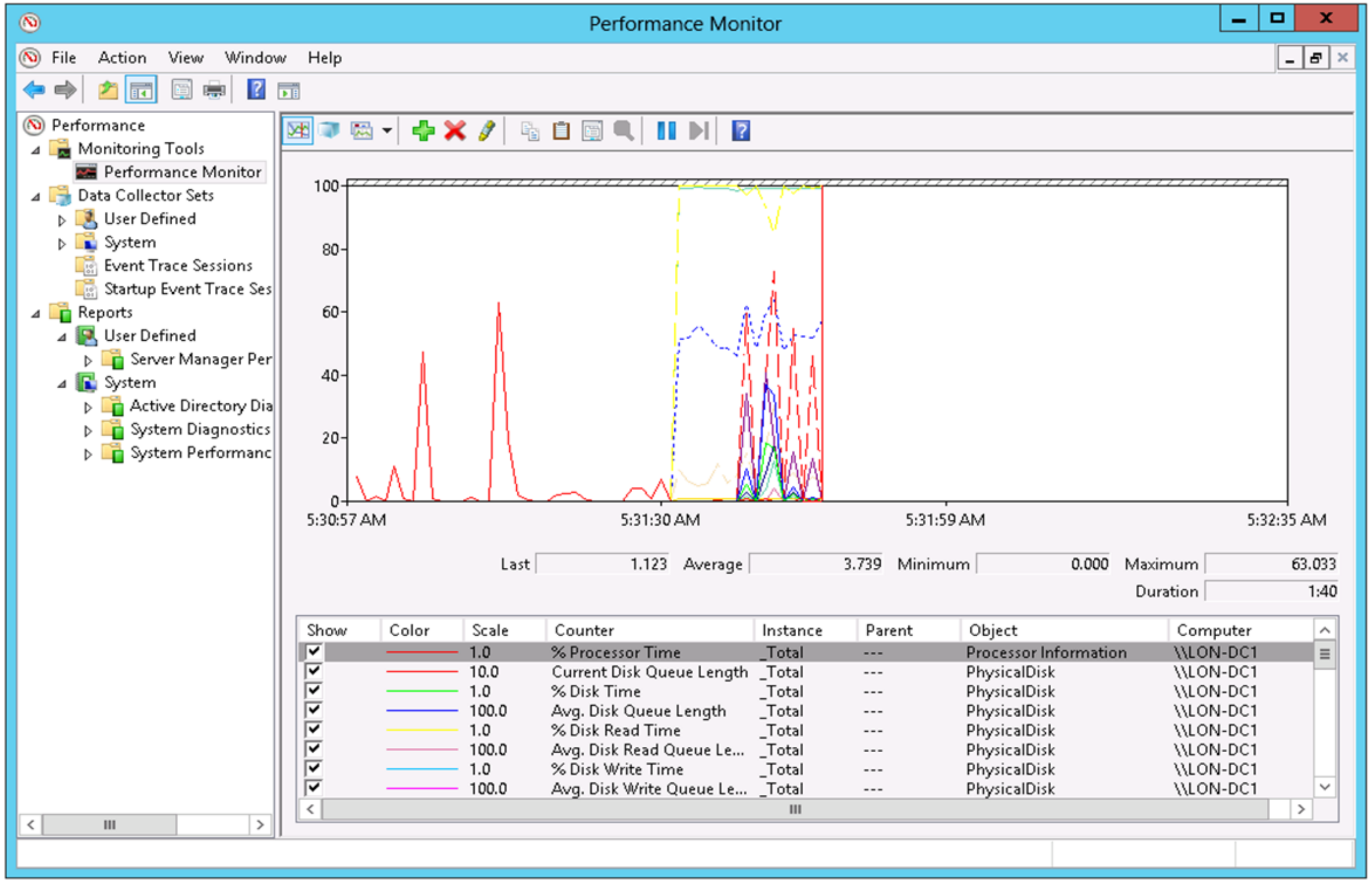
- CPU
- Disk
- Memory
- Network

Overview of monitoring tools

Windows Server provides the following tools to help with monitoring performance issues:

- Task Manager
- Resource Monitor
- Event Viewer
- Performance Monitor
- Windows PowerShell

What is Performance Monitor?



Last 1.123 Average 3.739 Minimum 0.000 Maximum 63.033

Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	🟥	1.0	% Processor Time	_Total	---	Processor Information	\\LON-DC1
☑	🟥	10.0	Current Disk Queue Length	_Total	---	PhysicalDisk	\\LON-DC1
☑	🟩	1.0	% Disk Time	_Total	---	PhysicalDisk	\\LON-DC1
☑	🟦	100.0	Avg. Disk Queue Length	_Total	---	PhysicalDisk	\\LON-DC1
☑	🟨	1.0	% Disk Read Time	_Total	---	PhysicalDisk	\\LON-DC1
☑	🟪	100.0	Avg. Disk Read Queue Le...	_Total	---	PhysicalDisk	\\LON-DC1
☑	🟦	1.0	% Disk Write Time	_Total	---	PhysicalDisk	\\LON-DC1
☑	🟪	100.0	Avg. Disk Write Queue Le...	_Total	---	PhysicalDisk	\\LON-DC1

What is Performance Monitor?

- You can use Performance Monitor to view current performance statistics or historical data gathered by using data collector sets
- Important performance counters include:
- CPU
- Memory
- Disk
- Network

What is Performance Monitor?

- Important performance counters include:
- AD DS:
- NTDS\ DRA Inbound Bytes Total/sec
- NTDS\ DRA Inbound Object
- NTDS\ DRA Outbound Bytes Total/sec
- NTDS\ DRA Pending Replication Synchronizations
- Security System-Wide Statistics\ Kerberos Authentications/sec
- Security System-Wide Statistics\ NTLM Authentications

What are data collector sets?

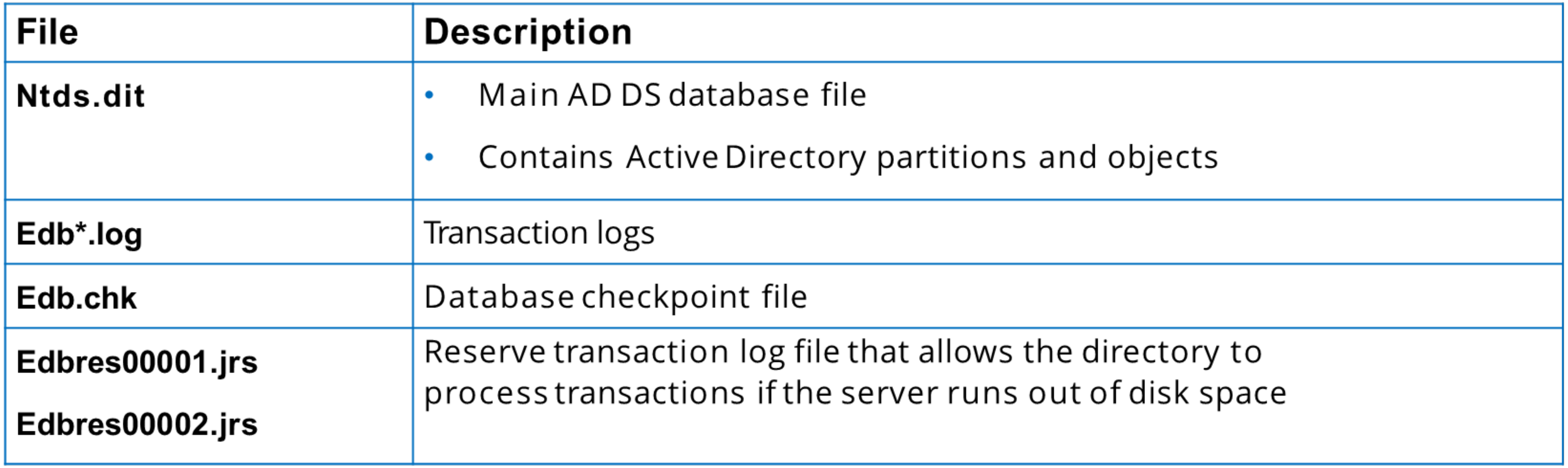
- You can use data collector sets to gather performance-related information
- Data collector sets can contain the following types of data collectors:
- Performance counters
- Event trace data
- System configuration information

Overview of the AD DS database

- The directory database stores Active Directory information
- Four Active Directory partitions on each domain controller are: domain,
- configuration, schema, and application (optional)

Overview of the AD DS database

- File-level components of the AD DS database are:



File	Description
Ntds.dit	• Main AD DS database file • Contains Active Directory partitions and objects
Edb*.log	Transaction logs
Edb.chk	Database checkpoint file
Edbres00001.jrs Edbres00002.jrs	Reserve transaction log file that allows the directory to process transactions if the server runs out of disk space

What is NtdsUtil?

- You can use NtdsUtil to:
- Manage and control single-master operations
- Perform Active Directory database maintenance:
- Perform offline defragmentation
- Create and mount snapshots
- Move database files

What is NtdsUtil?

- Clean domain-controller metadata:
- Domain-controller removal or demotion while not connected to a domain
- Reset DSRM:
- Password
- set dsrm

Understanding restartable AD DS

- Use the **Services** console to start or stop AD DS
- Three states of AD DS:
  - AD DS Started
  - AD DS Stopped
  - DSRM
- It is not possible to perform a system state restoration while AD DS is in Stopped state

Managing Active Directory snapshots

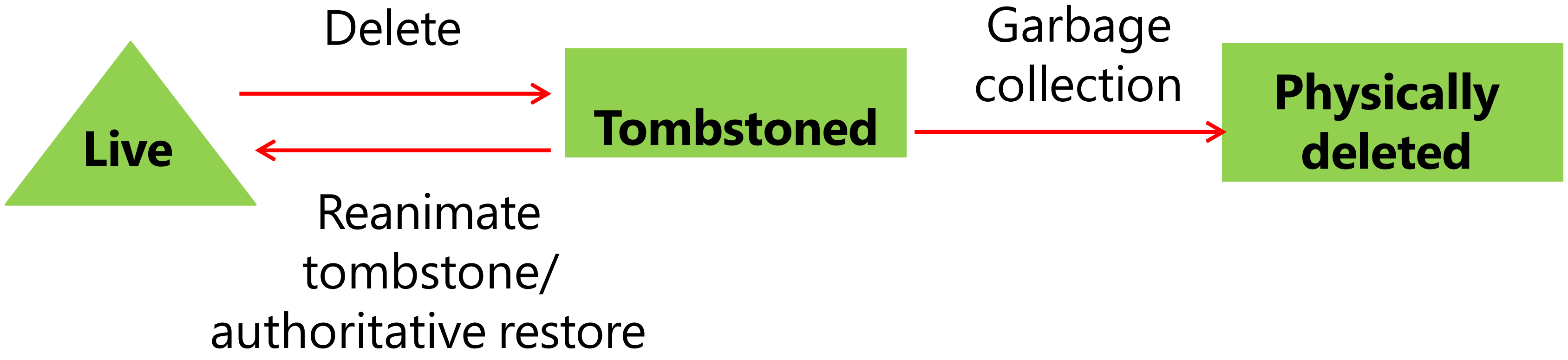
- Create a snapshot of AD DS with NtdsUtil
- Mount the snapshot with NtdsUtil
- View the snapshot:
- Right-click the root node of Active Directory Users and Computers, and then click Connect to Domain Controller
- Type serverFQDN:port

Managing Active Directory snapshots

- View read-only snapshot:
- Cannot directly restore data from the snapshot
- Recover data:
- Connect to the mounted snapshot, and then export/reimport objects’
- attributes with Ldifde
- Restore a backup from the same date as the snapshot

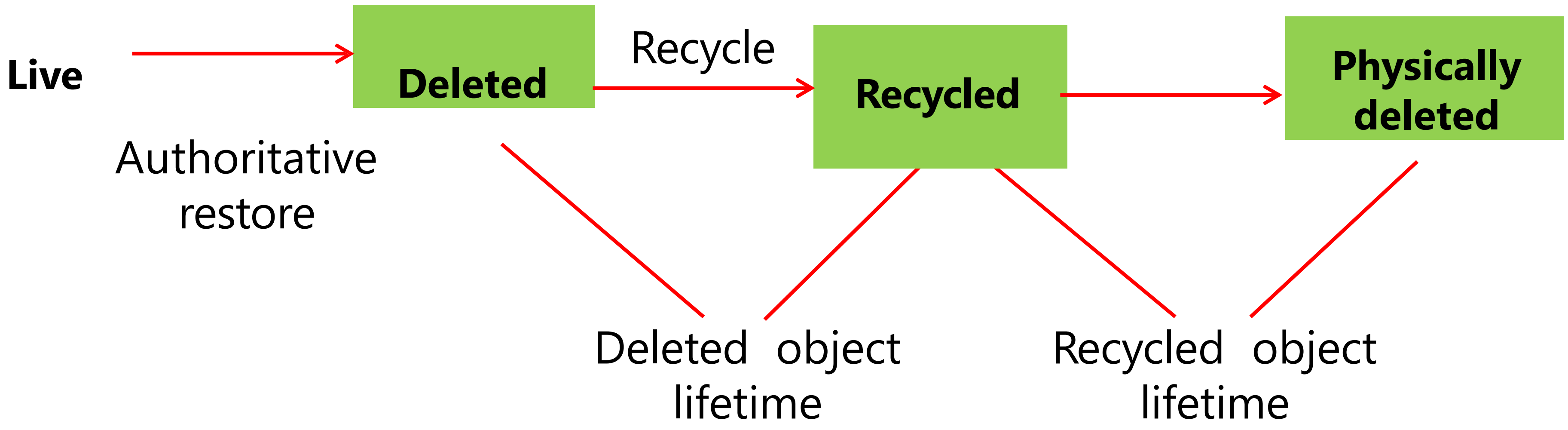
Deleting and restoring objects from AD DS

- Deleted objects are recovered through tombstone reanimation
- When an object is deleted, most of its attributes are cleared
- Authoritative restore requires Active Directory downtime



Configuring Active Directory Recycle Bin

- Active Directory Recycle Bin provides a way to restore deleted objects without Active Directory downtime
- Uses Active Directory module for Windows PowerShell or the Active Directory Administrative Center to restore objects



Additional backup and recovery tools

- Windows Server Backup
- Microsoft Azure Backup
- Data Protection Manager

Active Directory backup and recovery

- Nonauthoritative or normal restore
- Authoritative restore
- Full server restore
- Alternate location restore

Module 0X Review

- Installing and configuring domain controllers
- Managing objects in AD DS
- Advanced AD DS infrastructure management

- Implementing and administering AD DS sites and replication
- Implementing Group Policy
- Managing user settings with Group Policy

- Securing Active Directory Domain Services
- Deploying and managing AD CS
- Deploying and managing certificates

- Implementing and administering AD FS
- Implementing AD DS synchronization with Microsoft Azure AD
- Monitoring, managing, and recovering AD DS

THANK YOU!