ĐẠI HỌC ĐÀ NẴNG
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG VIỆT - HÀN
Vietnam - Korea University of Information and Communication Technology

Chapter 4

Installing and configuring domain controllers and ADDS

http://vku.udn.vn/

Contents

- Understanding Domain and Forest Functionality
- Planning the Domain structure
- Deploying a domain controller
- Installing and administering Active Directory

Understanding Domain and Forest Functionality

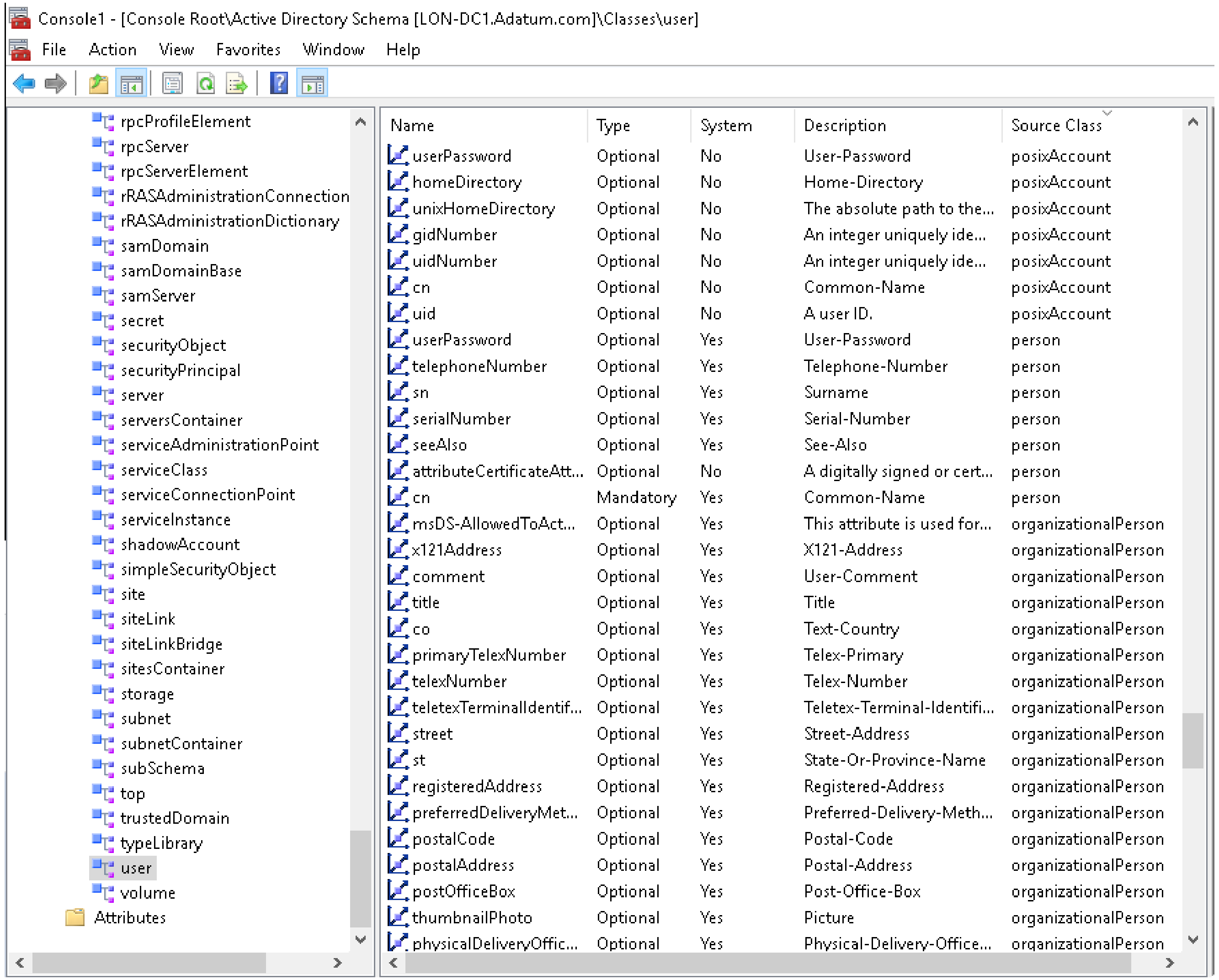
- Overview of AD DS
- What is the AD DS schema?
- What is an AD DS forest?
- What is an AD DS domain?
- What are OUs?
- What is new in AD DS in Windows Server 2016?
- What is Azure AD?
- Overview of AD DS administration tools
- Demonstration: Using the Active Directory Administrative Center to administer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

Overview of AD DS

AD DS is composed of both logical and physical components

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

What is the AD DS schema?

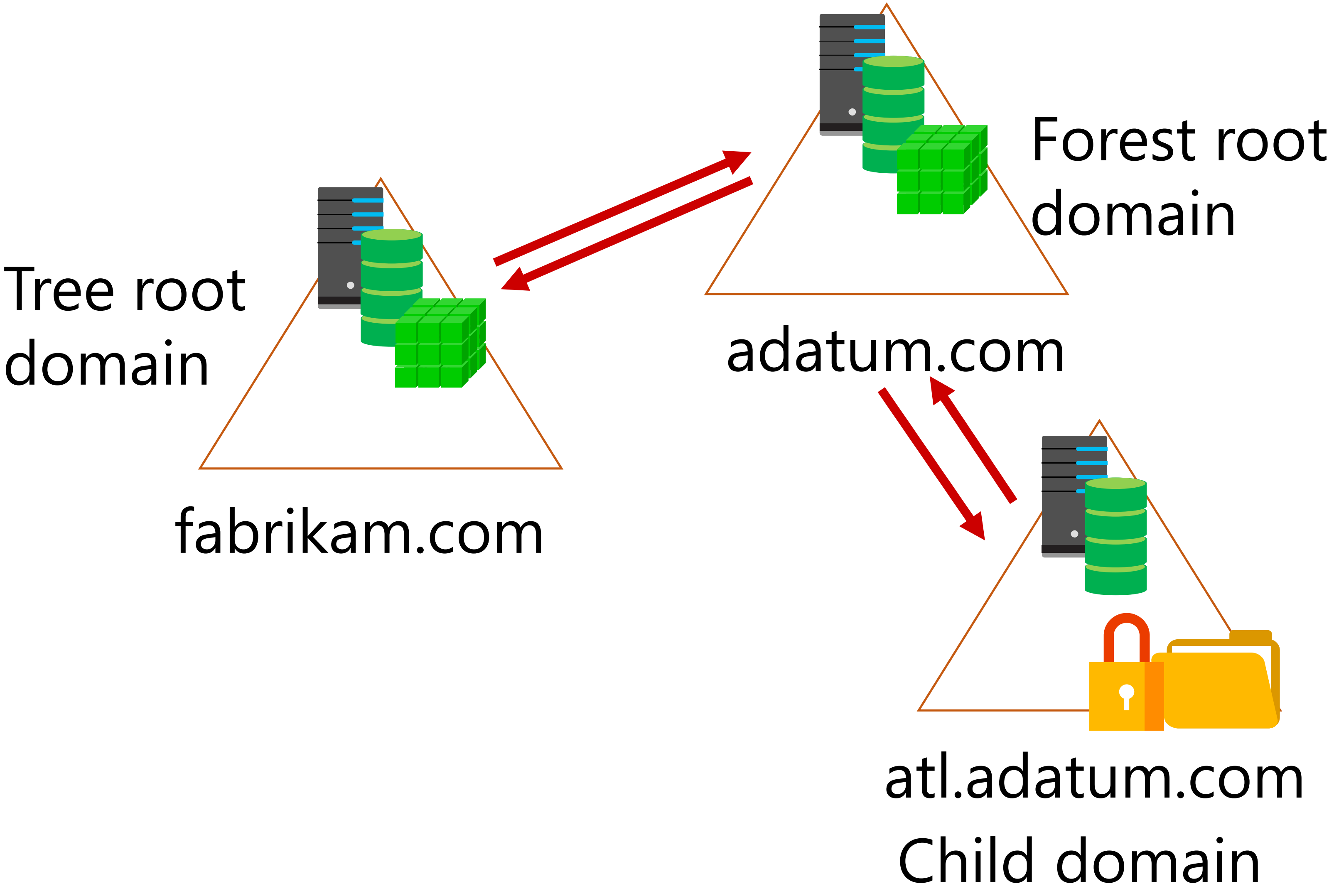


Console1 - [Console Root\Active Directory Schema [LON-DC1.Adatum.com]\Classes\user]

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

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

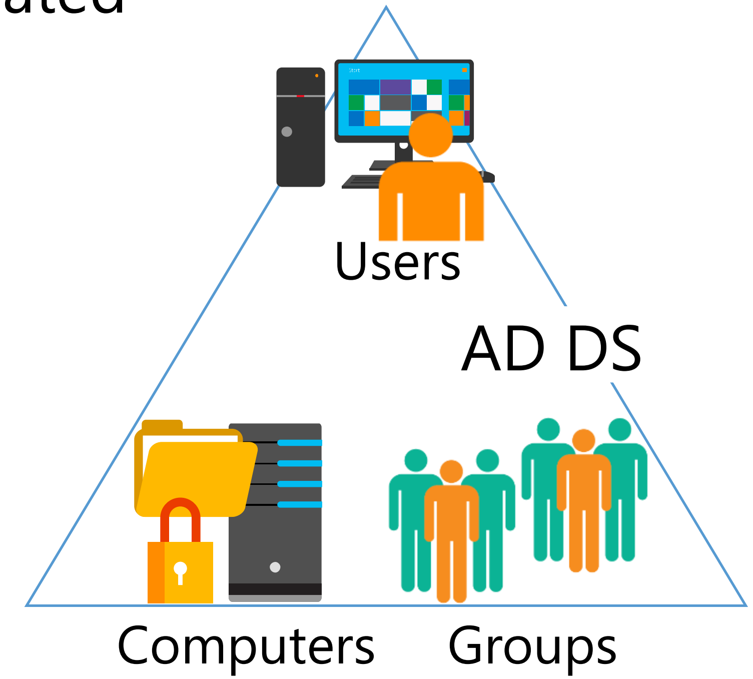
What is an AD DS forest?



What is an AD DS domain?

- AD DS requires one or more domain controllers
- All domain controllers hold a copy of the domain database, which is continually synchronized
- The domain is the context within which user accounts, computer accounts, and groups are created

- The domain is a replication boundary
- The domain is an administrative center for configuring and managing objects
- Any domain controller can authenticate any sign-in
  anywhere in the domain
- The domain provides authorization



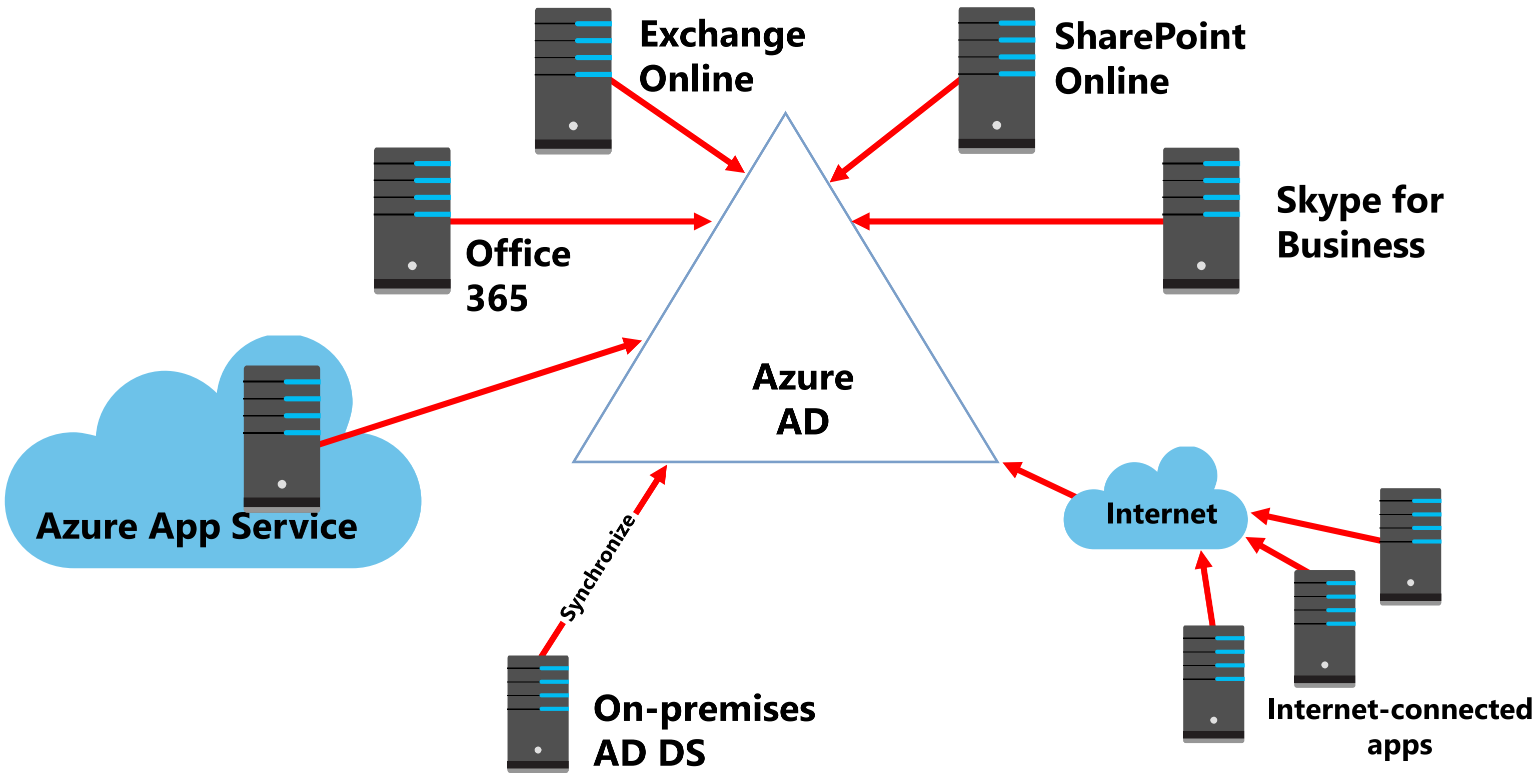
What are OUs?

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

What is new in AD DS in Windows Server 2016?

- PAM
- Azure AD Join
- Microsoft Passport

What is Azure AD?



Overview of AD DS administration tools

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

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

Demonstration: Using the Active Directory Administrative Center to administer and manage AD DS

In this demonstration, you will learn how to:

- Navigate within the Active Directory Administrative Center
- Perform an administrative task within the Active Directory Administrative Center
- Create objects
- View all object attributes
- Use the Windows PowerShell History viewer in the Active Directory Administrative Center

Planning the Domain structure

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

What is a domain controller?

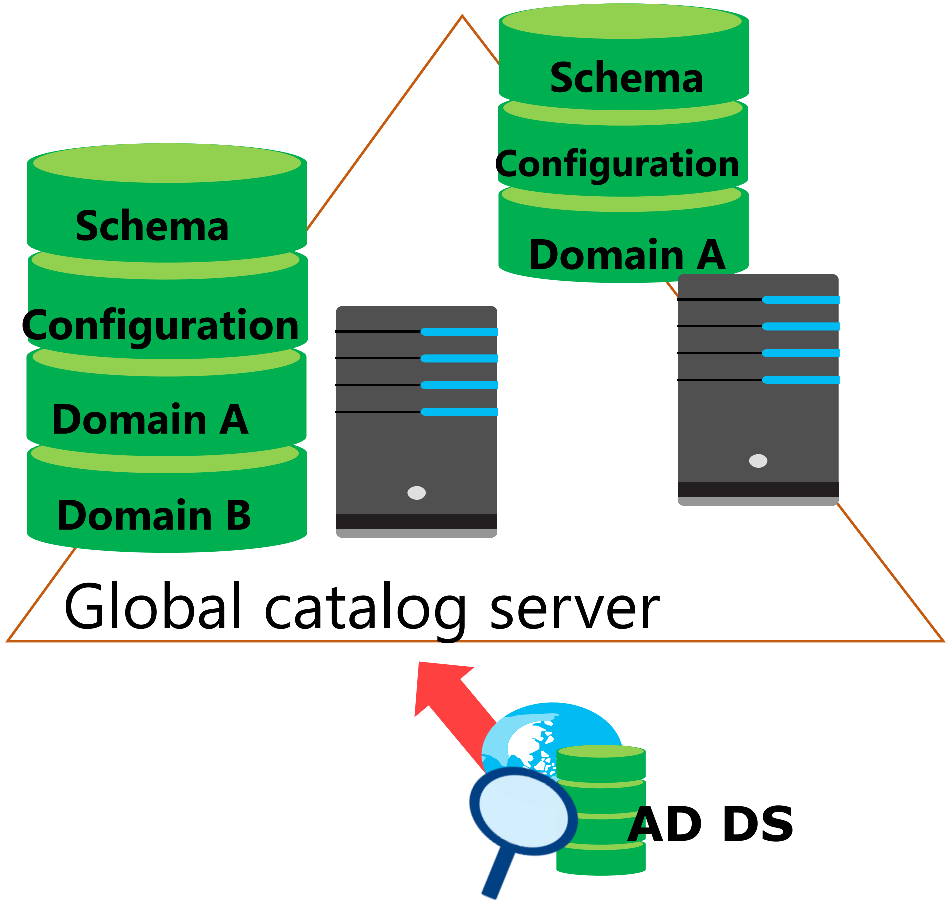
Domain controllers:

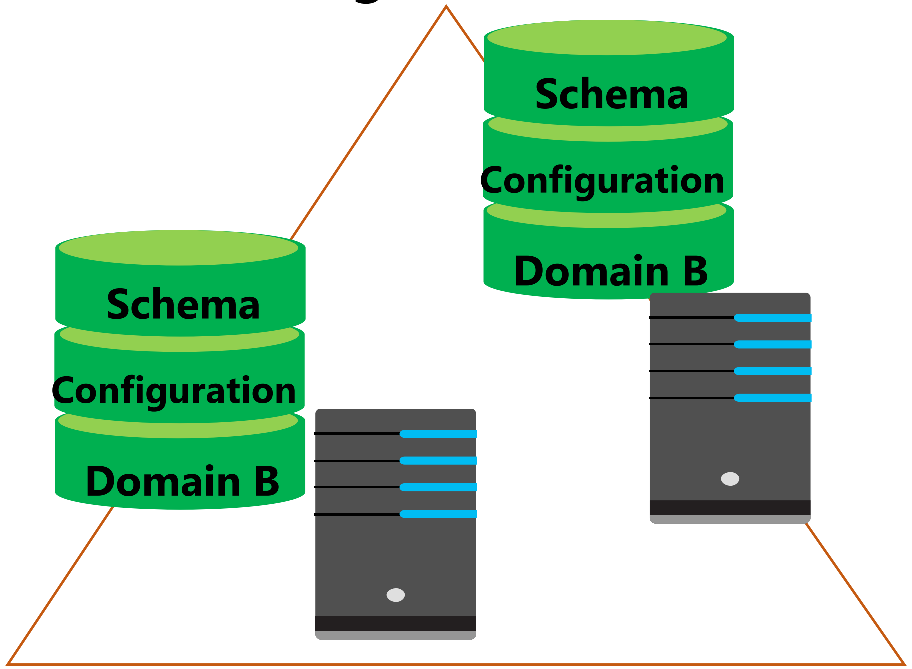
- Are servers that host the AD DS database (Ntds.dit) and SYSVOL
- Host the Kerberos authentication service and KDC services to perform authentication
- Have best practices for:
  - Availability:
    - Use at least two domain controllers in a domain
  - Security:
    - Use an RODC or BitLocker

What is a global catalog?

The global catalog:

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





Overview of domain controller SRV records

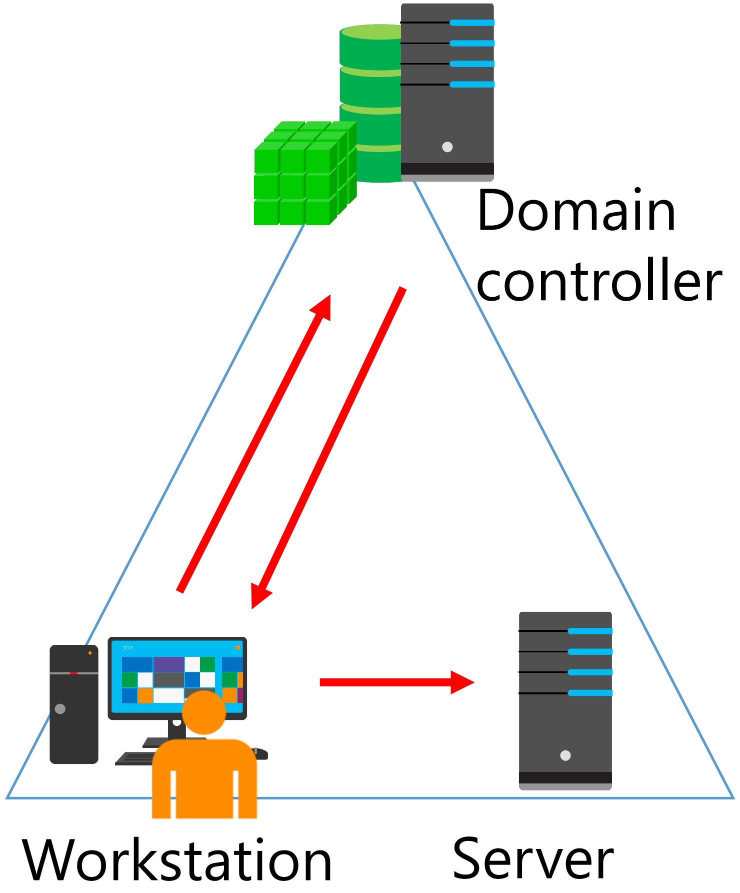
- Clients find domain controllers through DNS lookup
- Domain controllers dynamically register their addresses with DNS
- The results of DNS queries for domain controllers are returned in this order:
  1. A list of domain controllers in the same site as the client
  2. A list of domain controllers in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

Demonstration: Viewing the SRV records in DNS

In this demonstration, you will learn how to use DNS Manager to view SRV records

AD DS sign-in process

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



What are operations masters?

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

The five FSMOs :

Forest:

- Domain naming master
- Schema master

Domain:

- RID master
- Infrastructure master
- PDC emulator master

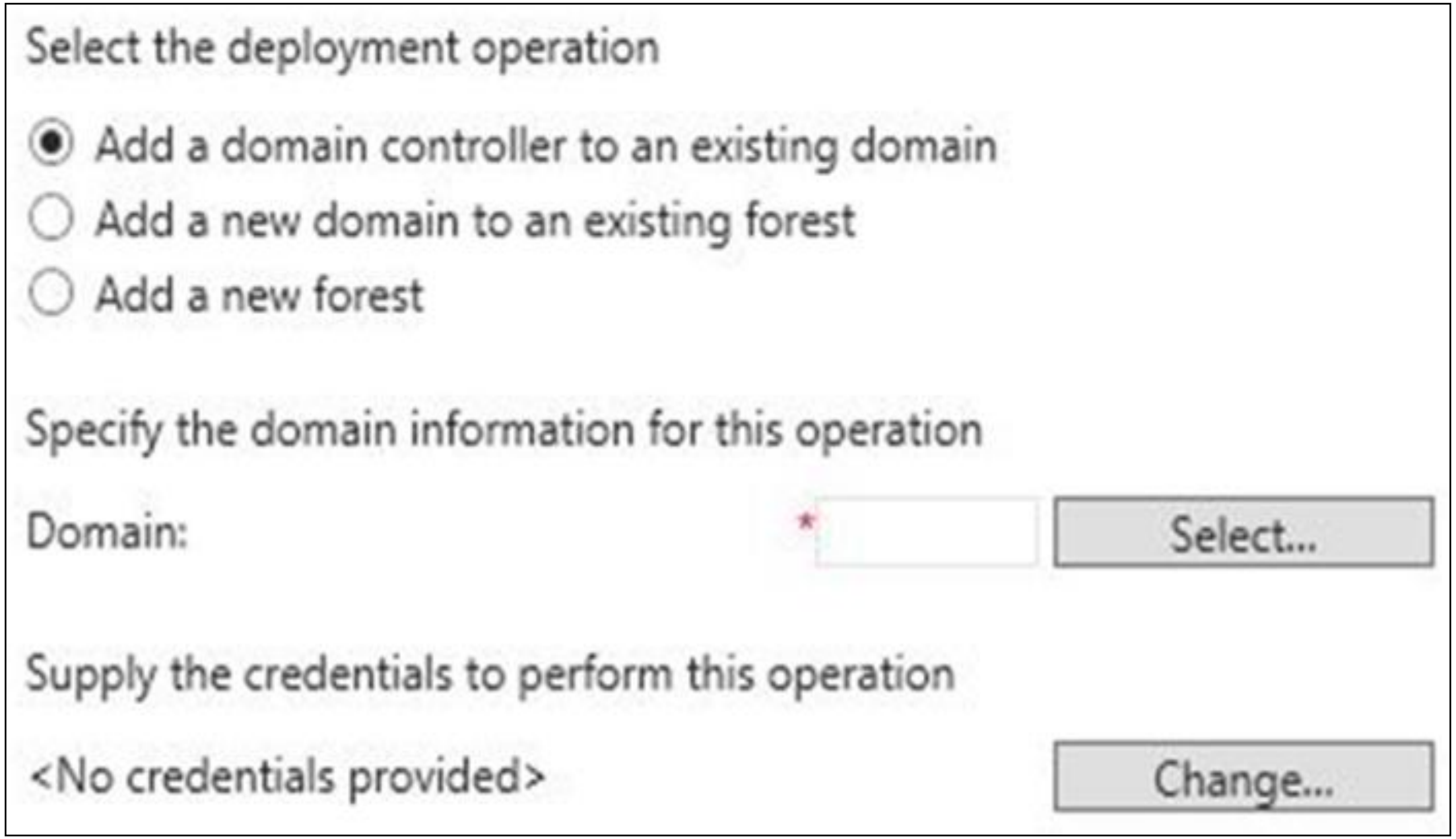
Transferring and seizing roles

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

Deploying a domain controller

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

Installing a domain controller from Server Manager



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>

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

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

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

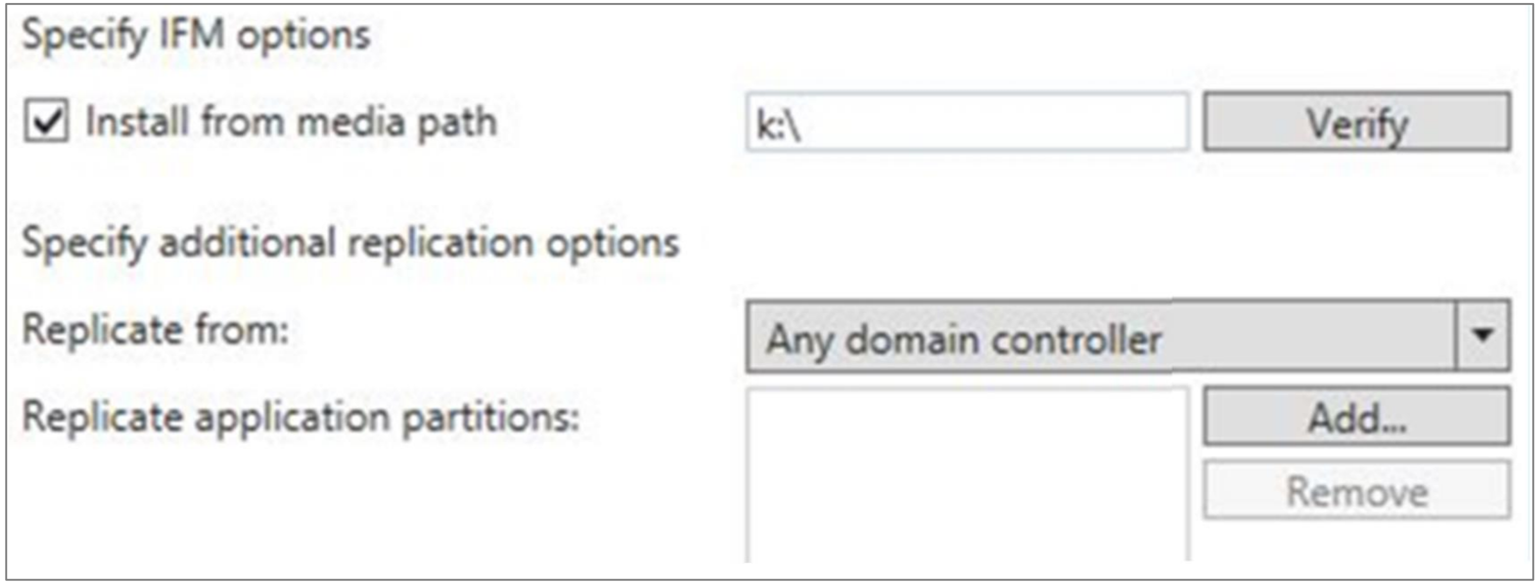
Upgrading a domain controller

Options to upgrade 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 (DLLs)

- Introduce a new server running Windows Server 2016 into the domain, and then promote it to be a domain controller (this option is usually preferred):
  - Benefit: The new server has no obsolete files and settings
  - Risk: It might require additional work to migrate administrators' files and settings

Installing a domain controller by installing from media



Specify IFM options

☑ Install from media path: k:\

Specify additional replication options

Replicate from: Any domain controller

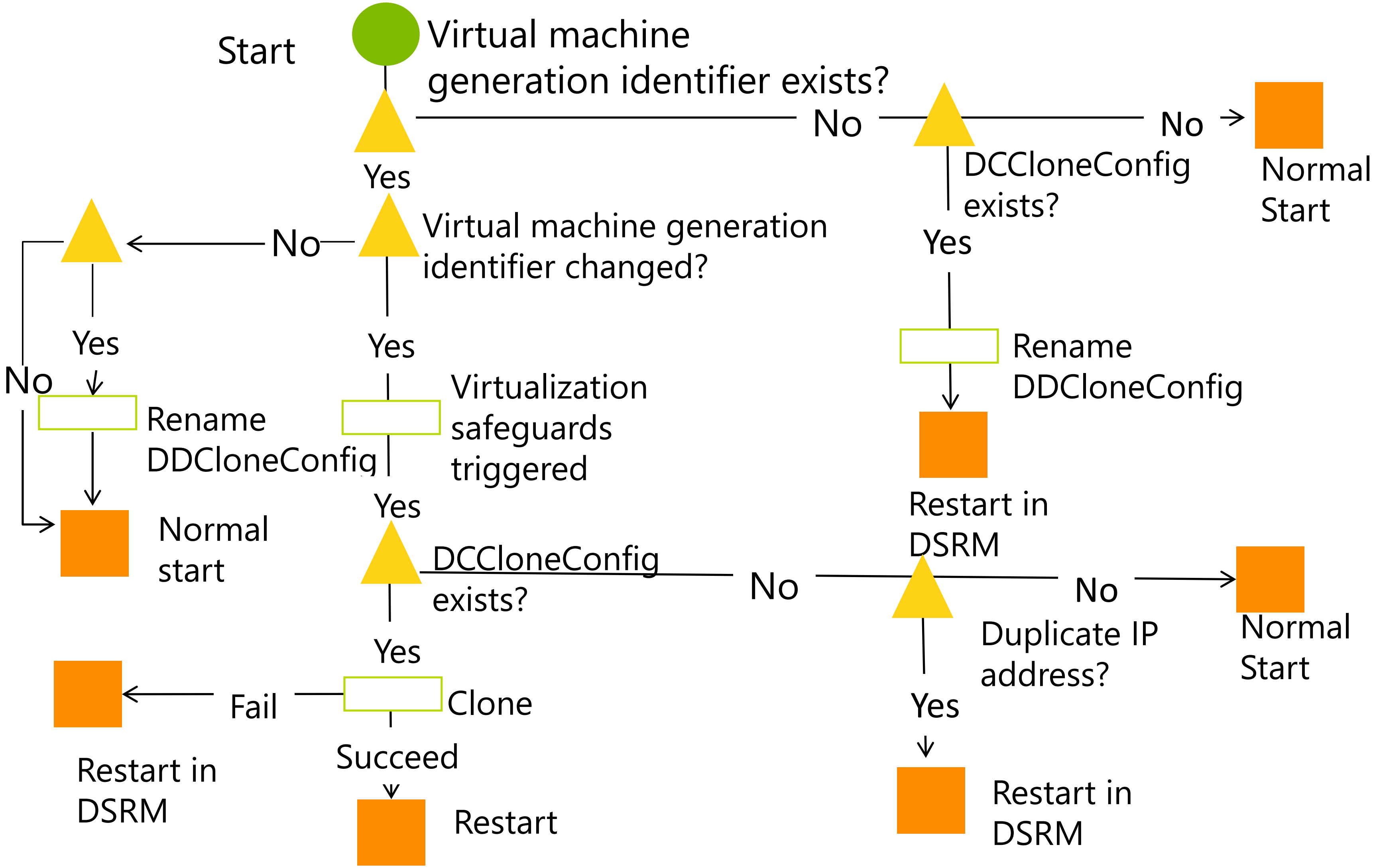
Replicate application partitions:

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

Cloning domain controllers

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

Cloning domain controllers



Demonstration: Cloning a domain controller

In this demonstration, you will learn how to:

- Prepare a source domain controller to be cloned
- Export the source virtual machine
- Create and start the cloned domain controller

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
- Be aware of improving security
- Consider taking advantage of cloning in your deployment or recovery strategy
- Start a maximum number of 10 new clones at the same time
- Consider using virtualization technologies that allow virtual machine guests to move between sites
- Adjust your naming strategy to allow for domain controller clones

Module Review and Takeaways

- Review Questions
- Common Issues and Troubleshooting Tips

Installing and administering Active Directory

- Managing user accounts
- Managing groups in AD DS
- Managing computer objects in AD DS
- Using Windows PowerShell for AD DS administration
- Implementing and managing OUs

Managing user accounts

- Creating user accounts
- Configuring user account attributes
- Demonstration: Managing user accounts
- Creating user profiles
- Managing inactive and disabled user accounts
- User account templates
- Demonstration: Using templates to manage accounts

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:

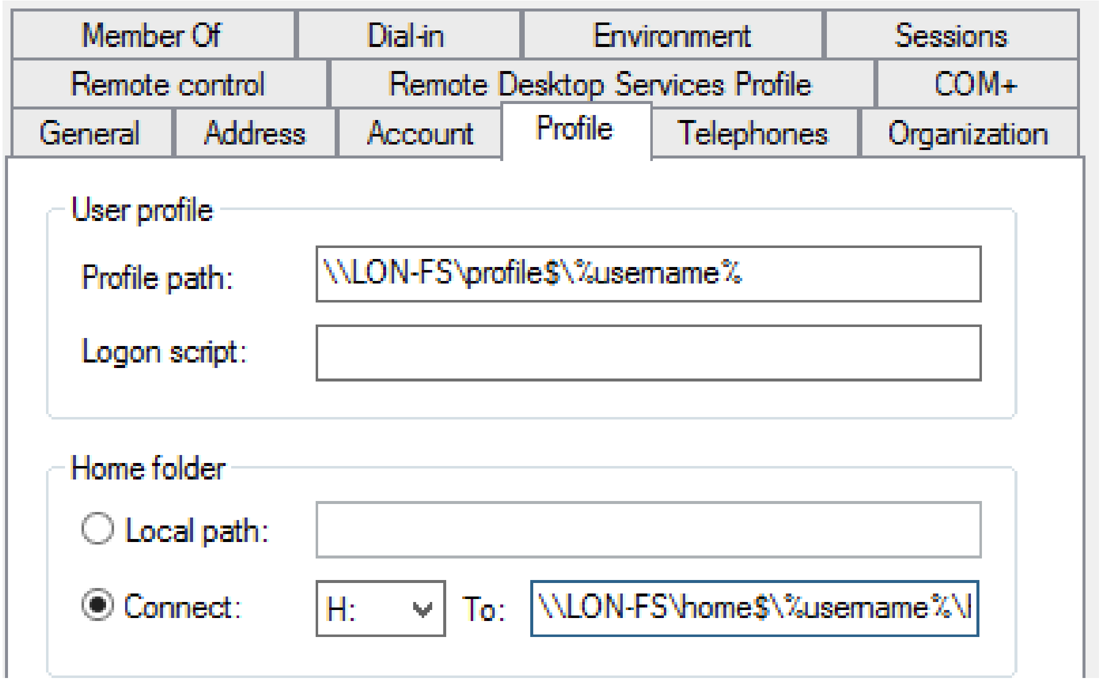
- Account
- Organization
- Member of
- Password Settings
- Profile
- Policy
- Silo
- Extensions

Demonstration: Managing user accounts

In this demonstration, you will see how to use the Active Directory Administrative Center to:

- Create a new user account
- Delete a user account
- Move a user account
- Configure user attributes:
  - Change department
  - Change group membership

Creating user profiles



User profile

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

Logon script:

Home folder

○ Local path:

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

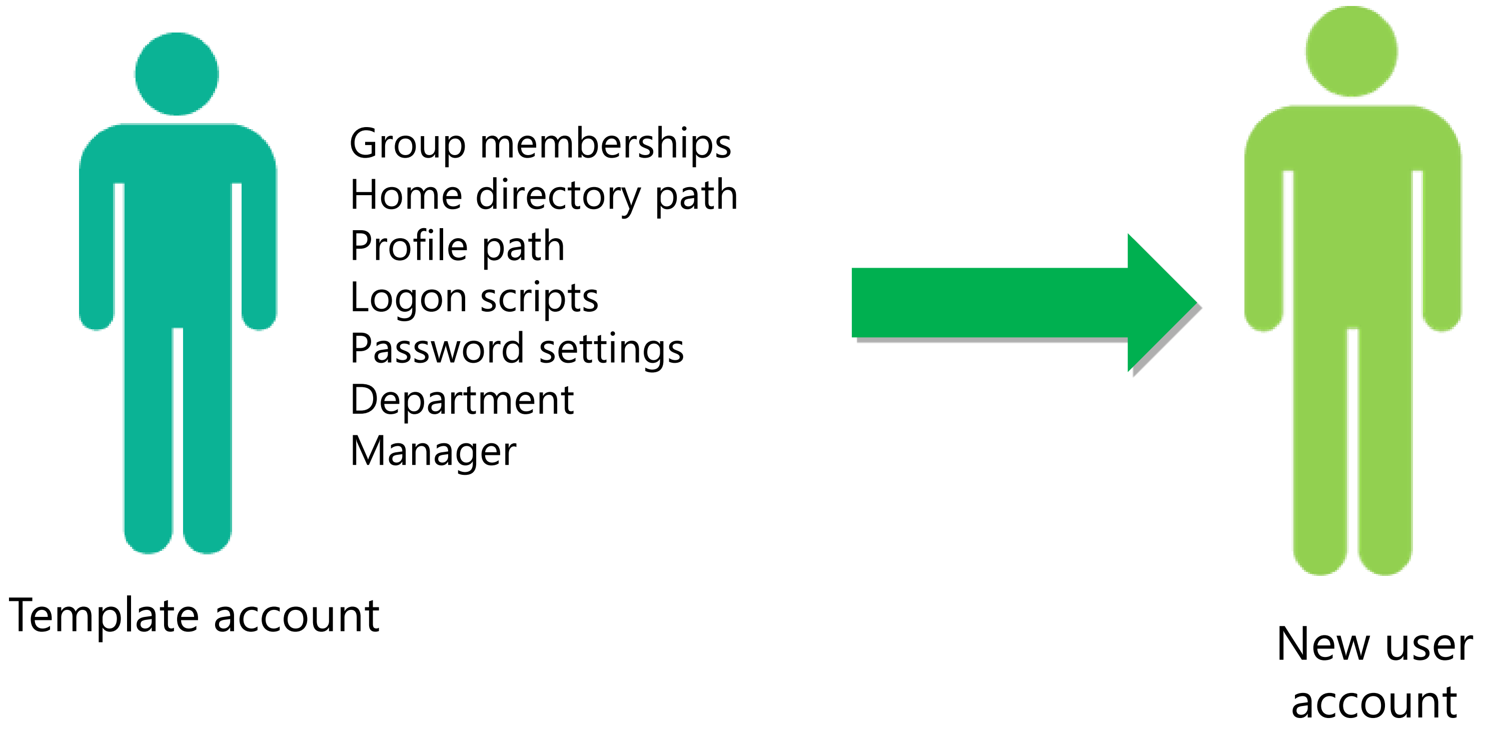
The Profile section of the User Properties window

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



Group memberships
Home directory path
Profile path
Logon scripts
Password settings
Department
Manager

Template account

New user account

Demonstration: Using templates to manage accounts

In this demonstration, you will see how to:

- Create a template account
- Create a new user based on the template

Managing groups in AD DS

- Group types
- Group scopes
- Implementing group management
- Managing group membership by using Group Policy
- Default groups
- Special identities
- Demonstration: Managing groups in Windows Server

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

Security groups and distribution groups can be converted to the other type of group

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
- 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

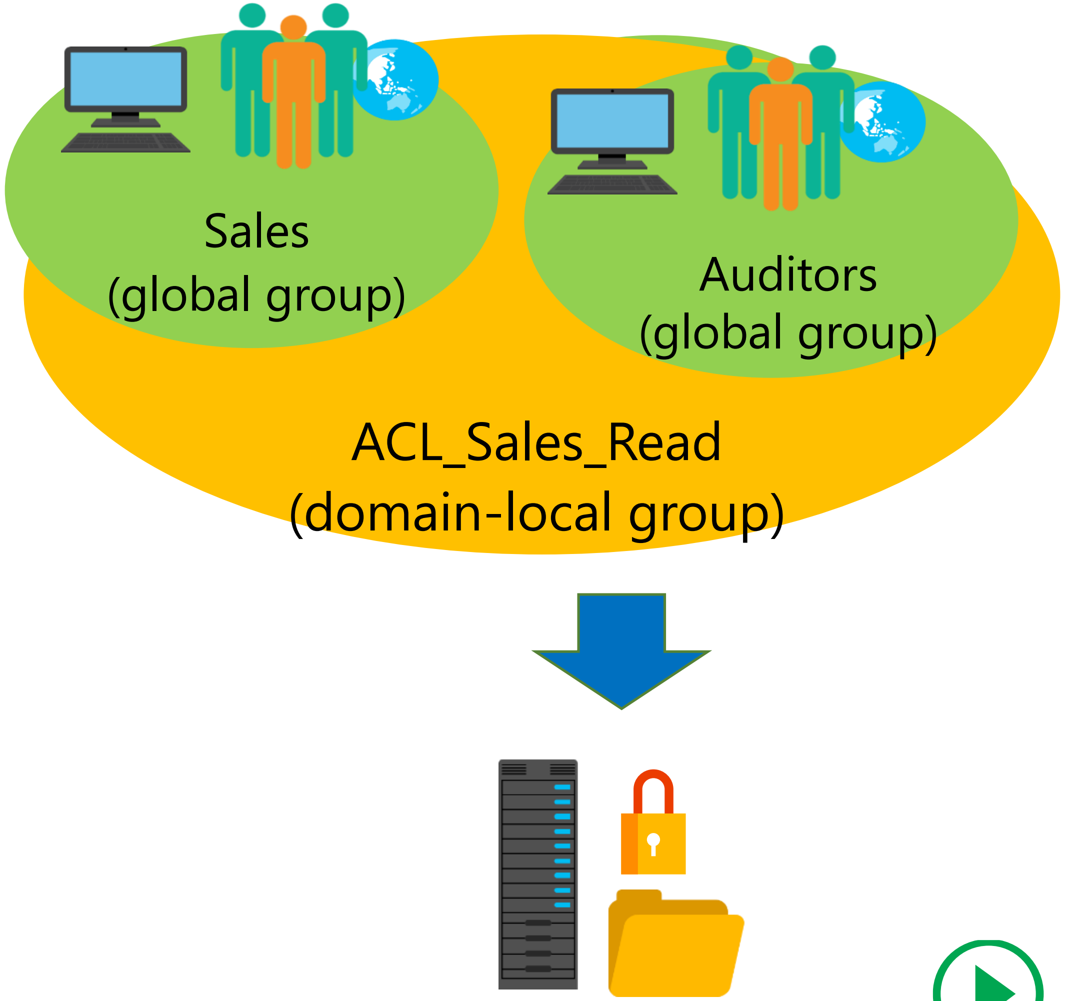
This best practice for nesting groups is known as IGDLA

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



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

Sales
(global group)

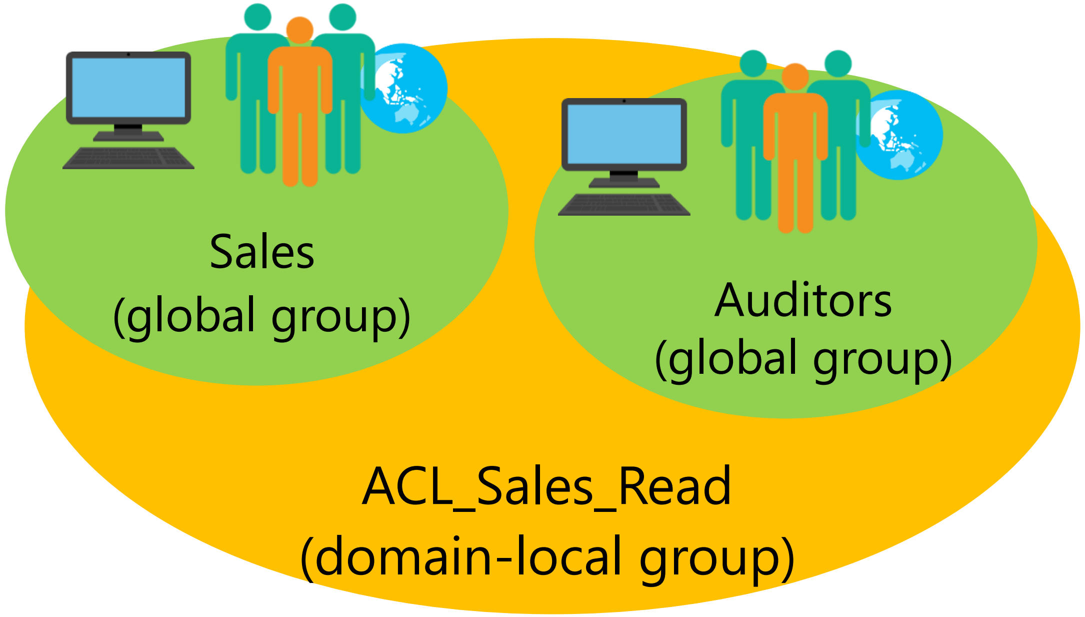
Auditors
(global group)

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



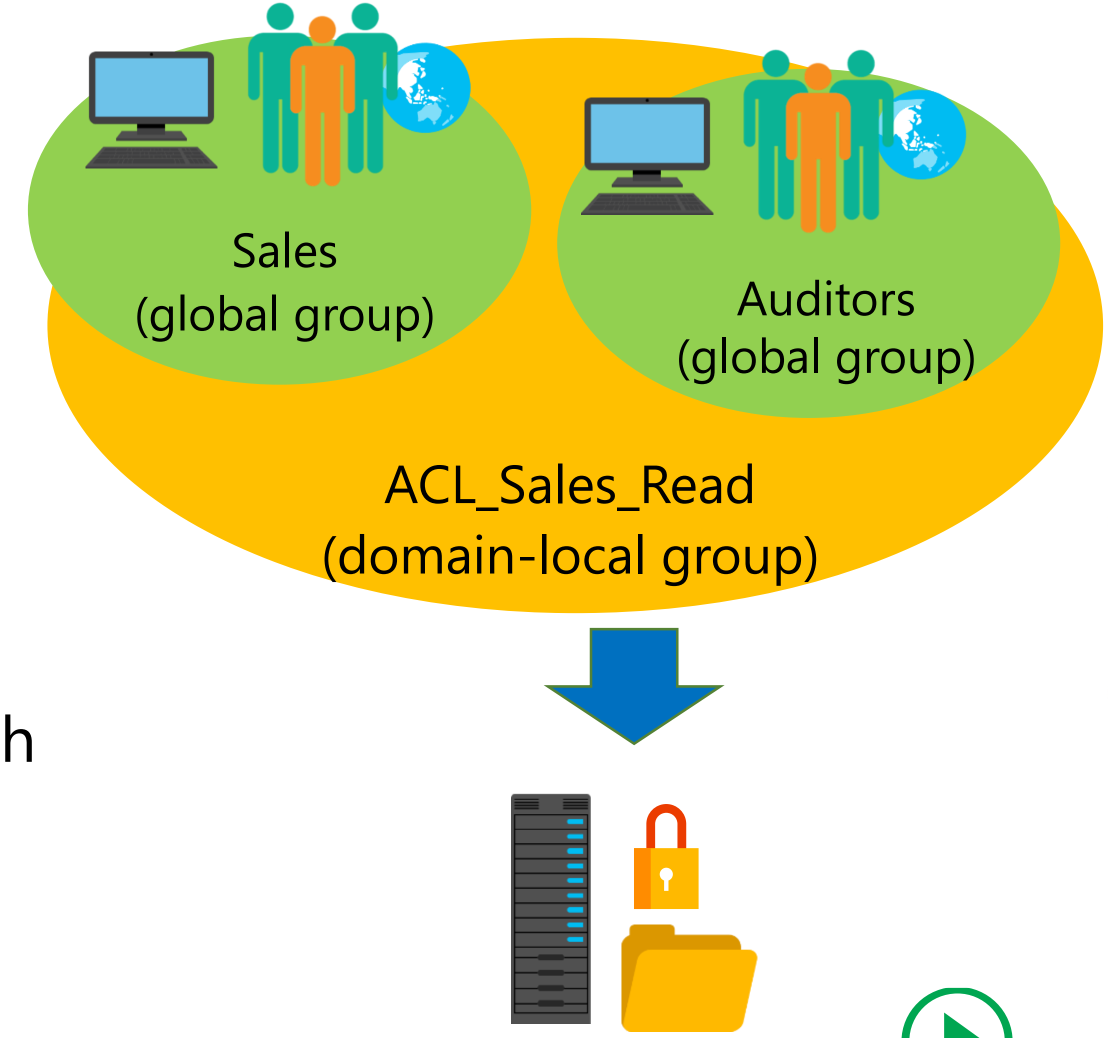
Implementing group management

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

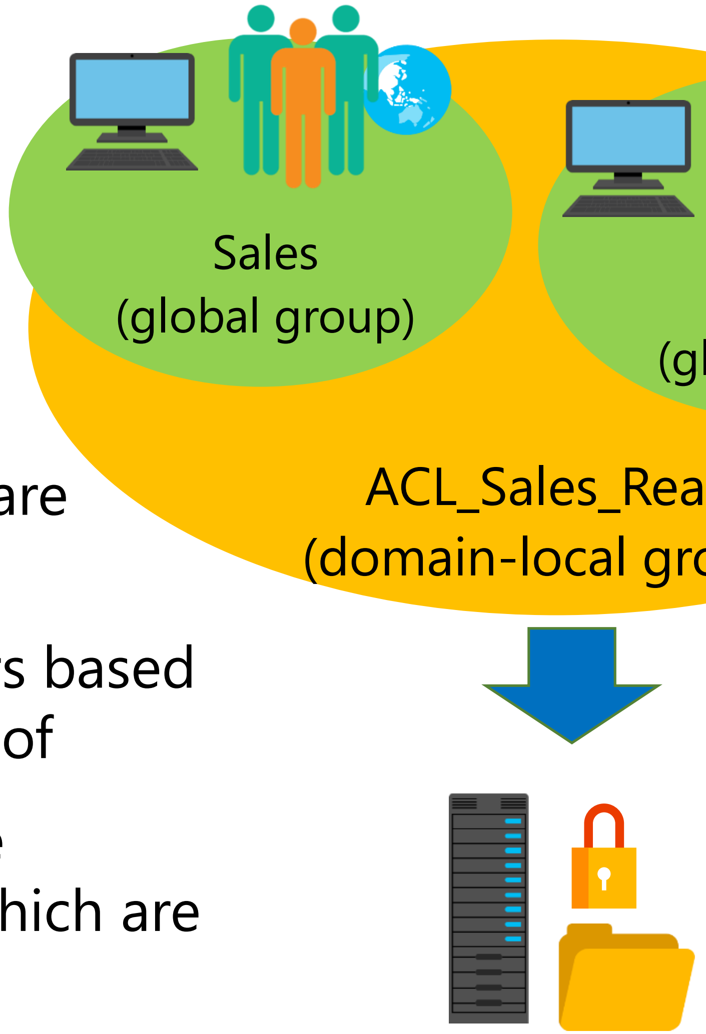
This best practice for nesting groups is known as IGDLA

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



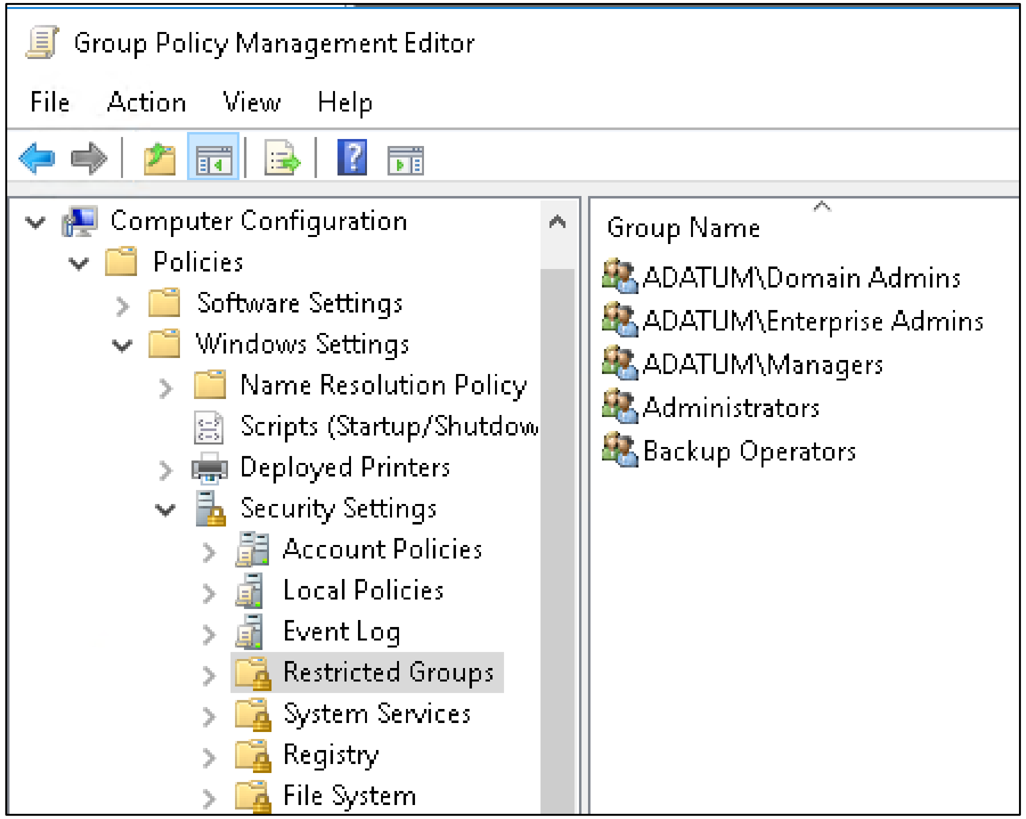
Sales
(global group)

Auditors
(global group)

ACL_Sales_Read
(domain-local group)

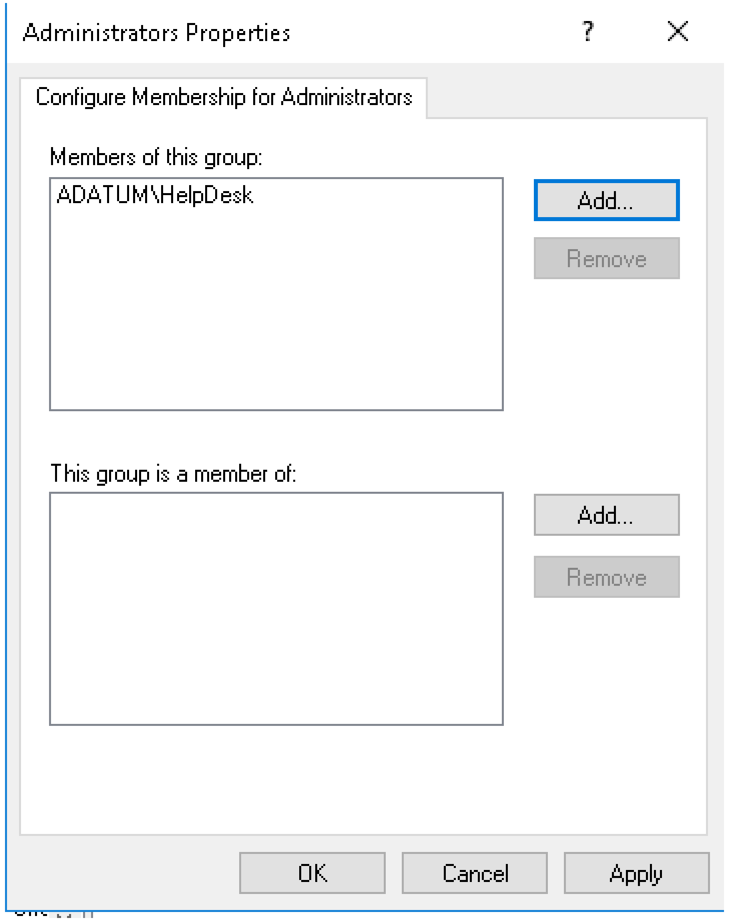
Managing group membership by using Group Policy

- Restricted Groups can simplify group management
- Both local and AD DS groups can be managed



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

Managing group membership by using Group Policy



Administrators Properties

Configure Membership for Administrators

Members of this group:

ADATUM\HelpDesk

This group is a member of:

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

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 membership is controlled by the operating system
  - 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

Demonstration: Managing groups in Windows Server

In this demonstration you will see how to:

- Create a new group and add members to the group
- Add users to the group
- Change the group type and scope
- Configure a manager for the group

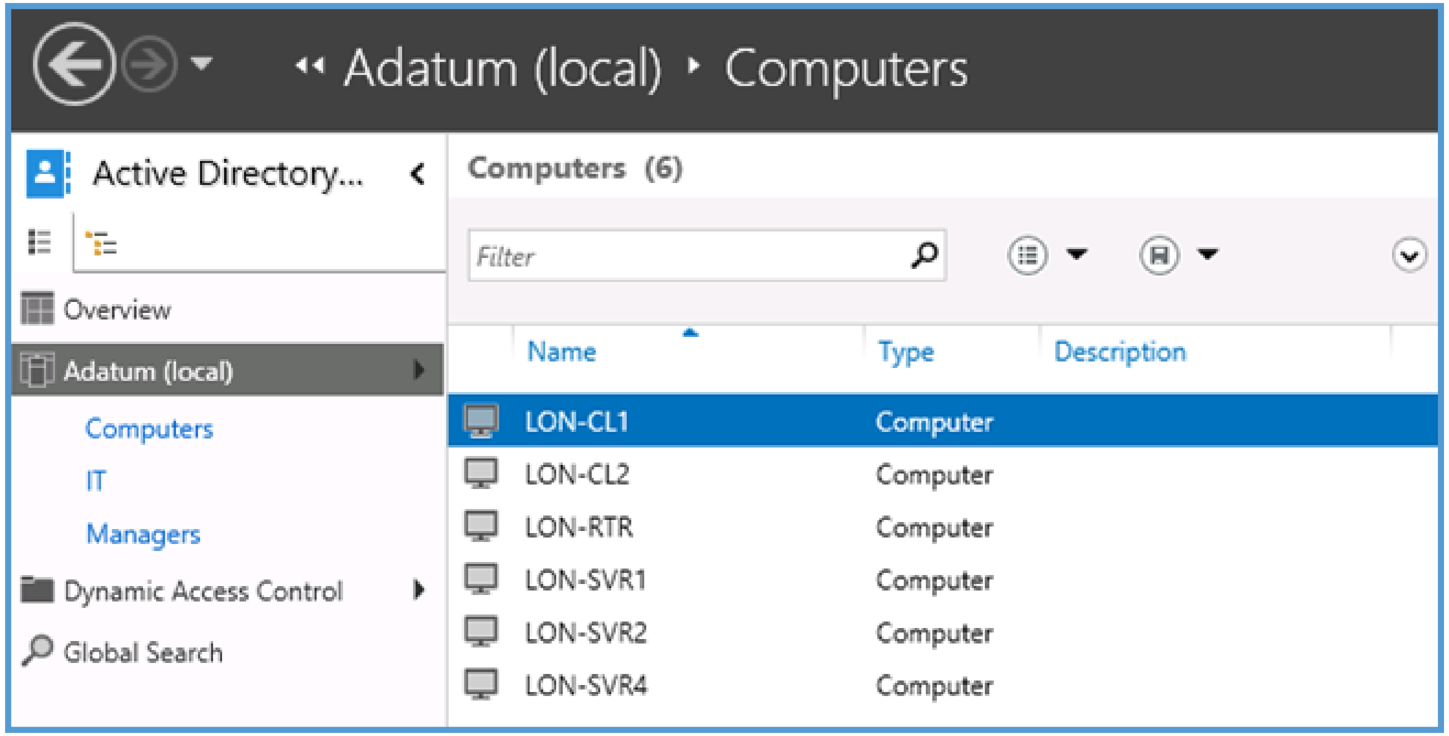
Managing computer objects in AD DS

- What is the Computers container?
- Specifying the location of computer accounts
- Controlling permissions to create computer accounts
- Joining a computer to a domain
- Computer accounts and secure channels
- Resetting the secure channel
- Performing an offline domain join

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



Adatum (local) ‣ Computers

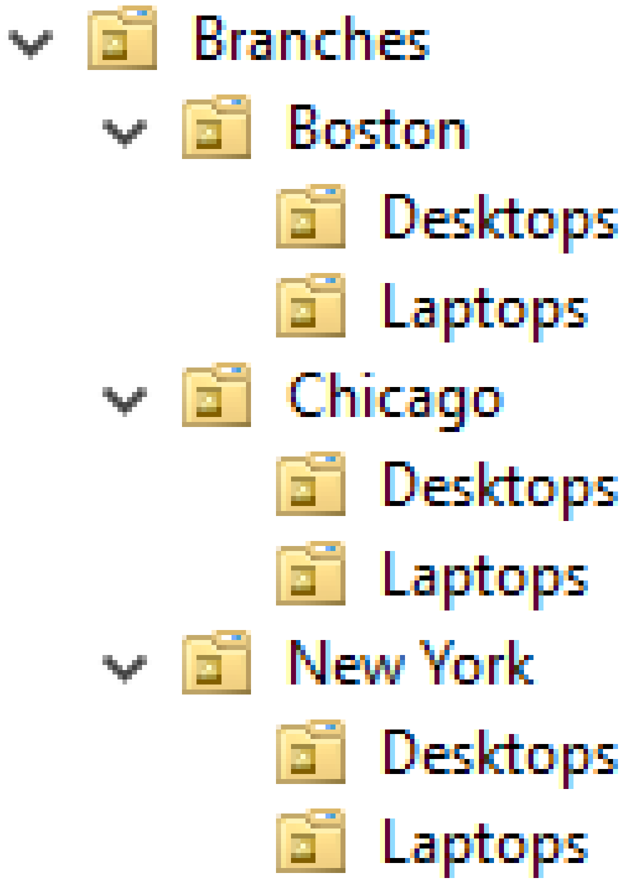
Computers (6)

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

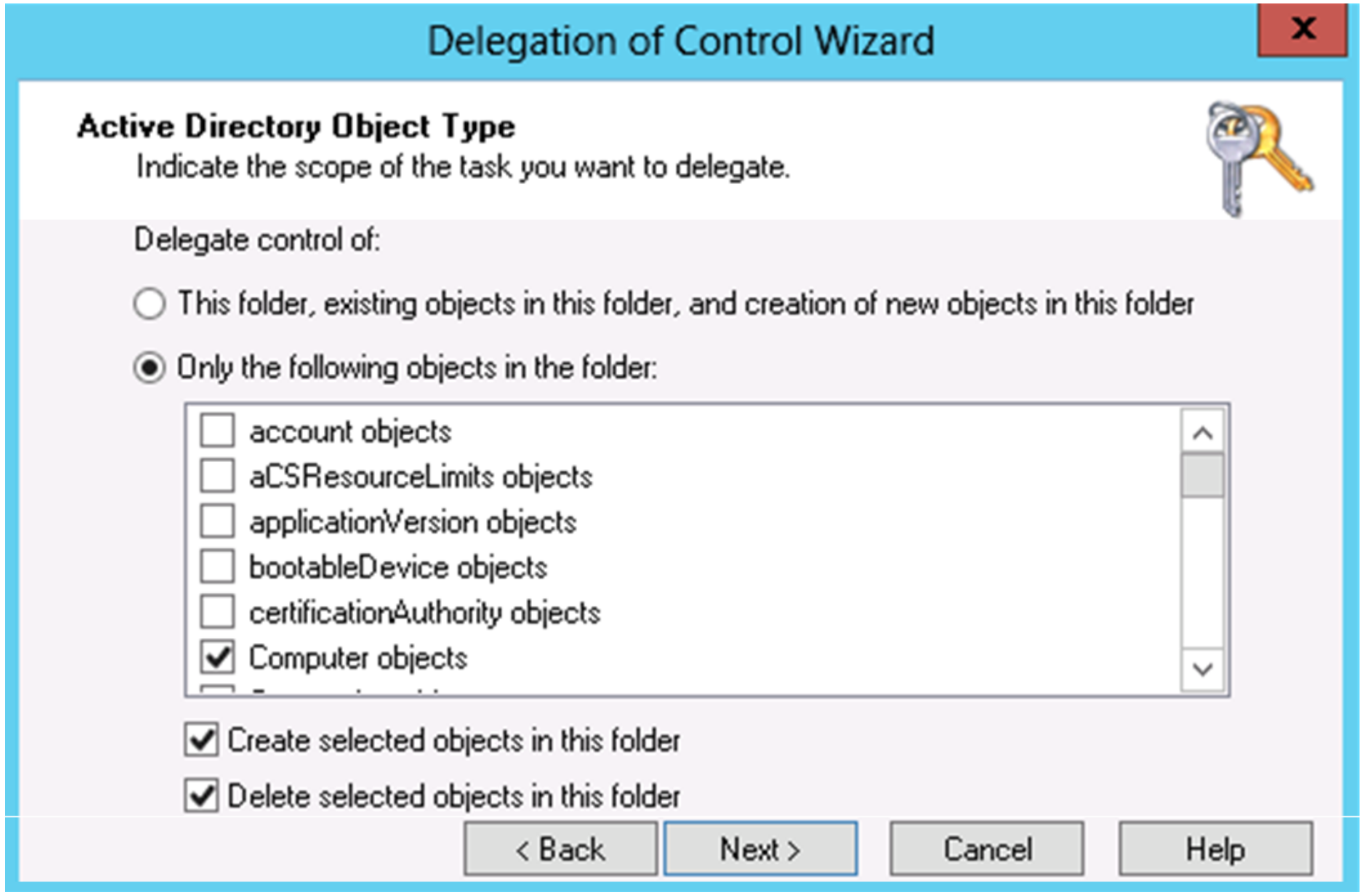
- Divide OUs:
  - By administration
  - To facilitate configuration with Group Policy



- 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



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

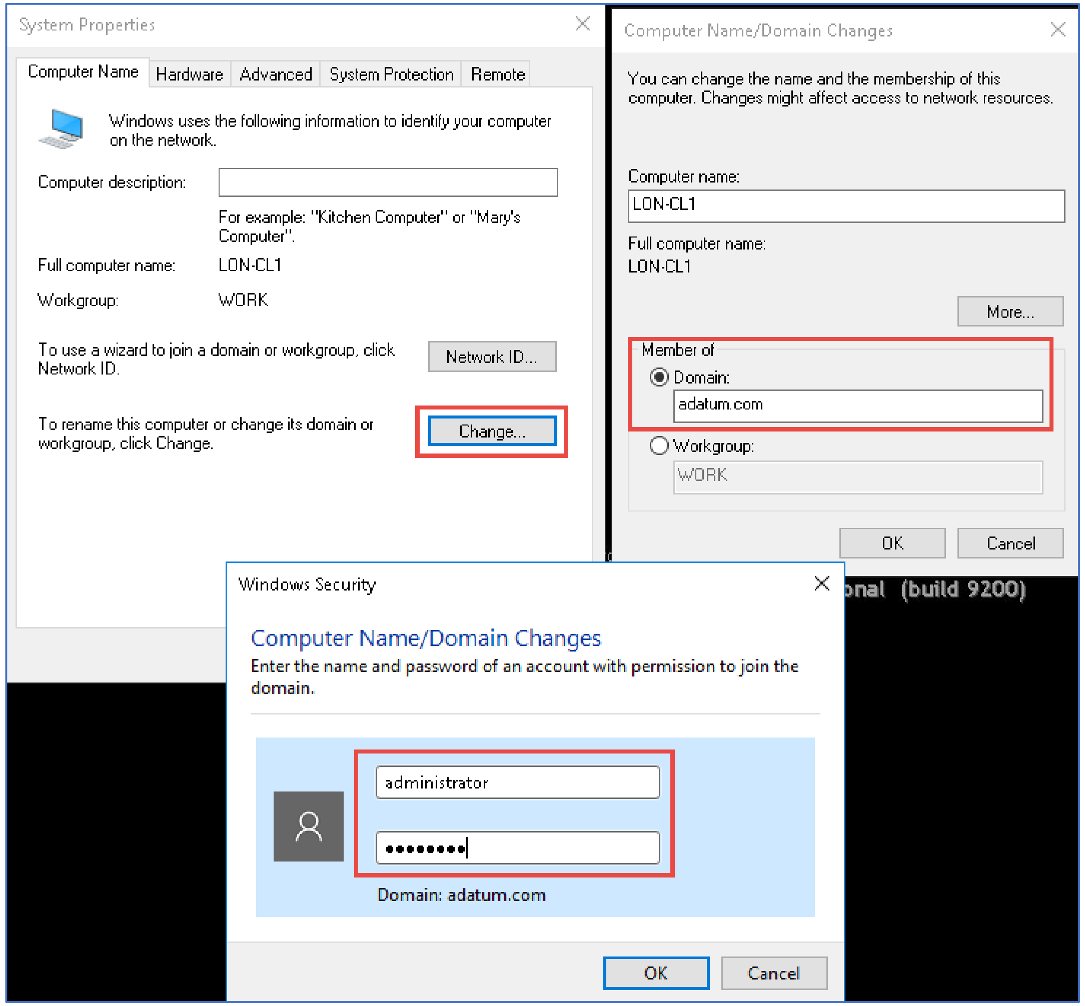
● Only the following objects in the folder:

- □ 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



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.

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

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

Performing an offline domain join

Use offline domain join to join computers to a domain when they cannot contact a domain controller

- Create a domain join file by using:

```
djoin.exe /Provision /Domain <DomainName>
/Machine <MachineName> /SaveFile <filepath>
```

- Import the domain join file by using:

```
djoin.exe /requestODJ /LoadFile <filepath>
/WindowsPath <path to the Windows directory of
the offline image>
```

Using Windows PowerShell for AD DS administration

- Using Windows PowerShell cmdlets to manage user accounts
- Using Windows PowerShell cmdlets to manage groups
- Using Windows PowerShell cmdlets to manage computer accounts
- Using Windows PowerShell cmdlets to manage OUs
- What are bulk operations?
- Demonstration: Using graphical tools to perform bulk operations
- Querying objects with Windows PowerShell
- Modifying objects with Windows PowerShell
- Working with CSV files
- Demonstration: Performing bulk operations with Windows PowerShell

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 "Sten Faerch" –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

Demonstration: Using graphical tools to perform bulk operations

In this demonstration, you will see how to use Active Directory Users and Computers to change the Office attribute for users in the Research OU as a bulk operation

Querying objects with Windows PowerShell

Parameter	Description
SearchBase	Defines the AD DS path to begin searching
SearchScope	Defines at what level below the SearchBase a search should be performed
ResultSetSize	Defines how many objects to return in response to a query
Properties	Defines which object properties to return and display
Filter	Defines a filter by using PowerShell syntax
LDAPFilter	Defines a filter by using LDAP query syntax

Descriptions of operators

-eq	Equal to	-gt	Greater than
-ne	Not equal to	-ge	Greater than or equal to
-lt	Less than	-like	Uses wildcards for pattern matching
-le	Less than or equal to		

Querying objects with Windows PowerShell

Show all the properties for a user account:

```
Get-ADUser –Name “Administrator” -Properties *
```

Show all the user accounts in the Marketing OU and all its subcontainers:

```
Get-ADUser –Filter * -SearchBase "ou=Marketing,dc=adatum,dc=com" -
SearchScope subtree
```

Show all of the user accounts with a last sign in date older than a specific date:

```
Get-ADUser -Filter {lastlogondate -lt "January 1, 2016"}
```

Show all of the user accounts in the Marketing department that have a last sign in date older than a specific date:

```
Get-ADUser -Filter {(lastlogondate -lt "January 1, 2016") -and
(department -eq "Marketing")}
```

Modifying objects with Windows PowerShell

Use the pipe character (|) to pass a list of objects to a cmdlet for further processing

```
Get-ADUser -Filter {company -notlike "*"} |
Set-ADUser -Company "A. Datum"
```

```
Get-ADUser -Filter {lastlogondate -lt "January 1,
2016"} | Disable-ADAccount
```

```
Get-Content C:\users.txt | Disable-ADAccount
```

Working with CSV files

The first line of a .csv file defines the names of the columns

```
FirstName,LastName,Department
Greg,Guzik,IT
Robin,Young,Research
Qiong,Wu,Marketing
```

A foreach loop processes the contents of a .csv file that have been imported into a variable

```
$users=Import-CSV –LiteralPath “C:\users.csv”
foreach ($user in $users) {
    Write-Host "The first name is:" $user.FirstName
    }
```

Demonstration: Performing bulk operations with Windows PowerShell

In this demonstration, you will see how to:

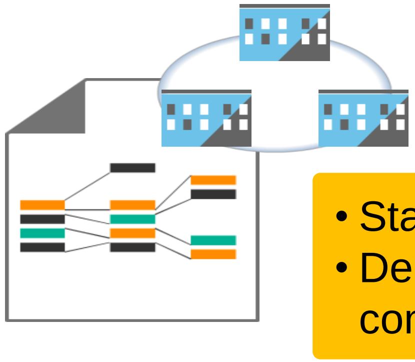
- Create a new global group in the IT department
- Add all users in the IT department to the group
- Set the address attributes for all users in the Research department
- Create a new OU
- Run a script to create new users from a .csv file
- Verify the accounts were modified and new accounts were created

Implementing and managing OUs

- Planning OUs
- OU hierarchy considerations
- Considerations for using OUs
- AD DS permissions
- Delegating AD DS permissions
- Demonstration: Delegating administrative permissions on an OU

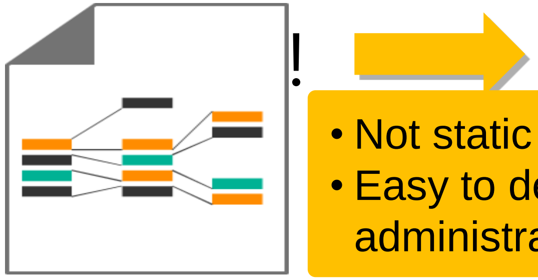
Planning OUs

Location-based strategy



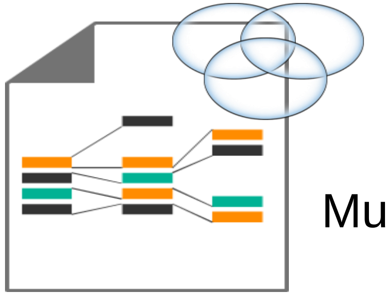
- Static
- Delegation can be complicated

Resource-based strategy

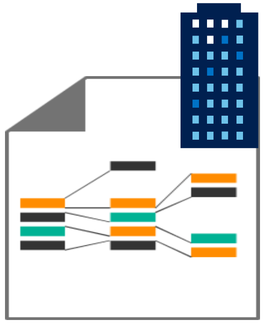


- Not static
- Easy to delegate administration

Hybrid strategy

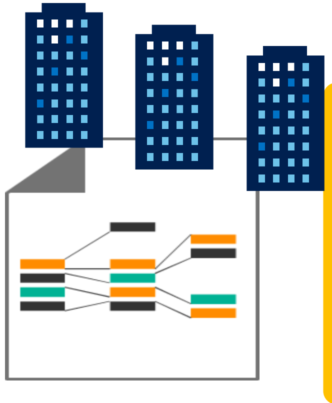


Organization-based strategy



- Not static
- Easy to categorize

Multitenancy-based strategy



- Static
- Easy to delegate administration
- Easy to include and separate new tenants

OU hierarchy considerations

Align OU strategy to administrative requirements, not the organizational chart because organizational charts are more subject to change than you 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 for 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

Demonstration: Delegating administrative permissions on an OU

In this demonstration you will see how to:

- Create a new OU
- Use the Delegation of Control Wizard to assign a task
- Use advanced OU security to assign granular permissions to the Research Managers group

Module Review and Takeaways

- Real-world Issues and Scenarios
- Tools
- Best Practice
- Common Issues and Troubleshooting Tips

Q&A