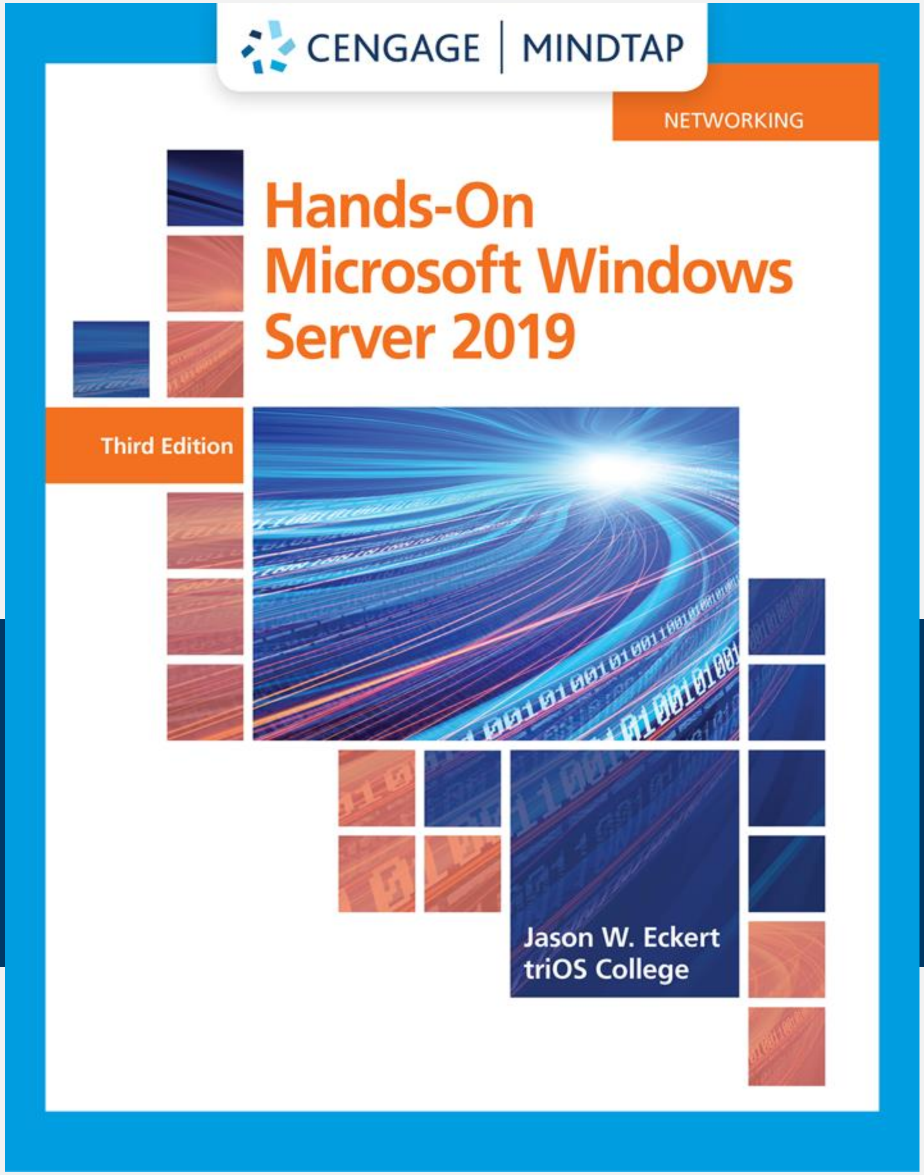


Introduction to Active Directory and Account Management

Module 4

Learning Objectives (1 of 3)

After completing this module you should be able to:

- Create and manage local user and group accounts
- Install and explain the purpose of Active Directory
- Outline the purpose of Active Directory objects, forests, trees, and trusts
- Describe the different types of Active Directory groups and their use within a forest
- Identify the features available within different domain and forest functional levels

Learning Objectives (2 of 3)

After completing this module you should be able to:

- Describe how sites can be used to control Active Directory replication
- Outline the function of the Active Directory global catalog and UGMC
- Identify the different FSMO roles available within a domain and forest
- Describe scenarios in which Azure Active Directory can be used within an organization

Learning Objectives (3 of 3)

After completing this module you should be able to:

- Use Active Directory Domains and Trusts to raise functional levels and create trust relationships
- View and raise functional levels using command line utilities
- Use Active Directory Sites and Services to manage sites and global catalog
- Use Active Directory Users and Computers to create and manage OU, user, group, and computer objects

Working with Local Users and Groups (1 of 7)

- Local user account authentication
  - Must provide valid user name and password
- Local user account assigned rights to the operating system
  - Examples: change system time or shut down the system
- Local user account granted access to resources
  - Based on the resource’s Access Control List (ACL)
- Local group accounts
  - Simplify assigning rights and permissions to multiple local user accounts

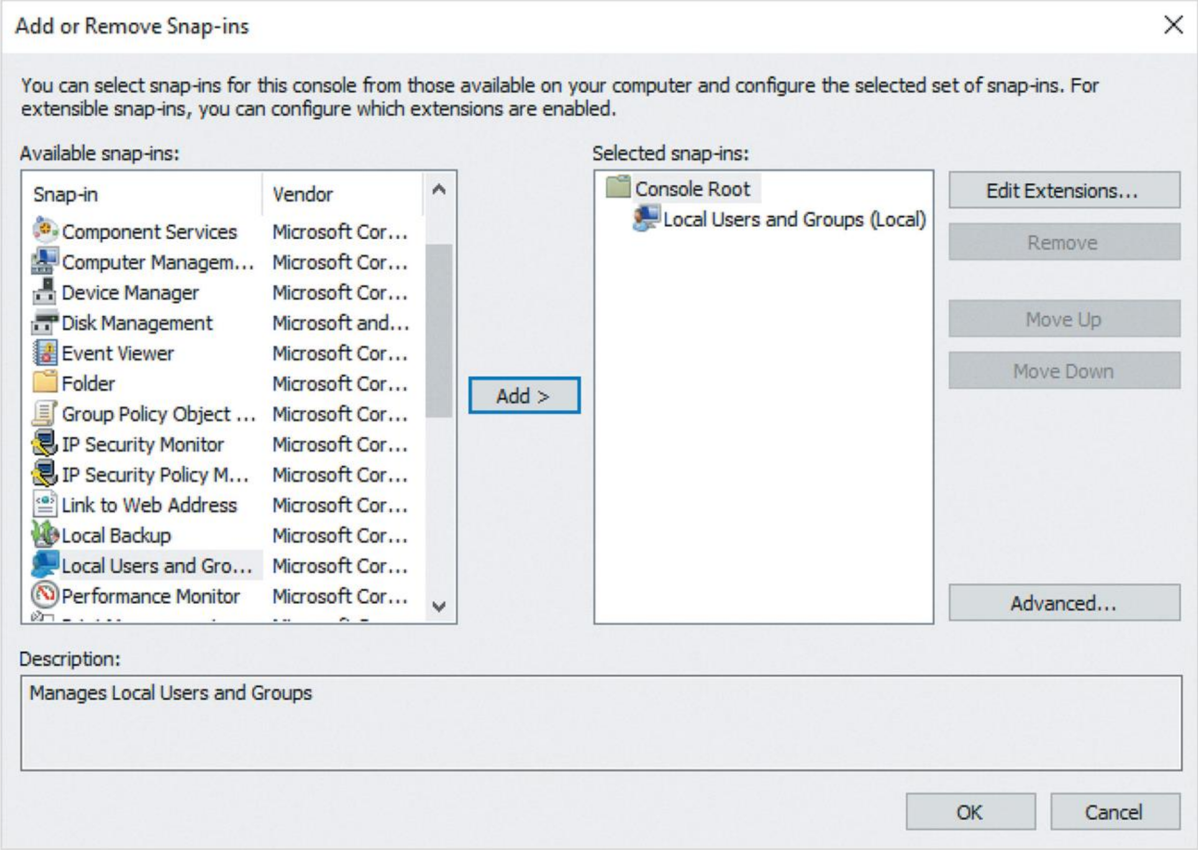
Working with Local Users and Groups (2 of 7)

- Security Accounts Manager (SAM) Registry database
  - Stores local user and group accounts
- Local user accounts used to authenticate users following workgroup installation
  - Administrator and Guest
- Local group accounts for assigning rights and permissions following system installation
  - Administrators, Guests, and Users

Working with Local Users and Groups (3 of 7)

- To create local user and group accounts
  - Use the Local Users and Groups MMC snap-in
- To create a new local user account
  - Select the Users folder from Local Users and Groups MMC snap-in
    - Choose appropriate user’s tasks after installation
- To create a new local group account
  - Select the Groups folder from Local Users and Groups MMC snap-in

Working with Local Users and Groups (4 of 7)



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Backup	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...
Performance Monitor	Microsoft Cor...

Selected snap-ins:

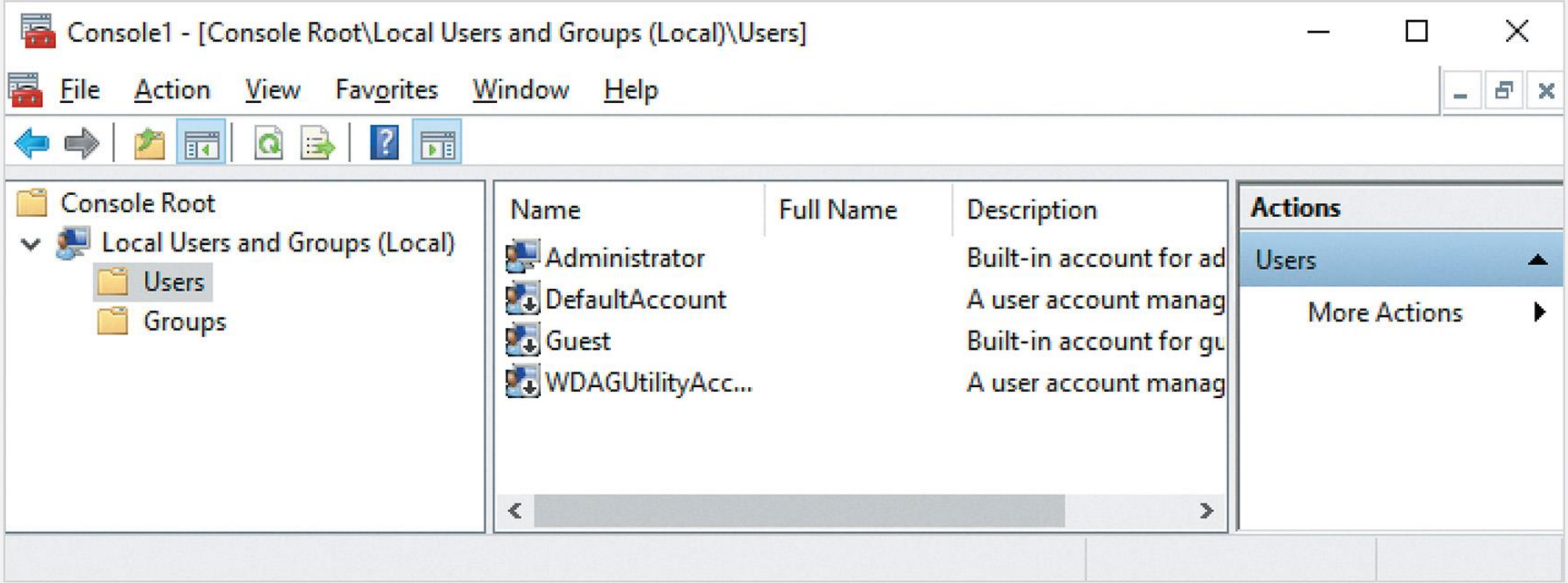
- Console Root
  - Local Users and Groups (Local)

Description:

Manages Local Users and Groups

Figure 4-1 Adding the Local Users and Groups MMC snap-in

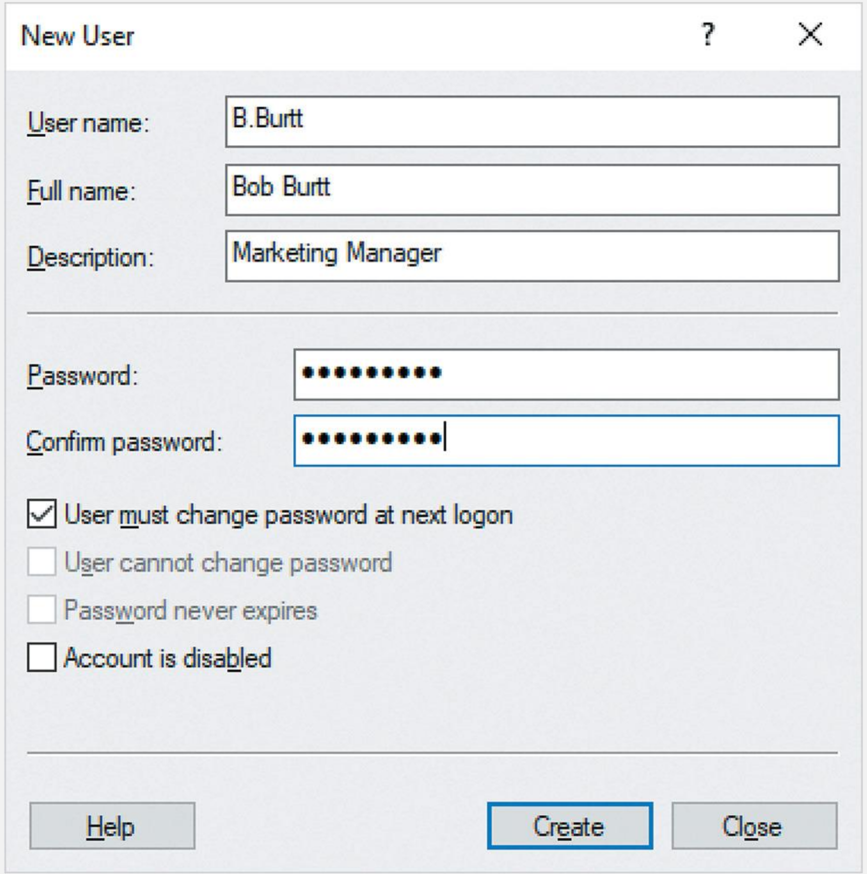
Working with Local Users and Groups (5 of 7)


Console1 - [Console Root\Local Users and Groups (Local)\Users]
File
Action
View
Favorites
Window
Help
Console Root
Local Users and Groups (Local)
Users
Groups
Actions
Users
More Actions

Name	Full Name	Description
Administrator		Built-in account for ad
DefaultAccount		A user account manag
Guest		Built-in account for gu
WDAGUtilityAcc...		A user account manag

Figure 4-2 The Local Users and Groups MMC snap-in

Working with Local Users and Groups (6 of 7)



New User

User name: B.Burtt

Full name: Bob Burtt

Description: Marketing Manager

Password: ●●●●●●●●●●

Confirm password: ●●●●●●●●●●

☑ User must change password at next logon

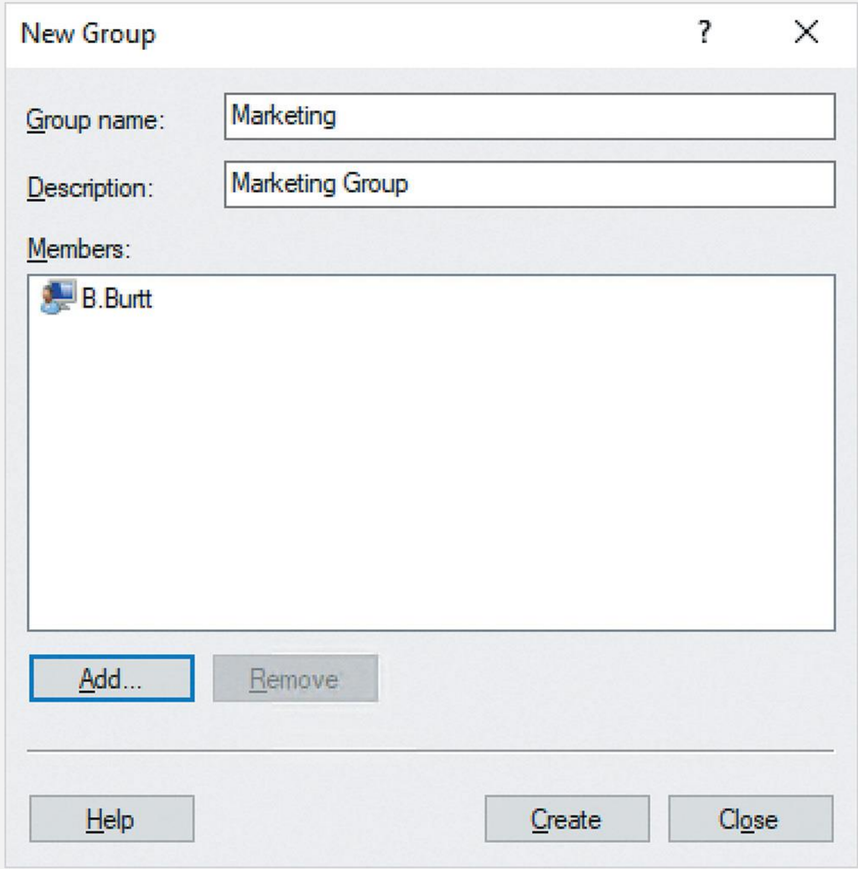
□ User cannot change password

□ Password never expires

□ Account is disabled

Figure 4-3 Creating a new local user account

Working with Local Users and Groups (7 of 7)



Group name: Marketing

Description: Marketing Group

Members:

B.Burtt

Figure 4-4 Creating a new local group account

Active Directory Basics

- Options for logging into an Active Directory domain computer
  - Local user account
  - Domain user account
    - Encrypted token and domain group account issued to the computer
- Domain user, group, and computer accounts stored as objects in a database
  - Active Directory database conforms to ITU X.500 standard
- Lightweight Directory Access Protocol (LDAP) provides quick access
- Active Directory Group Policy provides advantageous features

Active Directory Objects

- Active Directory schema
  - All available object types (classes) and associated properties (attributes)
  - Schema can be extended
- Leaf objects represent a user account, group account, or computer account
- Container objects within the Active Directory database
  - Group leaf objects for ease of administration and Group Policy application
  - Domains, organizational units (OUs), sites

Active Directory Forests, Trees, and Trusts (1 of 4)

- Active Directory forests
  - Provide for multiple domains within the same organization
  - Forest root domain: first domain in a forest
- Using additional domain controllers
  - Add them to the forest root domain
  - Configure them to host an Active Directory database for another domain within the same forest
- Active Directory tree has parent and child domains

Active Directory Forests, Trees, and Trusts (2 of 4)

- Trust relationship (trust)
  - Allows users to access resources within other domains
  - Requires access within the resource’s ACL
  - Trust relationships represented by arrow symbols in tree diagram
- Transitive property minimizes number of trust relationships needed
- Other types of trusts
  - Shortcut trust speeds up resource access
  - External trust, forest trust, realm trust

Active Directory Forests, Trees, and Trusts (3 of 4)

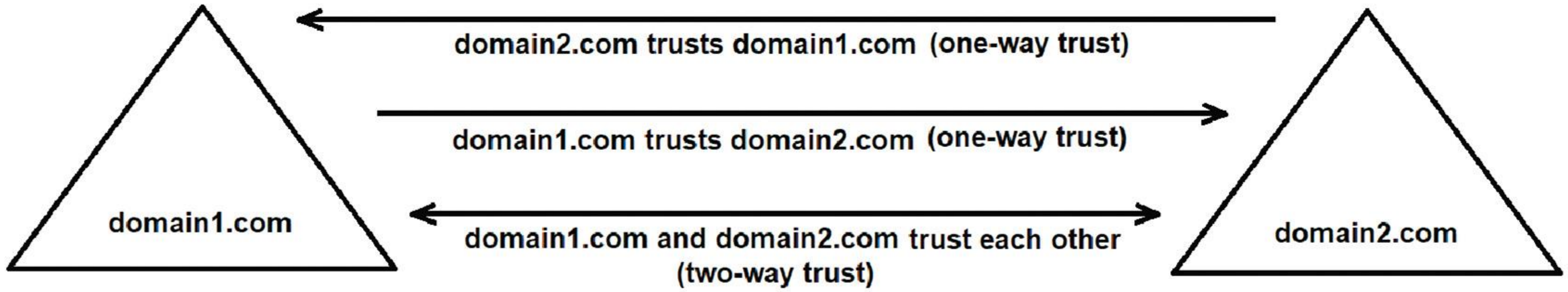

domain2.com trusts domain1.com (one-way trust)
domain1.com trusts domain2.com (one-way trust)
domain1.com
domain1.com and domain2.com trust each other (two-way trust)
domain2.com

Figure 4-7 Trust relationship types between domain1.com and domain2.com

Active Directory Forests, Trees, and Trusts (4 of 4)

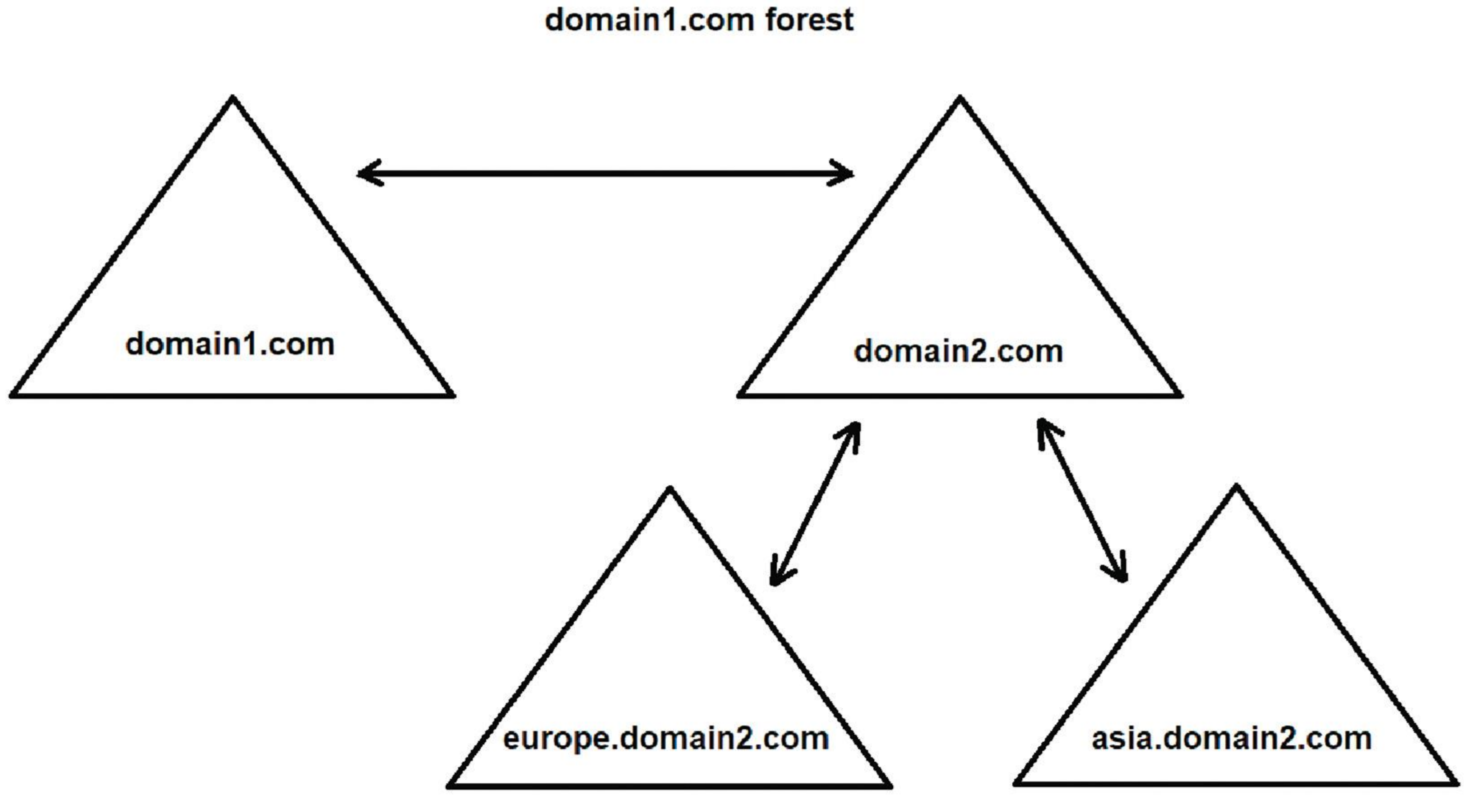


Figure 4-8 Default trust relationships within the domain1.com forest

Active Directory Groups (1 of 2)

- Two main types of group accounts
  - Distribution groups and security groups
- Group scopes
  - Organize rights and permissions assignments across multiple domains
  - Use a combination within a forest to organize the assignment of permissions
  - Global scope
  - Domain local scope
  - Universal scope

Active Directory Groups (2 of 2)

Table: 4-1 Active Directory group scopes		
Group scope	**Allowed members**	**Domains that can access the group**
Global	Objects located within the same domain as the global group	Any domain in the forest
Domain local	Objects located within any domain in the forest	Only the domain where the local group resides
Universal	Objects located within any domain in the forest	Any domain in the forest

Domain and Forest Functional Levels (1 of 3)

- Microsoft NT4 Server single sign-on implementation
  - Primary domain controller (PDC) and backup domain controllers (BDCs)
- Windows 2000 Server Active Directory required backward compatibility
- New Windows Server versions introduce additional Active Directory features
- Domain functional levels
  - Allow backward compatibility to older versions of Active Directory
- Active Directory forest functional level
  - Defines minimum domain functional level for each domain within the forest

Domain and Forest Functional Levels (2 of 3)

Table: 4-2 Windows Server 2019 domain functional levels	
Functional level	**New Active Directory features provided**
Windows Server 2008	Distributed File System (DFS) replication between domain controllers, Advanced Encryption Standard (AES) security for Kerberos authentication, and enhanced user account password policies
Windows Server 2008 R2	Service Principle Name (SPN) identification for network services
Windows Server 2012	Compound authentication, which creates Kerberos tickets with additional information used by other services, and Kerberos armoring, which creates a secure channel for authentication that is protected against network attacks
Windows Server 2012 R2	Additional encryption technologies for Kerberos authentication, as well as the ability to create authentication policies
Windows Server 2016	Additional Kerberos authentication features

Domain and Forest Functional Levels (3 of 3)

Table: 4-3 Windows Server 2019 forest functional levels	
Functional level	**New Active Directory features provided**
Windows Server 2008	No additional features beyond those within the Windows Server 2008 domain functional level
Windows Server 2008 R2	The ability to create and use the Active directory Recycle Bin to recover deleted objects
Windows Server 2012	No additional features beyond those within the Windows Server 2012 domain functional level
Windows Server 2012 R2	No additional features beyond those within the Windows Server 2012 R2 domain functional level
Windows Server 2016	The ability to use the Microsoft Identity Manager (MIM) to restrict malicious access to Active Directory using Privilege Access Management (PAM)

Sites and Active Directory Replication

- Active Directory database
  - Schema partition
  - Configuration partition
  - Domain partition
- Control Active Directory replication bandwidth usage
  - Site object (site) represents a physical location in an organization
    - Associated with one or more subnet objects representing IP networks containing domain controllers
    - Connected to other site objects using site link objects

Global Catalog

- Global catalog provides a list of all object names in a forest
  - Stored on at least one domain controller in the forest
  - Required to complete authentication process and log in to the domain
    - Cached credentials might provide access if global catalog not available
- User Principle Name (UPN) is a unique name in the global catalog
  - Users can use it to log in to their domain from any computer in the forest
- Global catalog updates
  - Issue might be resolved with Universal Group Membership Caching (UGMC)

FSMO Roles (1 of 3)

- Flexible Single Master Operations (FSMO) functions
  - Functions that must be coordinated from a single domain controller
- Domain controller configuration
  - To hold a single FSMO role
  - To hold all FSMO roles for its domain or forest
- Five FSMO roles available within Active Directory
  - First domain controller installed within the forest root domain contains all five
- Problem if domain controller holding an FSMO role becomes unavailable

FSMO Roles (2 of 3)

Table: 4-4 Active Directory FSMO roles		
FSMO Role	**Number per Domain or Forest**	**Function**
Schema Master	1 per forest	Must be contacted in order to modify the Active Directory schema. Any schema changes are then replicated by the Schema Master to all other domain controllers in the forest.
Domain Naming Master	1 per forest	Must be contacted in order to add or remove domains and trust relationships within the forest. Any changes to the domain and trust configuration of the forest are then replicated by the Domain Naming Master to all other domain controllers in the forest. For best performance, the domain controller that holds the Domain Naming Master should also hold a copy of the global catalog.
PDC Emulator	1 per domain	In legacy Active Directory domains, this role emulated a Windows NT4 PDC for backward compatibility. However, in modern Active Directory domains, the PDC Emulator coordinates user password changes and sends time information to each computer within the domain.

FSMO Roles (3 of 3)

Table: 4-4 Active Directory FSMO roles		
FSMO Role	**Number per Domain or Forest**	**Function**
RID Master	1 per domain	Issues sequential ranges of **Relative Identifiers (RIDs)** to domain controllers within the domain. RIDs are used to create unique SIDs for newly created objects in the domain. Because the RID Master generates unique ranges of RIDs for each domain controller, SIDs are guaranteed to be unique amongst domain objects. When a domain controller has exhausted its range of RIDs, it contacts the RID Master to obtain another range.
Infrastructure Master	1 per domain	Coordinates group membership, as well as the use of GUIDs and DNs between the current domain and other domains in the forest. Because the global catalog provides similar functionality, the Infrastructure Master should be placed on a domain controller that does not contain the global catalog.

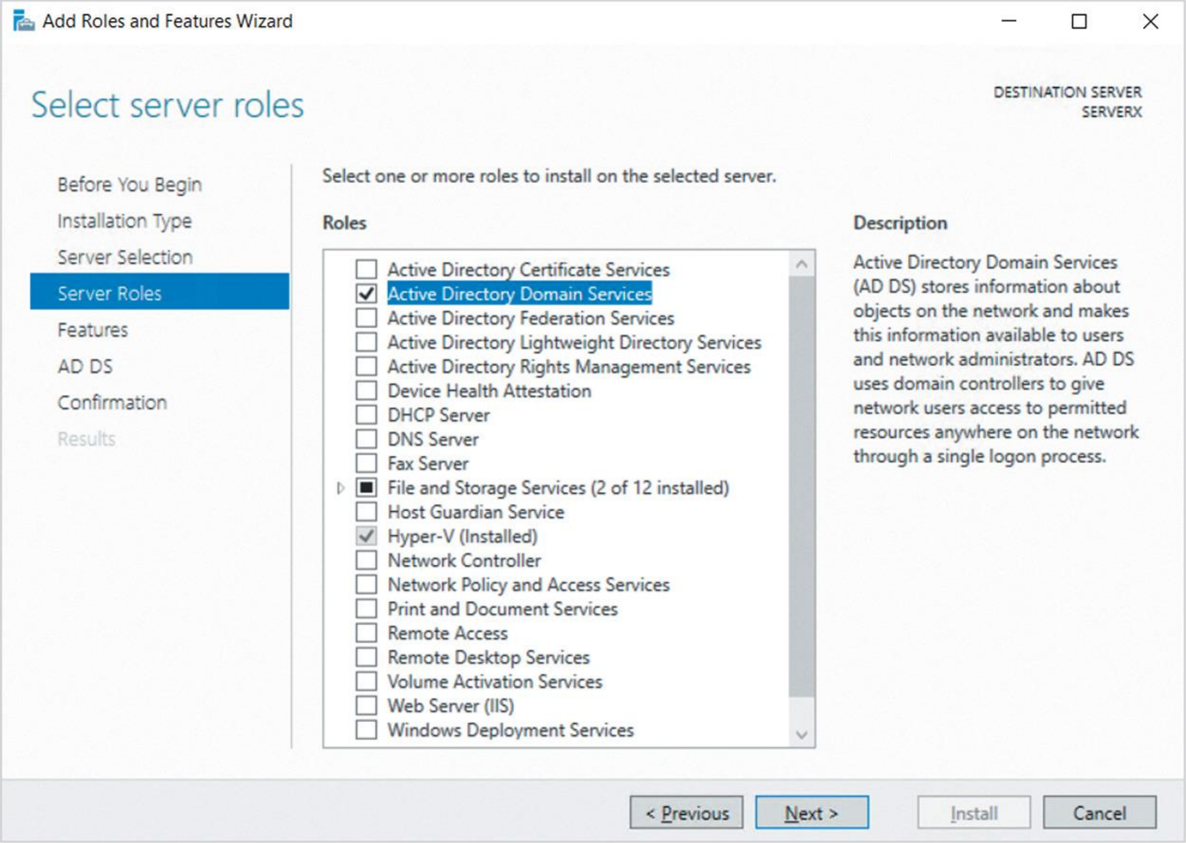
Azure Active Directory

- Active Directory service within the Microsoft Azure cloud
- Provides the same single sign-on features of Active Directory
- Designed to allow access to cloud applications
- Can be configured to trust an organization's Active Directory forest
- Can be configured to mirror an organization's Active Directory forest using a synchronization service
- Can be used to replace an Active Directory forest within an organization
  - If Internet connection is consistently robust

Installing Active Directory (1 of 3)

- Open Server Manager and select the Active Directory Domain Services role
- Progress through the Add Roles and Features Wizard
  - Installs files necessary to create a domain controller, management tools, and Windows PowerShell cmdlets
- Select *Promote this server to a domain controller* from the Add Roles and Features Wizard

Installing Active Directory (2 of 3)



Select server roles

DESTINATION SERVER
SERVERX

Select one or more roles to install on the selected server.

Roles

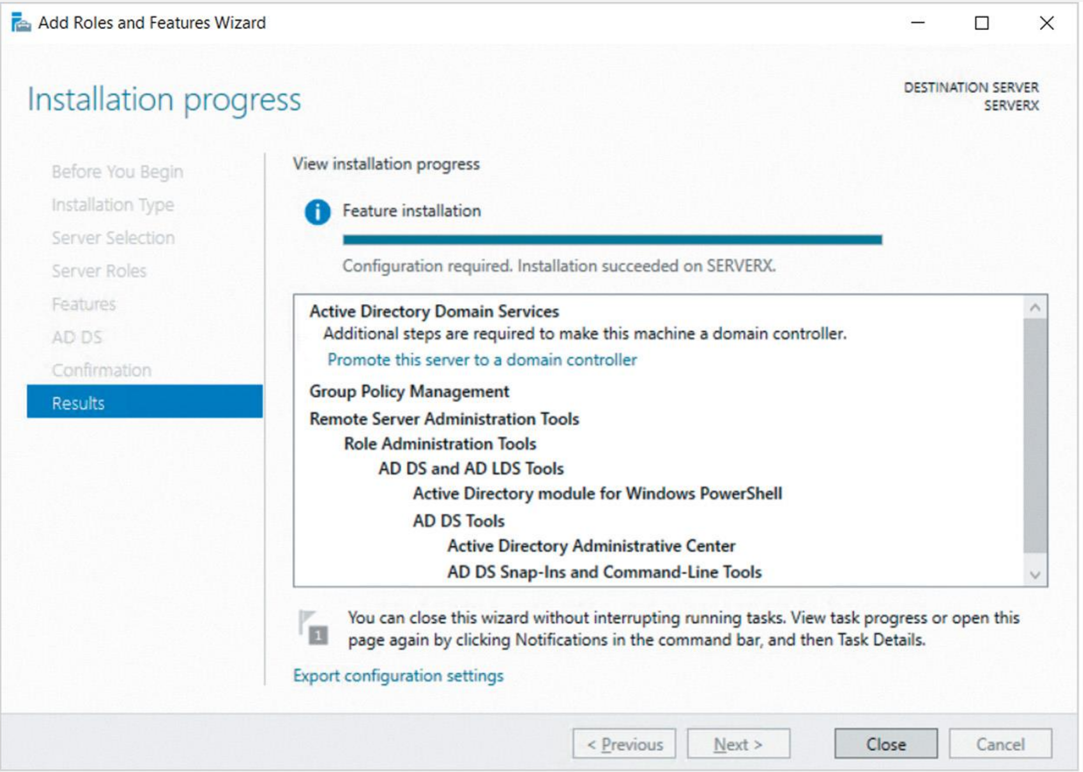
- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ▪ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- ☑ Hyper-V (Installed)
- □ Network Controller
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

Figure 4-11 Installing Active Directory Domain Services

Installing Active Directory (3 of 3)



View installation progress

Feature installation

Configuration required. Installation succeeded on SERVERX.

Active Directory Domain Services

Additional steps are required to make this machine a domain controller.

Promote this server to a domain controller

Group Policy Management

Remote Server Administration Tools

Role Administration Tools

AD DS and AD LDS Tools

Active Directory module for Windows PowerShell

AD DS Tools

Active Directory Administrative Center

AD DS Snap-Ins and Command-Line Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

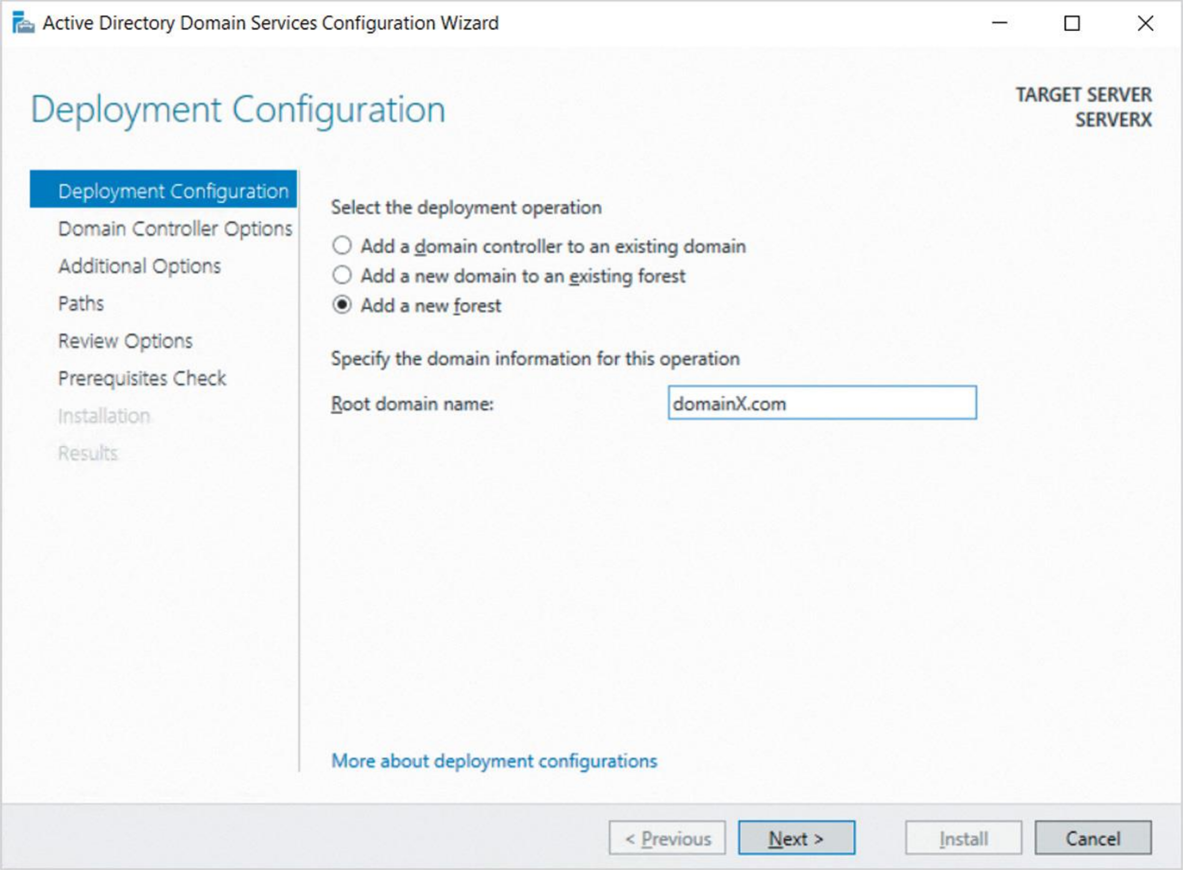
Export configuration settings

Figure 4-12 Completing the installation of Active Directory Domain Services

Installing a Forest Root Domain (1 of 5)

- Active Directory Domain Services Configuration Wizard
  - Select *Add a new forest* and specify new root domain name
  - Select domain controller options
    - Specify domain and forest functional levels, domain controller capabilities, and Directory Services Restore Mode (DSRM) password
  - Select DNS to specify DNS delegation
  - Select Additional Options to specify NetBIOS name
  - Select Paths to specify for folders
  - Review options and install

Installing a Forest Root Domain (2 of 5)



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
SERVERX

Select the deployment operation

○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

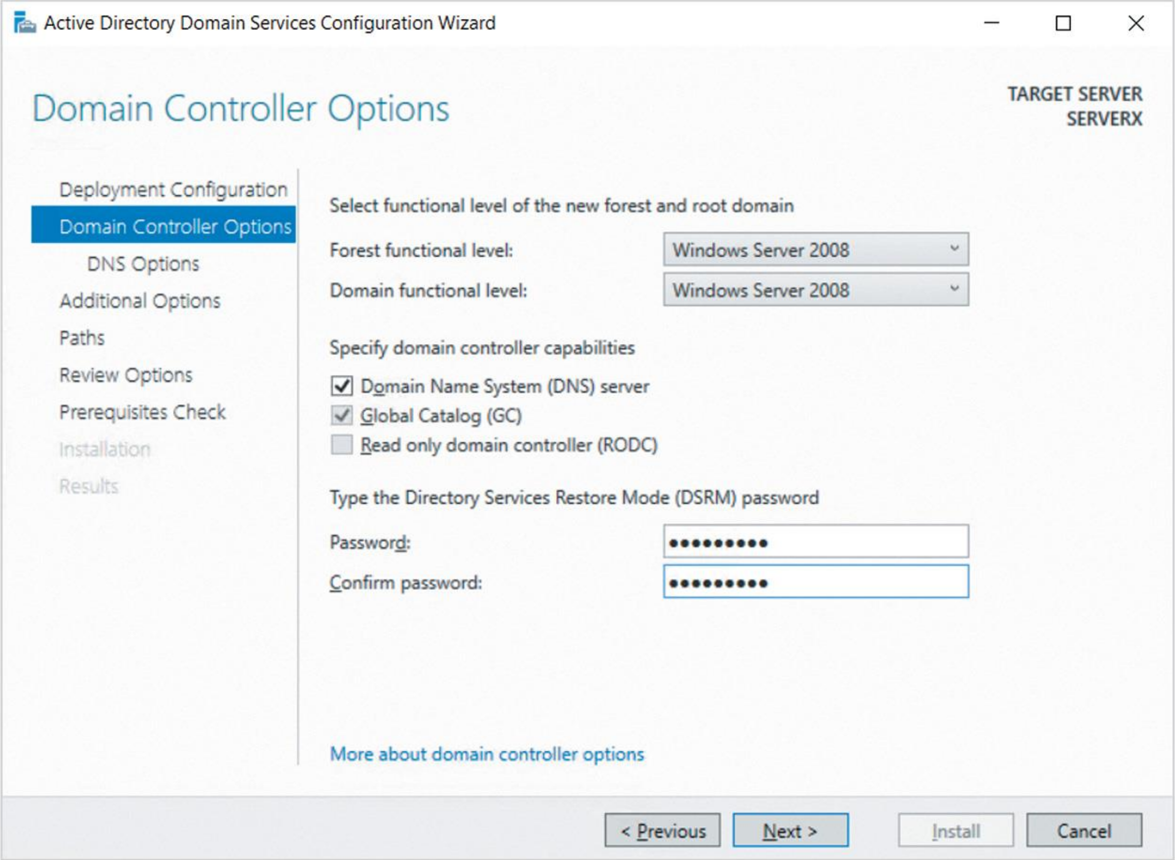
Specify the domain information for this operation

Root domain name: domainX.com

More about deployment configurations

Figure 4-13 Installing a forest root domain

Installing a Forest Root Domain (3 of 5)



Select functional level of the new forest and root domain

Forest functional level: Windows Server 2008

Domain functional level: Windows Server 2008

Specify domain controller capabilities

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

□ Read only domain controller (RODC)

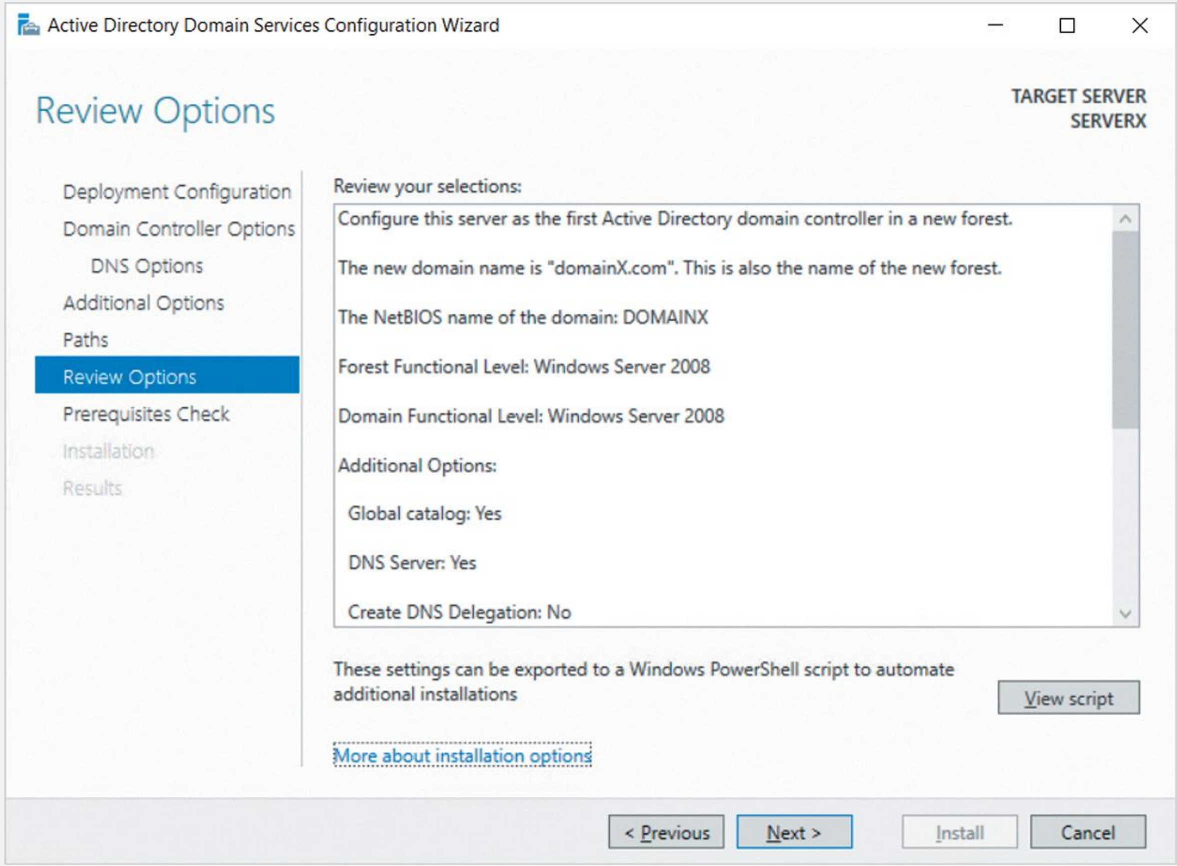
Type the Directory Services Restore Mode (DSRM) password

Password: •••••••••

Confirm password: •••••••••

Figure 4-14 Specifying domain controller options

Installing a Forest Root Domain (4 of 5)



Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "domainX.com". This is also the name of the new forest.

The NetBIOS name of the domain: DOMAINX

Forest Functional Level: Windows Server 2008

Domain Functional Level: Windows Server 2008

Additional Options:

Global catalog: Yes

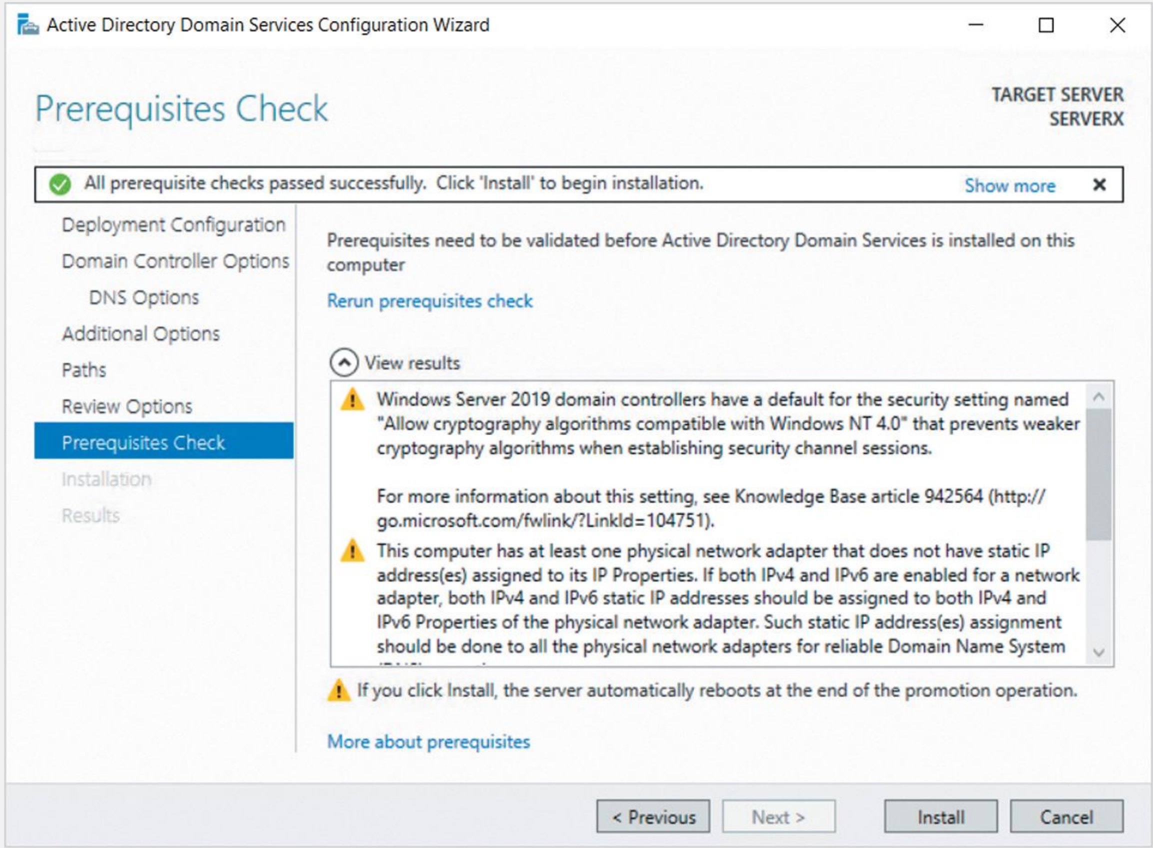
DNS Server: Yes

Create DNS Delegation: No

These settings can be exported to a Windows PowerShell script to automate additional installations

Figure 4-18 Reviewing Active Directory installation options

Installing a Forest Root Domain (5 of 5)



Prerequisites Check

TARGET SERVER
SERVERX

All prerequisite checks passed successfully. Click 'Install' to begin installation.

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

Rerun prerequisites check

View results

⚠ Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

⚠ This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System

⚠ If you click Install, the server automatically reboots at the end of the promotion operation.

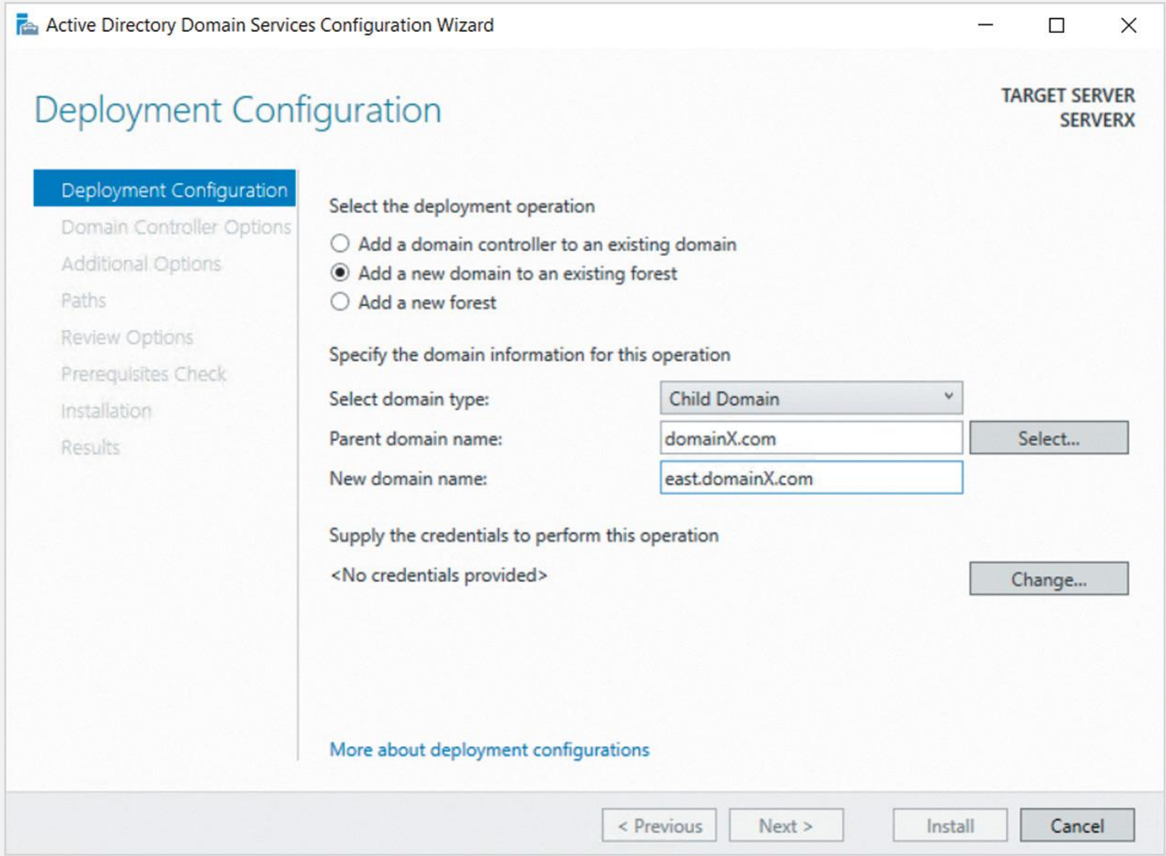
More about prerequisites

Figure 4-19 Checking prerequisites prior to Active Directory installation

Installing a Domain within an Existing Forest (1 of 2)

- Start the Active Directory Domain Services Configuration Wizard
  - Select *Add a new domain to an existing forest*
  - Adding a child domain
    - Specify name of the parent domain and name of the new child domain
  - Adding a new parent domain for a new tree
    - Select Tree Domain and specify the name of the parent domain
  - Authenticate as a user within a forest that is part of Enterprise Admins group
  - Progress through Wizard as if configuring a new forest root domain

Installing a Domain within an Existing Forest (2 of 2)



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
SERVERX

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

Select domain type: Child Domain

Parent domain name: domainX.com

New domain name: east.domainX.com

Supply the credentials to perform this operation

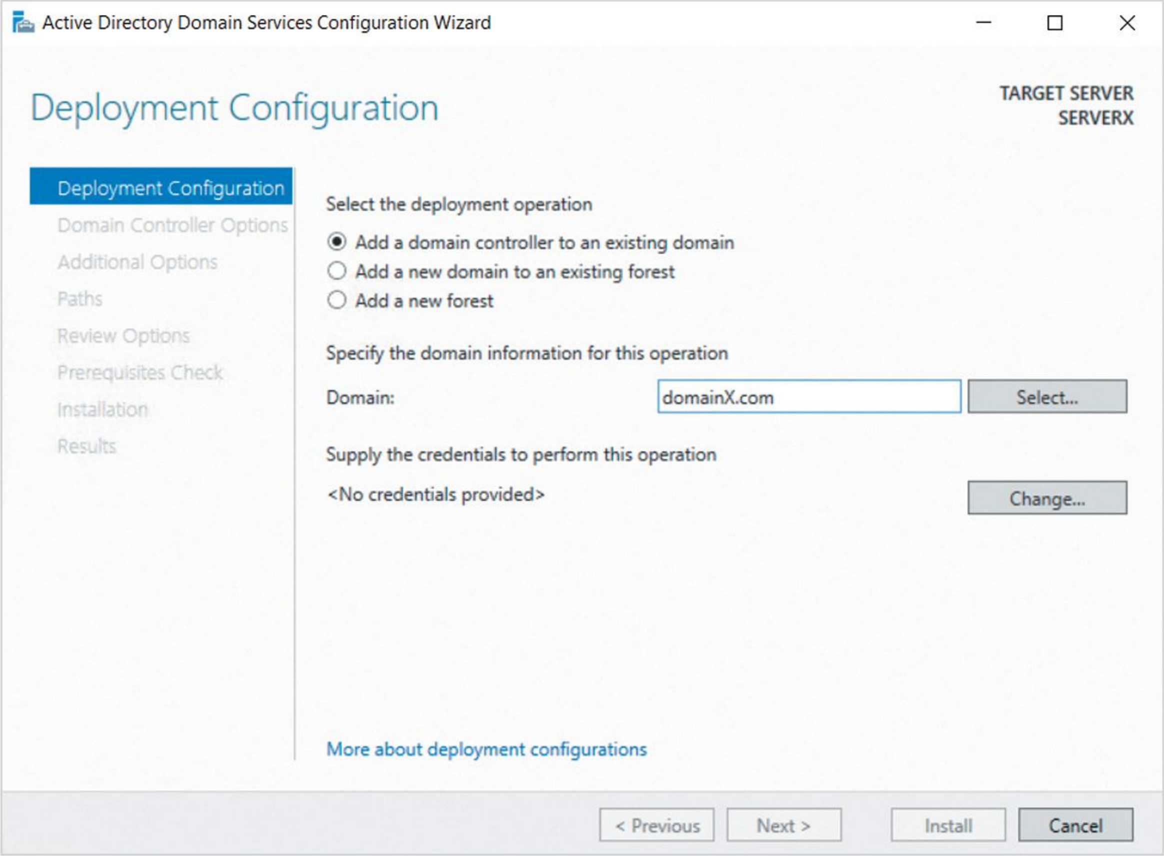
<No credentials provided>

Figure 4-21 Adding a new domain to a forest

Installing a Domain Controller within an Existing Domain (1 of 2)

- Start the Active Directory Domain Services Configuration Wizard
  - Select *Add a domain controller to an existing domain*
    - Specify the existing domain name within the Domain text box
  - Authenticate within the domain that is part of the Domain Admins group
    - Click Change and supply credentials
  - Progress through Wizard as if configuring a new forest root domain
    - No need to set the forest or domain functional levels
    - Can select where to obtain initial copy of Active Directory database

Installing a Domain Controller within an Existing Domain (2 of 2)



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
SERVERX

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: domainX.com

Supply the credentials to perform this operation

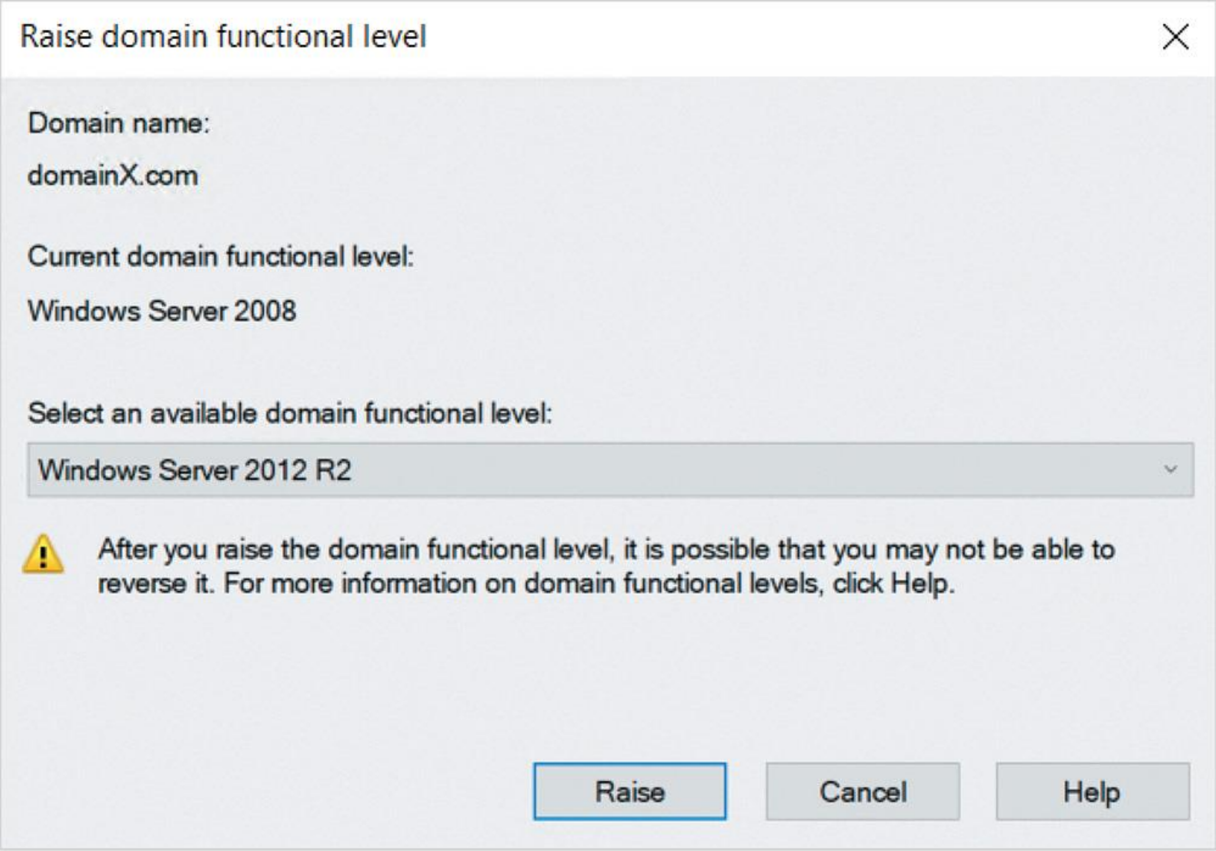
<No credentials provided>

Figure 4-22 Adding a new domain controller to an existing domain

Raising Functional Levels (1 of 3)

- Use the Active Directory Domains and Trusts tool
  - Select domain within the navigation pane
  - Click More Actions, Raise Domain Functional Level from the Actions pane
  - Select the appropriate functional level from the drop-down box, click Raise
- Can raise the forest functional level
  - Select Active Directory Domains and Trusts within the navigation pane
  - Click More Actions, Raise Forest Functional Level from the Actions pane
  - Select appropriate functional level from the drop-down box and click Raise

Raising Functional Levels (2 of 3)



Raise domain functional level

Domain name:

domainX.com

Current domain functional level:

Windows Server 2008

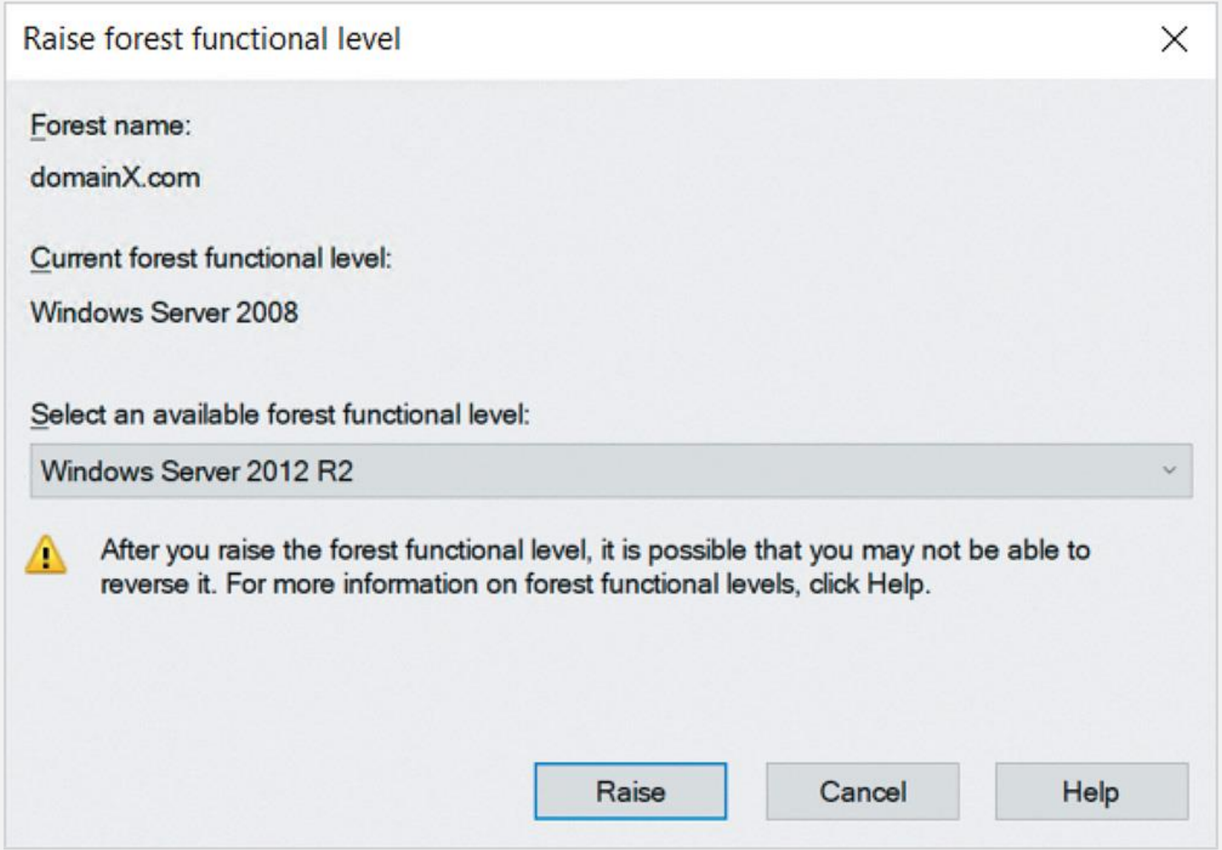
Select an available domain functional level:

Windows Server 2012 R2

After you raise the domain functional level, it is possible that you may not be able to reverse it. For more information on domain functional levels, click Help.

Figure 4-24 Raising the domain functional level

Raising Functional Levels (3 of 3)



Raise forest functional level

Forest name:

domainX.com

Current forest functional level:

Windows Server 2008

Select an available forest functional level:

Windows Server 2012 R2

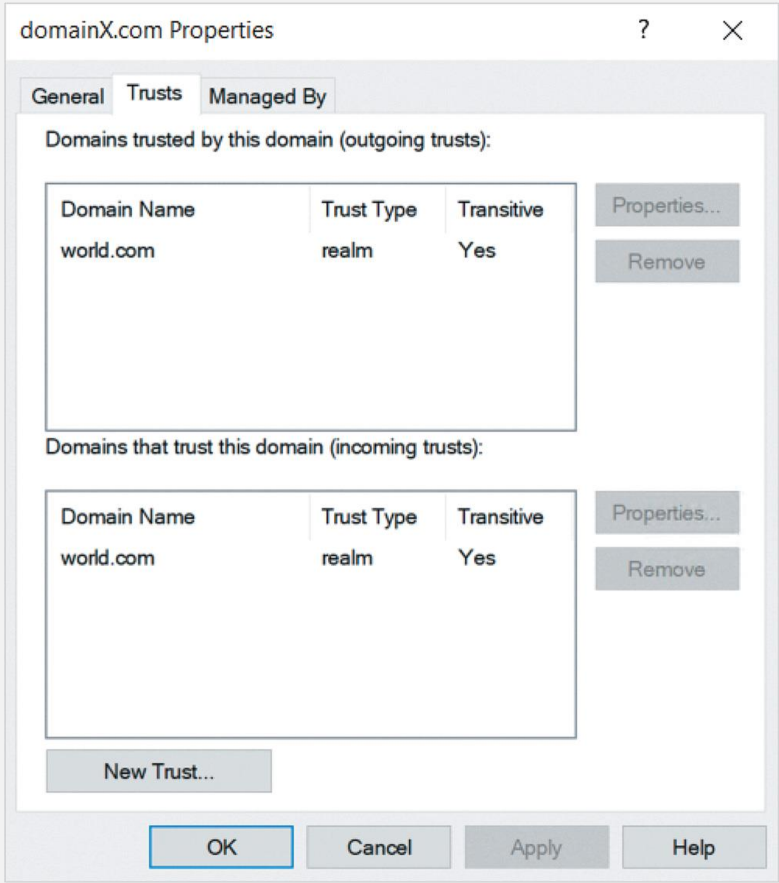
After you raise the forest functional level, it is possible that you may not be able to reverse it. For more information on forest functional levels, click Help.

Figure 4-25 Raising the forest functional level

Creating Trust Relationships (1 of 2)

- Use conditional forwarder to ensure DNS servers can resolve the DNS records
- Open the Active Directory Domains and Trusts tool
  - Select the domain within the navigation pane
  - Click More Actions, Properties from the Actions pane
- Domain window opens
  - Select the Trusts tab and click New Trust to start the New Trust Wizard
  - Choose options: external or forest; one-way outgoing or incoming or two-way; transitive or non-transitive, etc.
  - Select the trust and click Properties to validate or change trust settings

Creating Trust Relationships (2 of 2)



Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
world.com	realm	Yes

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
world.com	realm	Yes

Figure 4-28 Viewing trust relationships

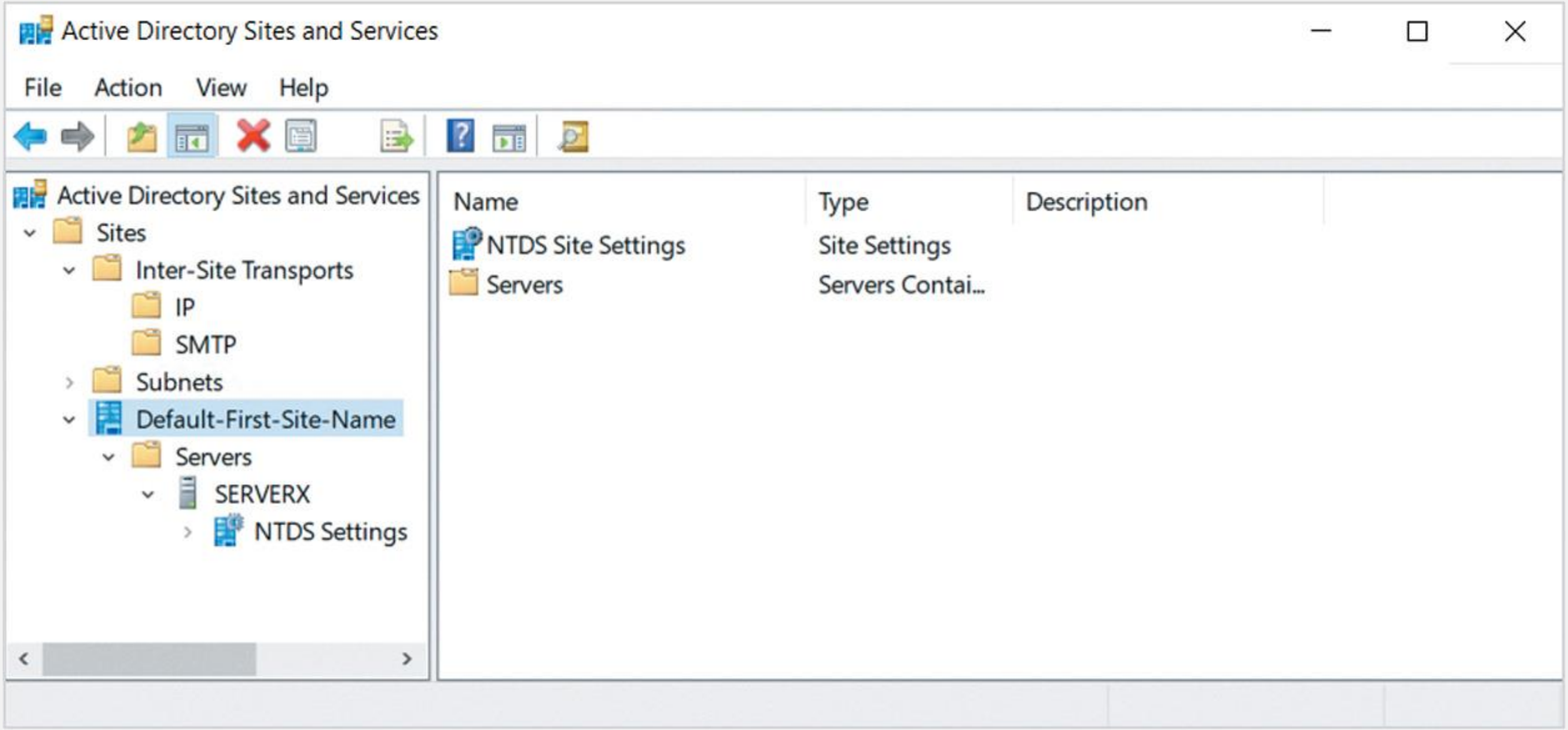
Managing FSMO Roles

- Command to view all FSMO roles held by domain controllers within your forest
  - `netdom query fsmo command`
- Other commands show domain controllers holding the forest-wide and domain-wide FSMO roles
- Fault tolerance may require movement of FSMO roles from one domain controller to another
  - Move one or multiple FSMO roles from one domain controller to another
  - If source domain controller offline, add the `–Force` option to the command
    - `Move-ADDirectoryServerOperationMasterRole`

Configuring Sites and Replication (1 of 6)

- Configuring sites
  - Open Active Directory Sites and Services tool
  - Right-click `Default-First-Site-Name` and rename
  - Right-click Sites folder to create additional sites
  - Supply site name and select the appropriate site link
  - Specify appropriate IP network and select the associated site
- Two protocols perform Active Directory replication
  - IP and Simple Mail Transfer Protocol (SMTP)

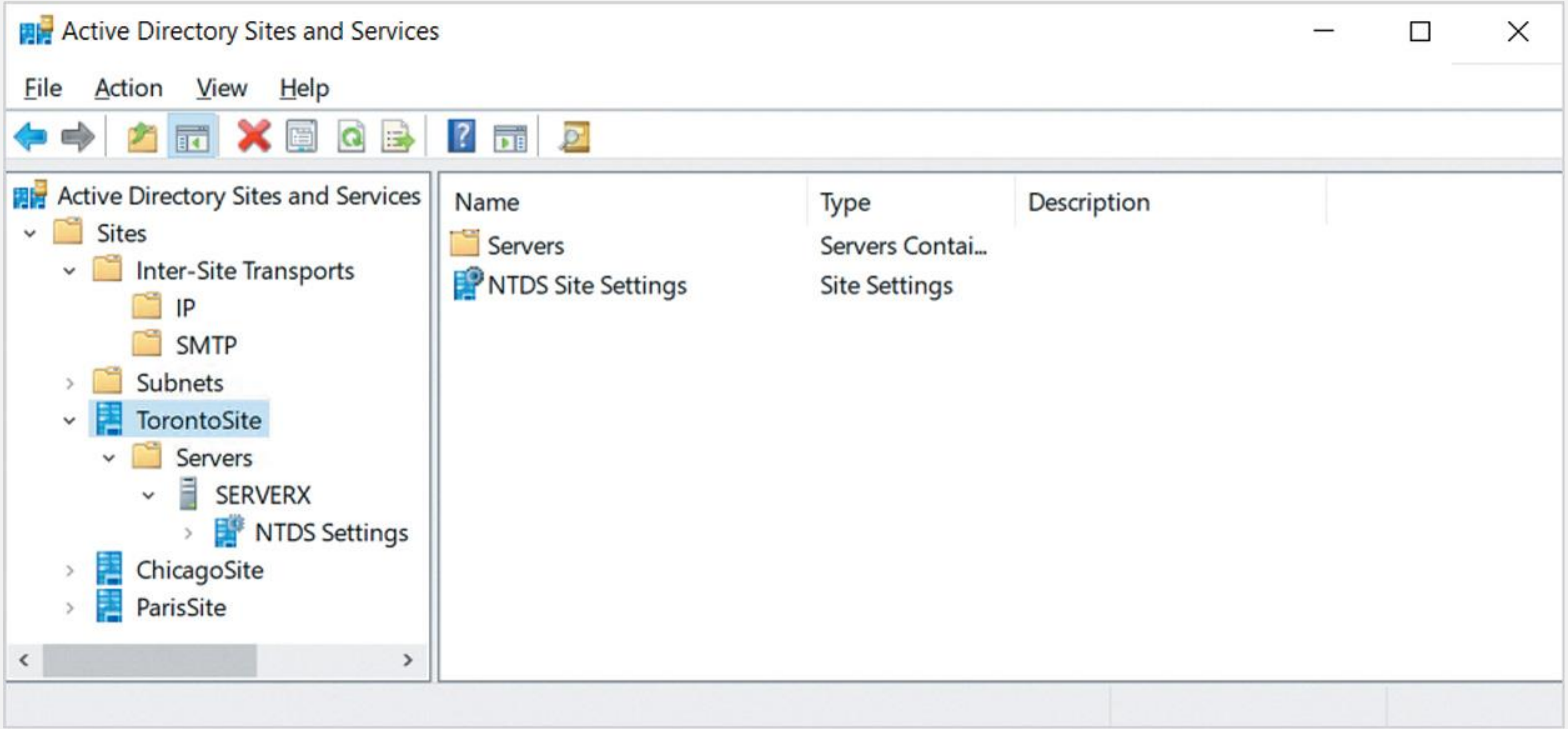
Configuring Sites and Replication (2 of 6)



Name	Type	Description
NTDS Site Settings	Site Settings	
Servers	Servers Contai...	

Figure 4-29 The Active Directory Sites and Services tool

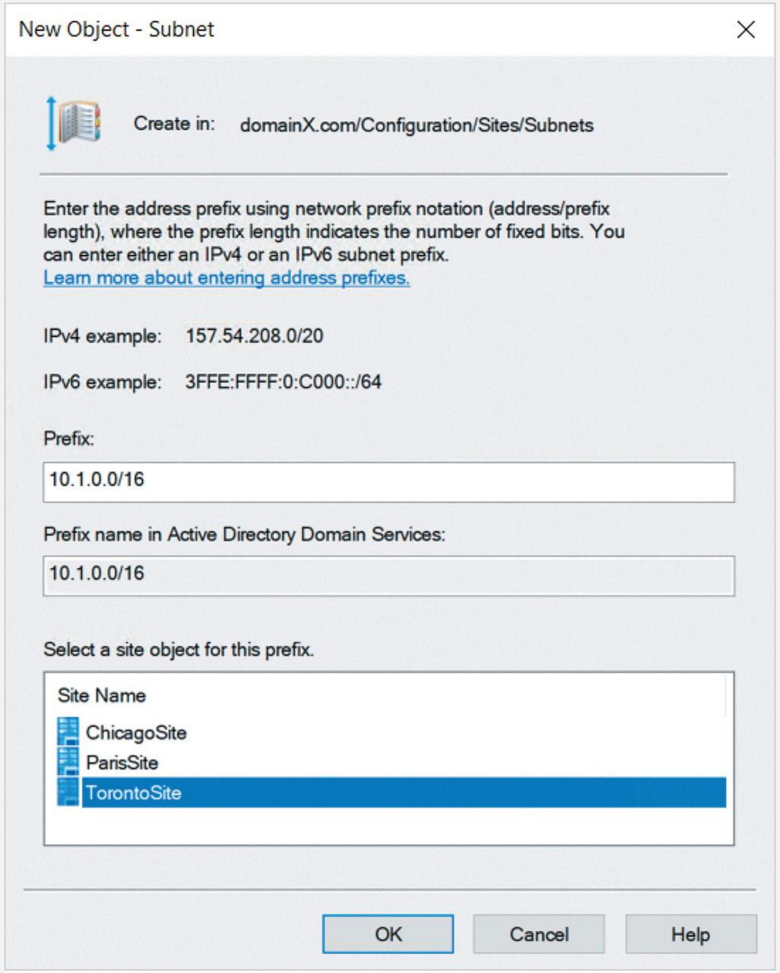
Configuring Sites and Replication (3 of 6)



Name	Type	Description
Servers	Servers Contai...	
NTDS Site Settings	Site Settings	

Figure 4-31 A sample site configuration

Configuring Sites and Replication (4 of 6)



New Object - Subnet

Create in: domainX.com/Configuration/Sites/Subnets

Enter the address prefix using network prefix notation (address/prefix length), where the prefix length indicates the number of fixed bits. You can enter either an IPv4 or an IPv6 subnet prefix.
Learn more about entering address prefixes.

IPv4 example: 157.54.208.0/20

IPv6 example: 3FFE:FFFF:0:C000::/64

Prefix: 10.1.0.0/16

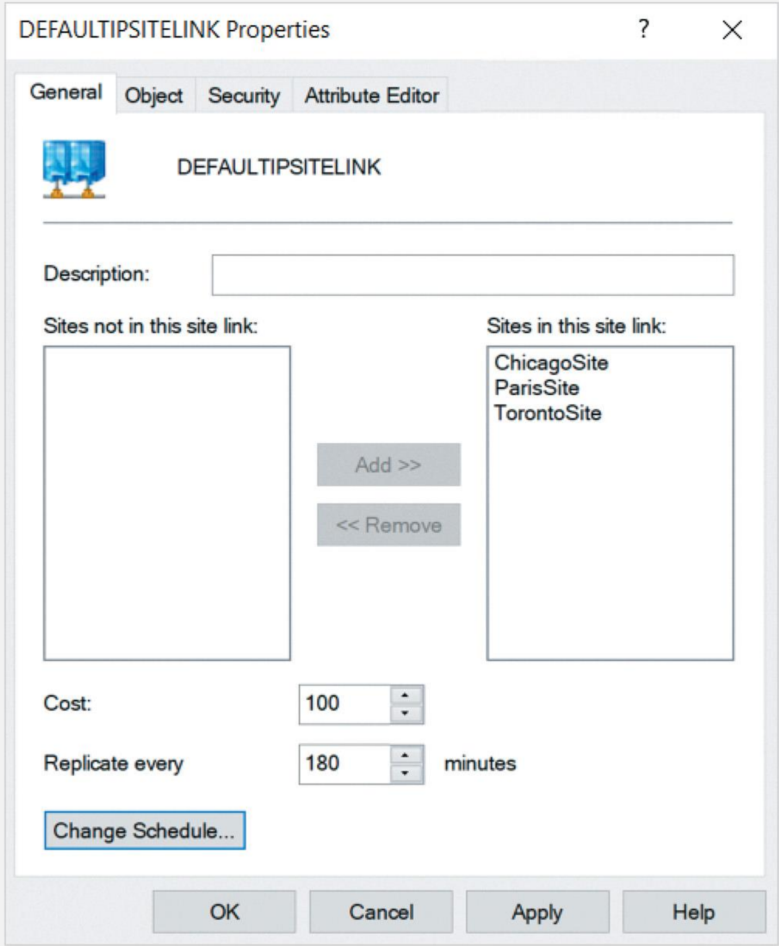
Prefix name in Active Directory Domain Services: 10.1.0.0/16

Select a site object for this prefix.

Site Name
- ChicagoSite
- ParisSite
- TorontoSite

Figure 4-32 Creating a new subnet object

Configuring Sites and Replication (5 of 6)



Description:

Sites not in this site link:

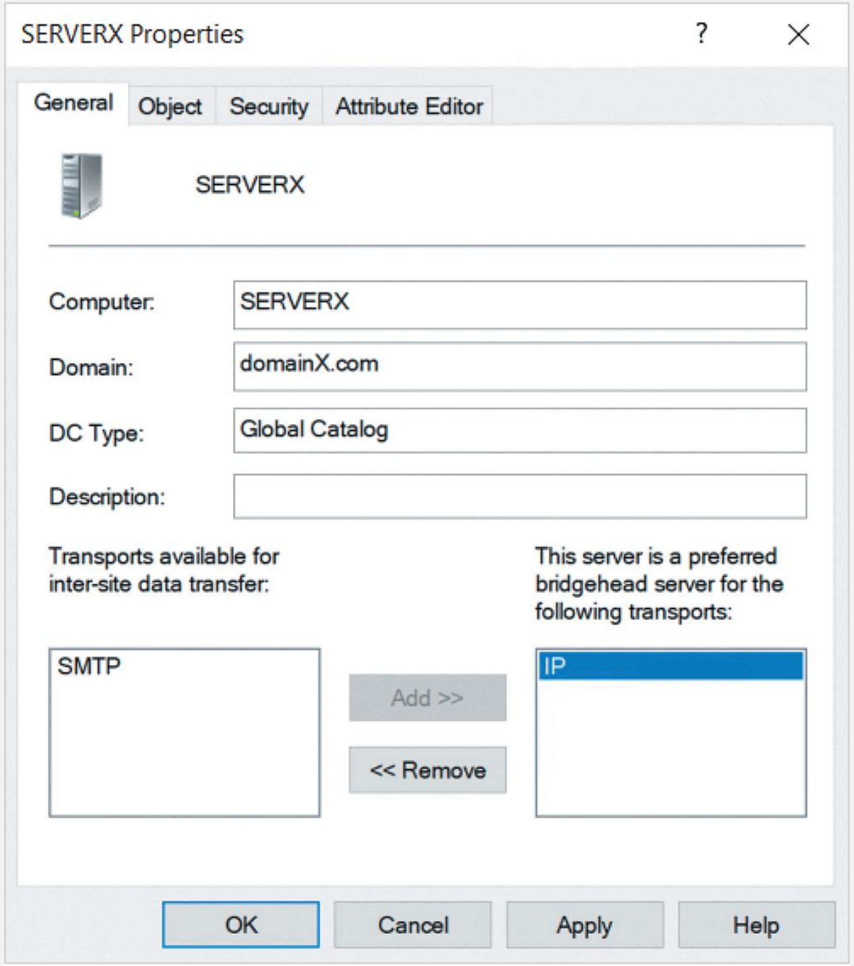
Sites in this site link:
ChicagoSite
ParisSite
TorontoSite

Cost: 100

Replicate every 180 minutes

Figure 4-33 Modifying the properties of the DEFAULTIPSITELINK

Configuring Sites and Replication (6 of 6)



Computer: SERVERX

Domain: domainX.com

DC Type: Global Catalog

Description:

Transports available for inter-site data transfer: SMTP

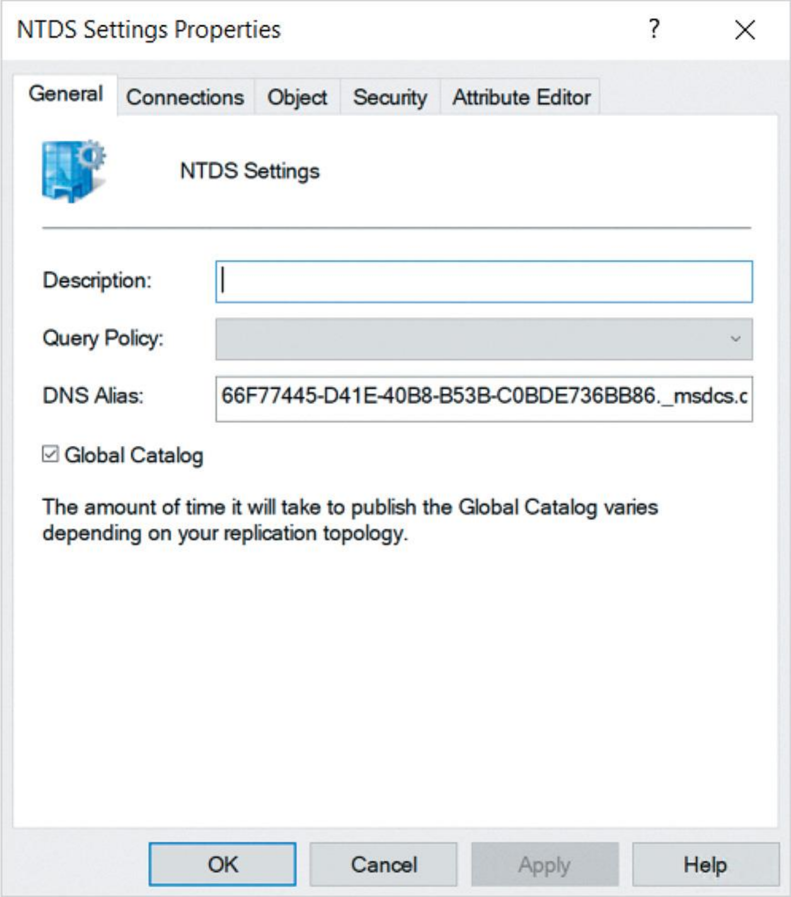
This server is a preferred bridgehead server for the following transports: IP

Figure 4-35 Configuring a bridgehead server

Configuring Global Catalog and UGMC (1 of 3)

- Configure a domain controller to host a copy of the global catalog
- Open Active Directory Sites and Services and click Properties
  - Right-click NTDS Settings under the server object for the domain controller
  - Select the Global Catalog option to place a copy of the global catalog on the domain controller
- UGMC can host a copy of the global catalog if replication concerns exist
  - Allows universal groups to be cached on domain controllers within the site
  - Allows fast logon

Configuring Global Catalog and UGMC (2 of 3)



NTDS Settings Properties

NTDS Settings

Description:

Query Policy:

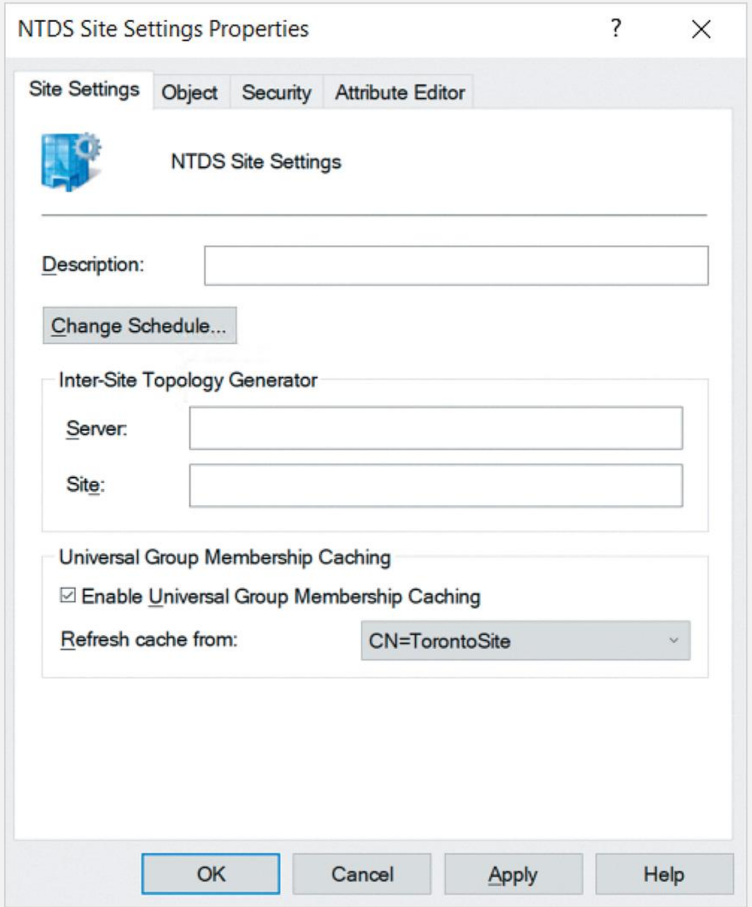
DNS Alias: 66F77445-D41E-40B8-B53B-C0BDE736BB86._msdcs.c

☑ Global Catalog

The amount of time it will take to publish the Global Catalog varies depending on your replication topology.

Figure 4-36 Configuring global catalog

Configuring Global Catalog and UGMC (3 of 3)



Description:

Inter-Site Topology Generator

Server:

Site:

Universal Group Membership Caching

☑ Enable Universal Group Membership Caching

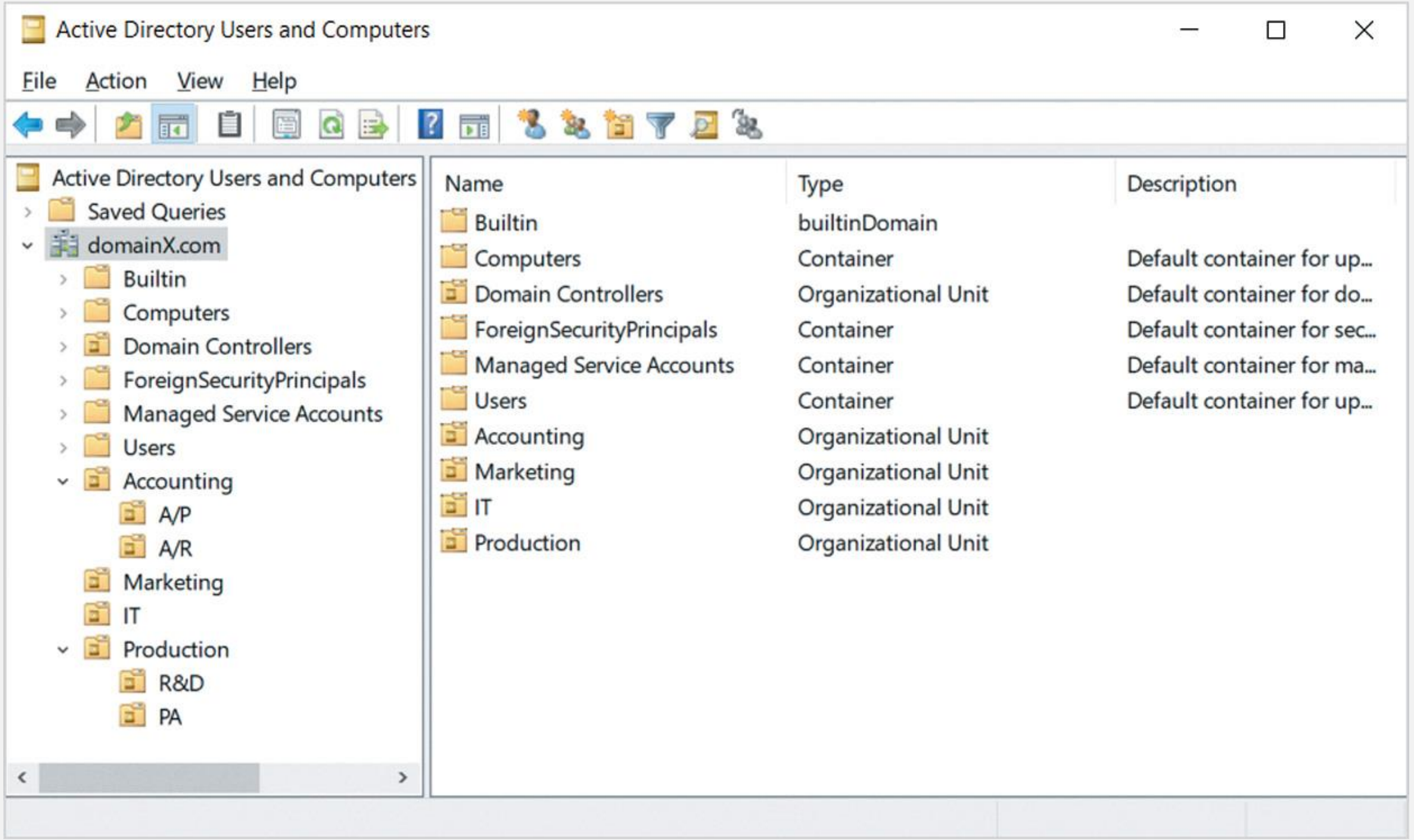
Refresh cache from: CN=TorontoSite

Figure 4-37 Enabling UGMC for a site

Working with Organizational Units (1 of 3)

- Open the Active Directory Users and Computers tool
  - New domain only has one OU called *Domain Controllers* by default
  - Other folders exist to organize the default objects within the domain
  - Create an OU
    - Right-click folder/domain object under which to create the OU
    - Click New, Organizational Unit
    - New window opens; supply the name of the OU
    - Verify *Protect container from accidental deletion* option

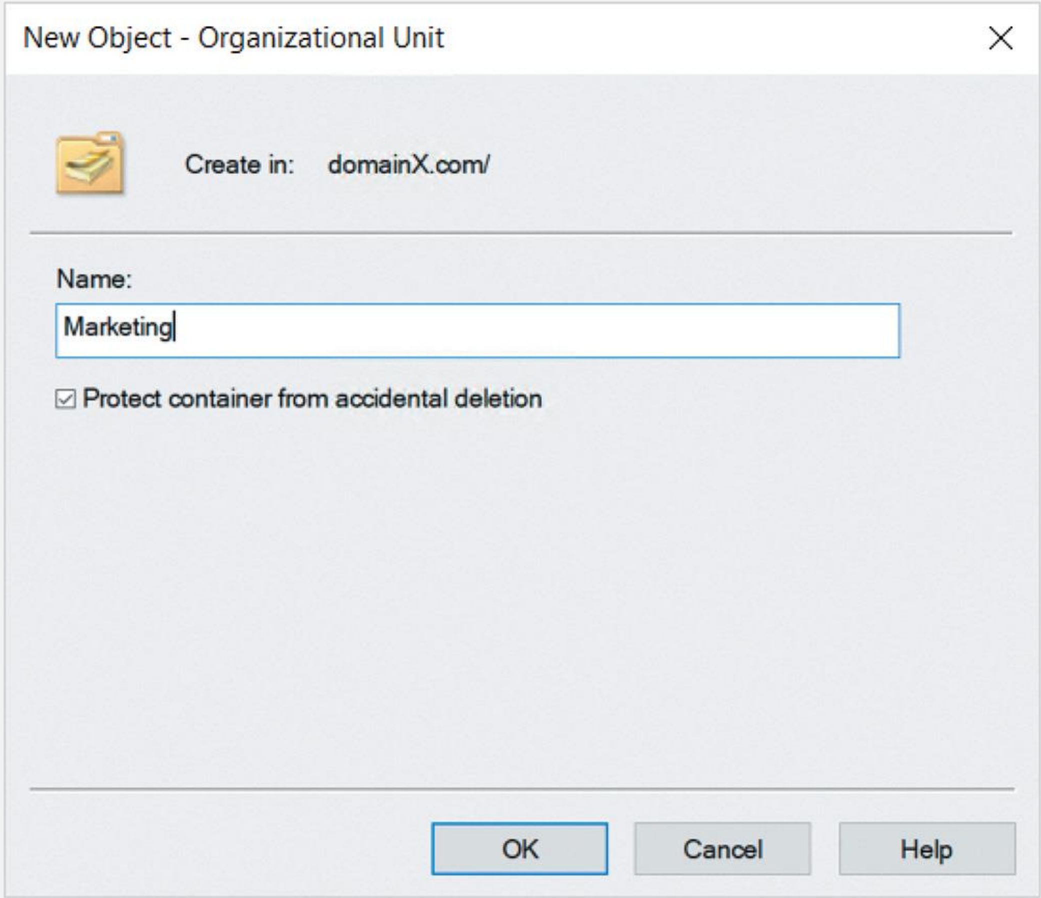
Working with Organizational Units (2 of 3)



Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Controllers	Organizational Unit	Default container for do...
ForeignSecurityPrincipals	Container	Default container for sec...
Managed Service Accounts	Container	Default container for ma...
Users	Container	Default container for up...
Accounting	Organizational Unit	
Marketing	Organizational Unit	
IT	Organizational Unit	
Production	Organizational Unit	

Figure 4-38 The Active Directory Users and Computers tool

Working with Organizational Units (3 of 3)


New Object - Organizational Unit

Create in: domainX.com/

Name:

Marketing

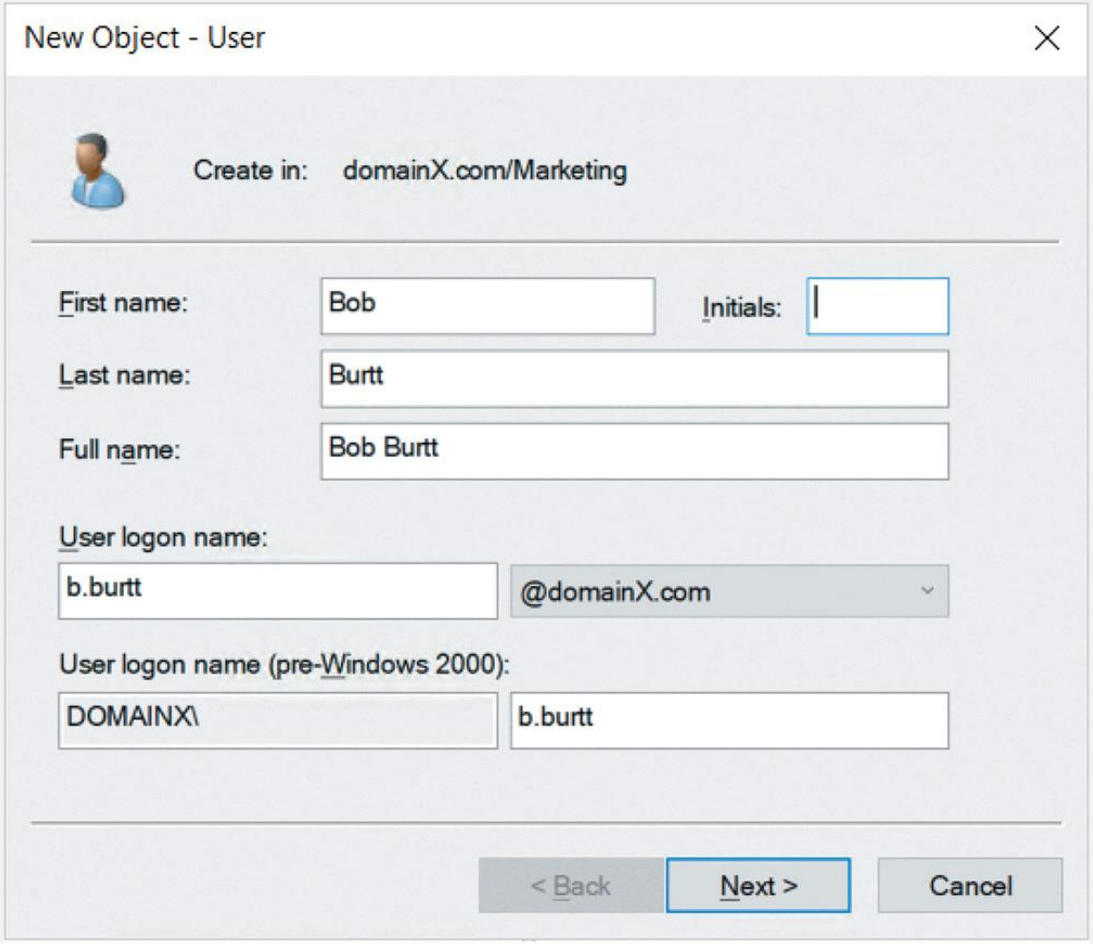
☑ Protect container from accidental deletion

Figure 4-39 Creating a new OU

Working with User Objects (1 of 4)

- Prior to a user logging in to an Active Directory domain:
  - Create a domain user account object for the user in the appropriate OU
    - Within Active Directory Users and Computers
    - Right-click the appropriate OU, click New, then click User
    - Opens the New Object – User wizard; supply appropriate information
    - Supply the new user password, account options
    - Create user object
    - Add the appropriate user attributes
    - Perform other common user management functions

Working with User Objects (2 of 4)



New Object - User

Create in: domainX.com/Marketing

First name: Bob

Initials:

Last name: Burtt

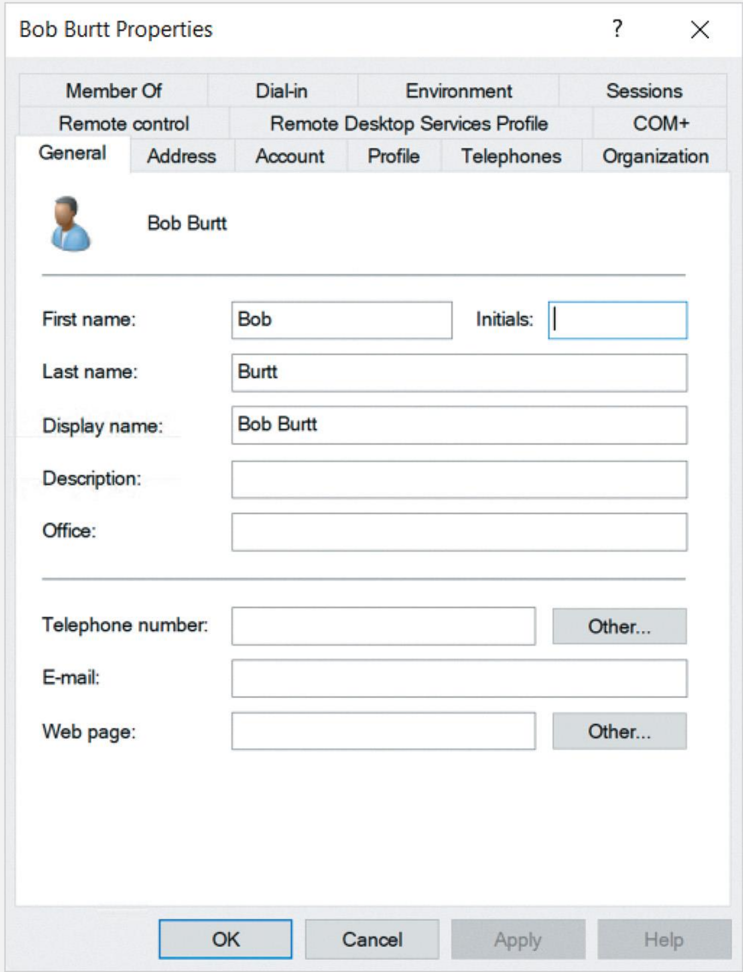
Full name: Bob Burtt

User logon name: b.burtt @domainX.com

User logon name (pre-Windows 2000): DOMAINX\ b.burtt

Figure 4-40 Creating a new user

Working with User Objects (3 of 4)


Bob Burtt Properties

Bob Burtt

First name: Bob

Initials:

Last name: Burtt

Display name: Bob Burtt

Description:

Office:

Telephone number:

E-mail:

Web page:

Figure 4-42 Setting attributes for a user object

Working with User Objects (4 of 4)

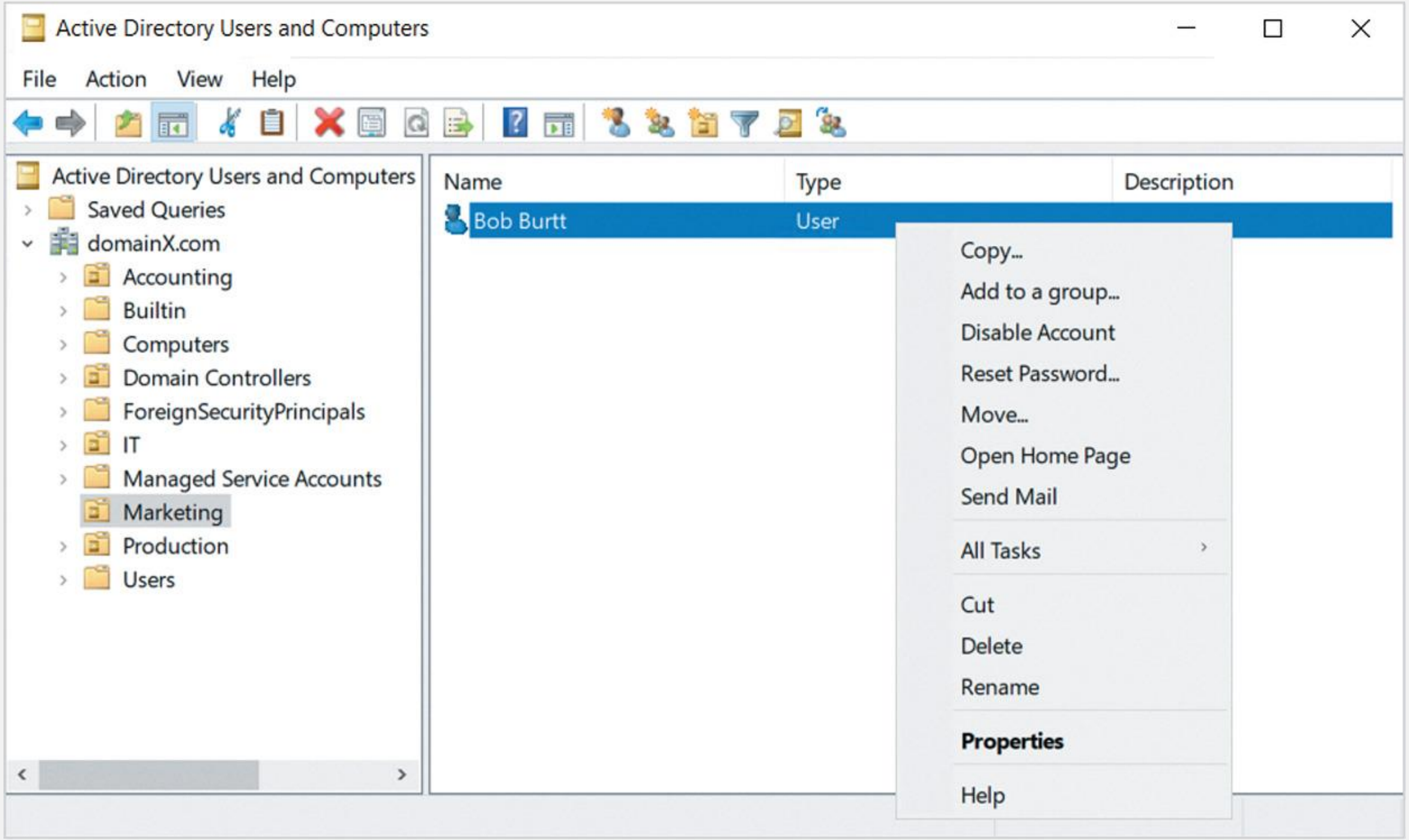


Figure 4-43 The right-click menu for a user object

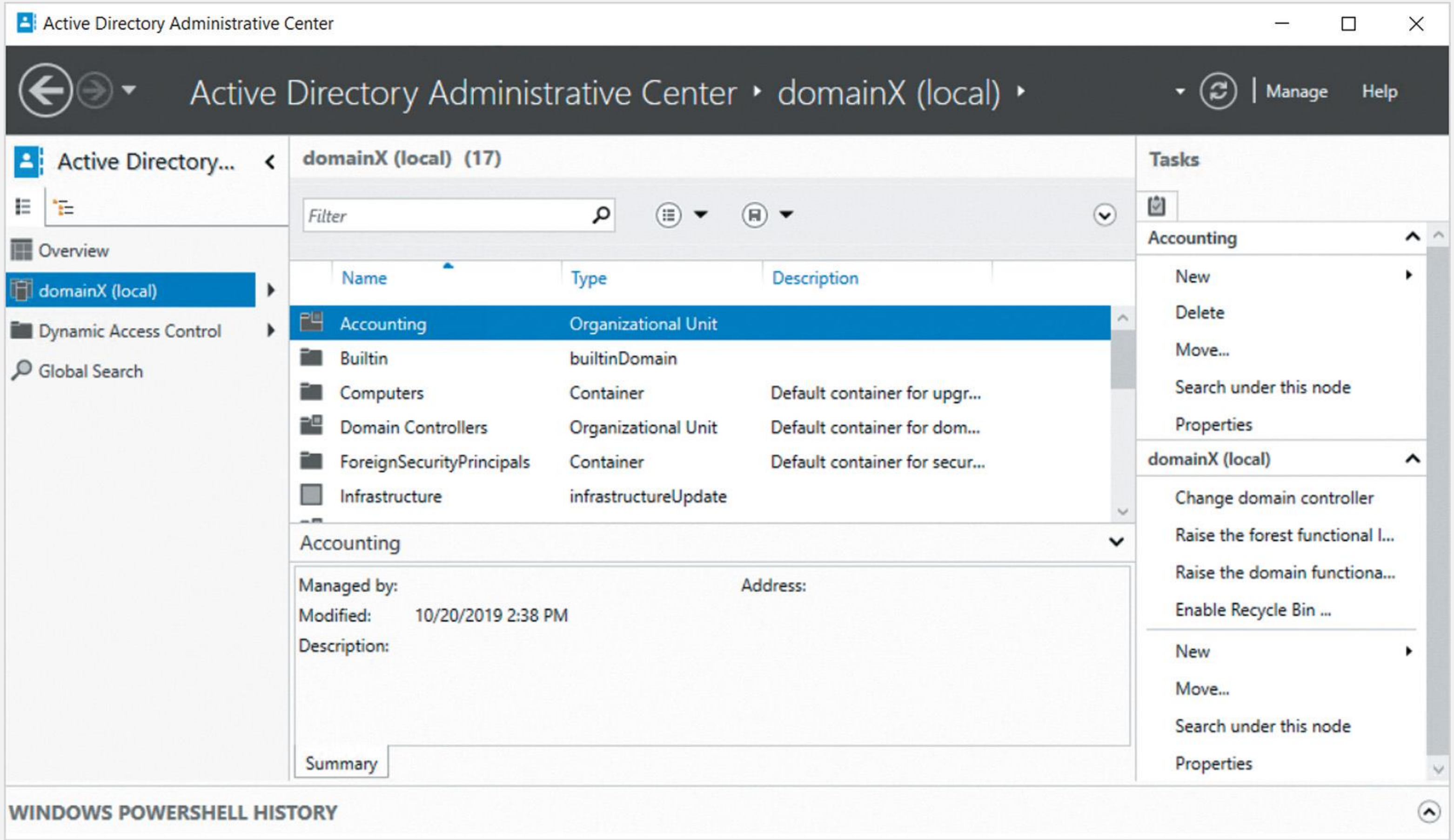
Working with Group Objects

- Group objects simplify the assignment of rights and permissions to users
- Create a group object using the New Object – Group window
  - Within Active Directory Users and Computers
  - Right-click the appropriate OU and click New, Group
  - Supply the group type, scope, and name
- Manage group membership
  - Within Active Directory Users and Computers
  - Click Properties and highlight the Members tab

Working with Computer Objects

- Two ways to move a computer account object to an OU
  - Open Active Directory Users and Computers
    - Right-click the computer account within the Computers folder
    - Click Move and select the target OU
  - Open Active Directory Users and Computers (prestage computer accounts)
    - Right-click the appropriate OU, and click New, Computer
- Encryption key within computer accounts needed for communication
- Handle computers joined to an Active Directory domain with hardware failure

Using the Active Directory Administrative Center



Name	Type	Description
Accounting	Organizational Unit	
Builtin	builtinDomain	
Computers	Container	Default container for upgr...
Domain Controllers	Organizational Unit	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secur...
Infrastructure	infrastructureUpdate	

Managed by:

Address:

Modified: 10/20/2019 2:38 PM

Description:

Figure 4-47 The Active Directory Administrative Center

Read-Only Domain Controllers

- Contains a read-only copy of the Active Directory database for the domain
- Object creation and management replicated from large office
  - Primary concern during replication is security
  - Replicate password attributes for users within the branch office only
- Install RODC using Active Directory Domain Services Configuration Wizard
- Can prestage a RODC computer account using the Active Directory Domain Services Installation Wizard
- Can delete RODC if stolen and reset computer account for stolen computers

Summary

- Convenient to log on to a system joined to an Active Directory domain
- Domain and forest function levels specify features and support
- Trust relationships assists with access
- Active Directory group scopes organize forest resource permission assignments
- Configure site links to control replication between domain controllers
- Active Directory database contains three partitions
- Azure Active Directory provides the same single sign-on features
- RODCs provide authentication within smaller branch offices