

MCA: Windows Server Hybrid Administrator Study Guide: AZ-800 & AZ-801

Chapter 7: Understanding Active Directory

Verifying the File System

The Windows Server 2022 platform supports three filesystems:

- File Allocation Table 32 (FAT32)
- Windows NT File System (NTFS)
- Resilient File System (ReFS)

Format Options on Windows Server 2022

New Simple Volume Wizard

Format Partition
To store data on this partition, you must format it first.

Choose whether you want to format this volume, and if so, what settings you want to use.

☐ Do not format this volume

☒ Format this volume with the following settings:

File system: NTFS
Allocation unit size: NTFS
Volume label: New Volume

☒ Perform a quick format

☐ Enable file and folder compression

< Back Next > Cancel

Resilient File System (ReFS)

- Created to help Windows Server maximize the availability of data and online operation.
- Allows the Windows Server 2022 system to continue to function despite some errors.
- Uses data integrity.

ReFS Features

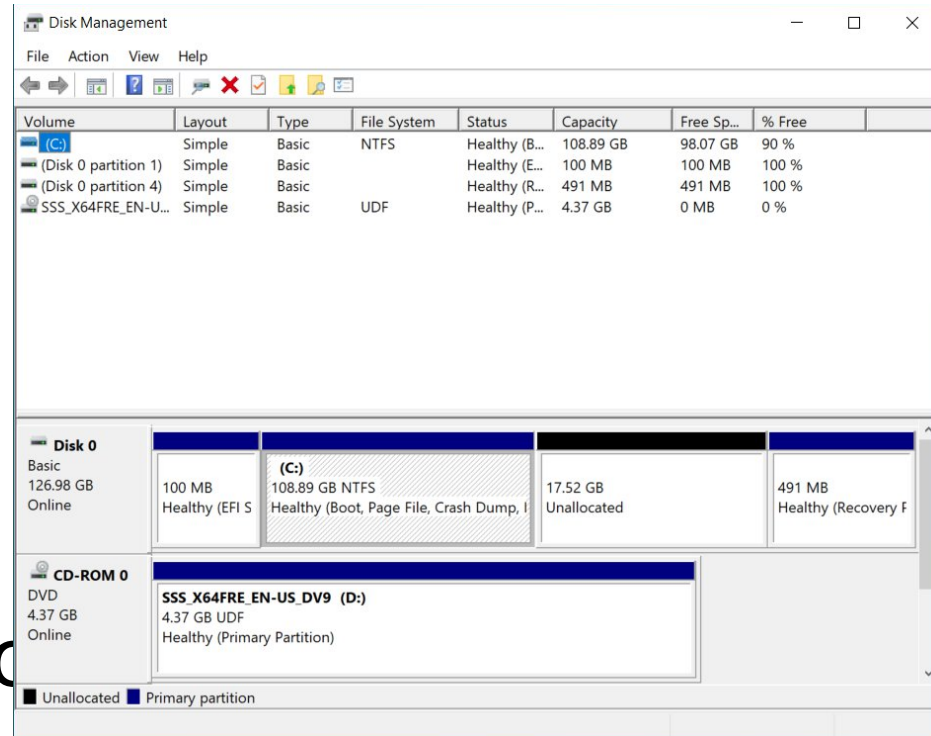
- Higher Data Availability
- Scalability
- Robust Disk Updating
- Data Integrity
- Application Compatibility

NTFS Features

- Disk Quotas
- File System Encryption
- Dynamic Volumes
- Mounted Drives
- Remote Storage
- Self-Healing NTFS
- Security

Setting Up the NTFS Partition

- Disk Management



- Co

– CONVERT C: /FS:NTFS

Basic Connectivity Tests

Before installing Active Directory, should perform several checks of the current configuration. Should test the following:

- Network Adapter
- TCP/IP
- Internet Access
- LAN Access
- Client Access
- Wide Area Network Access

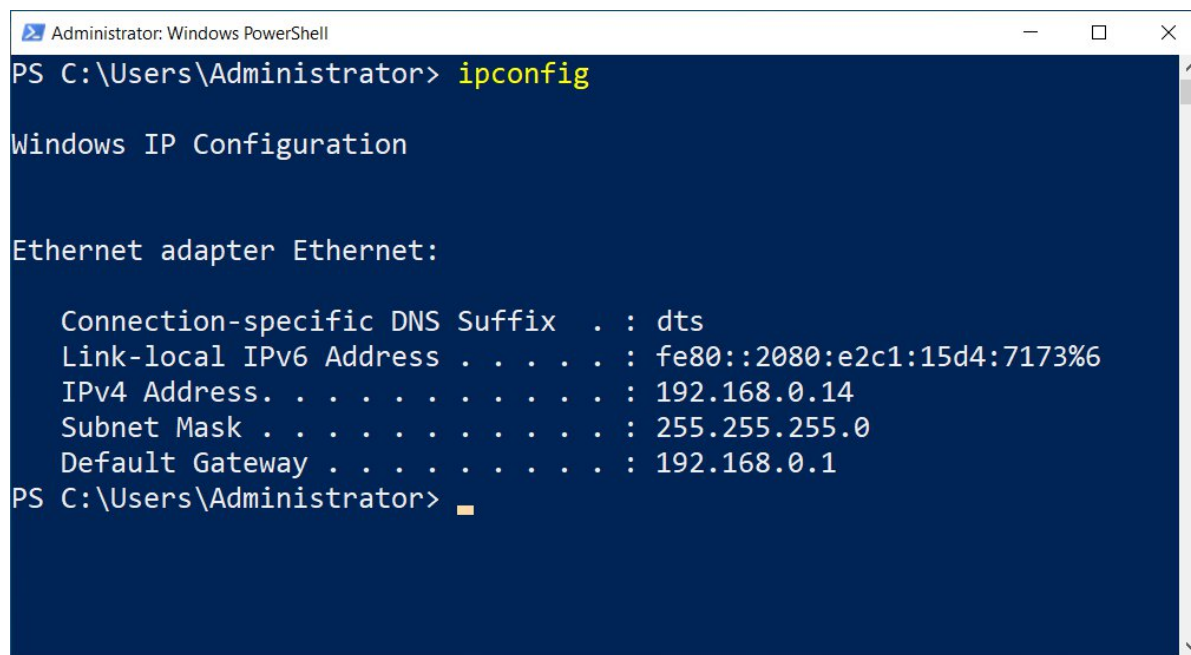
Testing Network Configuration

Can use several tools and techniques to verify that the network configuration is correct:

- Ipconfig Utility
- Ping Command
- TraceRT Command
- Browsing the Network
- Browsing the Internet

Using Ipconfig Utility

- Viewing TCP/IP information with the ipconfig utility



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : dts
    Link-local IPv6 Address . . . . . : fe80::2080:e2c1:15d4:7173%6
    IPv4 Address. . . . . : 192.168.0.14
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1
PS C:\Users\Administrator>
```

Using Ping and Tracert Commands

- The ping command - designed to test connectivity to other computers. To use this command simply type **ping** and then an IP address or hostname at the command line.
- The TraceRT command works just like the ping command except that the TraceRT command shows you every hop along the way. So, if one router or switch is down, the TraceRT command will show you where the trace stops.

Understanding Active Directory

- Active Directory is just a database that controls all the objects in your network.
- The first step when setting up Active Directory is to understand the different ways you can set it up. During the installation process, you need to understand the difference between:
 - Domains
 - Trees
 - Forests

Understanding Active Directory - Continued

- Domains are LOGICAL groupings of objects and not physical groupings.
- Trees are one or more domains that follow the same contiguous namespace.
- Forests are one or more Trees that are part of the same Active Directory structure.

During an Active Directory Installation

During the Active Directory installation, you will have the option to do the following:

- Add an additional Domain Controller to an existing Domain
- Add a new domain to an existing Tree
- Add a new Tree to an existing Forest
- Add a new Forest

Domain and Forest Functionality

Windows Server 2022 will support the following domain functional levels:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Comparing Domain Functional Levels

Domain Functional Feature	Windows Server 2008	Windows Server 2008 R2	Windows Server 2012	Windows Server 2012 R2	Windows Server 2016
Privileged access management	Disabled	Disabled	Disabled	Enabled	Enabled
Authentication assurance	Disabled	Enabled	Enabled	Enabled	Enabled
Fine-grained password policies	Enabled	Enabled	Enabled	Enabled	Enabled
Last interactive logon information	Enabled	Enabled	Enabled	Enabled	Enabled
Advanced Encryption Services (AES 128 and 256) support for the Kerberos protocol	Enabled	Enabled	Enabled	Enabled	Enabled
Distributed File System replication support for Sysvol	Enabled	Enabled	Enabled	Enabled	Enabled
Read-only domain controller (RODC)	Enabled	Enabled	Enabled	Enabled	Enabled
Ability to redirect the Users and Computers containers	Enabled	Enabled	Enabled	Enabled	Enabled
Ability to rename domain controllers	Enabled	Enabled	Enabled	Enabled	Enabled
Logon time stamp updates	Enabled	Enabled	Enabled	Enabled	Enabled
Kerberos KDC key version numbers	Enabled	Enabled	Enabled	Enabled	Enabled
Passwords for InetOrgPerson objects	Enabled	Enabled	Enabled	Enabled	Enabled
Converts NT groups to domain local and global groups	Enabled	Enabled	Enabled	Enabled	Enabled
SID history	Enabled	Enabled	Enabled	Enabled	Enabled
Group nesting	Enabled	Enabled	Enabled	Enabled	Enabled
Universal groups	Enabled	Enabled	Enabled	Enabled	Enabled

Forest Functionality

Windows Server 2022 forest functionality applies to all of the domains in a forest.

All domains have to be upgraded to before the forest can be upgraded.

There are five levels of forest functionality:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Forest Features

- Global Catalog Replication Enhancements
- Defunct Schema Classes and Attributes
- Forest Trusts
- Linked Value Replication
- Renaming Domains
- Other Features
 - Improved Replication Algorithms
 - AD FS (Trustbridge)
 - AD LDS
 - AD Recycle Bin

Planning the Domain Structure

- The DNS name of the domain
- The computer name or the NetBIOS name of the server (which will be used by previous versions of Windows to access server resources)
- Which domain function level will the domain operate in
- Whether or not other DNS servers are available on the network
- What type of DNS servers are available on the network and how many

Installing Active Directory

- Is a straightforward process as long as you plan adequately and make the necessary decisions beforehand.
- There are many ways that you can install Active Directory:
 - Use the Windows Server 2022 installation disk - Install from Media (IFM)
 - Use Server Manager
 - Use Windows PowerShell

Improved Active Directory Features

These include:

- Privileged Access Management (PAM)
- Azure AD Join
- Microsoft Passport

Read-Only Domain Controllers (RODC)

Windows Server 2022 supports another type of domain controller called the *read-only domain controller (RODC)*.

- This is a full copy of the Active Directory database without the ability to write to Active Directory.
- RODC gives an organization the ability to install a domain controller in a location (onsite or offsite) where security is a concern.

Adprep

Required to run in order to add the first Windows Server 2022 domain controller to an existing domain or forest.

- Run **Adprep /forestprep** - to add the first domain controller to an existing forest.
- Run **Adprep /domainprep** - to add the first domain controller to an existing domain.
- Run **Adprep /rodcprep** - to add the first RODC to an existing forest.

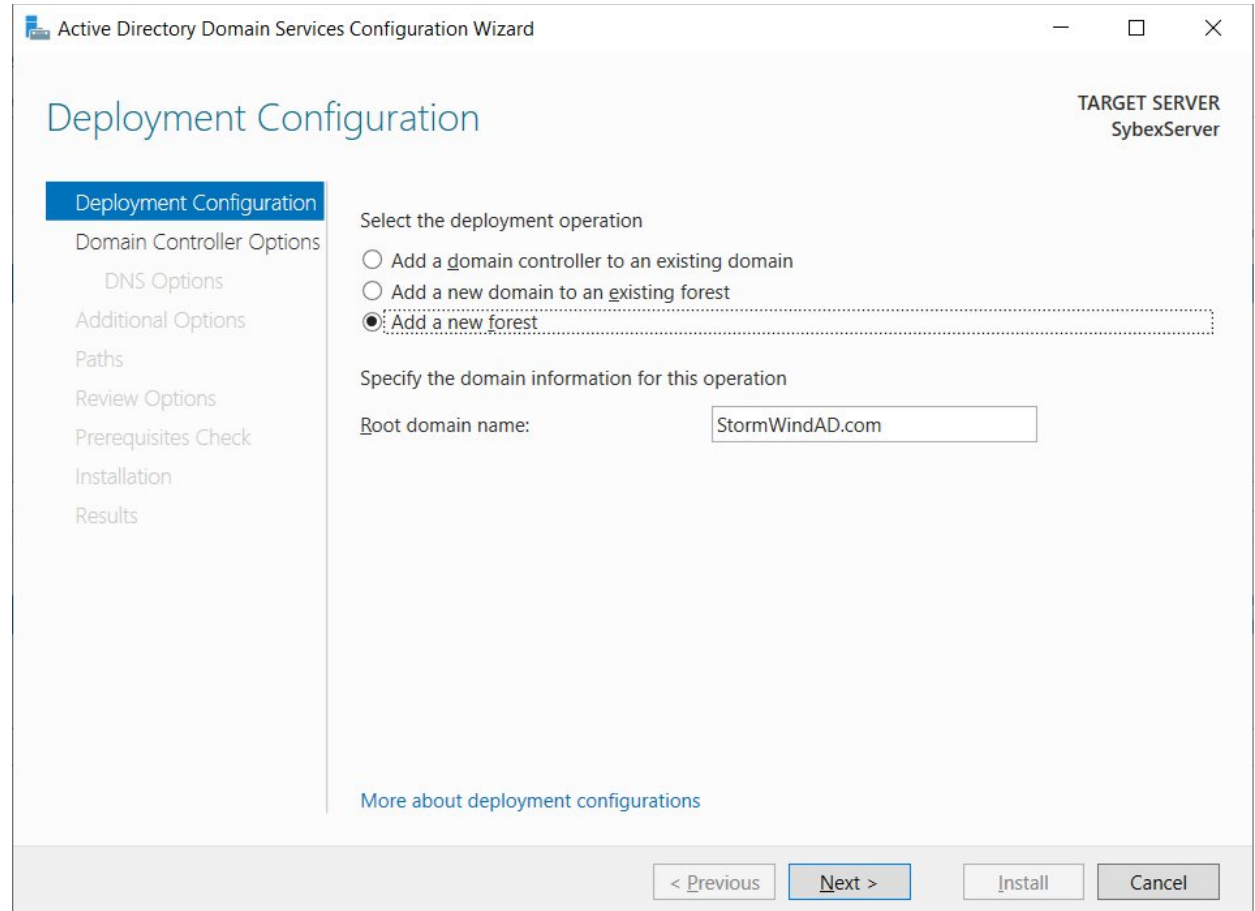
Active Directory Requirements

Requirement	Description
Adprep	When adding the first Windows Server 2022 domain controller to an existing Active Directory domain, Adprep commands run automatically as needed.
Credentials	When installing a new AD DS forest, the administrator must be set to local Administrator on the first server. To install an additional domain controller in an existing domain, you need to be a member of the Domain Admins group.
DNS	Domain Name System needs to be installed for Active Directory to function properly. You can install DNS during the Active Directory installation.
NTFS	The Windows Server 2022 drives that store the database, log files, and SYSVOL folder must be placed on a volume that is formatted with the NTFS file system.
RODCs	Read Only Domain Controllers can be installed as long as another domain controller (Windows Server 2008 or newer) already exists on the domain.
TCP/IP	You must configure the appropriate TCP/IP settings on your domain, and you must configure the DNS server addresses.

Promoting a Domain Controller

- The first step in installing Active Directory is promoting a Windows Server 2022 computer to a domain controller. This is known as *promotion*.
- Using Server Manager you can configure servers to be domain controllers after installation.
- Administrators also have the ability to promote domain controllers using Windows PowerShell.

New Forest Screen



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
SybexServer

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

☐ Add a domain controller to an existing domain

☐ Add a new domain to an existing forest

☒ Add a new forest

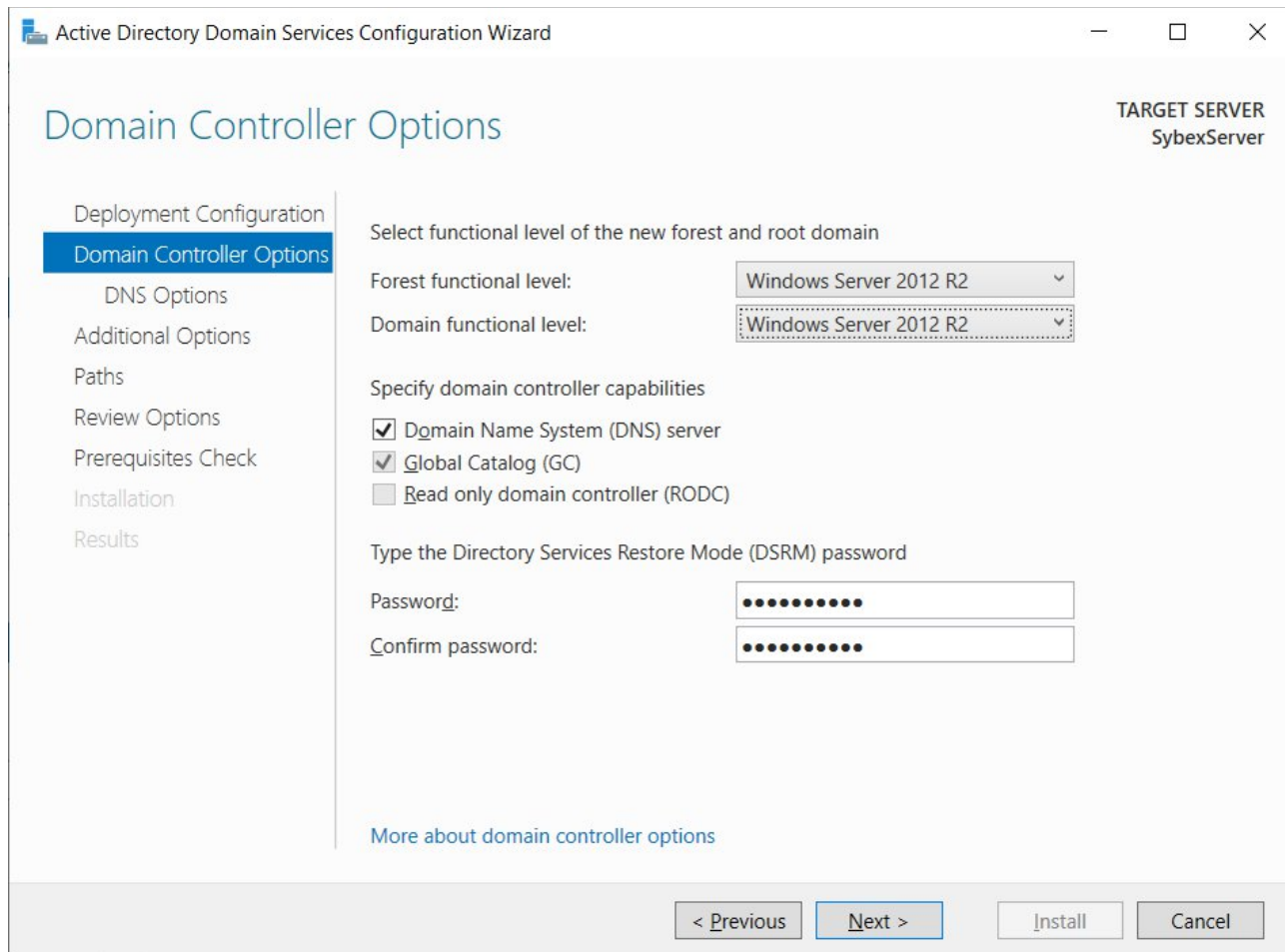
Specify the domain information for this operation

Root domain name: StormWindAD.com

[More about deployment configurations](#)

< Previous Next > Install Cancel

Domain Controller Options



Active Directory Domain Services Configuration Wizard

TARGET SERVER
SybexServer

Domain Controller Options

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012 R2

Domain functional level: Windows Server 2012 R2

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

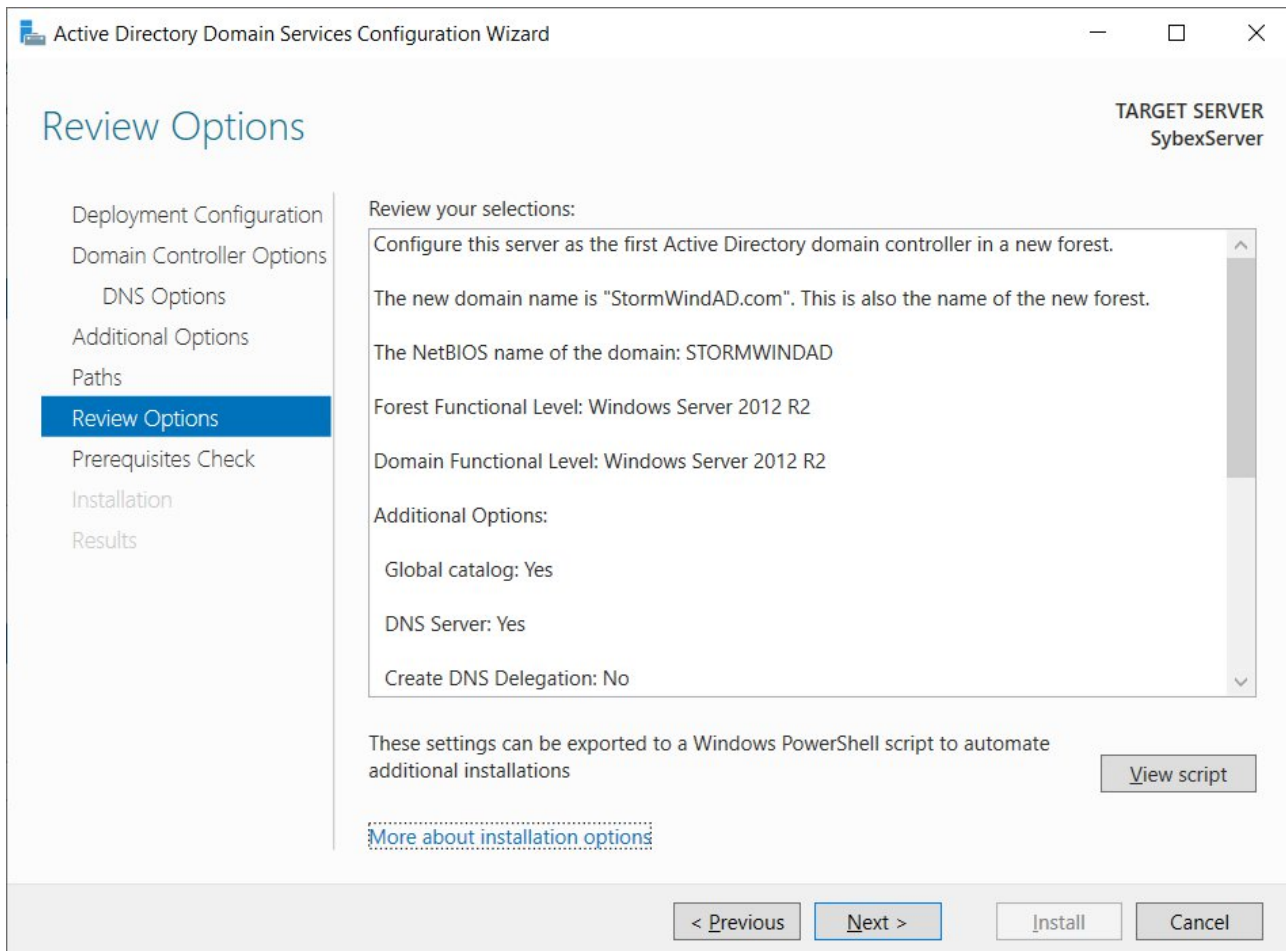
Password:

Confirm password:

[More about domain controller options](#)

< Previous Next > Install Cancel

Review Options Screen



Active Directory Domain Services Configuration Wizard

TARGET SERVER
SybexServer

Review Options

- Deployment Configuration
- Domain Controller Options
 - DNS Options
 - Additional Options
 - Paths
 - Review Options**
 - Prerequisites Check
 - Installation
 - Results

Review your selections:

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

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

The NetBIOS name of the domain: STORMWINDAD

Forest Functional Level: Windows Server 2012 R2

Domain Functional Level: Windows Server 2012 R2

Additional Options:

Global catalog: Yes

DNS Server: Yes

Create DNS Delegation: No

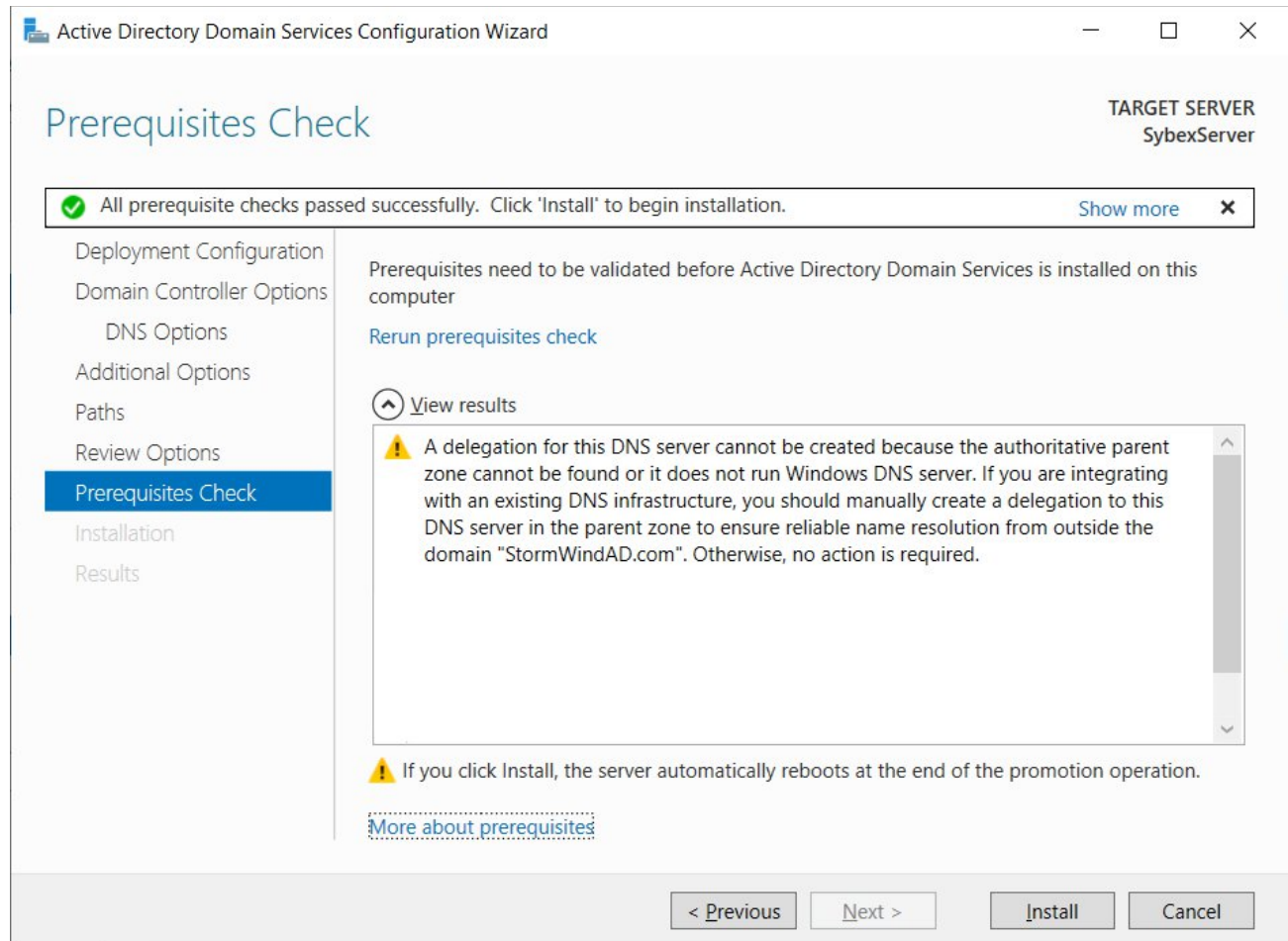
These settings can be exported to a Windows PowerShell script to automate additional installations

[View script](#)

[More about installation options](#)

< Previous Next > Install Cancel

Prerequisites Check Screen



Active Directory Domain Services Configuration Wizard

TARGET SERVER
SybexServer

Prerequisites Check

✓ All prerequisite checks passed successfully. Click 'Install' to begin installation. [Show more](#) ✕

- Deployment Configuration
- Domain Controller Options
 - DNS Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check**
- Installation
- Results

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

[Rerun prerequisites check](#)

⬆ View results

⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "StormWindAD.com". Otherwise, no action is required.

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

[More about prerequisites](#)

< Previous Next > Install Cancel

Using Install From Media to Install Additional Domain Controllers

- Windows Server 2022 allows you to install a domain controller using the IFM method by using the **Ntdsutil** or **PowerShell** utilities.
- They allow you to create installation media for an additional domain controller in a domain.
- Any objects that were created, modified, or deleted since the IFM was created must be replicated.

Verifying Active Directory Installation

- Using Event Viewer
- Using Active Directory Administrative Tools
 - Active Directory Administrative Center
 - Active Directory Domains and Trusts
 - Active Directory Sites and Services
 - Active Directory Users and Computers
 - Active Directory Module for Windows PowerShell

Active Directory Administrative Tools

- Active Directory Administrative Center - a Microsoft Management Console (MMC) snap-in that allows you to accomplish many Active Directory tasks from one central location.

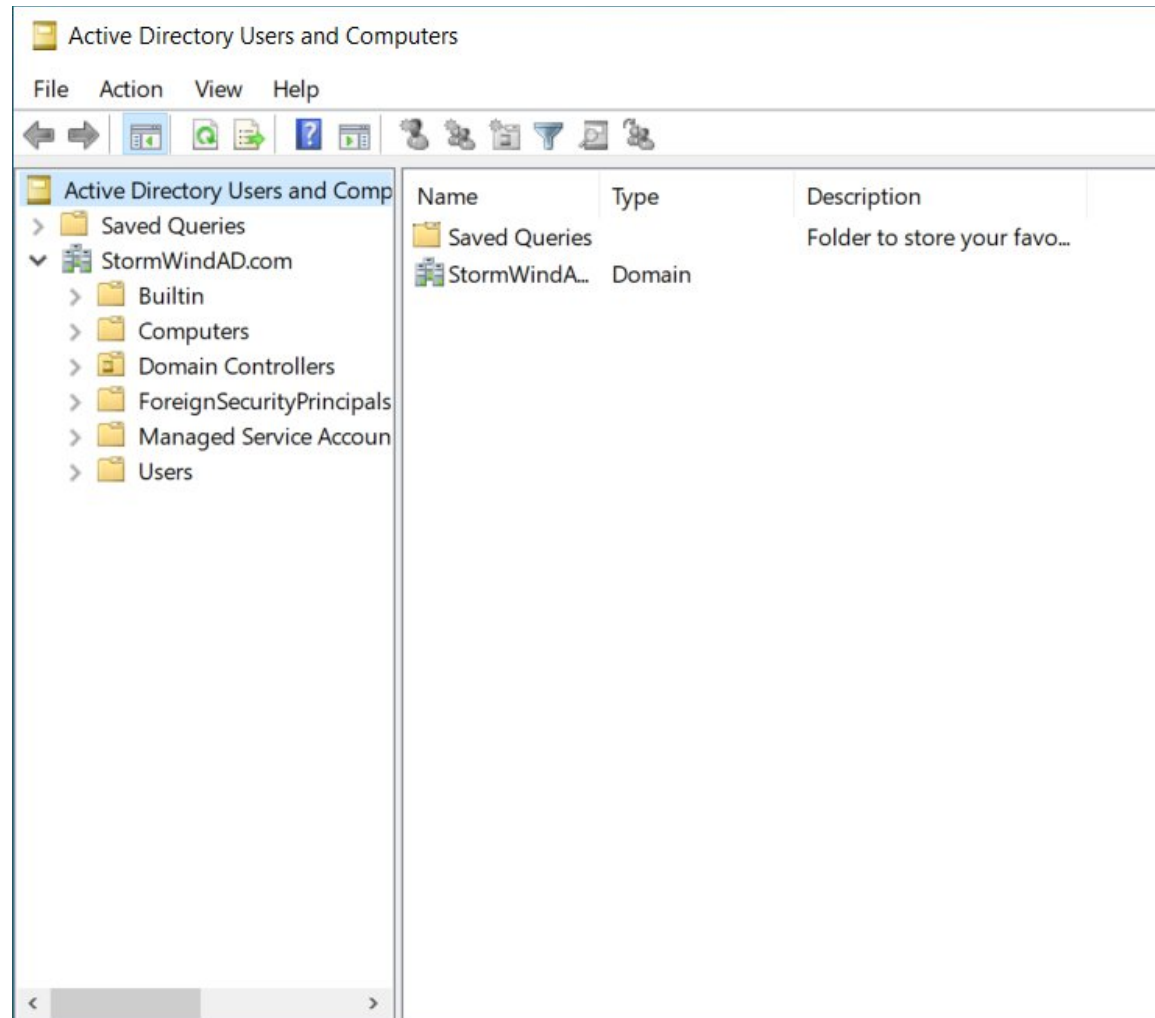
You can:

- Reset user passwords
- Create or manage user accounts
- Create or manage groups
- Create or manage computer accounts
- Create or manage organizational units (OUs) and containers
- Connect to one or several domains or domain controllers in the same instance of Active Directory Administrative Center
- Filter Active Directory data

Active Directory Administrative Tools - Continued

- Active Directory Domains and Trusts
 - MMC snap in tool to view and change information related to the various domains in an Active Directory environment and to set up shortcut trusts.
- Active Directory Sites and Services
 - To create and manage Active Directory sites and services to map to an organization's physical network infrastructure.
- Active Directory Users and Computers
 - To set machine- and user-specific settings across the domain.
- Active Directory Module for PowerShell
 - Contains a group of cmdlets to be used in managing Active Directory through PowerShell.

Active Directory Users and Computer Tool



Testing from Clients

- The best test of any solution is simply to verify that it works the way you had intended in your environment.
- There are a few tests to ensure that clients can view and access the various resources presented by Windows Server 2022 domain controllers. They include:
 - Verifying Client Connectivity
 - Joining a Domain

Verifying Client Connectivity

- If you are unable to see the recently promoted server on the network, there is likely a network configuration error.
- If only one or a few clients are unable to see the machine, the problem is probably related to client-side configuration. Ensure that the client computers have the appropriate TCP/IP configuration (including DNS server settings) and that they can see other computers on the network.

Verifying Client Connectivity - Continued

- If the new domain controller is unavailable from any of the other client computers, you should verify the proper startup of Active Directory.
- If Active Directory has been started, ensure that the DNS settings are correct.
- Test network connectivity between the server and the clients by accessing the network or by using the ping command.

Joining a Domain

- If Active Directory has been properly configured, clients and other servers should be able to join the domain.
- Once clients are able to join the domain successfully, they should be able to view Active Directory resources using the Network icon. This test validates the proper functioning of Active Directory and ensures that you have connectivity with client computers.

Creating and Configuring Application Data Partitions

- Windows Server 2022 uses a feature called application data partitions, which allows system administrators and application developers to store custom information within Active Directory.
- By default, after you create an Active Directory environment, you will not have any customer application data partitions. Therefore, the first step in making this functionality available is to create a new application data partition.

Creating Application Data Partitions

There are several tools to create data partitions:

- Third-Party Applications or Application-Specific Tools
- Active Directory Service Interfaces (ADSI)
- The LDP Tool – Ldp.exe
- Ntdsutil utility

Managing Replicas

- A *replica* is a copy of any data stored within Active Directory.
- *Replication* is the process by which replicas are kept up-to-date.
- Application data can be stored and updated on designated servers in the same way basic Active Directory information (such as users and groups) is synchronized between domain controllers.
- Application data partition replicas are managed using the *Knowledge Consistency Checker (KCC)*.

Removing Replicas

- Demotion – demote a domain controller that can no longer host an application data partition.
- If a domain controller contains a replica of application data partition information, you must remove the replica from the domain controller before you demote it.
- If a domain controller hosts a replica of the application data partition, then the entire application data partition is removed and will be permanently lost.

Using Ntdsutil

- The primary method by which system administrators create and manage application data partitions is through the ntdsutil command-line tool.
- Launch this tool simply by entering **ntdsutil** at a command prompt.

Ntdsutil Domain Management Commands

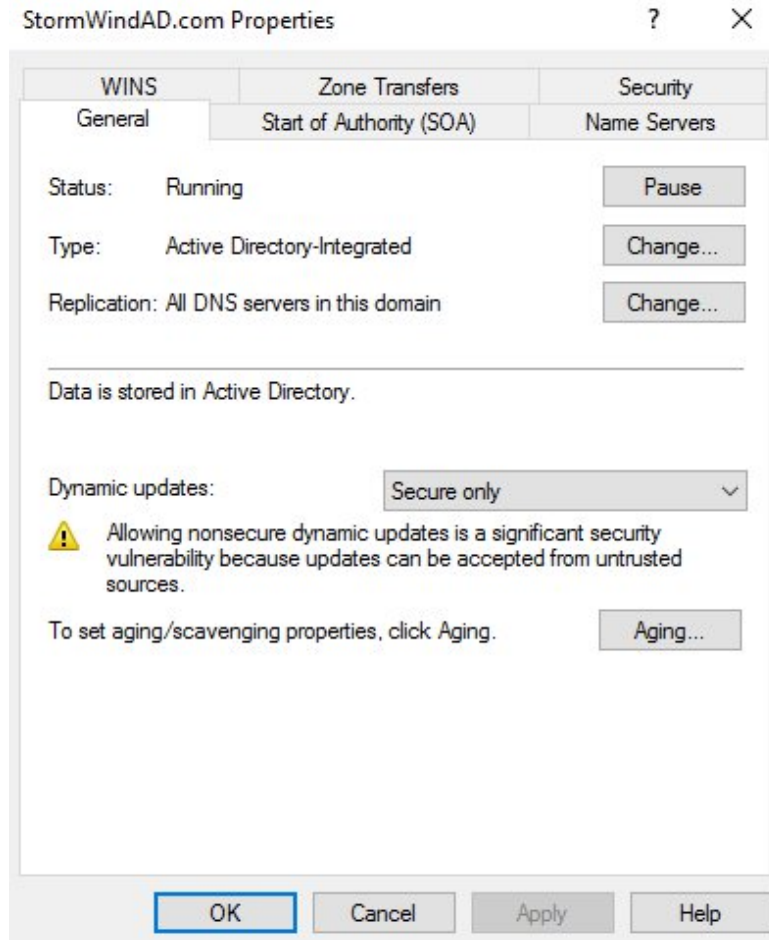
ntdsutil Domain Management Command	Purpose
Help or ?	Displays information about the commands that are available within the Domain Management menu of the <code>ntdsutil</code> command.
Connection or Connections	Allows you to connect to a specific domain controller. This will set the context for further operations that are performed on specific domain controllers.
Create NC <i>PartitionDistinguishedName</i> <i>DNSName</i>	Creates a new application directory partition.
Delete NC <i>PartitionDistinguishedName</i>	Removes an application data partition.
List NC Information <i>PartitionDistinguishedName</i>	Shows information about the specified application data partition.
List NC Replicas <i>PartitionDistinguishedName</i>	Returns information about all replicas for the specific application data partition.
Precreate <i>PartitionDistinguishedNameServerDNSName</i>	Pre-creates cross-reference application data partition objects. This allows the specified DNS server to host a copy of the application data partition.
Remove NC Replica <i>PartitionDistinguishedName DCDNSName</i>	Removes a replica from the specified domain controller.
Select Operation Target	Selects the naming context that will be used for other operations.
Set NC Reference Domain <i>PartitionDistinguishedName</i> <i>DomainDistinguishedName</i>	Specifies the reference domain for an application data partition.
Set NC Replicate NotificationDelay <i>PartitionDistinguishedName</i> <i>FirstDCNotificationDelay</i> <i>OtherDCNotificationDelay</i>	Defines settings for how often replication will occur for the specified application data partition.

DNS Integration with Active Directory

There are many benefits to integrating Active Directory and DNS services:

- Can configure and manage replication along with other Active Directory components.
- Can automate much of the maintenance of DNS resource records through the use of dynamic updates.
- Will be able to set specific security options on the various properties of the DNS service.

General Tab of DNS Zone Properties



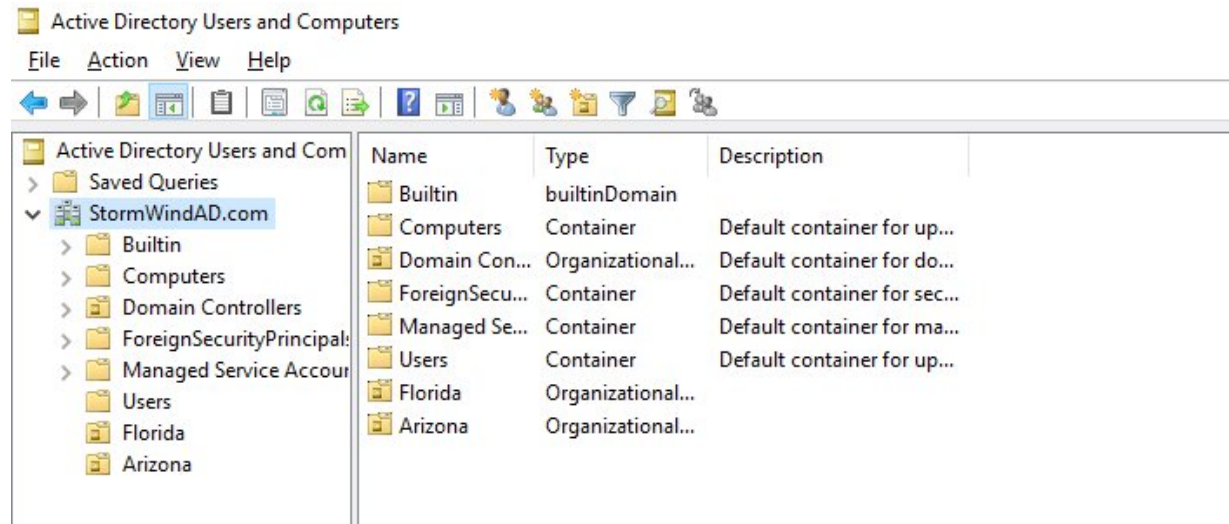
Security Principals

- Security principals are Active Directory objects that are assigned security identifiers (SIDs). A SID is a unique identifier that is used to manage any object which permissions can be assigned.
- Basic types of AD objects that server as security principals:
 - User Accounts
 - Groups
 - Security Groups
 - Distribution Groups
 - Computer Accounts

Overview of an Organizational Unit (OU)

- An *organizational unit (OU)* is a logical group of Active Directory objects.
- OUs serve as containers within which Active Directory objects can be created, but they do not form part of the DNS namespace.
- They are used solely to create organization within a domain.

Active Directory OUs



Active Directory Objects ⁽¹⁾

OUs can contain the following types of Active Directory objects:

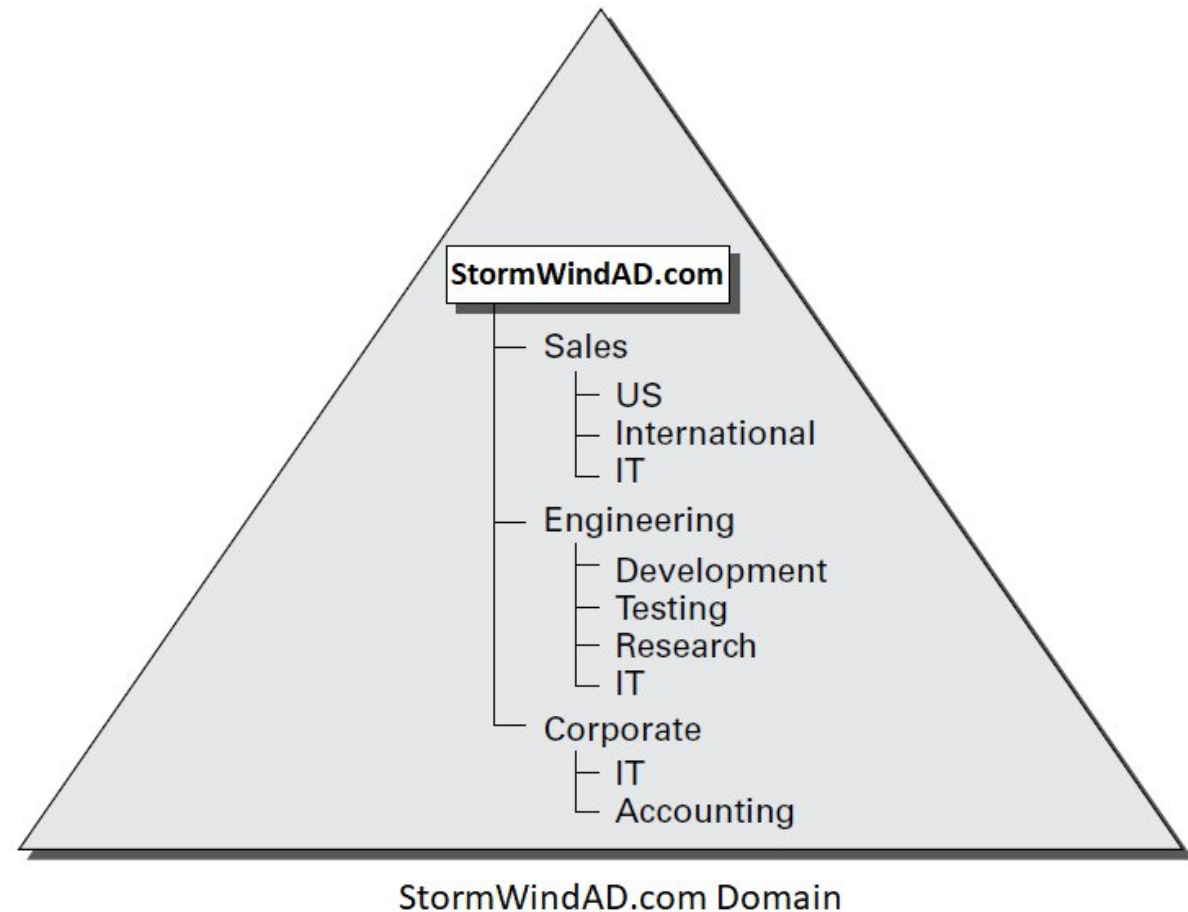
- Users
- Groups
- Computers
- Shared Folder objects
- Contacts
- Printers
- InetOrgPerson objects
- Microsoft Message Queuing (MSMQ)
Queue aliases
- Other OUs

Benefits of OUs

Benefits include:

- OUs are the smallest unit that can be assigned directory permissions.
- Can change the OU structure, is more flexible than the domain structure.
- The OU structure can support many different levels of hierarchy.
- Child objects can inherit OU settings.
- Can set Group Policy settings on OUs.
- Can delegate the administration of OUs and the objects within them to the appropriate users and groups.

Mapping a Business Organization to an OU Structure



OU Naming Considerations

- Keep the Names and Descriptions Simple
- Pay Attention to Limitations
- Pay Attention to the Hierarchical Consistency

OU Inheritance

- By default, OUs inherit the permissions of their new parent container when they are moved.
- Use the built-in tools provided with Windows Server 2022 and Active Directory.
- Can move or copy OUs only within the same domain.

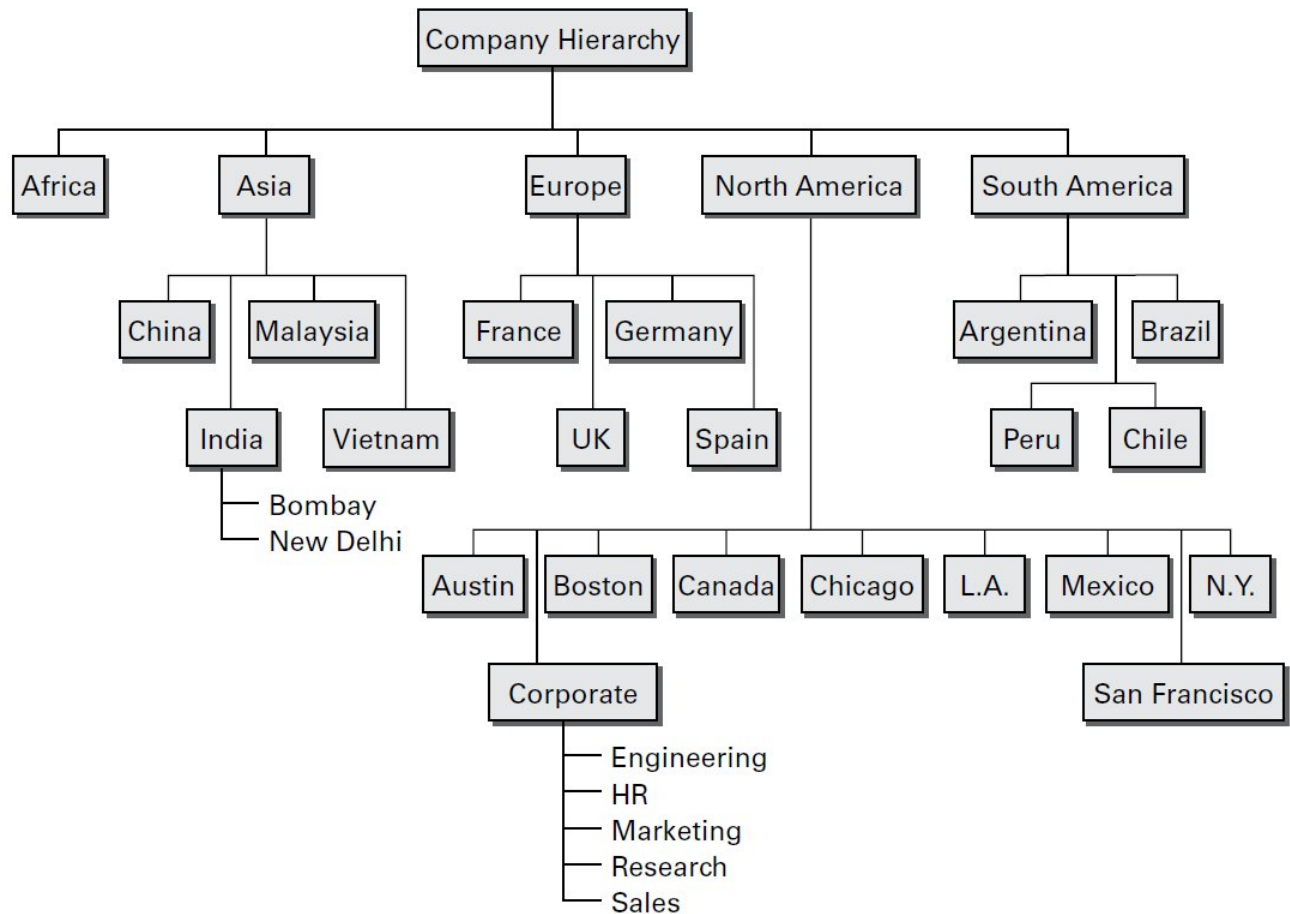
Delegating Administrative Control

- Delegation occurs when a higher security authority assigns permissions to a lesser security authority.
- You delegate to define responsibilities for OU administrators.
- Can delegate control only at the OU level and not at the object level within the OU.
- Delegation Concerns:
 - Parent-Child Relationships
 - Inheritance Settings

Applying Group Policies


- *Group policies* are collections of rules that can be applied to objects within Active Directory.
- Group Policy settings are assigned at the site, domain, and OU levels, and they can apply to user accounts and computer accounts.

Geographically Based OU Structure



New OU Dialog Box

New Object - Organizational Unit ×

 Create in: StomWindAD.com/

Name:

☐ Protect container from accidental deletion

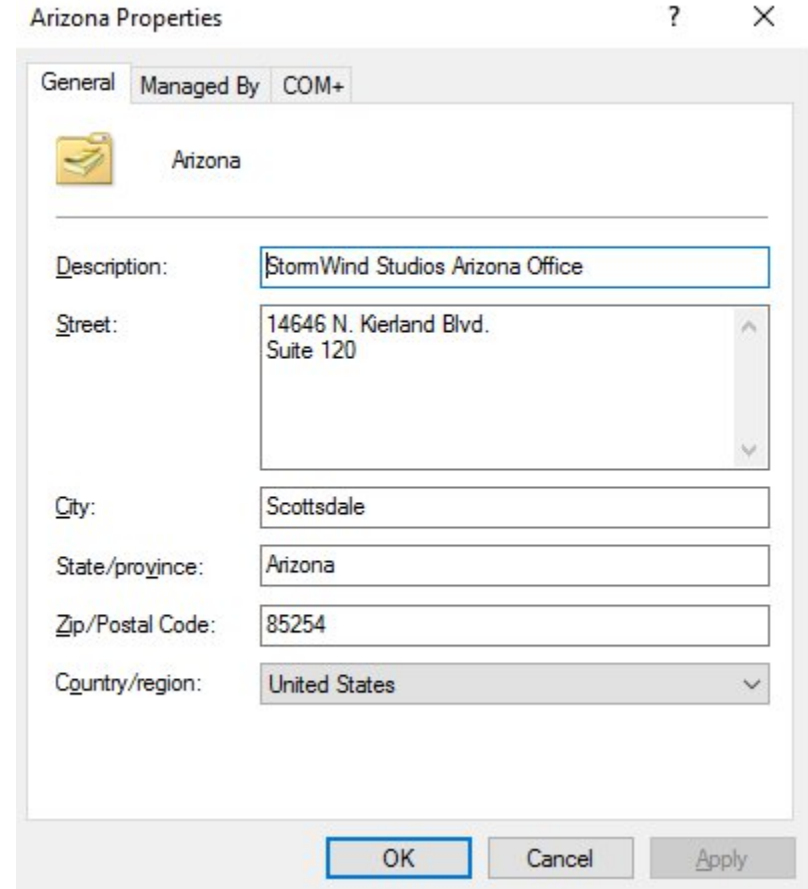
Managing OUs

The process of moving, deleting, and renaming OUs is fairly simple:

1. Open Active Directory Users and Computers by clicking Start ➤ Administrative Tools ➤ Active Directory Users And Computers.
2. Right-click on the OU that you wish to either move, delete or rename. Then, follow the prompts.

Administering OU Properties – General Tab

To modify the properties of an OU using the Active Directory Users and Computers administrative tool, right-click the name of any OU and select Properties.



Arizona Properties

General Managed By COM+

Arizona

Description: StormWind Studios Arizona Office

Street: 14646 N. Kierland Blvd.
Suite 120

City: Scottsdale

State/province: Arizona

Zip/Postal Code: 85254

Country/region: United States

OK Cancel Apply

Administering OU Properties – Managed By Tab

Arizona Properties ? X

General Managed By COM+

Name:

Office:

Street:

City:

State/province:

Country/region:

Telephone number:

Fax number:

Delegating Control of OUs

- A common administrative function related to AD involves managing all users within all OUs in the environment.
- Delegation – process by which a higher-level security administrator assigns permissions to another user.
- Can access the Delegation of Control Wizard through the Active Directory Users and Computers tool. The wizard walks you through the steps of selecting the objects for which you want to perform delegations, what permissions, and which users will have those permissions.

Active Directory Organization

- When looking at the Active Directory structure, will see objects that look like folders in Windows Explorer.
- These objects are containers, or *organizational units (OUs)*.
- Will see the following organizational sections within the Active Directory Users and Computers tool:
 - Built-In
 - Computer
 - Domain Controllers
 - Foreign Security Principals
 - Managed Service Accounts
 - Users

Active Directory Objects ⁽²⁾

Can create and manage several different types of Active Directory objects. The following are specific object types:

- Computer
- Contact
- Group
- InetOrgPerson
- MSIMaging-PSPs
- MSMQ Queue Alias
- Organizational Unit
- Printer
- Shared Folder
- User

Configuring the User Principal Name (UPN)

- The username followed by the @ sign and the domain name. At the time the user account is created, the UPN suffix is generated by default.
- The UPN is created as:
`UserName@DomainName`
- Change the UPN suffix, in Active Directory Users and Computers, choose a user and go into their properties.

Using Templates

- Allows an Active Directory administrator to create a default account and use that account to create all of the other users who match it.
- Fields that do not get copied over from a template:
 - Name
 - Logon Name
 - Password
 - Email
 - Phone
 - Description
 - Office
 - Web Page

Importing Objects from a File

There are two main applications for doing bulk imports of accounts:

- `ldifde.exe` - imports from line-delimited files.
- `csvde.exe` – imports using a comma-separated value file.

Offline Domain Join of a Computer

- Gives administrators the ability to preprovision computer accounts in the domain to prepare operating systems for deployments.
- Benefits of using offline domain join:
 - There is no additional network traffic for Active Directory state changes.
 - There is no additional network traffic for computer state changes to the domain controller.
 - Changes for both the Active Directory state and the computer state can be completed at a different times.


User Object Properties

- General
- Address
- Account
- Profile
- Telephone
- Organization
- Member Of
- Dial-In
- Environment
- Sessions
- Remote Control
- Remote Desktop Services Profile
- Personal Virtual Desktop
- COM+

Will Panek Properties ? X

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile		COM+

General Address Account Profile Telephones Organization

 Will Panek

First name: Will Initials:

Last name: Panek

Display name: Will Panek

Description: Instructor / Author

Office: Studio

Telephone number: 480-800-0054

E-mail: Will.Panek@Stormwind.com

Web page: www.StormwindStudios.com

Computer Object Properties

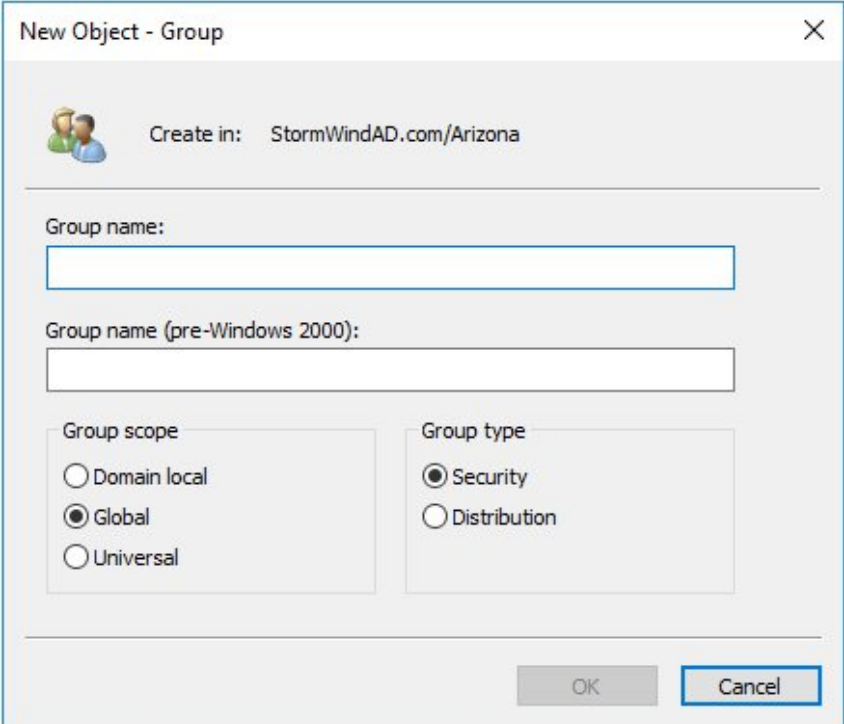
- Computer objects refer to the systems that clients are operating to be part of a domain.
- Computer object properties:
 - General
 - Operating System
 - Member Of
 - Delegation
 - Location
 - Managed By
 - Dial-In

Understanding Groups

- Active Directory groups simplify the administration of user accounts or computers in different AD domains by assembling them and assigning access rights.
- Once part of an AD group, a user can access all the resources and directory services common to the group without making multiple requests.

Group Properties

- Group Types:
 - Security
 - Distribution
- Group Scope:
 - Domain Local Groups
 - Global Groups
 - Universal Groups



New Object - Group

Create in: StormWindAD.com/Arizona

Group name:

Group name (pre-Windows 2000):

Group scope

☐ Domain local

☒ Global

☐ Universal

Group type

☒ Security

☐ Distribution

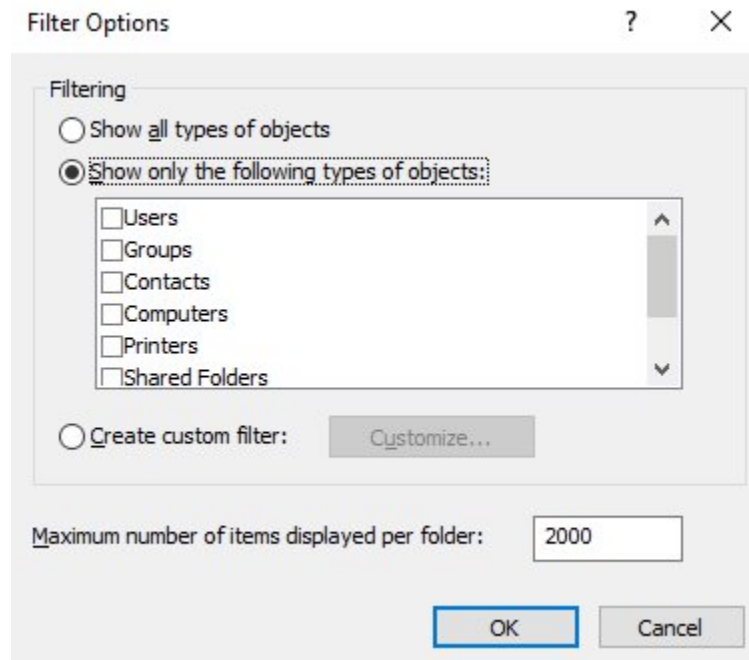
OK Cancel

Creating Group Strategies

- AGDLP (or AGLP). This acronym stands for a series of actions you should perform:
- **A** Accounts (Create your user accounts.)
- **G** Global groups (Put user accounts into global groups.)
- **DL** Domain local groups (Put global groups into domain local groups.)
- **P** Permissions (Assign permissions such as Deny or Apply on the domain local group.)

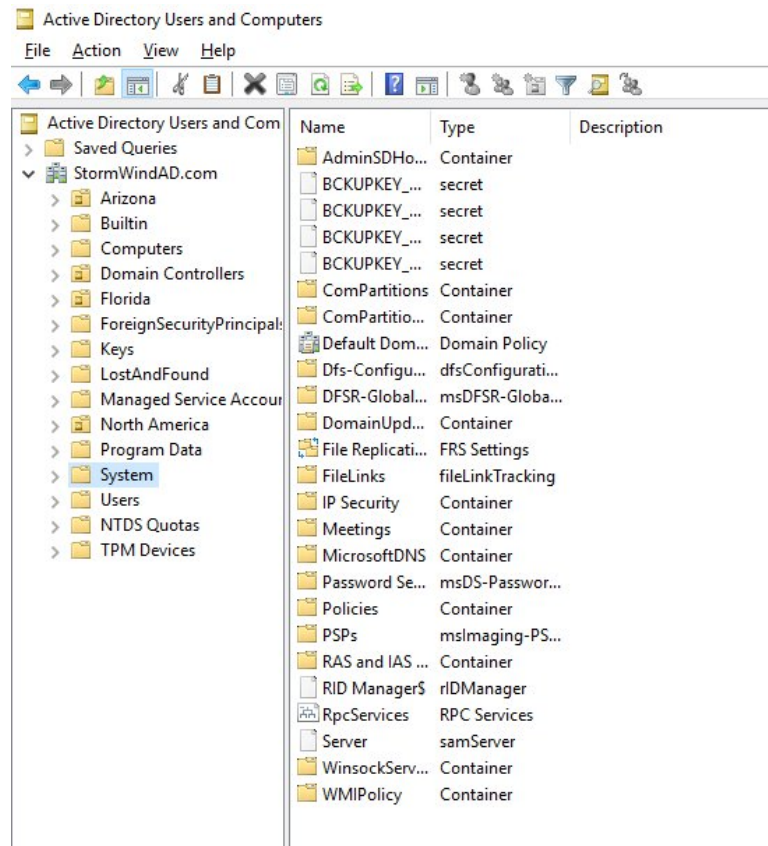
Filtering Active Directory Features

Can access the Filter Options dialog box by clicking the View menu in the MMC and choosing Filter Options.



Advanced Active Directory Features

Can enable the advanced options by choosing Advanced Features in the View menu.



Moving, Renaming, and Deleting Active Directory Objects

1. Open Active Directory Users and Computers by clicking Start ➤ Administrative Tools ➤ Active Directory Users And Computers.
 2. Expand the name of the domain.
 3. Select the desired OU and right-click.
- Can easily rename them by right-clicking an object and selecting Rename.
 - Can remove objects from Active Directory by right-clicking them and choosing Delete.

Dynamic Access Control

- Use of Dynamic Access Control (DAC) – allows you to identify data by using data classifications (both automatic and manual) and then control access to these files based on these classifications.
- DAC gives an administrator:
 - Ability to control file access by using a central access policy.
 - To set up AD RMS encryption.
 - Flexibility to configure file access and auditing to domain-based file servers.
 - To give users access to files and folders based on AD attributes

Managing Security and Permissions

- General practice for managing security is to assign users to groups and then grant permissions and logon parameters to the groups so that they can access certain resources.
- Can also assign Group Policy settings to all of the objects contained within an OU.
- The primary tool used to manage security permissions for users, groups, and computers is the Active Directory Users and Computers tool.

Permissions of Active Directory Objects

Permission	Explanation
Control Access	Changes security permissions on the object
Create Child	Creates objects within an OU (such as other OUs)
Delete Child	Deletes child objects within an OU
Delete Tree	Deletes an OU and the objects within it
List Contents	Views objects within an OU
List Object	Views a list of the objects within an OU
Read	Views properties of an object (such as a username)
Write	Modifies properties of an object

Configure Password Policies

- All administrator and user accounts that have been created and maintained in Azure AD have a password policy applied.
- With a password policy you can prohibit weak passwords and set parameters that will lock out an account after a specified number of failed login attempts.

Azure AD Password Policy Requirements

Property	Requirements
Characters allowed	Uppercase characters (A - Z) Lowercase characters (a - z) Numbers (0 - 9) Symbols: - @ # \$ % ^ & * - _ ! + = [] { } \ : ' , . ? / ` ~ " () ; < > - blank space
Characters not allowed	Unicode characters
Password length	Passwords require - A minimum of eight characters - A maximum of 256 characters
Password complexity	Passwords require three out of four of the following categories: - Uppercase characters - Lowercase characters - Numbers - Symbols
Password not recently used	When a user changes or resets their password, the new password can't be the same as the current or recently used passwords.
Password isn't banned by Azure AD Password Protection	The password can't be on the global list of banned passwords for Azure AD Password Protection, or on the customizable list of banned passwords specific to your organization.

Fine-Grained Password Policies (FGPPs)

- In Azure AD DS you can define FGPPs to manage user security.
- These can control account lockout settings or minimum password length and complexity.
- A default FGPP is created and applied to all users in an Azure AD DS managed domain.

Create User Accounts in Azure AD DS

Two ways that a user account can be created in Azure AD DS, they are:

- Can be synchronized in from Azure AD. This includes cloud-only user accounts created directly in Azure, and hybrid user accounts synchronized from an on-premises AD DS environment using Azure AD Connect.
- Can be manually created in a managed domain, and don't exist in Azure AD.

Default Account Lockout Policy

All users will have the following account lockout policies applied by default:

- Account lockout duration: 30
- Number of failed logon attempts allowed: 5
- Reset failed logon attempts count after: 2 minutes
- Maximum password age (lifetime): 90 days

Custom Password Policies

This will override the default policy.

To create a custom password policy in a managed domain, you must be signed in to a user account that's a member of the AAD DC Administrators group.

Custom Password Policy – Password Settings

The screenshot shows the 'Password Settings' console window. The left sidebar has 'Password Settings' selected. The main area is divided into three sections: 'Password Settings', 'Directly Applies To', and 'Extensions'. The 'Password Settings' section contains various checkboxes and input fields for password policy enforcement. The 'Directly Applies To' section shows a list of users with columns for 'Name' and 'Mail'. The 'Extensions' section shows a list of groups or user names, including 'CREATOR OWNER', 'SELF', 'SYSTEM', and 'AAD DC Administrators'. The window has standard Windows window controls at the top and bottom right.

Tasks: TASKS SECTIONS

Password Settings

Directly Applies To

Extensions

Name: *
Precedence: * 1

☒ Enforce minimum password length
Minimum password length (characters): * 7

☒ Enforce password history
Number of passwords remembered: * 24

☒ Password must meet complexity requirements

☐ Store password using reversible encryption

☐ Protect from accidental deletion

Description:

Password age options:

☒ Enforce minimum password age
User cannot change the password within (days): * 1

☒ Enforce maximum password age
User must change the password after (days): * 365

☒ Enforce account lockout policy:
Number of failed logon attempts allowed: * 4
Reset failed logon attempts count after (mins): * 30
Account will be locked out:
☒ For a duration of (mins): * 30
☐ Until an administrator manually unlocks the account

Directly Applies To

Name Mail

Add...

Remove

Extensions

Security Attribute Editor

Group or user names:

- CREATOR OWNER
- SELF
- SYSTEM
- AAD DC Administrators

More Information

OK Cancel

Enable Password Block Lists

- Azure AD Password Protection can detect and block known weak passwords and their variants, and can block additional weak passwords that you set by creating a custom banned password list.
- Azure AD Password Protection has a default global banned password list that is automatically applied to all users in your Azure AD tenant.
- The Azure AD Identity Protection team constantly analyzes Azure AD security telemetry data to look for passwords that are commonly used, compromised or weak. When found they are added to the global banned password list.

Custom Banned Password List

- Works with the global banned password list.
- The custom banned password list is limited to a maximum of 1000 terms and is not designed to block large lists of passwords.
- Organizational-specific terms can be added to the custom banned password list.

Password Error Messages

If a user tries to reset a password to something that's on the global or custom banned password list, they see one of the following:

- Unfortunately, your password contains a word, phrase, or pattern that makes your password easily guessable. Please try again with a different password.
- Unfortunately, you can't use that password because it contains words or characters that have been blocked by your administrator. Please try again with a different password.

Considerations and Limitations

The following considerations and limitations apply to the custom banned password list:

- Can contain up to 1000 terms.
- Is case-insensitive.
- Considers common character substitution, such as "o" and "0", or "a" and "@".
- The minimum string length is four characters, and the maximum is 16 characters.

Configure a Custom Banned Password List

1. Sign in to the Azure portal using an account with global administrator permissions.
2. Search for and select Azure Active Directory, then choose Security on the left-hand side.
3. Under the Manage menu header, select Authentication methods, then Password protection.
4. Set the option for Enforce custom list to Yes.
5. Add strings to the Custom banned password list, one string per line.
6. Leave the option for Enable password protection on Windows Server Active Directory to No.
7. To enable, select Save.

Manage Protected Users

- The Protected Users security group was designed to help protect from credential theft attacks. By default, members of the Protected Users security group are non-configurable and the only way to modify the protections for an account is to remove the account from the security group.
- To add users to the Protected Users group you can use Active Directory Administrative Center (ADAC), Active Directory Users and Computers (ADUC), or Windows PowerShell.

Publishing Active Directory Objects

- An important aspect of managing Active Directory objects is that a system administrator can control which objects users can see.
- The act of making an Active Directory object available is known as *publishing*.
- The two main types of publishable objects are:
 - Printer objects
 - Shared Folder objects

PowerShell for Active Directory

Command	Explanation
Add-ADComputerServiceAccount	This command allows an administrator to add service accounts to Active Directory.
Add-ADGroupMember	This command allows you to add users to an Active Directory group.
Disable-ADAccount	Administrators can use this command to disable an Active Directory account.
Enable-ADAccount	Administrators can use this command to enable an Active Directory account.
Get-ADComputer	This command allows you to view one or more Active Directory computers.
Get-ADDomain	Administrators can use this command to view an Active Directory domain.
Get-ADFineGrainedPasswordPolicy	This command allows you to view the Active Directory fine-grained password policies.
Get-ADGroup	Administrators can use this command to view Active Directory groups.
Get-ADGroupMember	This command allows you to view the users in an Active Directory group.
Get-ADServiceAccount	Administrators can use this command to view the Active Directory service accounts.
Get-ADUser	This command allows you to view one or more Active Directory users.
New-ADComputer	Administrators can use this command to create a new Active Directory computer.
New-ADGroup	Administrators can use this command to create a new Active Directory group.
New-ADServiceAccount	This command is the <i>only</i> way that you can create a new Managed Service Account.
New-ADUser	Administrators can use this command to create a new Active Directory user.
Set-ADAccountPassword	This command allows you to modify the password of an Active Directory account.
Unlock-ADAccount	Administrators can use this command to unlock an Active Directory account.