



IDENTITY WITH WINDOWS SERVER

20742 (55351AC)

Module 1: Deploy Active Directory services

Module overview

Active Directory Domain Services (AD DS) is the cornerstone of on-premises networks for many organizations worldwide. AD DS delivers authentication and authorization by using domain controllers (DCs) for on-premises apps and services. In this module, you'll learn how to configure those DCs to suit your specific organizational needs. You'll also learn how to integrate AD DS with Microsoft Azure Active Directory (Azure AD) to provide single sign-on (SSO) for users that access both on-premises and cloud-based apps.

The lessons in this module are:

- Lesson 1: Components of AD DS
- Lesson 2: AD DS DCs
- Lesson 3: Deploy AD DS DCs
- Lesson 4: Azure AD overview



Lesson 1: Components of AD DS

Lesson 1 overview

AD DS is a hierarchical directory service that stores security principals, such as users, groups, and computers. It's important that you understand this hierarchical structure, and know how to implement its elements: forests, trees, domains, OUs, and sites. DCs host a writable instance of AD DS and provide authentication and authorization services for users and computers. It's vital that you understand the components of AD DS and how they interact.

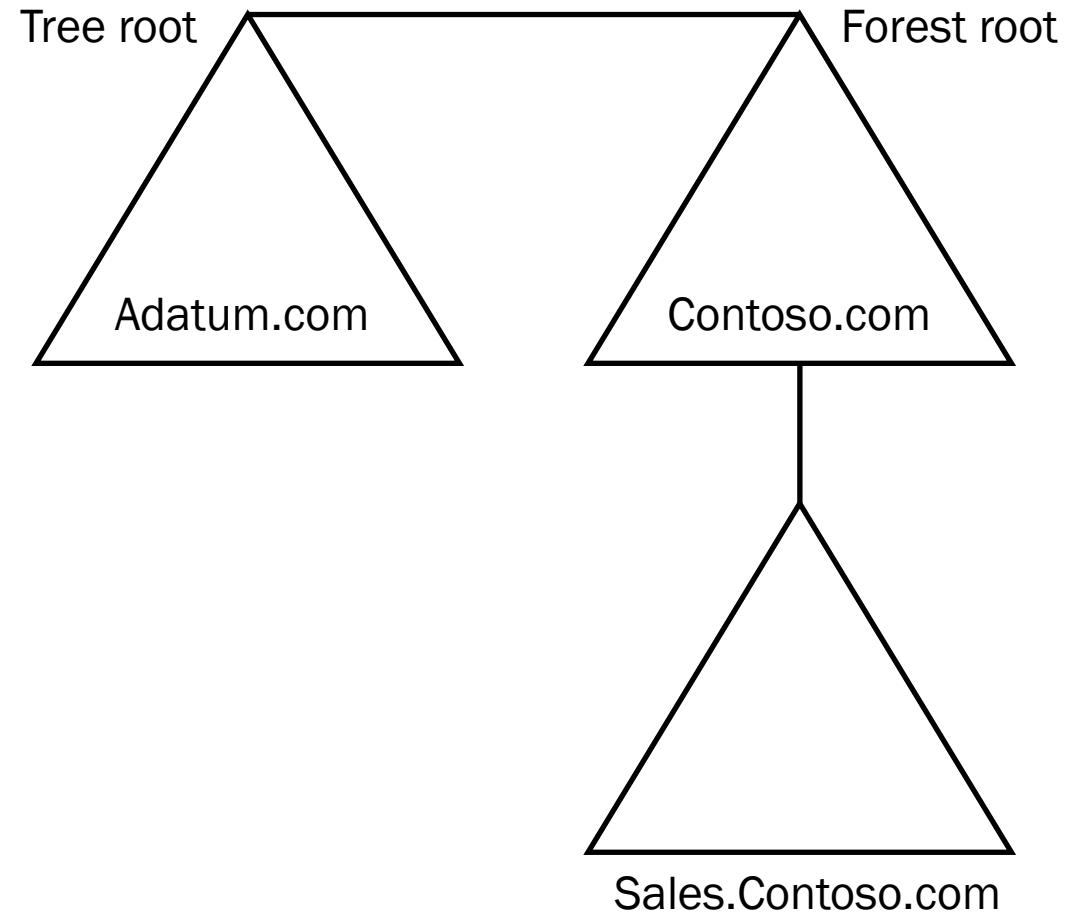
The topics in this lesson are:

- What is an AD DS forest?
- What is an AD DS domain?
- What are organizational units (OUs)?
- What is the AD DS schema?
- Overview of AD DS administration tools
- Demonstration: Manage AD DS

What is an AD DS forest?

An AD DS forest is:

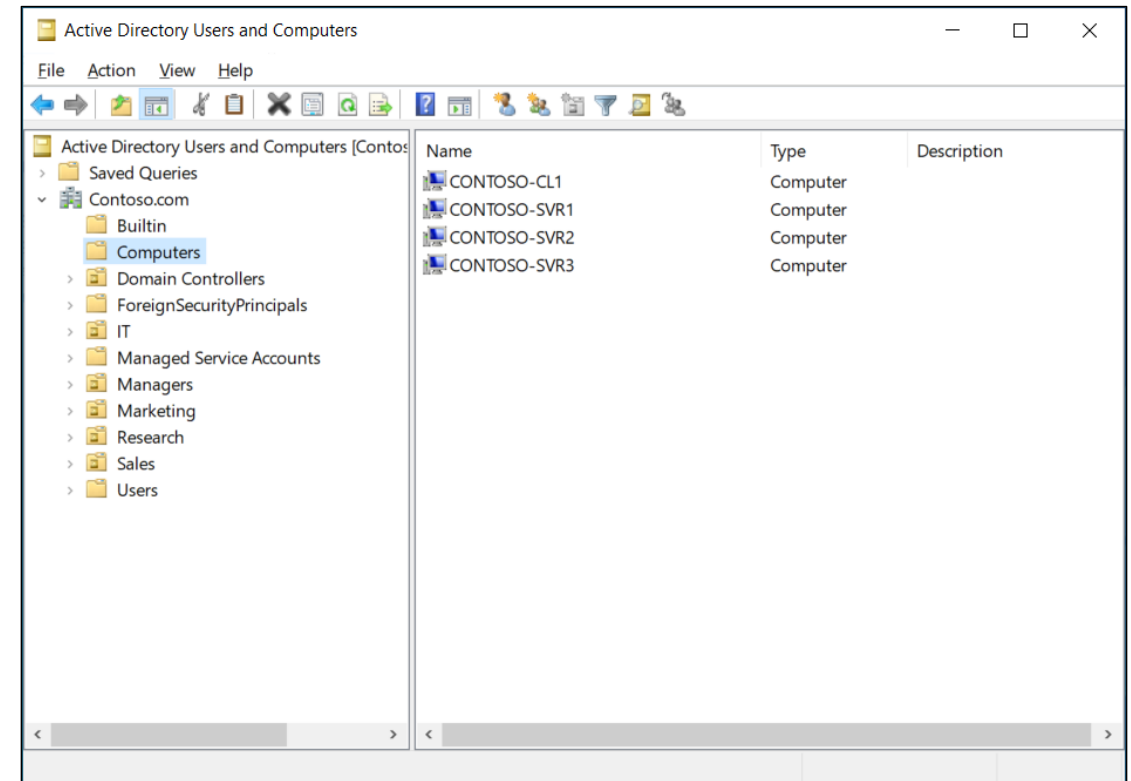
- A collection of one or more AD DS domains in one or more AD DS trees with:
 - A common AD DS schema.
 - A shared global catalog.
- A replication boundary.
- A security boundary.



What is an AD DS domain?

A domain is:

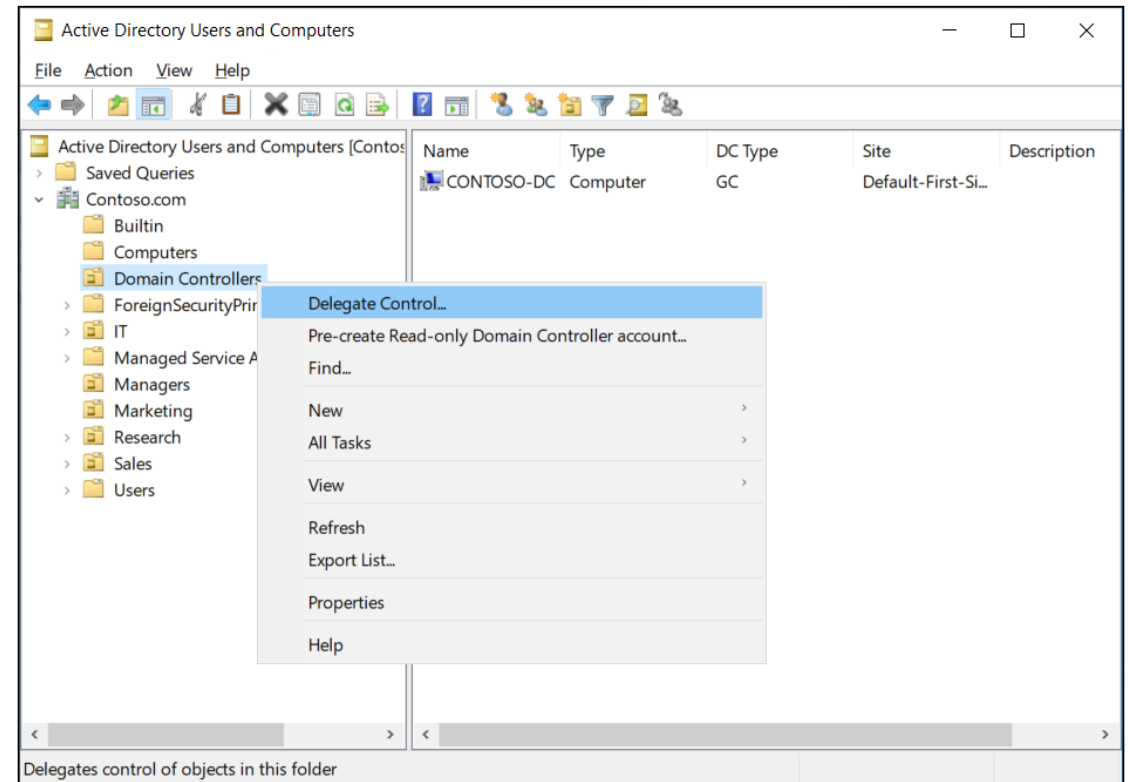
- A delegated administrative unit.
- A replication boundary.



What are organizational units (OUs)?

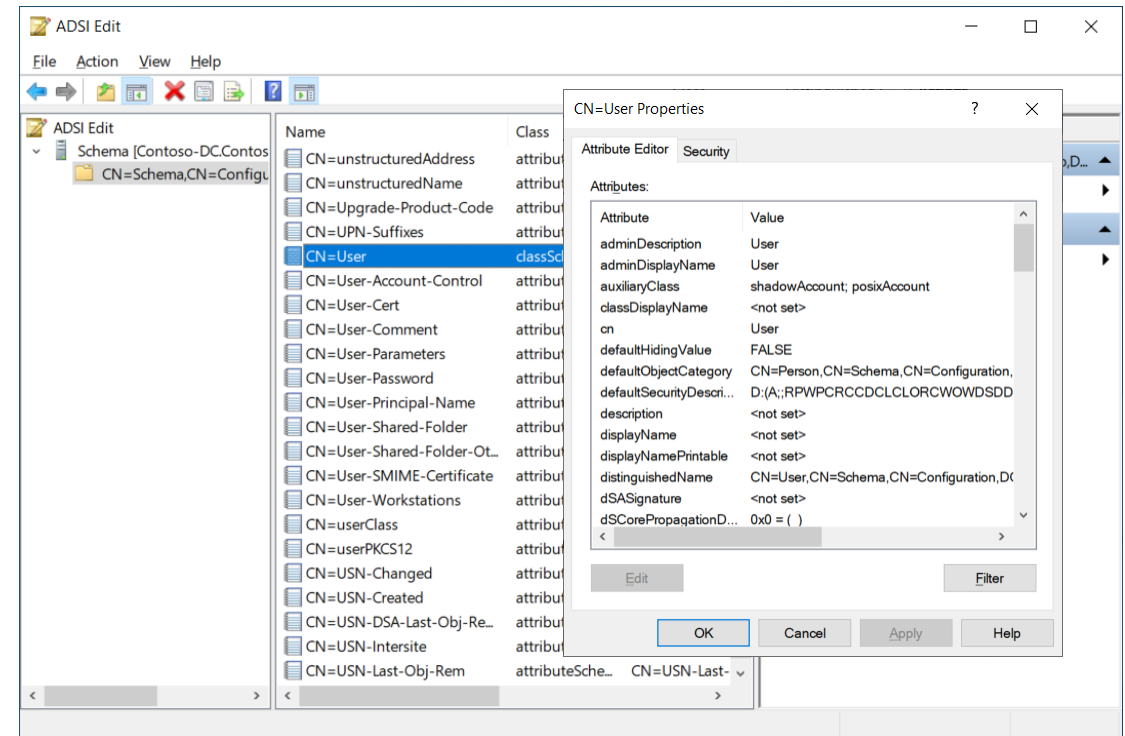
OUs enable you to group objects together for two purposes:

- Group Policy application
- Administrative delegation



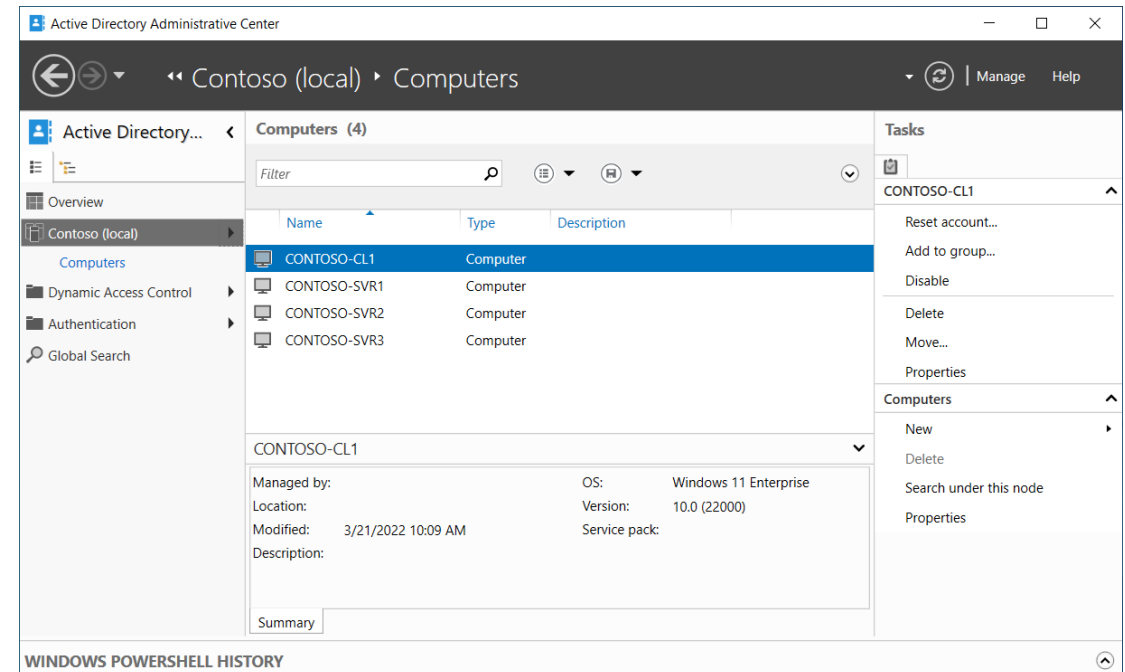
What is the AD DS schema?

- The schema defines the:
 - Types of objects
 - Attributes of those objects
 - Structure of AD DS
- If you need to install a directory-aware app, you might need to make changes to the schema:
 - Members of Schema Admins can make schema changes.



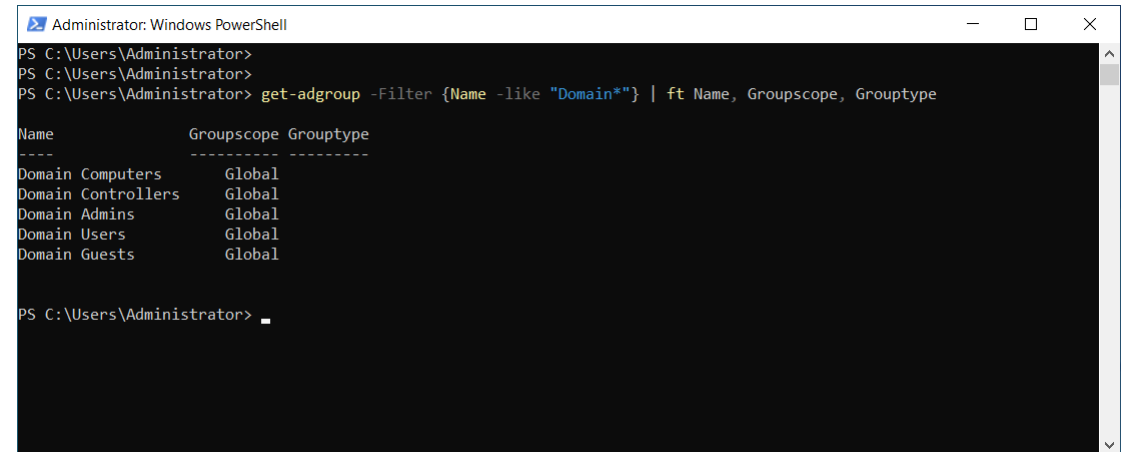
Overview of AD DS administration tools (1 of 6)

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



Overview of AD DS administration tools (2 of 6)

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



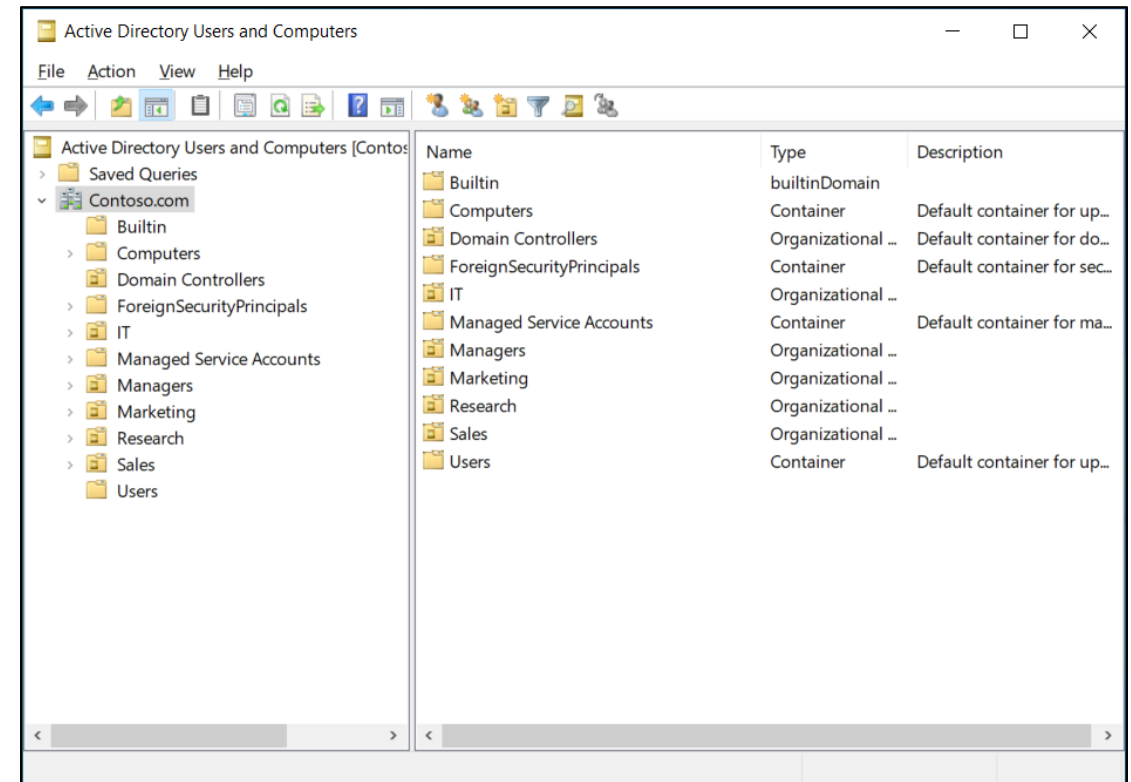
```
Administrator: Windows PowerShell
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> get-adgroup -Filter {Name -like "Domain*"} | ft Name, Groupscope, Grouptype

Name                Groupscope Grouptype
-----
Domain Computers    Global
Domain Controllers  Global
Domain Admins        Global
Domain Users         Global
Domain Guests        Global

PS C:\Users\Administrator> _
```

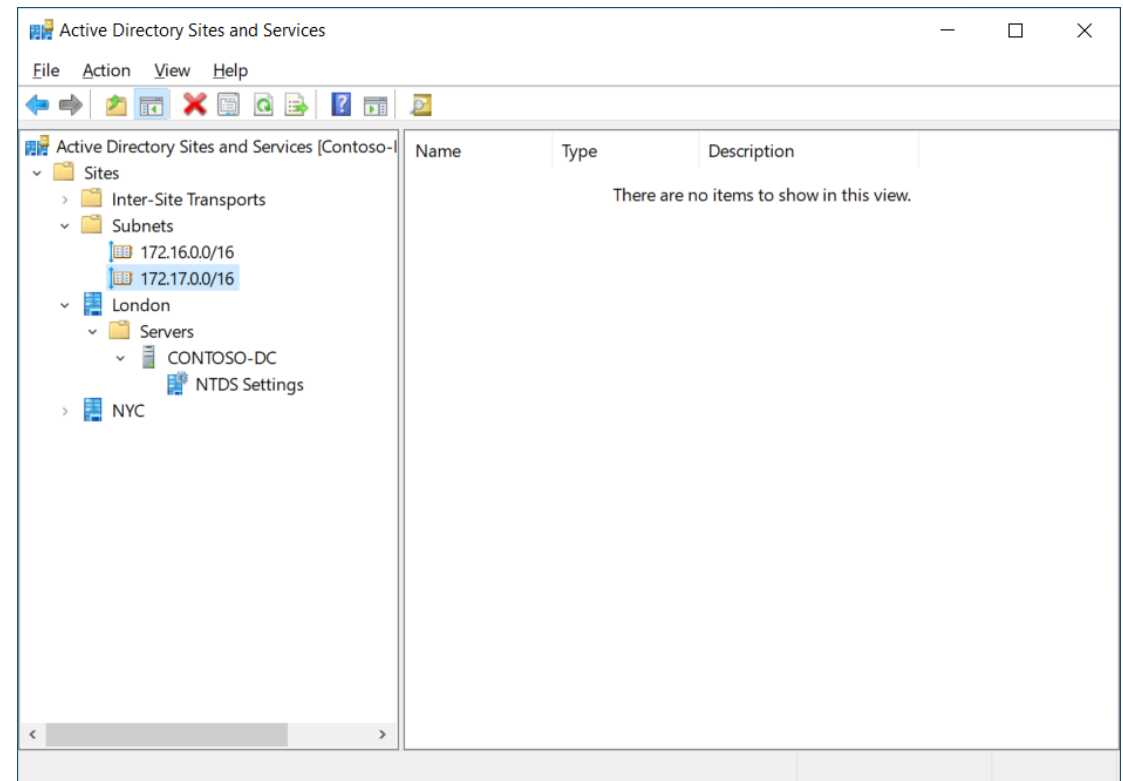
Overview of AD DS administration tools (3 of 6)

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



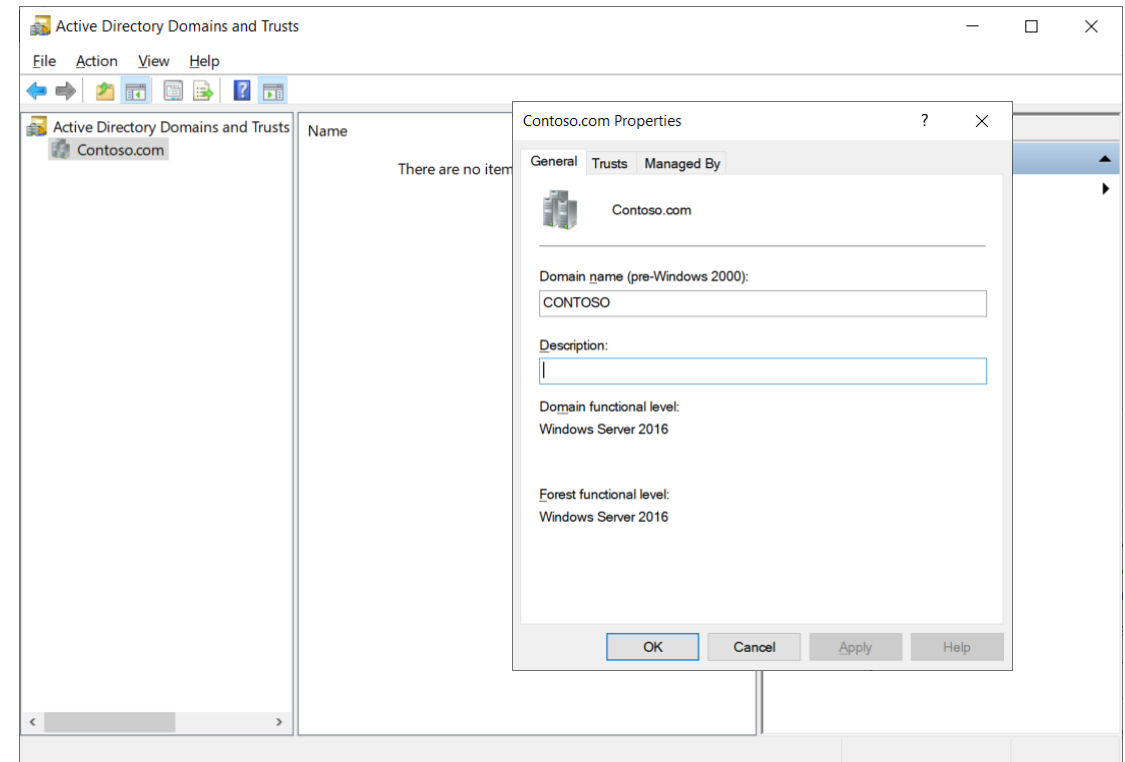
Overview of AD DS administration tools (4 of 6)

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



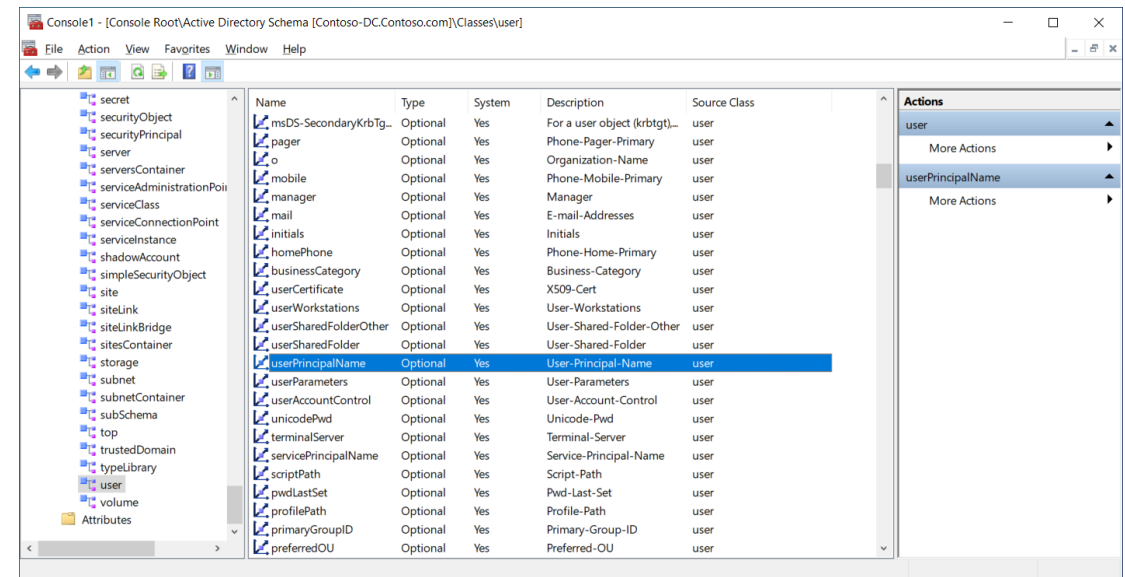
Overview of AD DS administration tools (5 of 6)

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



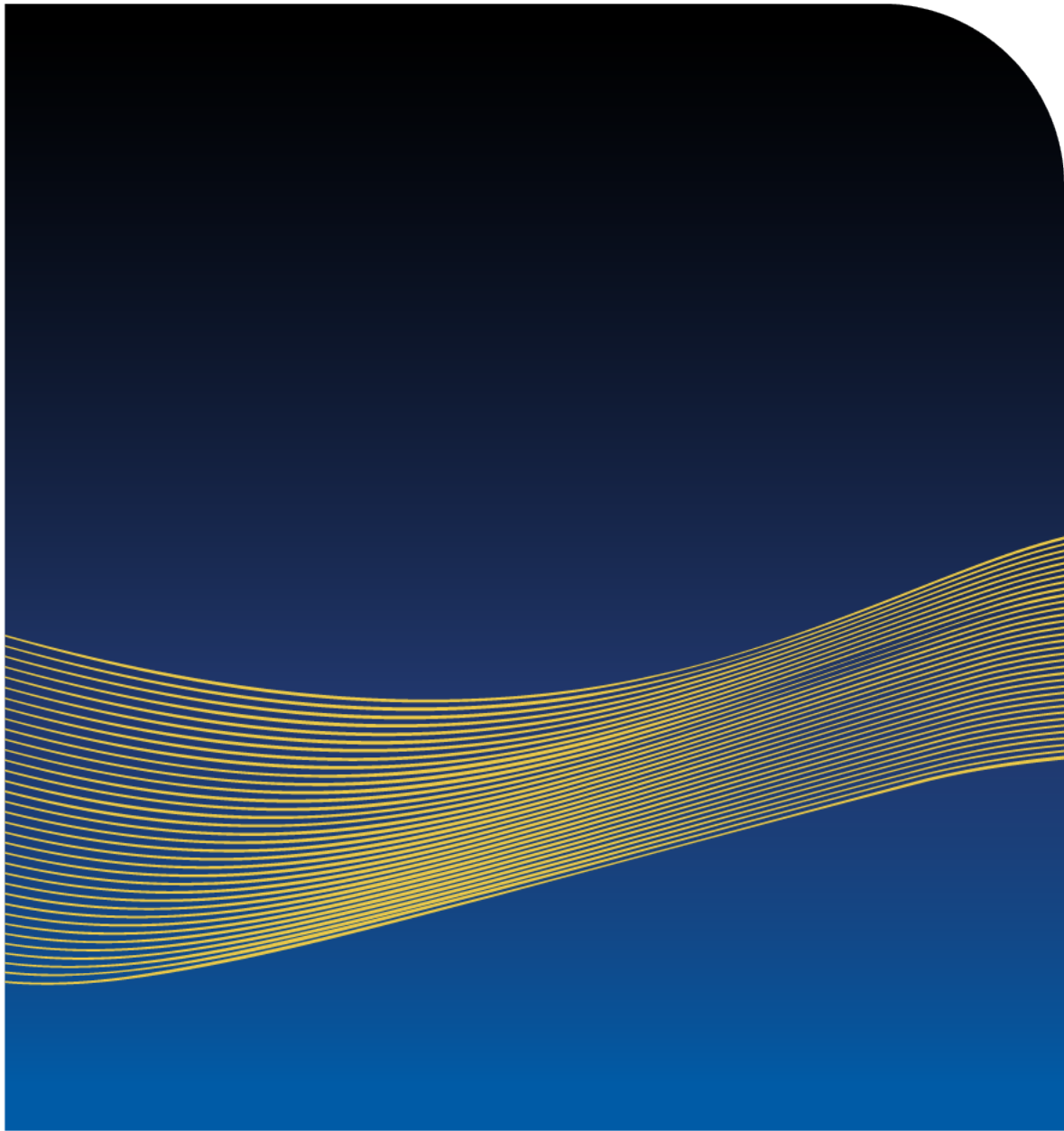
Overview of AD DS administration tools (6 of 6)

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





Demonstration: Manage AD DS



Lesson 2: AD DS DCs

Lesson 2 overview

To effectively manage AD DS, you must understand what DCs do, and how you can configure their behavior. This includes developing skills including server management, AD DS sign-in, and Domain Name System (DNS) configuration and management.

The topics in this lesson are:

- What is a DC?
- What are global catalog servers?
- Overview of service (SRV) records
- Demonstration: Review SRV records in Domain Name System (DNS)
- How does the AD DS sign-in process work?
- Overview of operations masters
- Transfer and seize roles

What is a DC?

- A Windows Server computer installed with the AD DS role and then promoted into the directory.
- DCs:
 - Provide authentication and authorization services.
 - Implement Kerberos as an authentication protocol.
 - Advertise their services using SRV records in DNS.
 - Support LDAP.
 - Store a copy of the AD DS database in a file named **Ntds.dit**.
 - Maintain a copy of the **SYSVOL** folder.
 - Use multimaster replication to maintain the synchronized state of both **Ntds.dit** and **SYSVOL**.

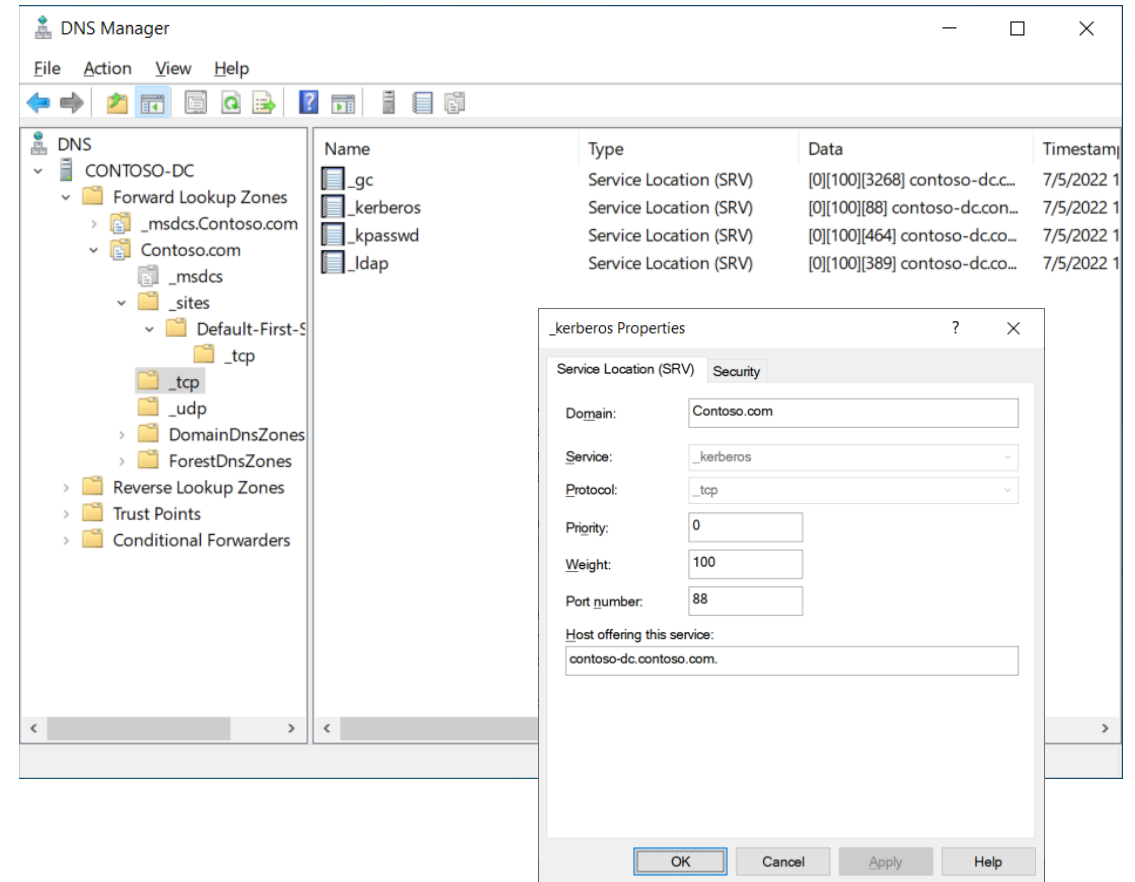
What are global catalog servers?

- *A global catalog server:*
 - Is a DC that has been selected to host a replica of an additional AD DS partition.
 - Contains a subset of attributes for all objects in the forest.
- Current recommendations for deploying global catalog servers are:
 - For a single domain environment, make all DCs global catalog servers.
 - In multi-domain environments, ensure that any DCs holding the infrastructure operations master role are not global catalog servers (unless all DCs are global catalog servers).
 - Ensure you have at least one global catalog server per physical AD DS site.

Overview of service (SRV) records

DCs register SRV records with their configured DNS server that identify the AD DS services that they provide. These records are:

- **_kerberos.** The authentication service is available on port 88 over TCP and UDP.
- **_kpasswd.** The Kerberos password service is available on port 464 over TCP and UDP.
- **_ldap.** Directory access is available on TCP port 389.
- **_gc.** The global catalog is available on TCP port 3268.

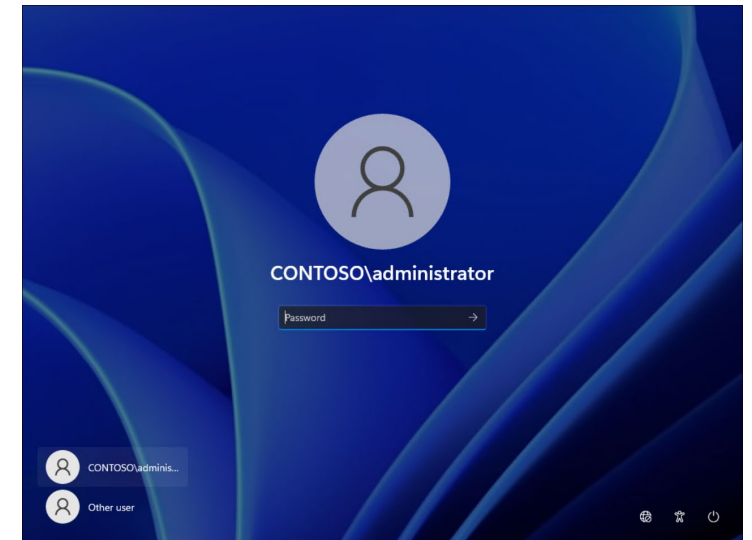




Demonstration: Review SRV records in Domain Name System (DNS)

How does the AD DS sign-in process work?

1. A user enters their username and password.
2. The user's computer routes the sign-in details to a DC.
3. The AD DS database is used to authenticate the user sign-in credentials.
4. The DC generates an access token for the user, known as a *TGT*.
5. The TGT is returned to the user's computer.
6. The user's computer presents the TGT to the DC.
7. The DC generates a service ticket to enable the user to authenticate on their computer.

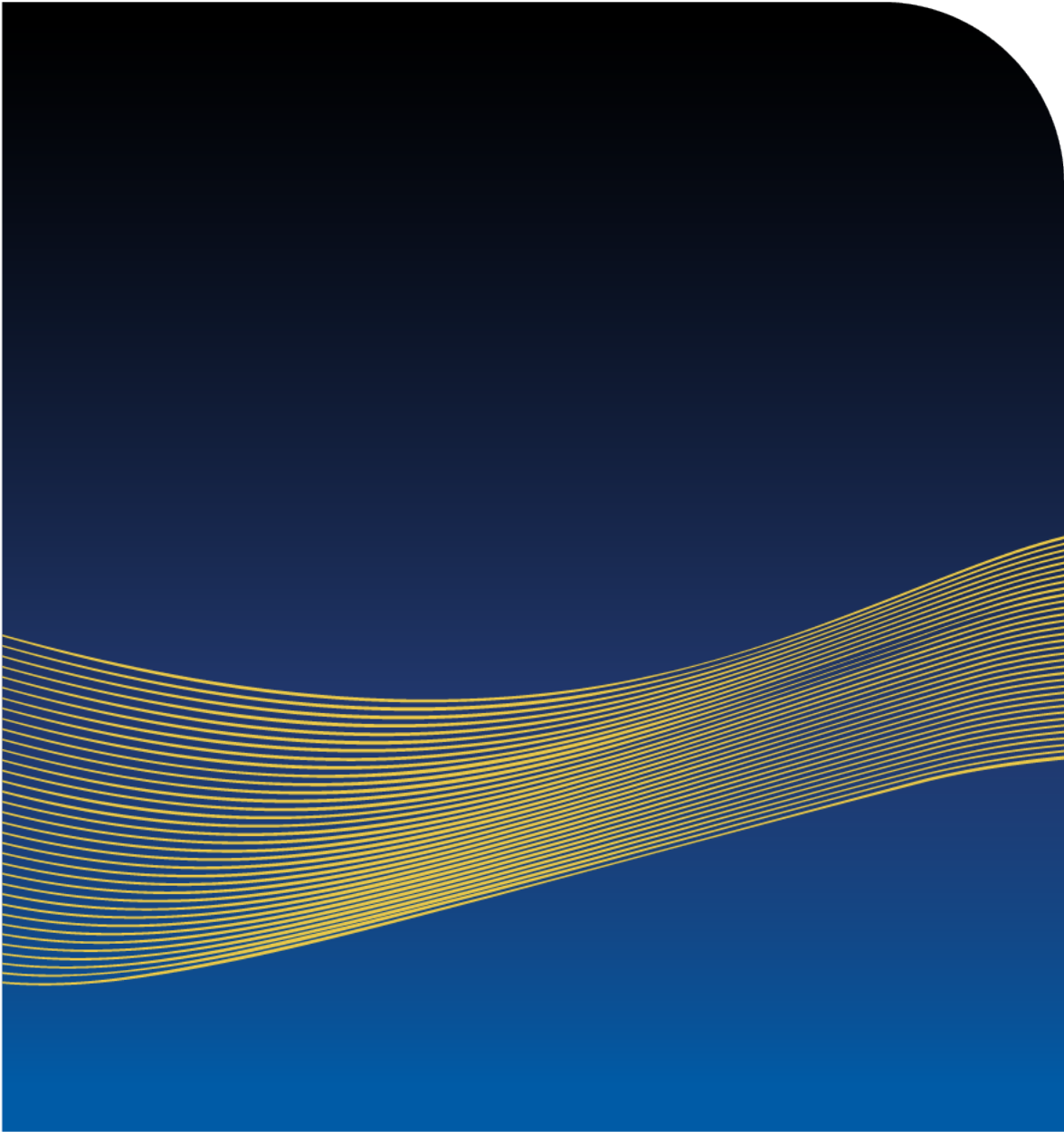


Overview of operations masters

- The forest root domain contains two forest-wide operations master roles:
 - Schema master
 - Domain naming master
- Each domain in your organization—including the forest root—hosts the following domain-level operations master roles:
 - PDC emulator
 - Infrastructure master
 - RID master

Transfer and seize roles

- Impact operations masters unavailability:
 - Schema master: Low
 - Domain naming master: Low
 - PDC emulator: High
 - Infrastructure master: Low
 - RID master: Medium
- Review current role holders:
 - `Get-ADForest | fl SchemaMaster, DomainNamingMaster`
 - `Get-ADDomain | fl InfrastructureMaster, PDCEmulator, RIDMaster`
- Seize roles:
 - `Move-ADDirectoryServerOperationsMasterRole -Identity "Contoso-SVR1" -OperationsMasterRole PDCEmulator, RIDMaster -Force`



Lesson 3: **Deploy AD DS DCs**

Lesson 3 overview

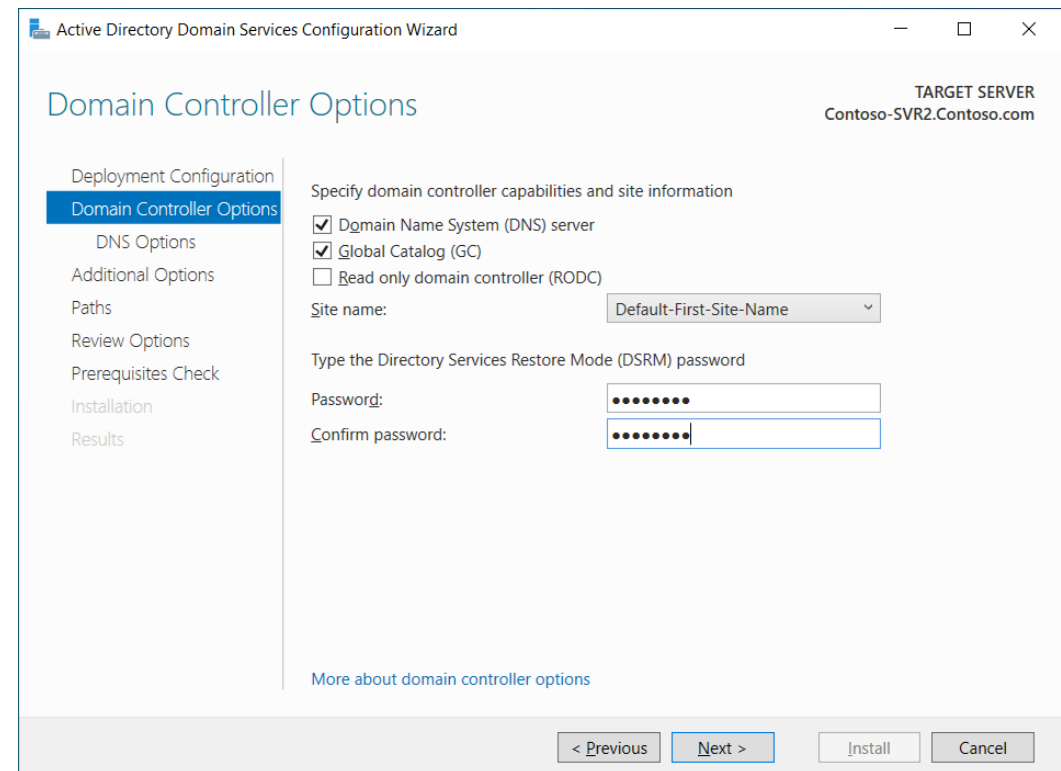
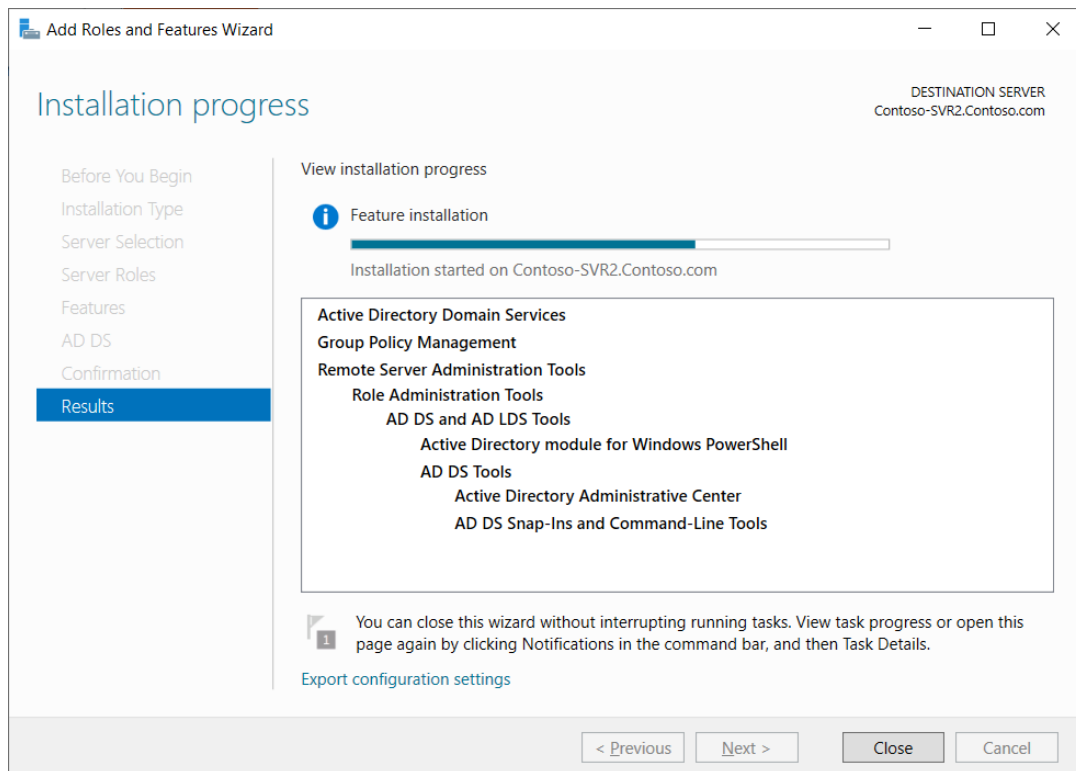
As you've learned, DCs are servers that host an instance of the AD DS database. It's important that you know how to manage DCs, including understanding how to deploy additional DCs.

The topics in this lesson are:

- Install a DC from Server Manager
- Install a DC on a Server Core
- Upgrade a DC
- Install a DC from media
- Clone DCs
- Best practices for DC virtualization

Install a DC from Server Manager

After installing the Active Directory Domain Services role, you must promote the server by running the **Active Directory Domain Services Configuration Wizard**.



Install a DC on a Server Core

- Using Server Manager:
 - Open Server Manager on another computer, connect to the target Server Core server, and then add the role in the usual way.
 - Run the **Active Directory Domain Services Configuration Wizard**.
- Using Windows PowerShell:
 - Run the **Install-WindowsFeature AD-Domain-Services** Windows PowerShell command.
 - Run the **Install-ADDSDomainController** Windows PowerShell command.

Upgrade a DC

Two possible approaches you can take to upgrade your DCs to Windows Server 2022:

- Perform an in-place operating systems upgrade for existing DCs.
- Deploy additional Windows Server computers running Windows Server 2022:
 - Promote them as additional DCs in your existing domain.
 - Transfer operations master roles.
 - Demote the DCs running the earlier version of Windows Server and remove them from the directory.

Install a DC from media

If you want to deploy a DC to a location that has a low bandwidth network connection to your main datacenter, consider using the **install from media** option.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> ntdsutil
C:\Windows\system32\ntdsutil.exe: activate instance ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create SYSVOL full c:\ifm
Creating snapshot...
Snapshot set {3ec0c9ad-3bb1-44a1-887d-99d636cdc284} generated successfully.
Snapshot {a577faec-3f3d-4482-868b-f8edac1cb5c8} mounted as C:\$SNAP_202207060918_VOLUMEC$\
Snapshot {a577faec-3f3d-4482-868b-f8edac1cb5c8} is already mounted.
Snapshot {a577faec-3f3d-4482-868b-f8edac1cb5c8} is already mounted.
Initiating DEFRAGMENTATION mode...
Source Database: C:\$SNAP_202207060918_VOLUMEC$\Windows\NTDS\ntds.dit
Target Database: c:\ifm\Active Directory\ntds.dit

Defragmentation Status ( complete)

0  10  20  30  40  50  60  70  80  90 100
|---|---|---|---|---|---|---|---|---|---|
.....█
```

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the Windows logo, the text 'Active Directory Domain Services Configuration Wizard', and standard window controls. The main content area is titled 'Additional Options' in blue. On the right side, it identifies the 'TARGET SERVER' as 'Contoso-SVR2.Contoso.com'. A left-hand navigation pane lists several steps: 'Deployment Configuration', 'Domain Controller Options', 'DNS Options', 'Additional Options' (which is highlighted with a blue background), 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main pane displays the 'Specify Install From Media (IFM) Options' section. It features a checkbox labeled 'Install from media' which is checked. Below this is a 'Path:' label followed by an empty text box and a 'Verify' button. Further down, the 'Specify additional replication options' section shows a 'Replicate from:' label and a dropdown menu currently set to 'Any domain controller'. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A link that says 'More about additional options' is located just above the 'Next >' button.

Clone DCs

Prepare the source DC:

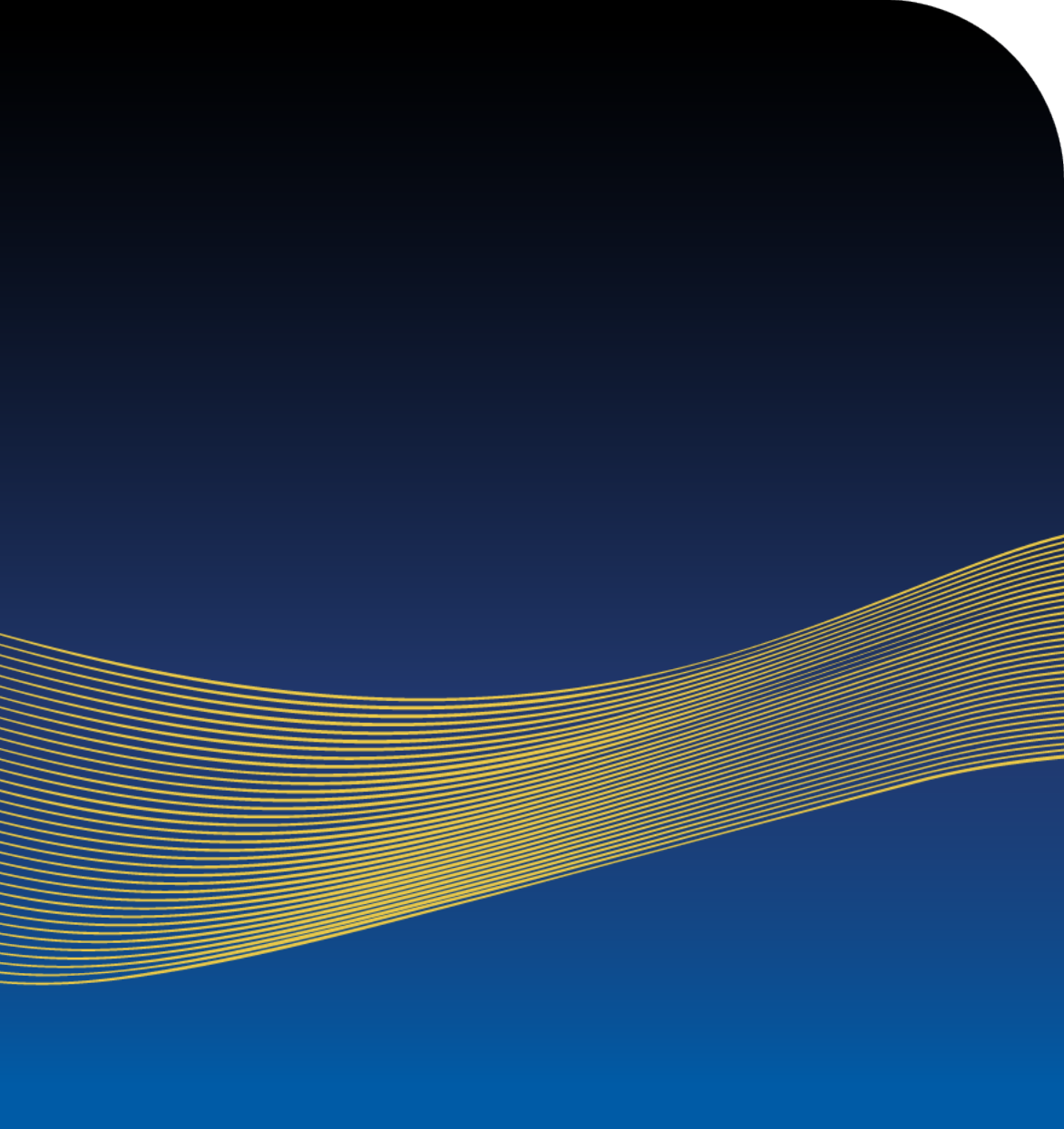
1. Add the source DC to the **Cloneable Domain Controllers** group.
2. Check that any apps installed on the source DC support cloning.
3. Create the **DCCloneConfig.xml** file.
4. Export the source DC.

Create DC clones:

1. Verify that the PDC emulator operations master role holder is online.
2. Verify that a global catalog server is online.
3. Use the Import function to create your clones.
4. If necessary, individually configure the clones.
5. Start the clones and verify their functionality.

Best practices for DC virtualization

- Deploy at least two virtualized DCs. This helps avoid a single point of failure and helps improve performance.
- Synchronize time. Ensure all computer clocks—virtual or physical—are synchronized.
- Implement a hypervisor that:
 - Supports VM generation IDs. For example, Microsoft Hyper-V.
 - Enables you to move VMs between sites.
- Avoid checkpoints. Due to the multimaster nature of the AD DS database, checkpoints could easily create inconsistencies.



Lesson 4:

Azure AD overview

Lesson 4 overview

Both Azure and Microsoft 365 are underpinned with Azure AD, which provides for authentication and authorization for cloud apps and services. Microsoft also provides Azure AD Domain Services, which is a managed directory service in Azure. It's important that you know whether to implement Azure AD Domain Services to support your on-premises apps as you migrate to the cloud, or whether Azure AD is the more appropriate choice.

The topics in this lesson are:

- What is Azure AD?
- How does Azure AD compare with AD DS?
- Azure AD editions
- Azure AD administration tools
- Azure AD Domain Services (Azure AD DS)

What is Azure AD?

- Azure AD is designed to provide authentication and authorization for users and devices that want to access cloud apps.
- Using Azure AD you can:
 - Provide SSO for cloud apps from multiple providers.
 - Synchronize on-premises AD DS with Azure AD, enabling SSO for on-premises users.
- Azure AD provides the following features:
 - Conditional access
 - MFA
 - Intuitive web-based management console
 - Compliance with authentication standards and protocols widely used on the internet

How does Azure AD compare with AD DS?

AD DS addresses the needs of on-premises administrators, and has the following features:

- A hierarchical structure based on containers
- A granular security model
- Security based on groups
- Configuration through Group Policy
- Support for on-premises directory access and authentication protocols:
 - LDAP and Kerberos

Azure AD addresses the needs of cloud administrators, and has the following features:

- A flat architecture
- Less granular security model
- Security that implements RBAC
- Configuration based on groups
- Support for cloud-based directory access and authentication protocols:
 - SAML
 - OAuth

Azure AD editions (1 of 2)

- Four editions:
 - Free
 - Microsoft Office 365 apps
 - Premium P1
 - Premium P2
- All editions support:
 - SSO
 - RBAC
 - Device registration
 - MFA
- Azure AD for Office 365 adds:
 - Unlimited directory objects
 - Company branding
 - Self-service password reset
 - Device writeback

Azure AD editions (2 of 2)

Azure AD Premium P1 adds:

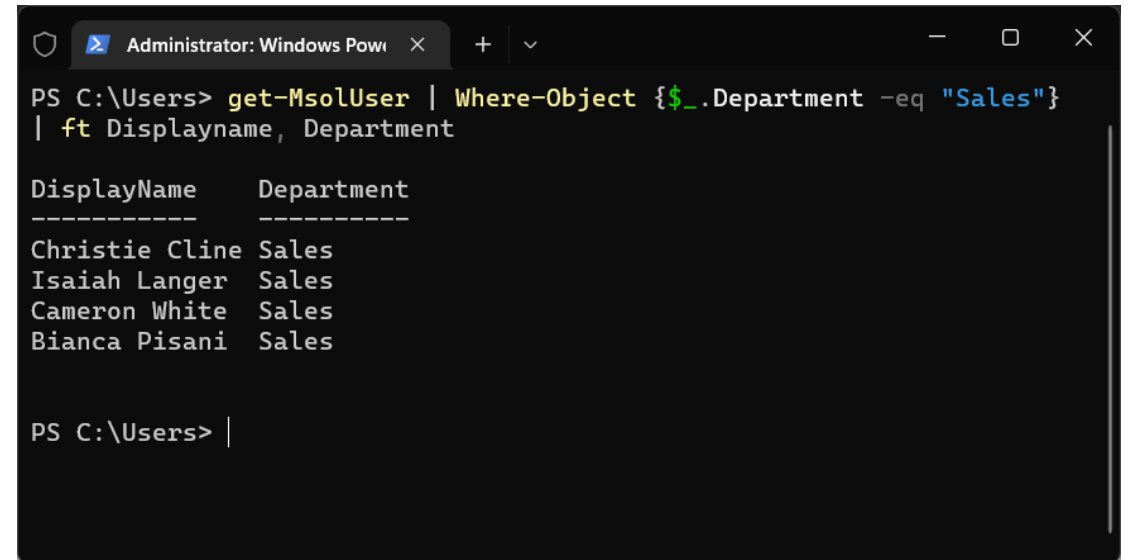
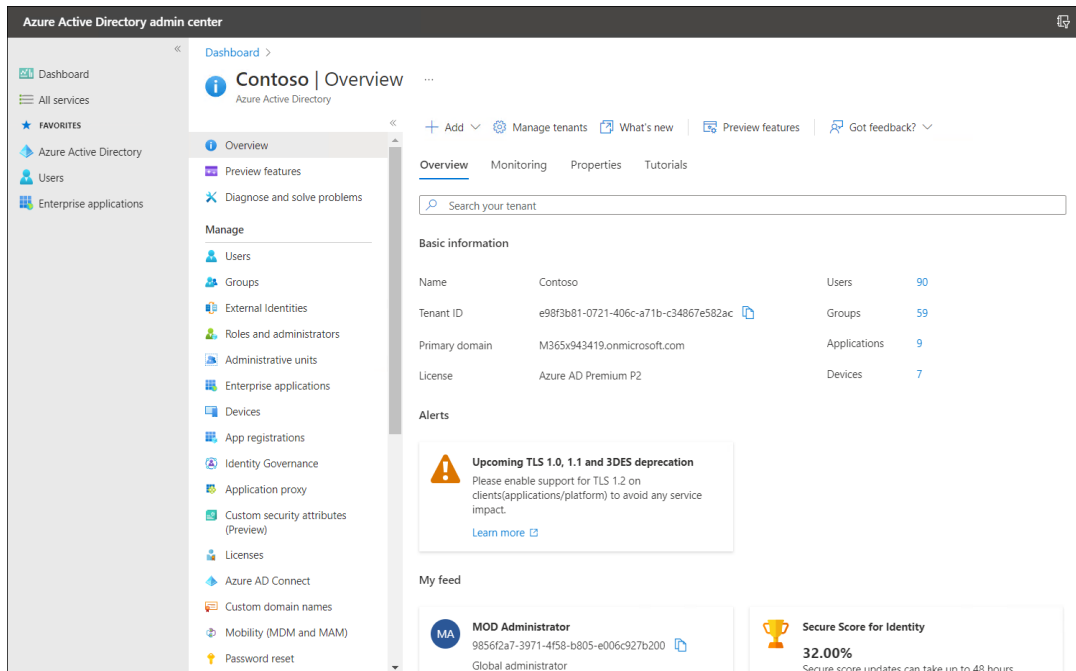
- Synchronization with AD DS
- Device write-back to AD DS identities
- Seamless SSO
- Support for hybrid identity
- Application proxy
- Dynamic groups
- Group naming policies
- Conditional access
- Microsoft Identity Manager
- Azure Information Protection P1
- Security and activity reporting

Azure AD Premium P2 adds:

- Azure AD Identity Protection
- Privileged Identity Management
- Defender for Cloud Apps
- Azure Information Protection Premium P2

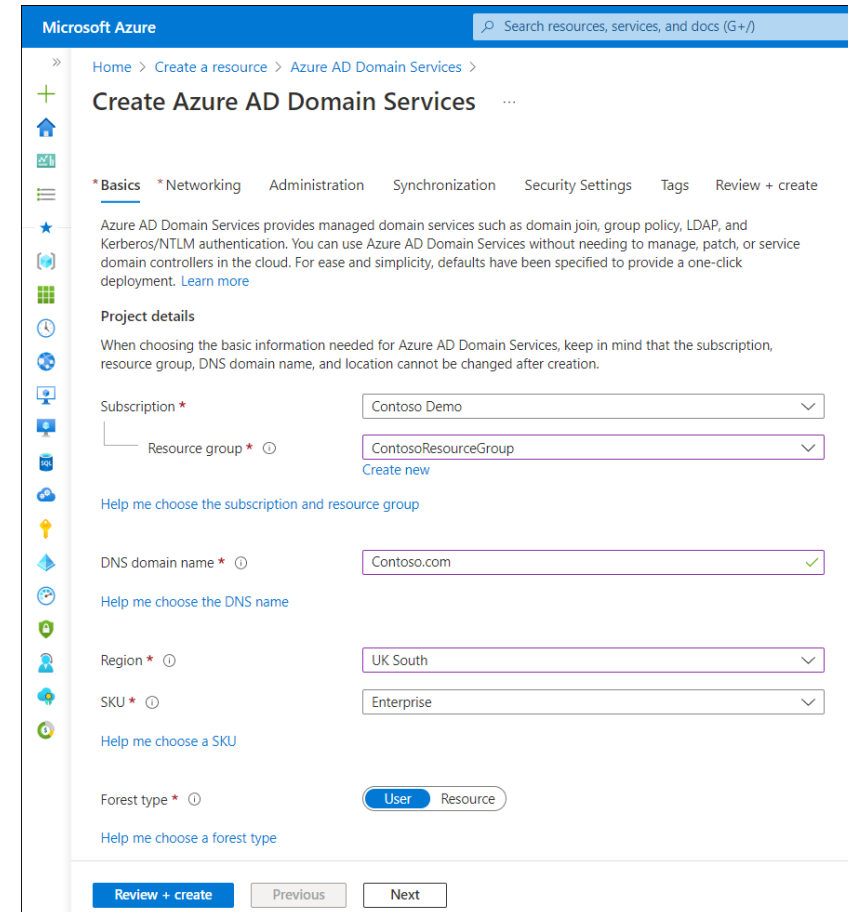
Azure AD administration tools

You can administer Azure AD from a web portal and from Windows PowerShell.



Azure AD Domain Services (Azure AD DS)

- Azure AD Domain Services:
 - Resembles functionality of on-premises AD DS.
 - Is serverless, and doesn't require IaaS VMs running as DCs.
 - Supports:
 - LDAP
 - Kerberos
 - GPOs
- By using Azure AD Domain Services, you can consider migrating your on-premises directory-aware apps to the cloud.



Microsoft Azure

Home > Create a resource > Azure AD Domain Services >

Create Azure AD Domain Services

* Basics * Networking Administration Synchronization Security Settings Tags Review + create

Azure AD Domain Services provides managed domain services such as domain join, group policy, LDAP, and Kerberos/NTLM authentication. You can use Azure AD Domain Services without needing to manage, patch, or service domain controllers in the cloud. For ease and simplicity, defaults have been specified to provide a one-click deployment. [Learn more](#)

Project details

When choosing the basic information needed for Azure AD Domain Services, keep in mind that the subscription, resource group, DNS domain name, and location cannot be changed after creation.

Subscription * Contoso Demo

Resource group * ContosoResourceGroup [Create new](#)

[Help me choose the subscription and resource group](#)

DNS domain name * Contoso.com ✓

[Help me choose the DNS name](#)

Region * UK South

SKU * Enterprise

[Help me choose a SKU](#)

Forest type * User Resource

[Help me choose a forest type](#)

[Review + create](#) [Previous](#) [Next](#)



Lab 1: Deploy and administer AD DS

Knowledge check (1 of 5)

1. Which of the following options are forest-wide operations master roles?
 - a. Domain naming master
 - b. PDC emulator
 - c. RID master
 - d. Schema master
 - e. Infrastructure master
2. You want to add an attribute to the global catalog for the **User** class object. How do you achieve this?

Knowledge check (2 of 5)

3. How many DCs should be global catalog servers?
4. On which port is Kerberos accessible?
5. When should you consider seizing the PDC emulator role?
6. Which PowerShell cmdlet can you use to promote a DC?
7. Your organization wants to move all its apps to the cloud. However, you have a directory-aware app running in your on-premises AD DS environment. Which directory service or services should you deploy in the cloud to meet your organizational needs?

Knowledge check (3 of 5)

1. Which of the following options are forest-wide operations master roles?
 - a. Domain naming master
 - b. Schema master
2. You want to add an attribute to the global catalog for the User class object. How do you achieve this?
 - Use the Active Directory Schema snap-in to add the attribute to the global catalog.

Knowledge check (4 of 5)

3. How many DCs should be global catalog servers?
 - The recommended best practice is to make all DCs into global catalog servers.
4. On which port is Kerberos accessible?
 - TCP and UDP port 88
5. When should you consider seizing the PDC emulator role?
 - If the PDC emulator role holder goes offline unexpectedly, seize the role and allocate it to another DC. If you're planning to take the PDC emulator role holder offline, then transfer the role ahead of time.

Knowledge check (5 of 5)

6. Which PowerShell cmdlet can you use to promote a DC?
 - **Install-ADDSDomainController**
7. Your organization wants to move all its apps to the cloud. However, you have a directory-aware app running in your on-premises AD DS environment. Which directory service or services should you deploy in the cloud to meet your organizational needs?
 - Azure AD Domain Services is a managed PaaS directory. It's similar to AD DS and would be ideal to host direct-aware apps in the cloud.

Thank you

©2022 Waypoint Ventures, LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.