Microsoft

Tag 3

AZ-800
Administer Windows Server Hybrid Core Infrastructure

Guten Morgen!

Agenda AZ-800

1 Deploy and manage identity infrastructure – Windows Server
2 Deploy and manage identity infrastructure – Hybrid

3 Administering Windows Server Hybrid Core Infrastructure – Windows Server
4 Administering Windows Server Hybrid Core Infrastructure – Hybrid

5 Manage virtualization and containers – Windows Server
6 Manage virtualization and containers – Hybrid

7 Implement and manage networking infrastructure – Windows Server
8 Implement and manage networking infrastructure – Hybrid

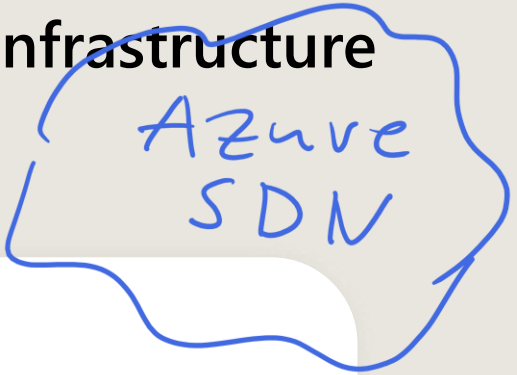
9 Configure storage and file services – Windows Server
10 Configure storage and file services – Hybrid

Lab
178
10x

TCP/IP DNS
~~DHCP~~

NTFS
Blob (= S3 Object store)
Share SMB 3.1

Implement and manage an on-premises and hybrid networking infrastructure *(Network infrastructure services in Windows Server)*



- Deploy and manage DHCP
- Implement Windows Server DNS
- Implement IP address management
- Implement remote access
- Lab 07 – Implementing and configuring network infrastructure services in Windows Server

IP IPv6

Deploy and manage DHCP

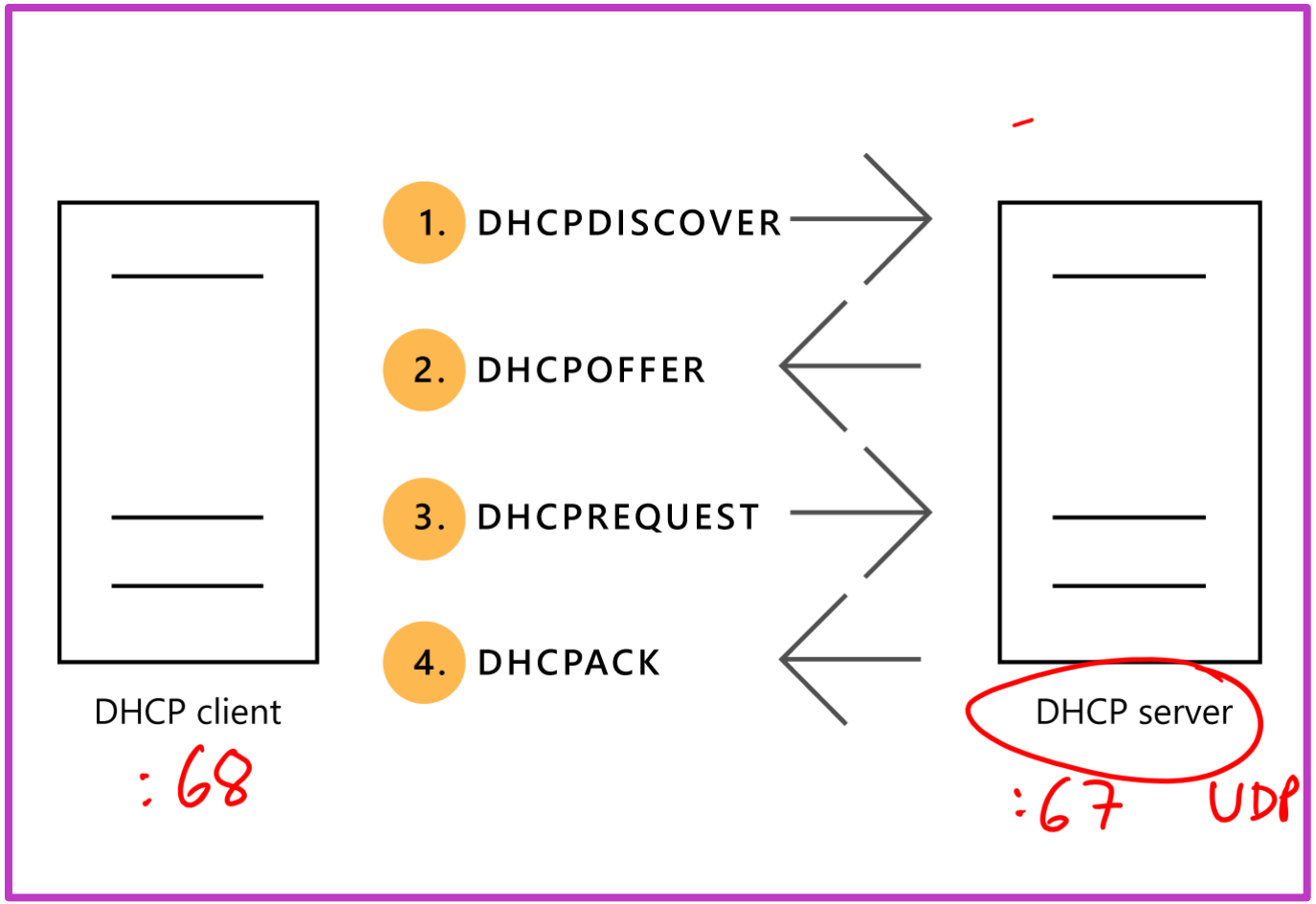
Learning Objectives – Deploy and manage DHCP

- Use DHCP to simplify IP configuration
- Install and configure the DHCP role
- Configure DHCP options
- Configure DHCP scopes
- Select DHCP high availability options
- Implement DHCP failover
- Learning recap

Use DHCP to simplify IP configuration

TCP / IP
Vint Cerf 32 Bit

- Dynamic Host Control Protocol (DHCP) is a network management protocol.
- The main benefit of using DHCP is for auto assignment of IP addresses.
- DHCP works with the four-step communication process known as DORA. Discover, Offer, Request and Acknowledge.
- When the DHCP lease reaches 50% of the lease time, the client automatically attempts to renew the lease
- DHCP version 6 (DHCPv6) supports stateful and stateless configurations for configuring clients in an IPv6 environment



:53 DNS
UDP

Install and configure the DHCP role (1 of 2)

Two ways to install the DHCP Server role:

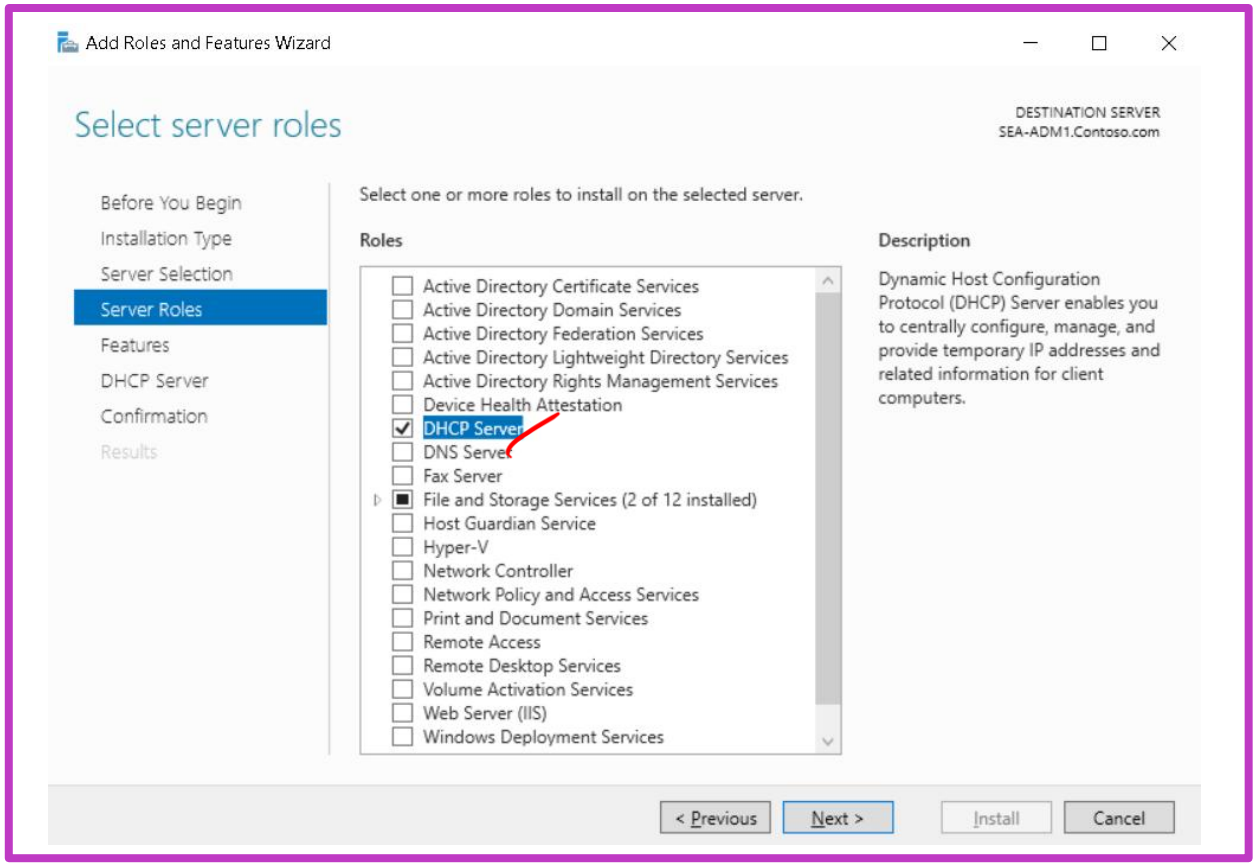
- Use Roles & Features in Windows Admin Center or the Add Roles and Features Wizard in the Server Manager console.
- Use the following Windows PowerShell command:

```
Add-WindowsFeature DHCP –IncludeManagementTools
```

To manage a DHCP server by using Windows Admin Center, you must install the DHCP management cmdlets on the DHCP server

To create the DHCP management groups by using Windows PowerShell, run the following command:

```
Add-DhcpServerSecurityGroup -Computer
DhcpServerName
```



Install and configure the DHCP role (2 of 2)

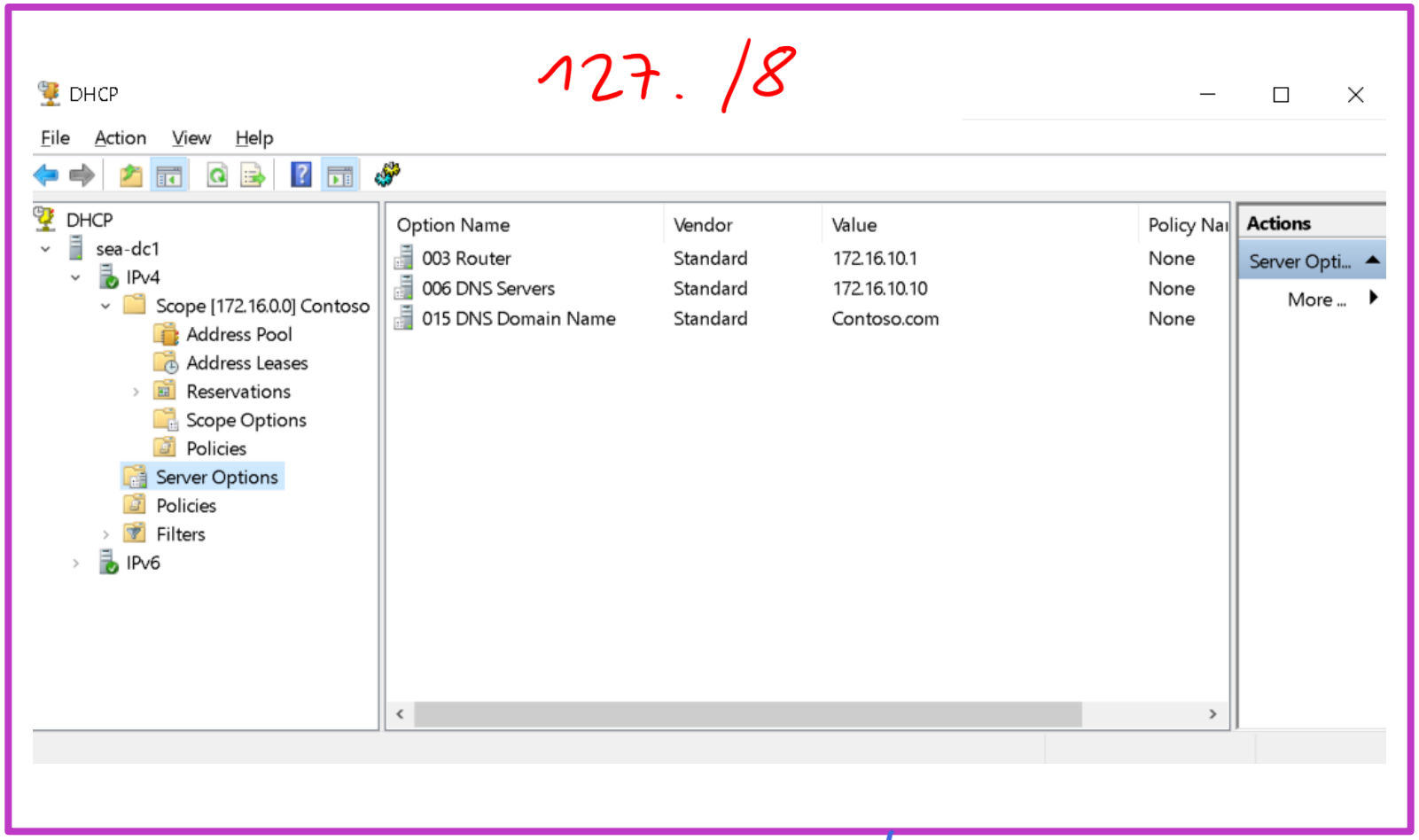
- DHCP server must be authorized in the Active Directory domain before it can support DHCP clients.
- Authorizing the DHCP server is one of the post-installation tasks that you must perform after you install the DHCP server.
- A standalone DHCP server is a computer that is running Windows Server, is not a member of an AD DS, and has the DHCP Server role installed and configured
- When you detect unauthorized DHCP servers, you should disable the DHCP service on them.
- You can find the IP address of the unauthorized DHCP server by running the ipconfig /all command on the DHCP client computer that obtained the incorrect IP address information.

Configure DHCP options

IANA 192.168 /16
10. /8
172.16. /12
} Private

127. /8

- DHCP options can be configured from DHCP console.
- Most DHCP options are configured at the scope level because the scope level represents a subnet where all clients have the same configuration needs.



Enno Rey

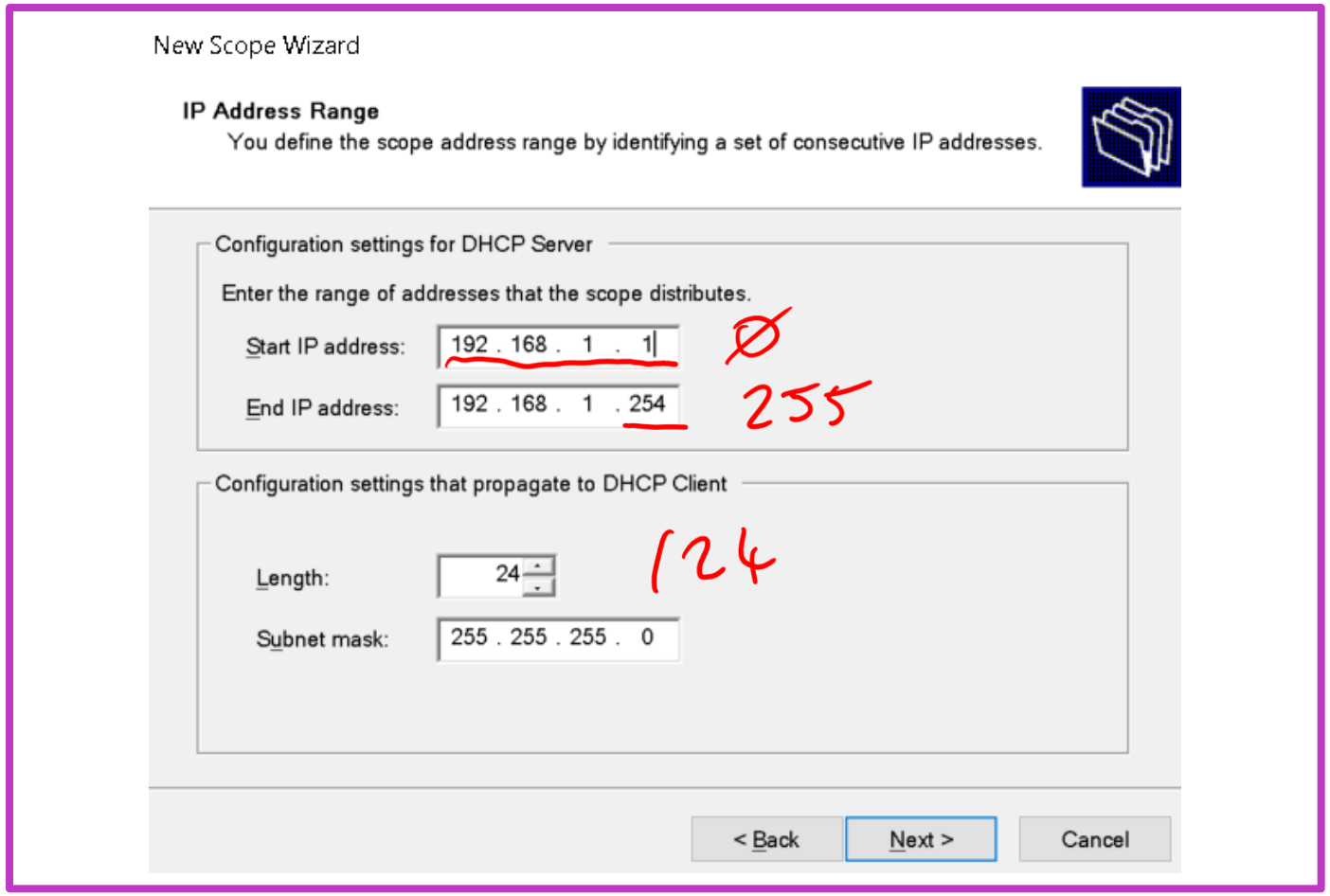
fe80::/

Configure DHCP scopes (1 of 2)

A DHCP scope is a range of IP addresses that are available for lease and that a DHCP server manages.

To create and configure a scope, you must define the following properties:

- Name and description
- IP address range
- Subnet mask
- Exclusions
- Delay
- Lease duration
- Options
- Activation



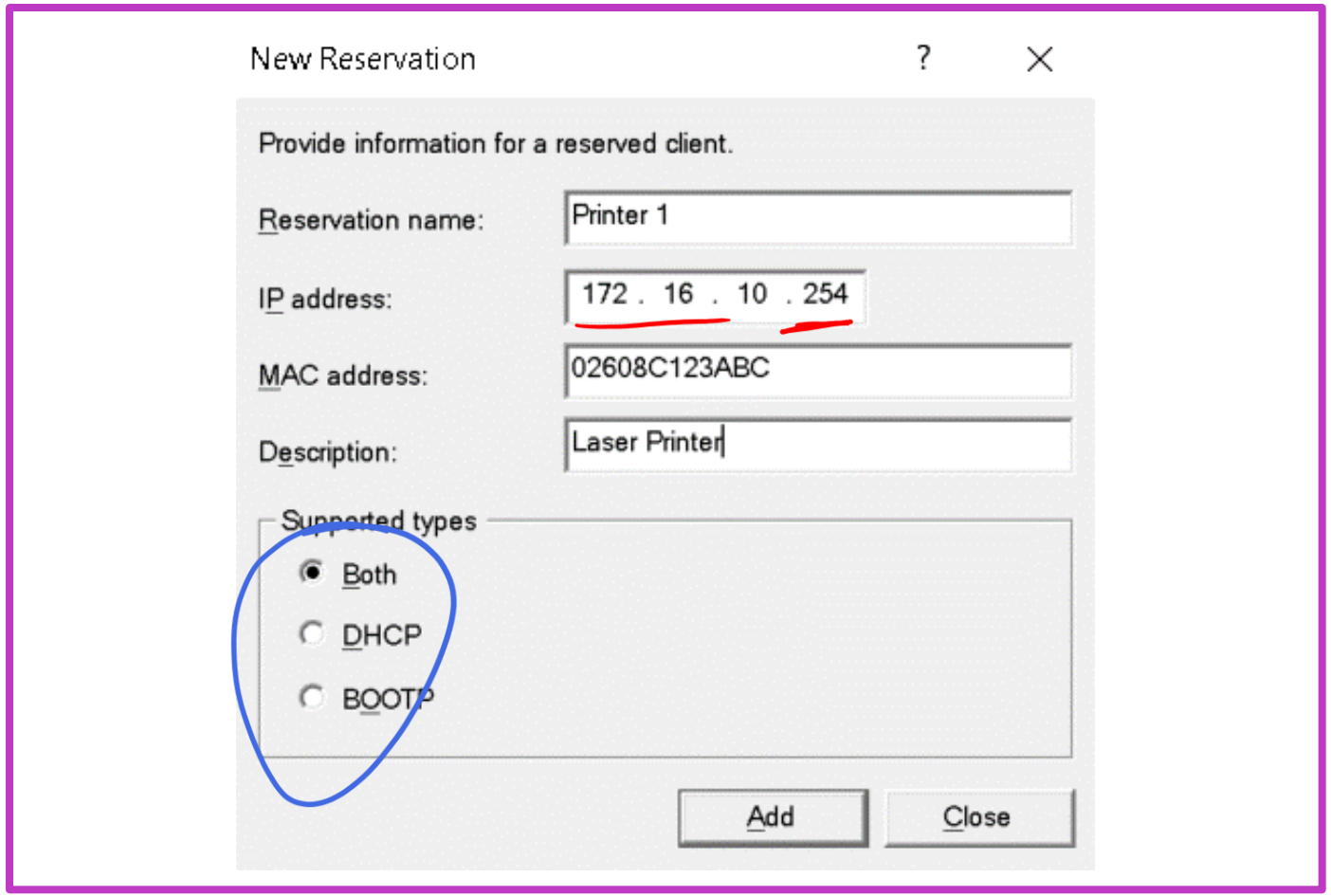
Configure DHCP scopes (2 of 2)

You can use following common windows PowerShell cmdlets to manage the DHCP scopes:

- Add-DhcpServerv4Scope
- Get-DhcpServerv4Scope
- Get-DhcpServerv4ScopeStatistics
- Remove-DhcpServerv4Scope
- Set-DhcpServerv4Scope

You must provide the following information to create the reservation in the New Reservation dialog box:

- Reservation name
- IP address
- MAC address
- Description



Demonstration – Create a DHCP scope using the DHCP console

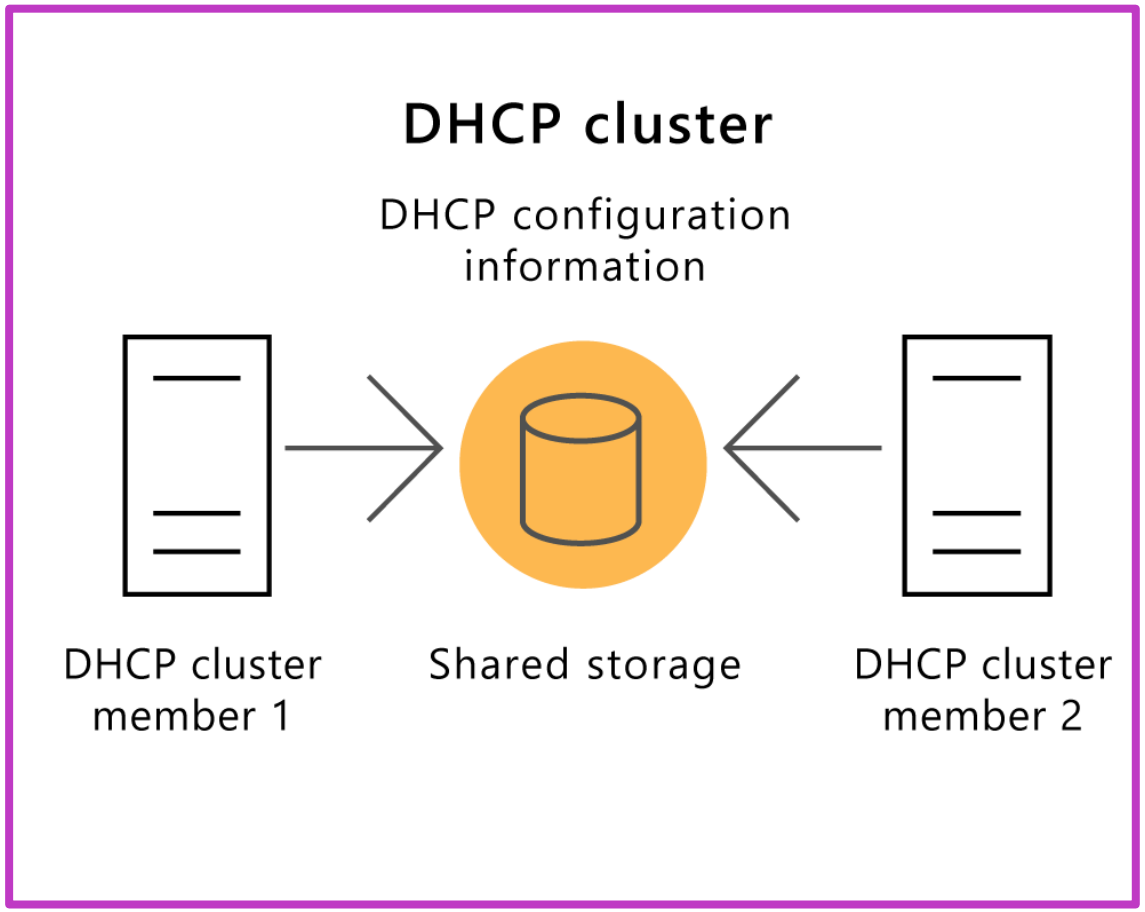
In the DHCP console, create a new scope

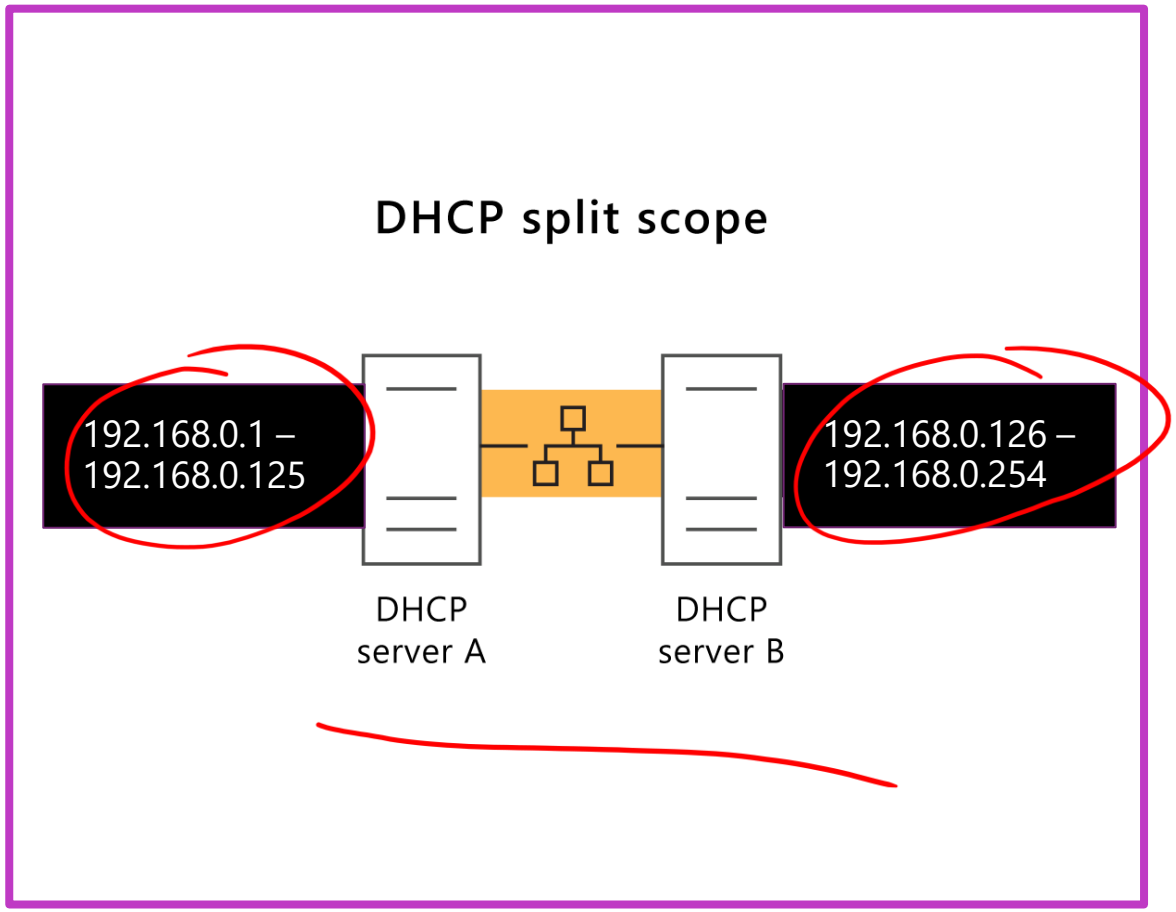
Define the properties of the scope

Activate the scope

Add a reservation and define the properties

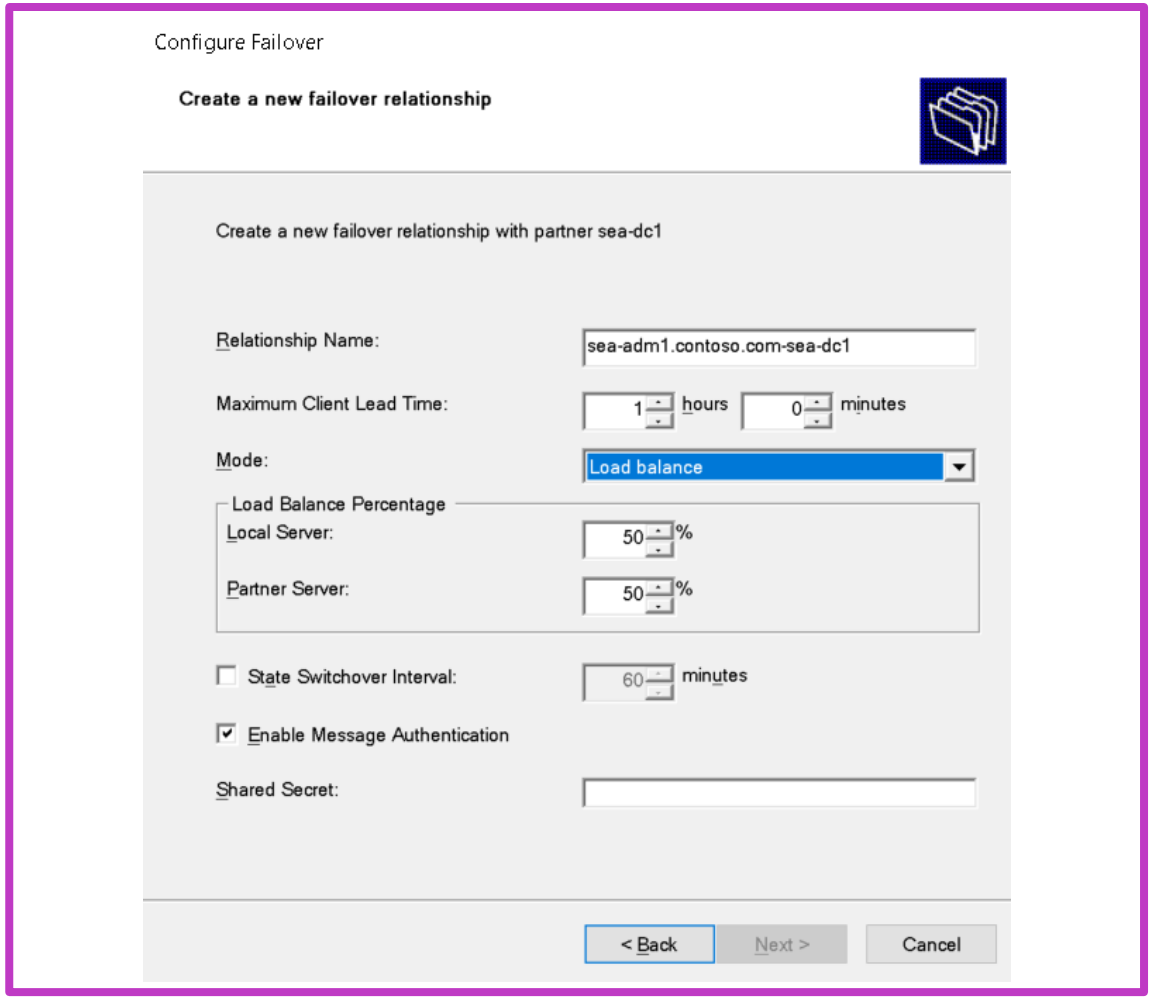
Select DHCP high availability options





Implement DHCP failover

- The DHCP failover feature allows two DHCP servers to work together to provide IP address information to clients.
- You can configure only two DHCP servers in a failover relationship, and you can configure these only for IPv4 scopes.
- To configure DHCP Failover, establish a failover relationship between the two DHCP servers and give the relationship a unique name.
- To configure failover in the DHCP Management console, use the Configuration Failover Wizard.
- You can configure failover in one of the two modes:
  - Load balance
  - Hot standby



Learning recap – Deploy and manage DHCP

Microsoft Learn Modules (docs.microsoft.com/Learn)

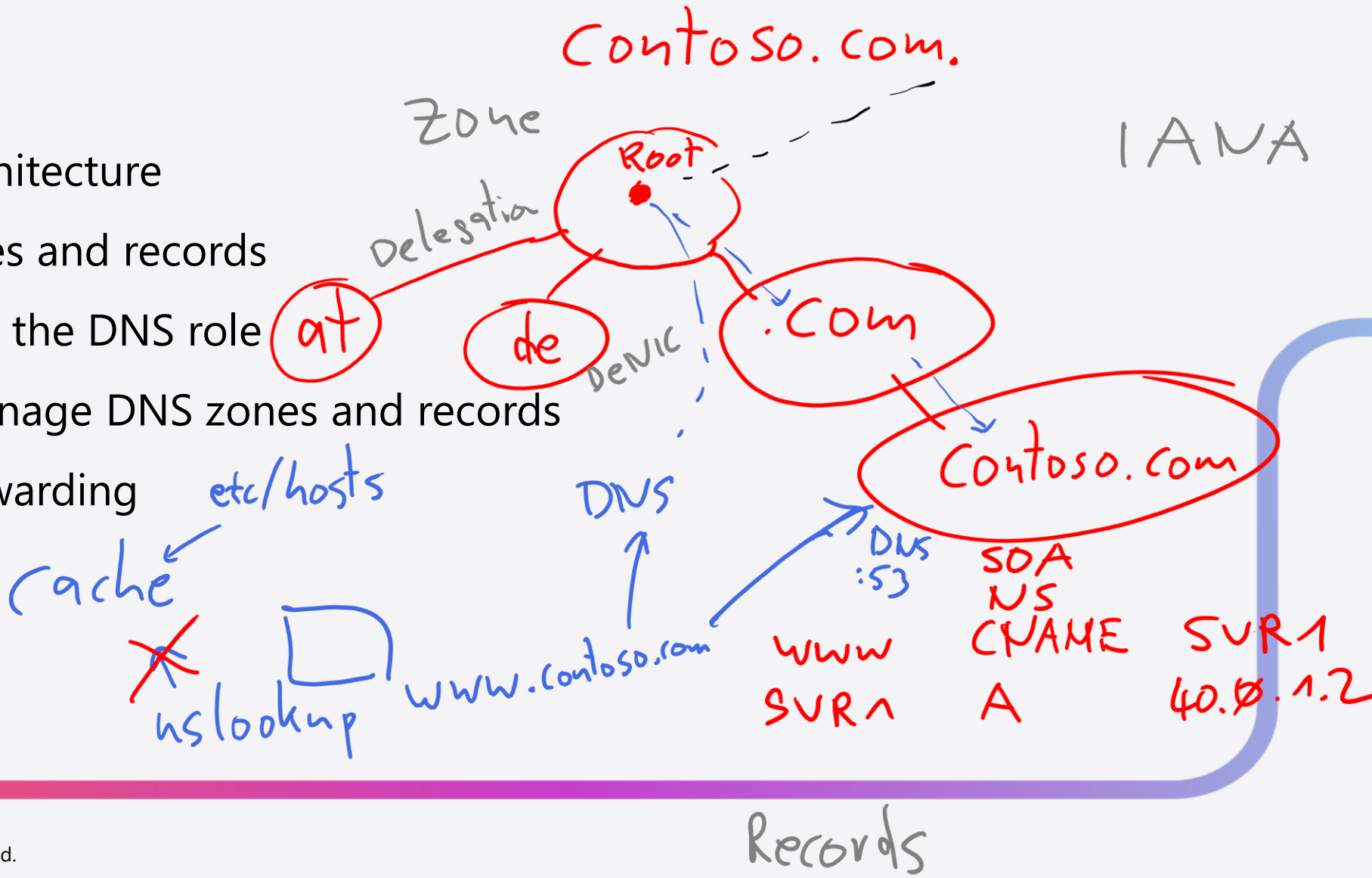
Deploy and manage DHCP

Module assessment

Implement Windows Server DNS

Learning Objectives – Implement Windows Server DNS

- Explore the DNS architecture
- Work with DNS zones and records
- Install and configure the DNS role
- Demonstration - manage DNS zones and records
- Implement DNS forwarding
- Learning recap



Explore the DNS architecture (1 of 2)

- Domain Name Service (DNS) provides hostname resolutions to IP address.
- DNS servers can also resolve IP addresses into names. That is called reverse lookup.
- The most common use for DNS is resolving fully qualified domain names (FQDNs), such as sea-dc1.contoso.com, to its IP addresses.
- A DNS server responds to requests for DNS records which are initiated by DNS clients.
- DNS Namespace is an organized hierarchical structure.

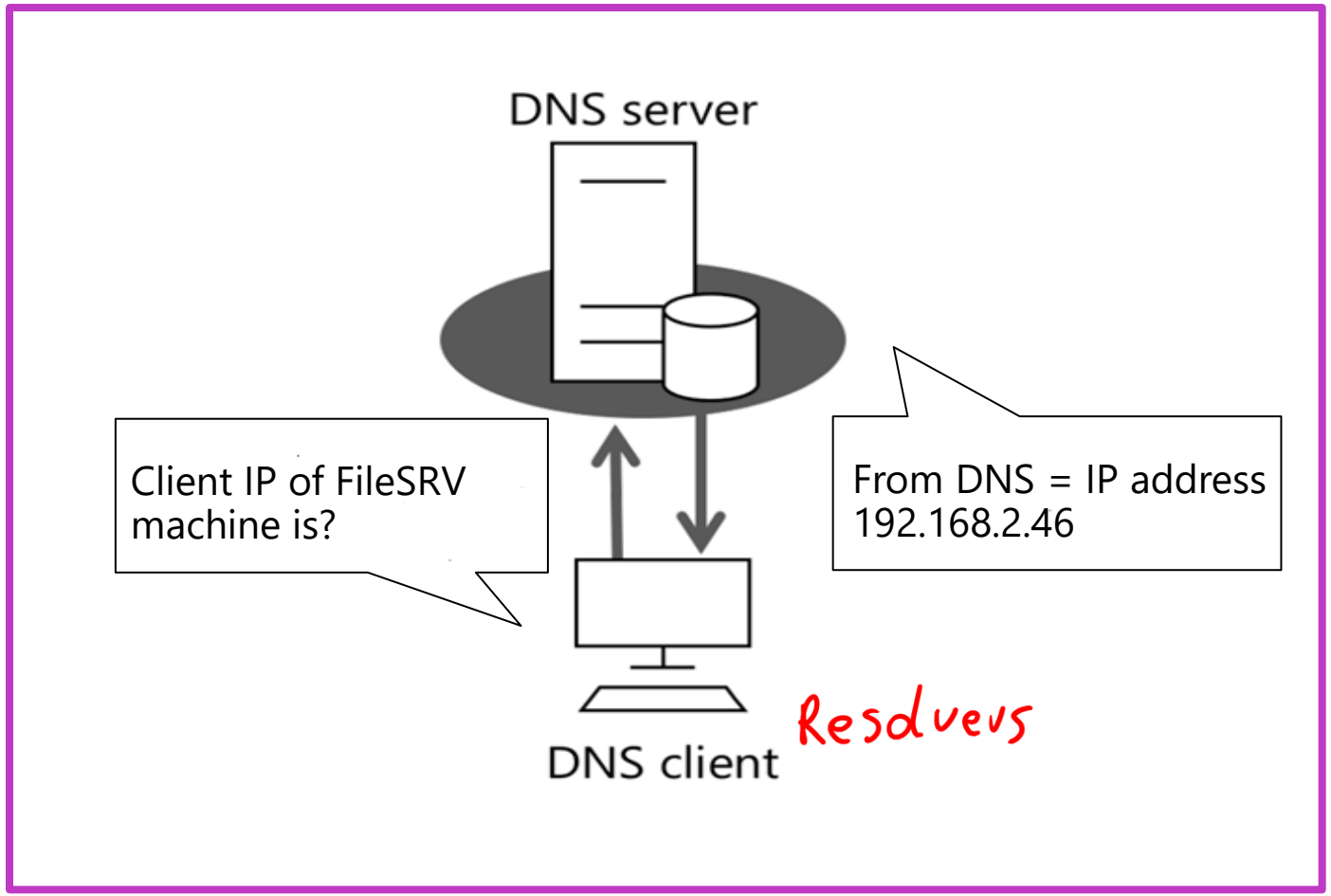
Explore the DNS architecture (2 of 2)

DNS resolvers

- A DNS resolver is a server that resolves DNS queries.
- The DNS Client service sends DNS requests to the DNS server. After receiving a response from the DNS server, the client caches the response for future use.

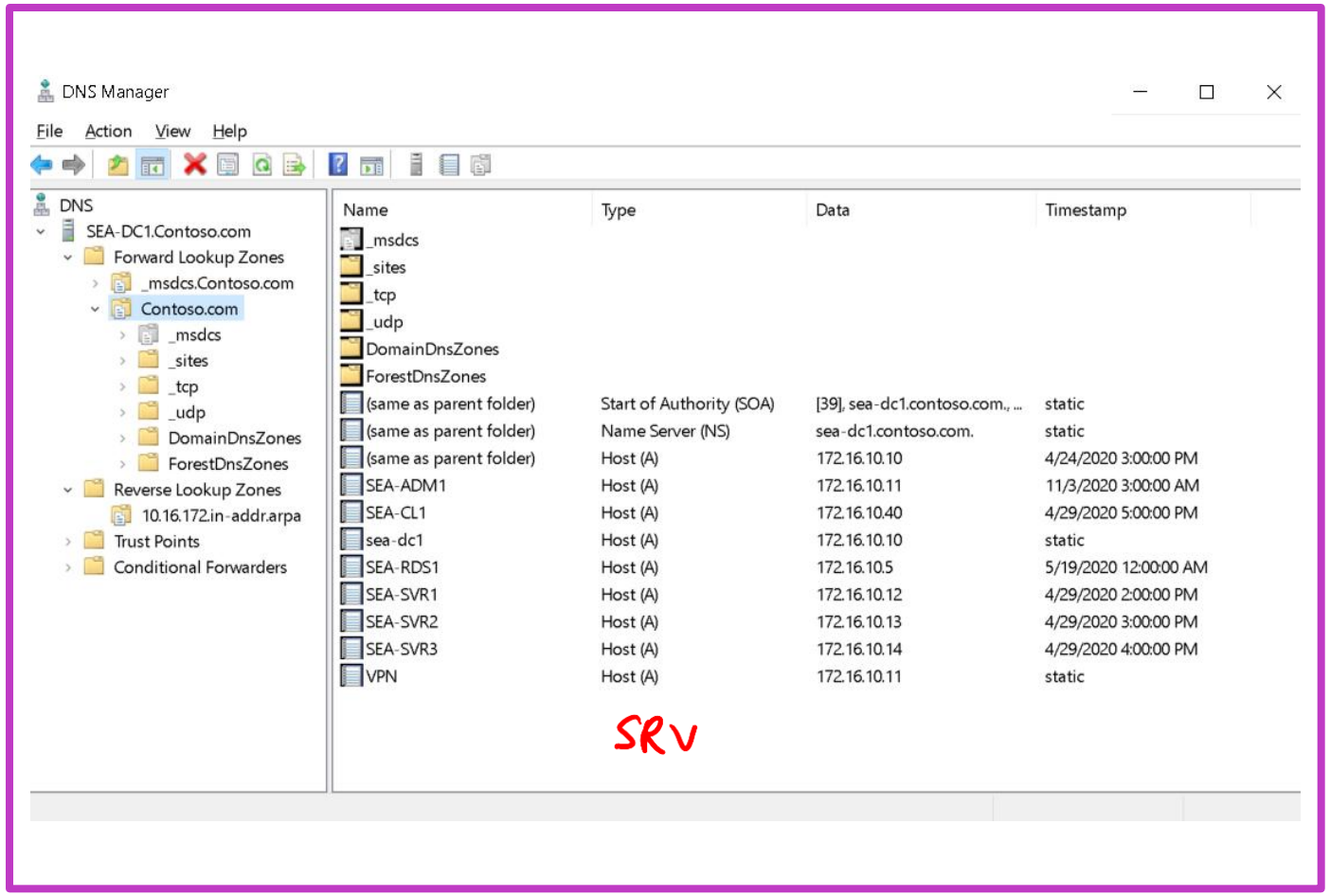
Computer names and hostnames

- A hostname is a user-friendly name that's associated with a host's IP address and identifies it as a TCP/IP host.
- A NetBIOS name is a nonhierarchical name that may be used by some legacy applications.



Work with DNS zones and records (1 of 2)

- A ***DNS zone*** is the specific portion of a DNS namespace (such as contoso.com) that's hosted on a DNS server.
- ***Forward lookup zones*** can hold a wide variety of different resource records, but the most common record type is a host (A) record.
- ***Reverse lookup zones*** are used only for resolving an IP address to a name.
- To create, edit, or delete resource records, you must use the primary zone.
- A secondary zone is a read-only copy of a primary zone.



Work with DNS zones and records (2 of 2)

All forward lookup and reverse lookup DNS zones contain the following records:

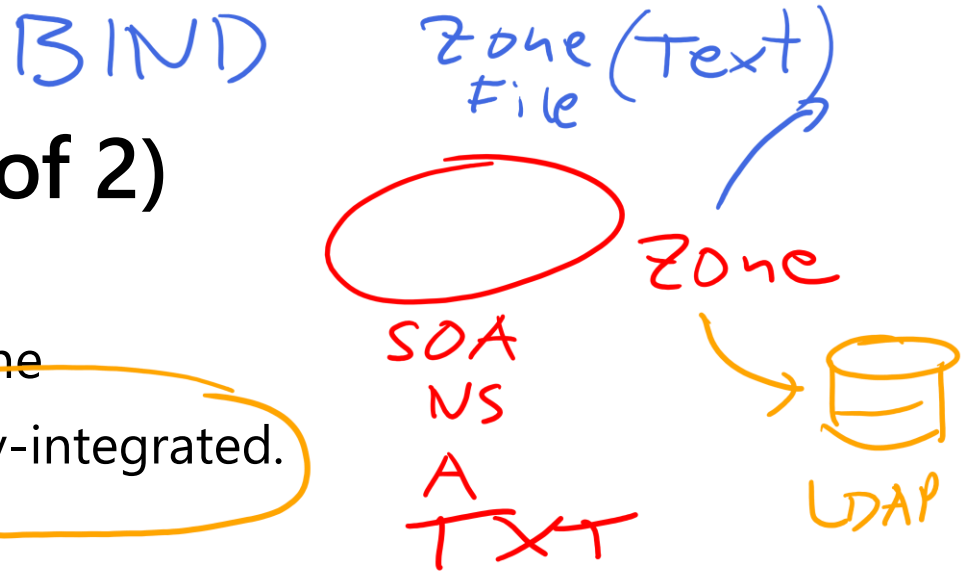
- Start of authority (SOA)
- Name server (NS)

A pointer record is used to resolve an IP address to a name

All resource records are configured with a time to live (TTL)

DNS record type	Description
Host (A)	Used to resolve a name to an IPv4 address.
Host (AAAA)	Used to resolve a name to an IPv6 address.
Alias (CNAME)	Used to resolve a name to another name.
Service location (SRV)	Used by applications to identify the location of servers hosting that application. For example, AD DS uses SRV records to identify the location of domain controllers and related services.
Mail exchanger (MX)	Used to identify email servers for a domain.
Text (TXT)	Used to store arbitrary strings of information in DNS.

Install and configure the DNS role (1 of 2)



- If you create a zone file, the zone is a standard primary zone
- If you store the zone in AD DS, the zone is Active Directory-integrated.
- A secondary zone is always stored in a zone file.
- If you configure a zone to be Active Directory-integrated, the zone data is stored in AD DS and replicated to domain controllers.
- If you choose to allow zone transfers, you can control them with the following options:
  - To any server
  - Only to servers listed on the Name Servers tab
  - Only to the following servers
- You can configure each DNS zone with security settings for dynamic updates.
- There are multiple Windows PowerShell cmdlets that can be used to manage DNS zones

Install and configure the DNS role (2 of 2)

Manual creation records in DNS:

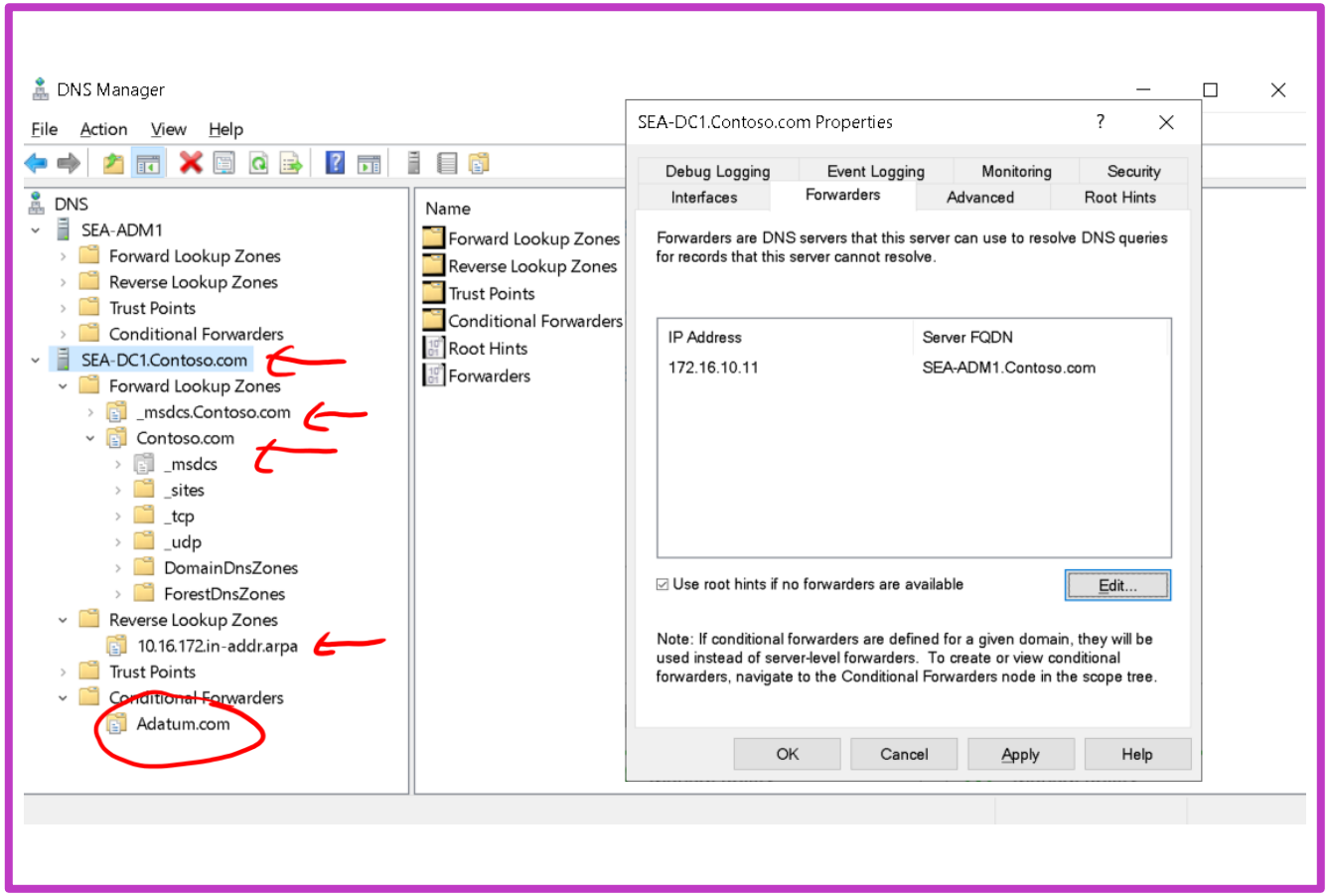
- You can create resource records by using DNS manager, Windows Admin Center, or Windows PowerShell
- The following list of Windows PowerShell cmdlets can be used to create DNS resource records.
  - Add-DnsServerResourceRecord
  - Add-DnsServerResourceRecordA
  - Add-DnsServerResourceRecordAAAA
  - Add-DnsServerResourceRecordCNAME
  - Add-DnsServerResourceRecordMX
  - Add-DnsServerResourceRecordPtr

Dynamic creation records in DNS

- The dynamic update creates host and pointer records for the client.
- Dynamic DNS makes it easier for you to manage DNS,
- When dynamic DNS is enabled, the current IP address for a computer registers automatically after an IP address change.

Implement DNS forwarding

- You can configure each DNS server with one or more forwarders.
- Forwarders are commonly used for internet name resolution.
- You can configure conditional forwarding for individual DNS domains.
- When you create a conditional forwarder, you can choose whether to store it locally on a single DNS server or in AD DS.
- Stub zones contain only Nameserver records and participate in zone transfers.
- Conditional forwarders perform recursion and don't participate in zone transfers.



Learning recap – Implement Windows Server DNS

Module assessment

Microsoft Learn Modules (docs.microsoft.com/Learn)

Implement Windows Server DNS

Implement IP Address Management

IPAM

Learning Objectives – Implement IP Address Management

- Define IP Address Management
- Deploy IP Address Management
- Administer IP Address Management
- Configure IP Address Management options
- Manage DNS zones with IP Address Management
- Manage DHCP servers with IP Address Management
- Use IP Address Management to manage IP addressing
- Learning recap

Define IP Address Management (1 of 3)

The benefits of using IPAM include:

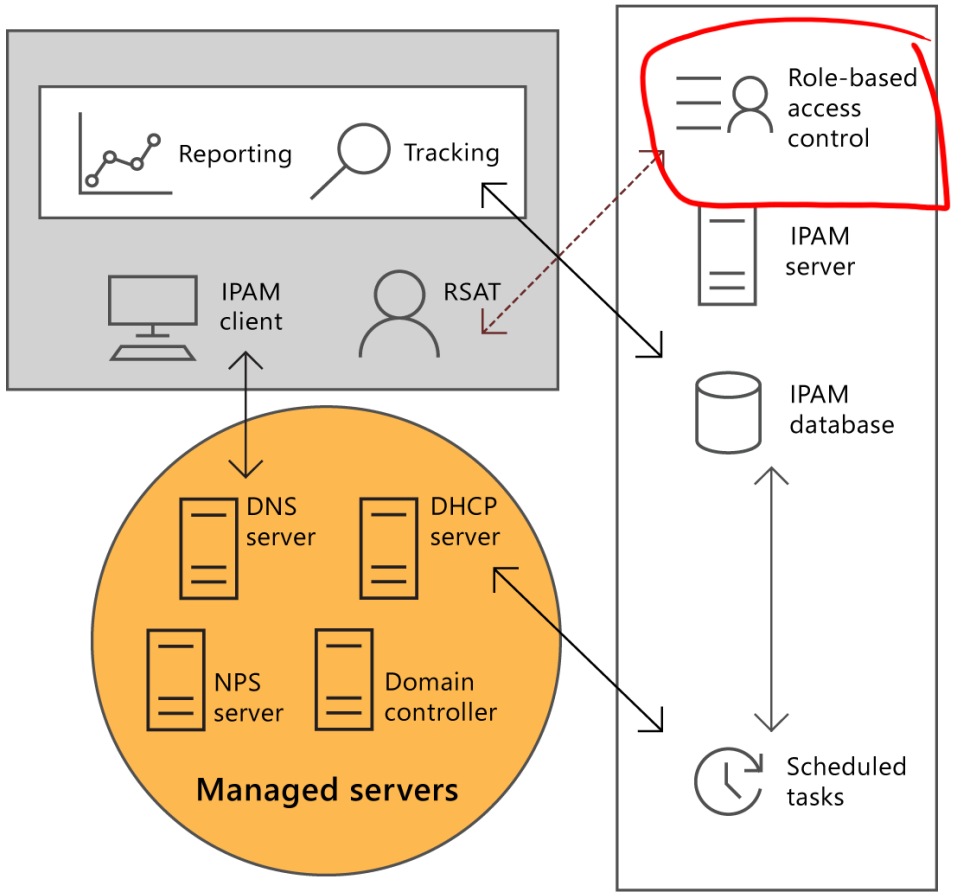
- IPv4 and IPv6 address space planning and allocation
- IP address space utilization statistics and trend monitoring
- Static IP inventory management, lifetime management, and DHCP and DNS record creation and deletion
- Service and zone monitoring of DNS servers
- IP address lease and sign-in event tracking

The Four Modules of IPAM

- IPAM discovery
- IP address space management
- Multiserver management and monitoring
- Operational auditing and IP address tracking

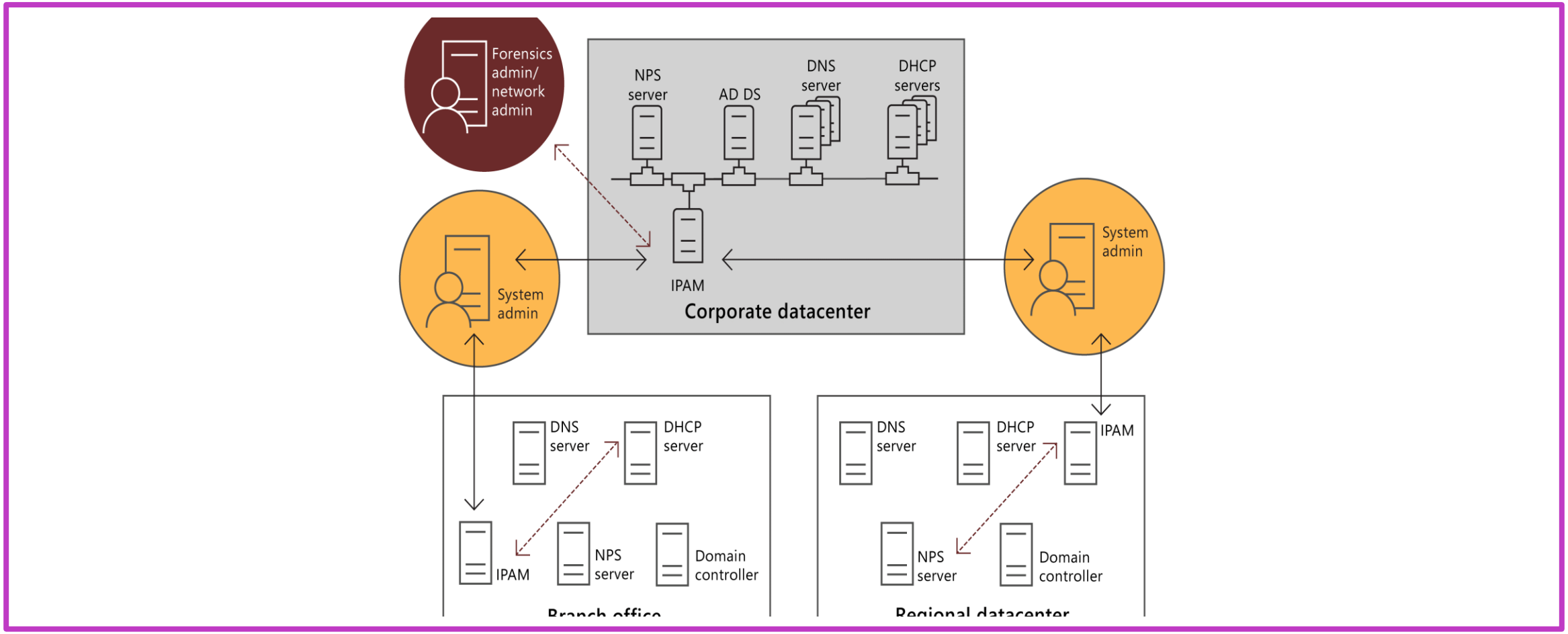
Define IP Address Management (2 of 3)

Centralized topology



Define IP Address Management (3 of 3)

Distributed topology



Deploy IP Address Management (1 of 2)

IPAM server requirements

- The IPAM server must be a member server in a domain.
- The IPAM server should be a single-purpose server
- The IPAM server needs access to the database.
- IPAM needs plenty of storage.

IPAM deployment considerations

- Sign in to the IPAM server with a domain account.
- You can define the scope of discovery to a subset of domains in the forest.
- A single IPAM server can support up to 150 DHCP servers, 6,000 DHCP scopes, 500 DNS servers, and 150 DNS zones.
- IP address utilization trends are provided only for IPv4.
- IP address reclamation support is provided only for IPv4.
- IPAM doesn't check for IP address consistency with routers and switches.

Deploy IP Address Management (2 of 2)

Deploy IPAM servers

1. Install the IPAM Server feature
2. Provision IPAM servers
3. Configure and run server discovery.
4. Choose and manage the discovered servers

Deploy IPAM clients

- If you install the IPAM role on a Windows server with the Desktop Experience, then the IPAM client is installed automatically on the IPAM server
- If you install the IPAM role on Server Core, then you need to manually install the IPAM client on another Windows Server used for management or a Windows client to manage IPAM remotely
- IPAM installation varies based on the operating system:
  - Windows Server
  - Windows 10

Administer IP Address Management (1 of 2)

Component	Description
Role	A role is a collection of IPAM operations. You can associate a role with a user or group in Windows by using an access policy. Nine built-in administrator roles are available for convenience, but you can also create custom roles to meet your business requirements. You can create and edit roles from the Access Control tab in the IPAM node in Server Manager.
Access scope	An access scope determines the objects to which a user has access. You can use access scopes to define administrative domains in IPAM console.
Access policy	An access policy combines a role with an access scope to assign permissions to a user or group.

To define and establish fine-grained control for users and groups, you can use RBAC to customize:

- Roles
- Access scopes
- Access policies

Administer IP Address Management (2 of 2)

IPAM security groups

Group name	Description
IPAM Administrators	Members of this group have privileges to access all IPAM data and to perform all IPAM tasks.
IPAM MSM Administrators	Members of this group can manage DHCP servers, scopes, policies, and DNS servers and associated zones and records.
IPAM DNS Administrators	Members of this group can manage DNS servers and their associated DNS zones and resource records.
DNS Record Administrators	Members of this group can manage DNS resource records.

Group name	Description
IPAM ASM Administrators	Members of this group can perform IP address space tasks, in addition to common IPAM management tasks.
IP Address Record Administrators	Members of this group can manage IP addresses, including unallocated addresses. Members can create and delete IP address instances.
IPAM DHCP Administrators	Members of this group can manage DHCP servers and their scopes.
IPAM DHCP Scope Administrators	Members of this group can manage DHCP scopes.
IPAM DHCP Reservations Administrators	Members of this group can manage DHCP reservations.

Configure IP Address Management options (1 of 2)

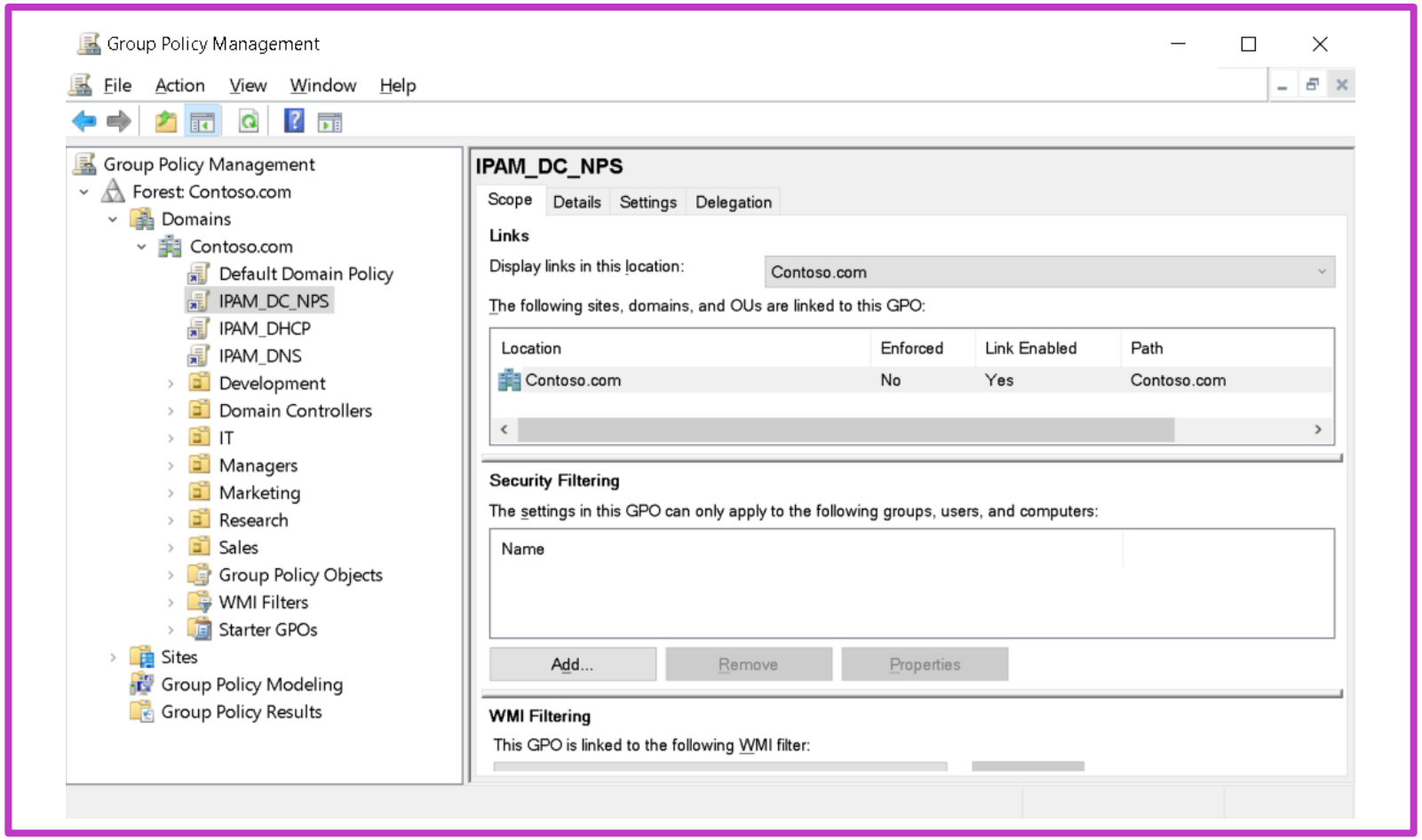
GPO provisioning – You need to create the GPOs in the following table.

GPO name	Description
<Prefix>_DHCP	This GPO applies settings that allow IPAM to monitor, manage, and collect information from managed DHCP servers on the network. It sets up IPAM provisioning scheduled tasks and adds Windows Defender Firewall inbound rules for Remote Event Log Management (RPC-EMAP and RPC), Remote Service Management (RPC-EMAP and RPC), and DHCP Server (RPCSS-In and RPC-In).
<Prefix>_DNS	This GPO applies settings that allow IPAM to monitor and collect information from managed DNS servers on the network. It sets up IPAM provisioning scheduled tasks and adds Windows Defender Firewall inbound rules for RPC (TCP, Incoming), RPC Endpoint Mapper (TCP, Incoming), Remote Event Log Management (RPC-EMAP and RPC), and Remote Service Management (RPC-EMAP and RPC).
<Prefix>_DC_NPS	This GPO applies settings that allow IPAM to collect information from managed domain controllers and NPS servers on the network for IP address tracking purposes. It sets up IPAM provisioning scheduled tasks and adds Windows Defender Firewall inbound rules for Remote Event Log Management (RPC-EMAP and RPC) and Remote Service Management (RPC-EMAP and RPC).

Configure IP Address Management options (2 of 2)

Create the required GPOs

- To create the GPOs required by IPAM, you can use the Invoke-IpamGpoProvisioning Windows PowerShell cmdlet.
- When you run the cmdlet without a server name, the computer account from the local computer is added as a member of the IPAMUG group in AD DS.
- You must add the computer account of the IPAM server to this group.

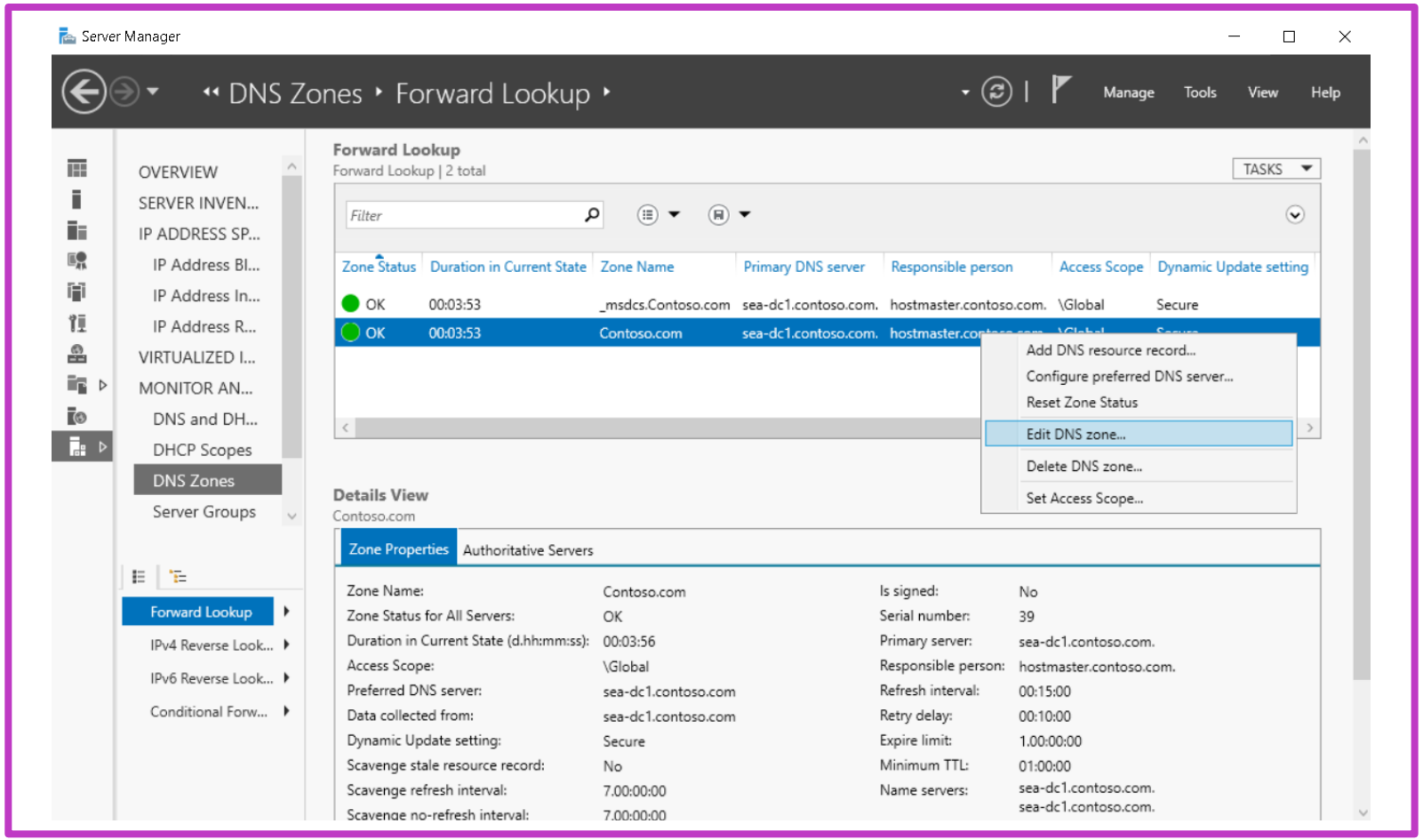


Manage DNS zones with IP Address Management

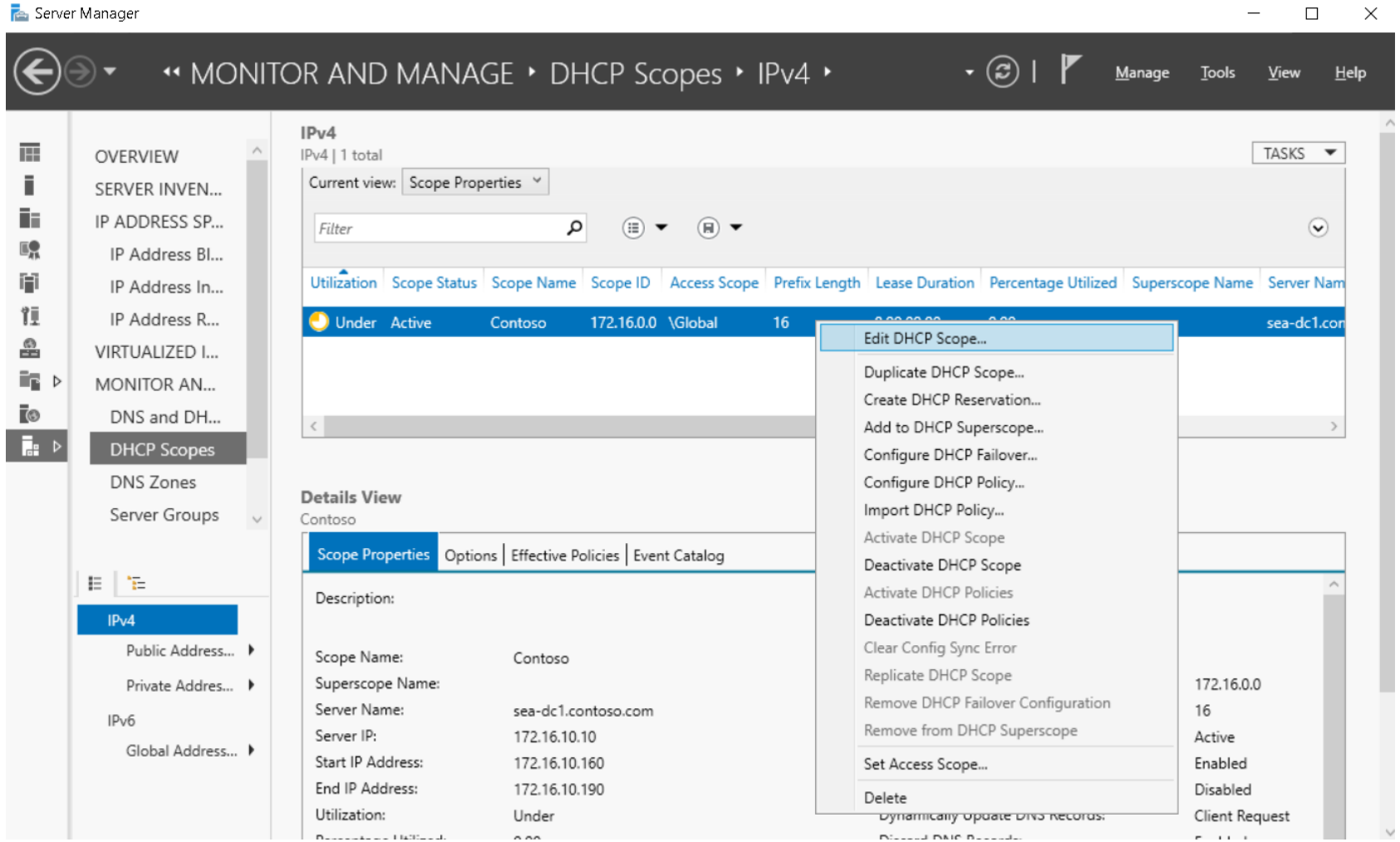
Perform DNS management

You can use IPAM to perform the following DNS management tasks:

- Examine DNS servers and zones
- Create new zones
- Create DNS records
- Manage conditional forwarders
- Open the DNS console for any server that IPAM manages



Manage DHCP servers with IP Address Management (1 of 3)



Manage DHCP servers with IP Address Management (2 of 3)

Configure DHCP servers

- Examine DHCP scope information across all servers.
- Edit DHCP server properties. You can edit server properties such as DHCP audit logging, DNS dynamic update configuration, and media access control (MAC) address filtering.
- Edit DHCP server options. You can configure and create DHCP server options based on vendor or user classes.
- Configure DHCP vendor or user classes. You can examine and modify user and vendor classes.
- Configure DHCP policy. You can edit DHCP policy properties and conditions.
- Import DHCP policy. You can import DHCP policies by using files that other DHCP servers export.
- Add DHCP MAC address filters. You can add DHCP MAC address filters to allow or deny DHCP address assignments based on MAC addresses.
- Activate and deactivate DHCP policies. You can control the implementation of DHCP policies.
- Replicate DHCP servers. This option replicates the configuration of failover scopes on a server to failover partner servers.
- Launch the DHCP console. You can open the DHCP console for the selected server.

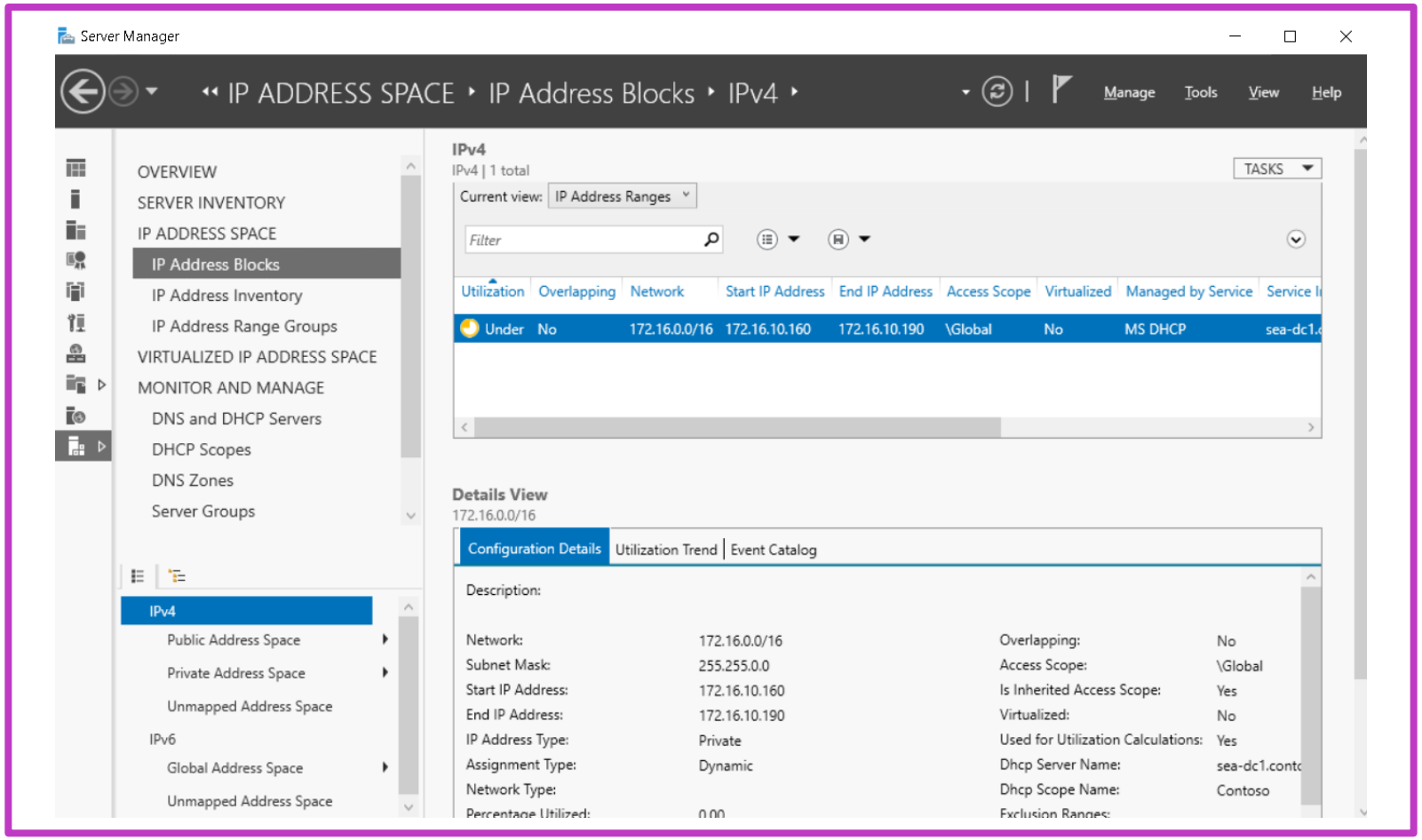
Manage DHCP servers with IP Address Management (3 of 3)

Configure DHCP scopes

- Edit the DHCP scope properties.
- Duplicate a DHCP scope. Use a DHCP scope as a template for creating a new scope on the same server or on a different server.
- Create a DHCP reservation.
- Add to a DHCP superscope.
- Configure a DHCP Failover.
- Import a DHCP policy.
- Activate and deactivate DHCP scopes.
- Activate and deactivate DHCP policies for the selected scope.
- Replicate a DHCP scope.
- Remove a DHCP Failover configuration.
- Remove a scope from a DHCP superscope.

Use IP Address Management to manage IP addressing (1 of 3)

- IPAM automatically discovers address spaces and utilization data from the DHCP servers that IPAM manages.
- IT can also import IP address information from CSV files.
- Administrators can use IPAM to detect overlapping IP address ranges that are defined on different DHCP servers.



Use IP Address Management to manage IP addressing (2 of 3)

You can customize the available components of the IP address space in the IPAM Administration Console by using any of the following views.

View	Description
IP address blocks	IP address blocks are the highest-level entities within an IP address space organization.
IP address ranges	IP address ranges are the next hierarchical level of IP address space entities after IP address blocks.
IP addresses	IP addresses are the addresses that make up the IP address range.
IP address inventory	The IP Address Inventory view lists of all IP addresses in the enterprise along with their device names and types.
IP address range groups	Using IPAM, you can organize IP address ranges into logical groups called IP address range groups.

Use IP Address Management to manage IP addressing (3 of 3)

In Server Manager, in the IPAM node, monitoring and management of DHCP and DNS servers is organized into the views listed in the following table.

View	Description
DNS and DHCP servers	By default, managed DHCP and DNS servers are arranged by their network interface in /32 subnets for IPv4 and /128 subnets for IPv6. You can select the view so that it displays only DHCP scope properties, only DNS server properties, or both.
DHCP scopes	This view enables scope utilization monitoring. Utilization statistics are automatically collected periodically from a managed DHCP server. You can track important scope properties such as Name, ID, Prefix Length, and Status
DNS zone monitoring	Zone monitoring can be enabled for forward lookup zones. Zone status is based on events that IPAM collects. The status of each zone is summarized.
Server groups	You can organize managed DHCP and DNS servers into logical groups.

Learning recap – Implement IP Address Management

Module assessment

Microsoft Learn Modules (docs.microsoft.com/Learn)

Implement IP Address Management

RRAS

NPS

RADIUS

Implement remote access

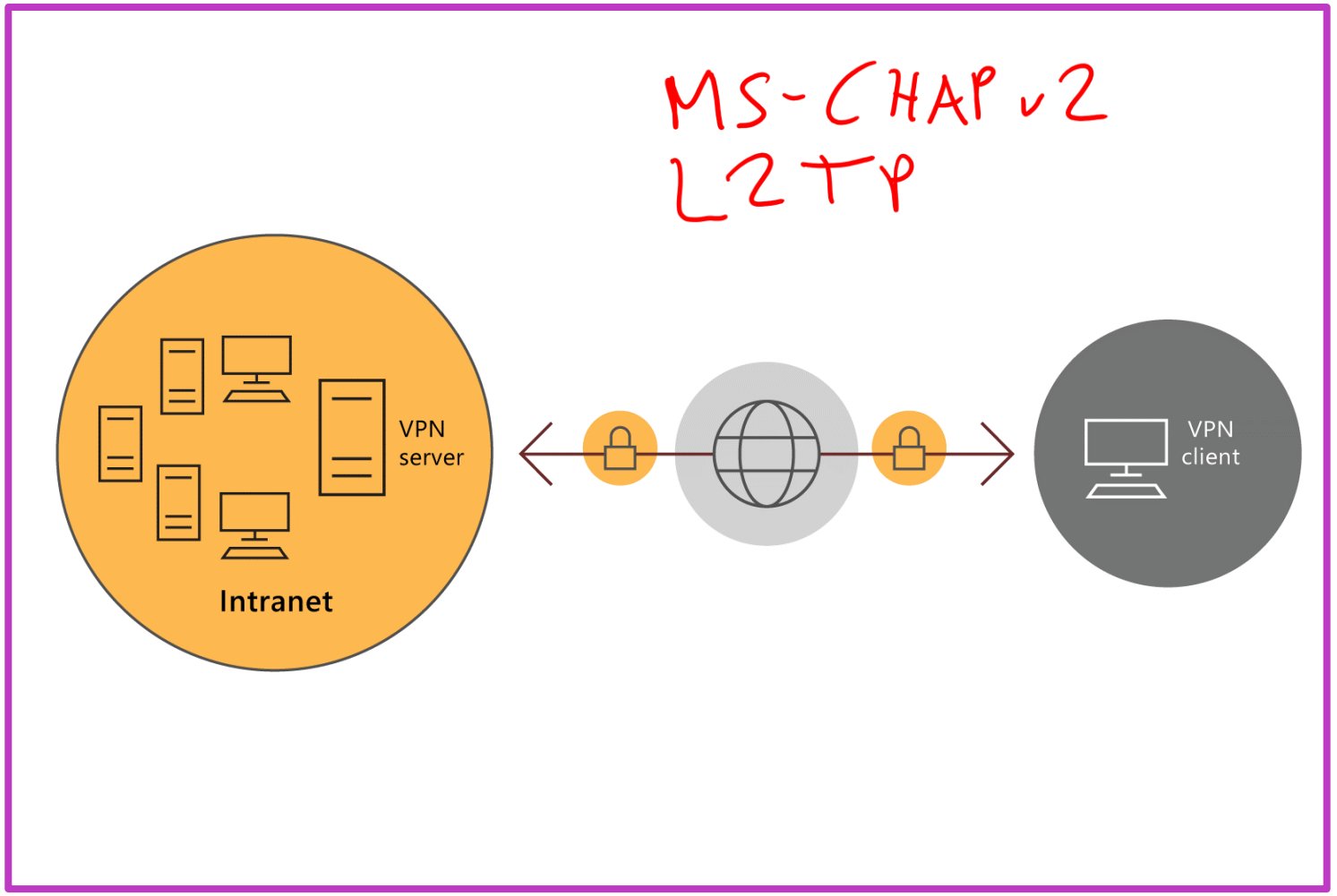
Learning Objectives – Implement remote management

- Examine the remote access options in Windows Server
- Select and set up VPNs
- Use NPS to create and enforce network access policies
- Plan and implement NPS
- Deploy a PKI for remote access
- Use Web Application Proxy as a reverse web proxy
- Learning recap

Examine the remote access options in Windows Server (1 of 3)

Supported remote access features

- VPN – VPN creates secure tunnel over the internet to access resources, data and applications from remote locations.
- Routing – Routing works with routing tables and supports routing protocols.
- Web Application Proxy – Web Application Proxy provides reverse proxy functionality for users who must access their organization's internal web applications from the internet.

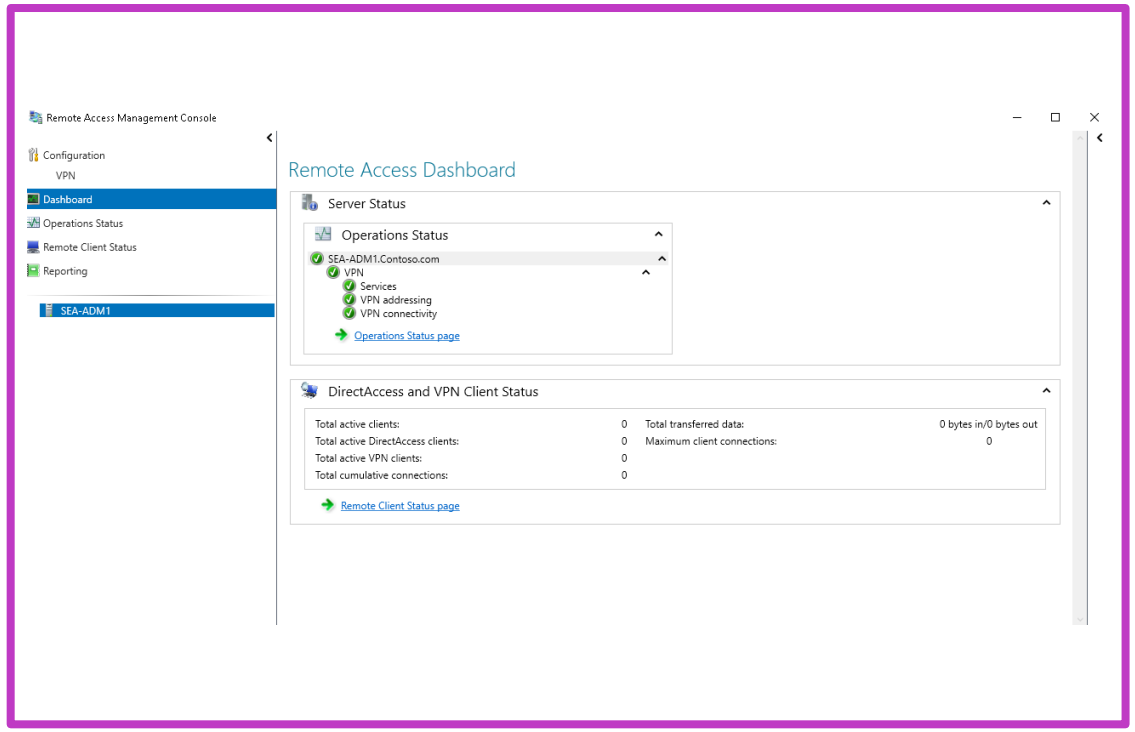


Examine the remote access options in Windows Server (2 of 3)

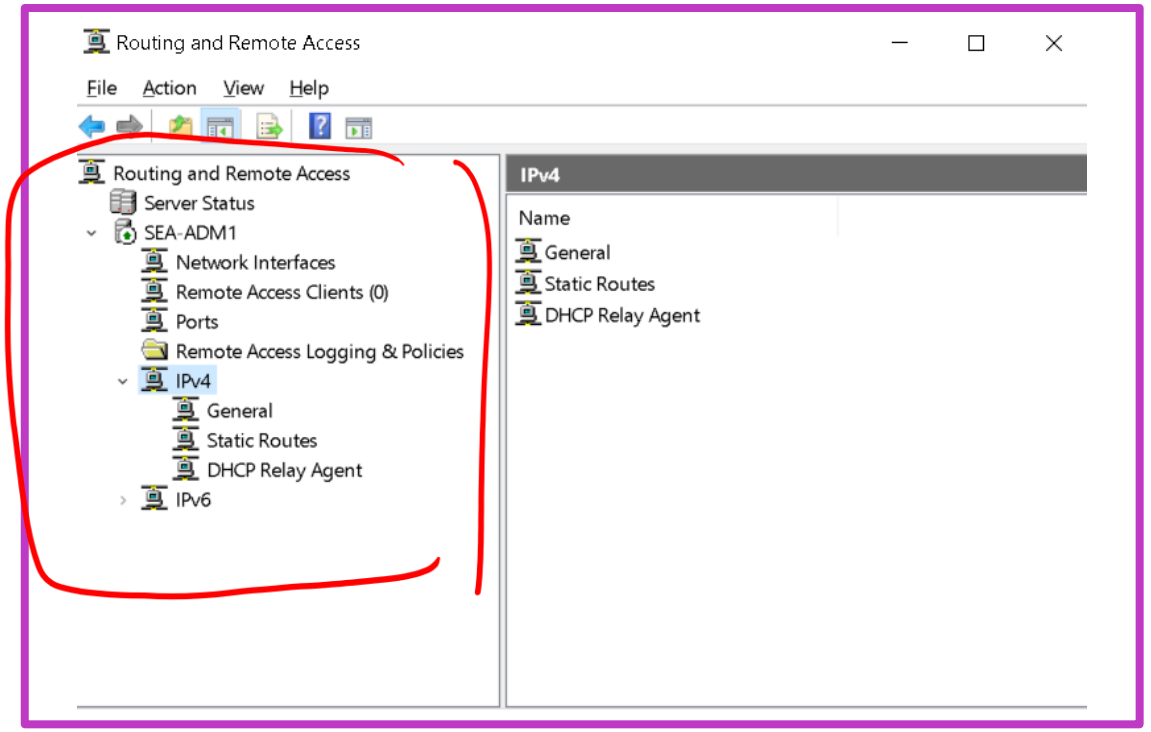
1. Remote access to data files
2. Remote access to desktop apps
3. Remote access to web-based apps

Examine the remote access options in Windows Server (3 of 3)

Remote Access Management console



Routing and Remote Access console



Select and set up VPNs

Select a tunneling protocol

VPN connections can use one of the following tunneling protocols:

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol with Internet Protocol Security (L2TP/IPsec)
- Secure Socket Tunneling Protocol (SSTP)
- Internet Key Exchange version 2 (IKEv2)

Select an authentication option

Method	Description
PAP	It uses plaintext passwords and is the least secure authentication protocol
CHAP	It is a challenge-response authentication protocol that uses the industry-standard MD5 hashing scheme to encrypt the response.
MS-CHAPv2	It is a challenge-response authentication protocol that uses the industry-standard MD5 hashing scheme to encrypt the response.
EAP	If you use Extensible Authentication Protocol (EAP), an arbitrary authentication mechanism authenticates a remote access connection.

Use NPS to create and enforce network access policies

Use NPS to implement network-access authentication, authorization, and accounting with any combination of the following functions:

- RADIUS server
  - NPS is the Microsoft implementation of a RADIUS server
  - NPS enables the use of a heterogeneous set of wireless, switch, remote access, or VPN equipment
- RADIUS proxy
  - When using NPS as a RADIUS proxy, you configure connection request policies that indicate which connection requests the NPS server will forward to other RADIUS servers and to which RADIUS servers you want to forward connection requests.
- RADIUS accounting
  - You can configure NPS to perform RADIUS accounting for user authentication requests, Access-Accept messages, Access-Reject messages, accounting requests and responses, and periodic status updates.

Plan and implement NPS (1 of 2)

Choose an NPS authentication method

- PAP
- Shiva Password Authentication Protocol (SPAP)
- CHAP
- MS-CHAP
- MS-CHAP v2
- EAP

NPS accounting

- You can log user authentication requests and accounting requests to log files in text format or database format
- You can log to a stored procedure in a Microsoft SQL Server database.

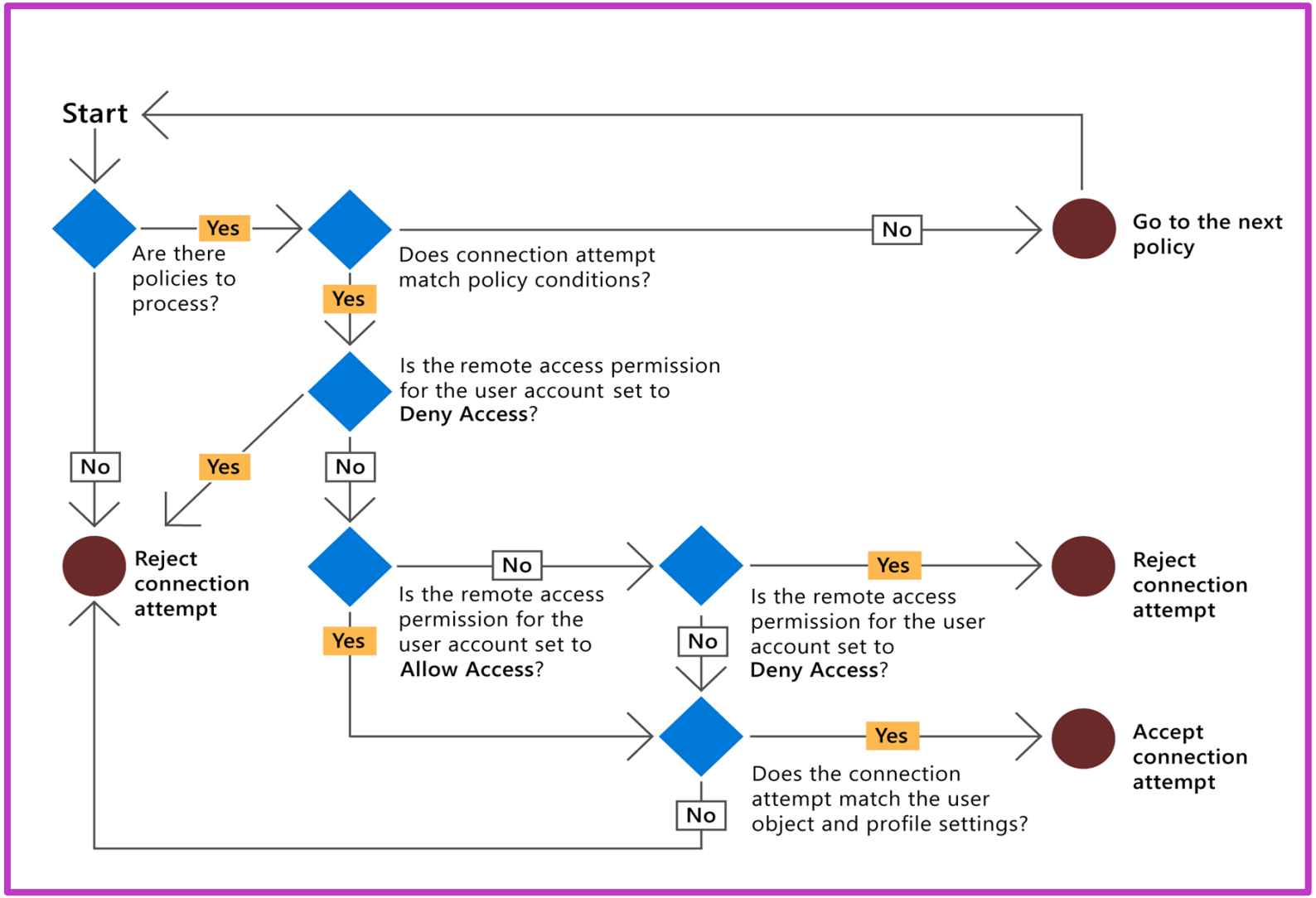
Plan and implement NPS (2 of 2)

NPS supports:

- Connection request policies
- Network policies

Each network policy has four categories of properties:

- Overview
- Conditions
- Constraints
- Settings



Deploy a PKI for remote access

Methods for obtaining certificates

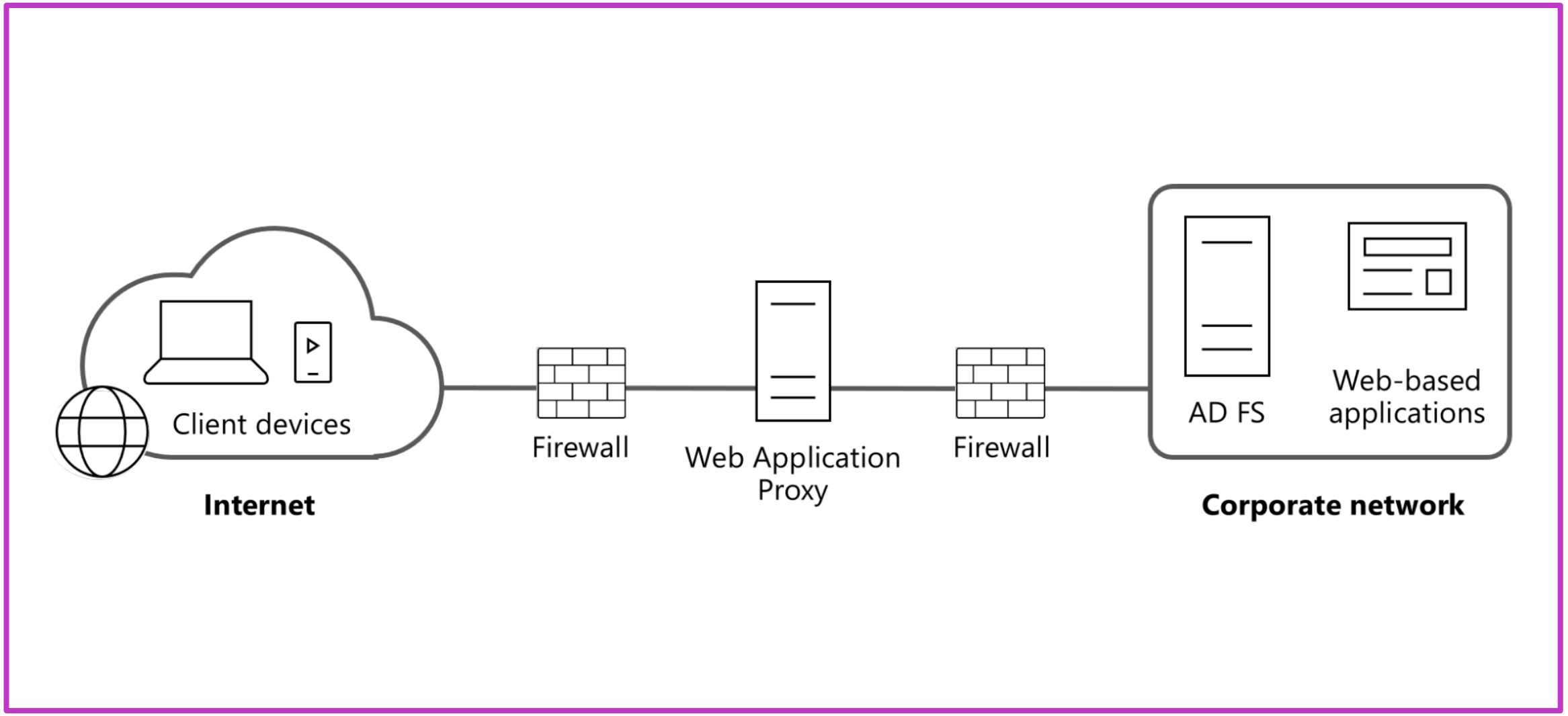
To obtain certificates, you can:

- Create your own private CA by using Windows Server.
- Purchase certificates from a public CA
- Purchase certificates from a public CA
- Generate self-signed certificates by using PowerShell

Advantages and disadvantages of certificates issued by private and public CAs

CA type	Advantages	Disadvantages
Private CA	A private CA provides greater control over certificate management and has a lower cost when compared to a public CA. There is no cost per certificate. You also have the option to use customized templates and automatic enrollment.	By default, certificates by private CAs aren't trusted by external clients (web browsers and operating systems) and require greater administration.
Public CA	A certificate issued by a public CA is trusted by many external clients (web browsers and operating systems) and requires minimal administration.	The cost is higher when compared to a private CA. Cost is based per certificate. Certificate procurement is also slower.

Use WAP as a reverse web proxy (1 of 3)



Use WAP as a reverse web proxy (2 of 3)

1. **AD FS preauthentication** – Only authorized users can send data packets to the web application. AD FS preauthentication significantly reduces the attack surface for a web app.

2. **Pass-through preauthentication** – The user is connected to the web application through Web Application Proxy. The web application proxy rebuilds the data packets as they are delivered to the web app. The web app is responsible for authenticating users.

3. **AD FS preauthentication benefits**

   AD FS preauthentication provides the following benefits over pass-through preauthentication:

   - SSO
   - Multifactor authentication (MFA)
   - Multifactor access control

Use WAP as a reverse web proxy (3 of 3)

You can publish your web app by using Web Application Proxy console or Windows PowerShell cmdlets.

The Windows PowerShell cmdlets for managing published apps are:

- `Add-WebApplicationProxyApplication`
- `Get-WebApplicationProxyApplication`
- `Set-WebApplicationProxyApplication`

When you publish your web app, you must provide the following information:

- The type of preauthentication, for example, pass-through.
- The application to publish.
- The external URL of the application, for example, https://lon-svr1.adatum.com.
- A certificate whose subject name covers the external URL, for example, lon-svr1.adatum.com.
- The URL of the backend server, which is entered automatically when you enter the external URL.

Learning recap – Implement remote access

Microsoft Learn Modules (docs.microsoft.com/Learn)

Implement remote access

Module assessment

Lab 07 – Implementing and configuring network infrastructure services in Windows Server

Lab 07: Implementing and configuring network infrastructure services in Windows Server

Lab scenario

Contoso, Ltd. is a large organization with complex requirements for network services. To help meet these requirements, you will deploy and configure DHCP so that it is highly available to ensure service availability. You will also set up DNS so that Trey Research, a department within Contoso, can have its own DNS server in the testing area. Finally, you will provide remote access to Windows Admin Center and secure it with Web Application Proxy

Objectives

- Deploy and configure DHCP
- Deploy and configure DNS

End of presentation