WILEY

SYBEX
A Wiley Brand

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

Chapter 6: Configuring DHCP and IPAM

Understanding DHCP

- Dynamic Host Configuration Protocol (DHCP)
- A protocol that allows users to get required information so that they can properly communicate on the network.
- DHCP's job is to centralize the process of IP address and option assignment. Can configure a DHCP server with a range of addresses (called a pool) and other configuration information and let it assign all of the IP parameters—addresses, default gateways, DNS server addresses, and so on.

DHCP

- DORA Process
  - Discover
  - Offer
  - Request
  - Acknowledge

Advantages of DHCP

- Configuration of large and even midsized networks is much simpler.
- Once you enter the IP configuration information in one place—the server.
- IP addresses are conserved because DHCP assigns them only when requested.
- IP configuration becomes almost completely automatic.
- It allows a preboot execution environment (PXE) client to get a TCP/IP address.

Disadvantages of DHCP

- DHCP can become a single point of failure for your network.
- If the DHCP server contains incorrect information, the misinformation will automatically be delivered to all of your DHCP clients.
- If you want to use DHCP on a multisegment network, you must put either a DHCP server or a relay agent on each segment, or you must ensure that your router can forward Bootstrap Protocol (BOOTP) broadcasts.

Ipconfig Lease Options

- ipconfig /renew
- ipconfig /release
- ipconfig /setclassidclassID

DHCP Scope

- Contiguous range of addresses.
- Usually one scope per physical subnet, and a scope can cover a Class A, Class B, or Class C network address or a TCP/IP v6 address.
- DHCP uses scopes as the basis for managing and assigning IP addressing information.

DHCP Superscope

- A superscope enables the DHCP server to provide addresses from more than one scope to clients on the same physical subnet.
- Helpful when clients within the same subnet have more than one IP network and need IPs from more than one address pool.
- Microsoft's DHCP snap-in allows you to manage IP address assignment in the superscope, though you must still configure other scope options individually for each child scope.

SYBEX

Exclusions

- Exclusions are IP addresses within the range that you never want automatically assigned.
- These excluded addresses are off-limits to DHCP.
- Typically use exclusions to tag any addresses that you never want the DHCP server to assign at all.
- Might use exclusions to set aside addresses that you want to permanently assign to servers that play a vital role in your organization.

Reservations

- Reservations are IP addresses within the range for which you want a permanent DHCP lease.
- Reserve a particular IP address for a particular device.
- The device still goes through the DHCP process (that is, its lease expires, and it asks for a new one), but it always obtains the same addressing information from the DHCP server.

DHCP Address Pool

- The range of IP addresses that the DHCP server can assign is called its address pool.

- Example, you set up a new DHCP scope covering the 192.168.1 subnet. This gives you 255 IP addresses in the pool. After adding an exclusion from 192.168.1.240 to 192.168.1.254, will be left with 241 (255 – 14) IP addresses in the pool.

DHCP Relay Agent

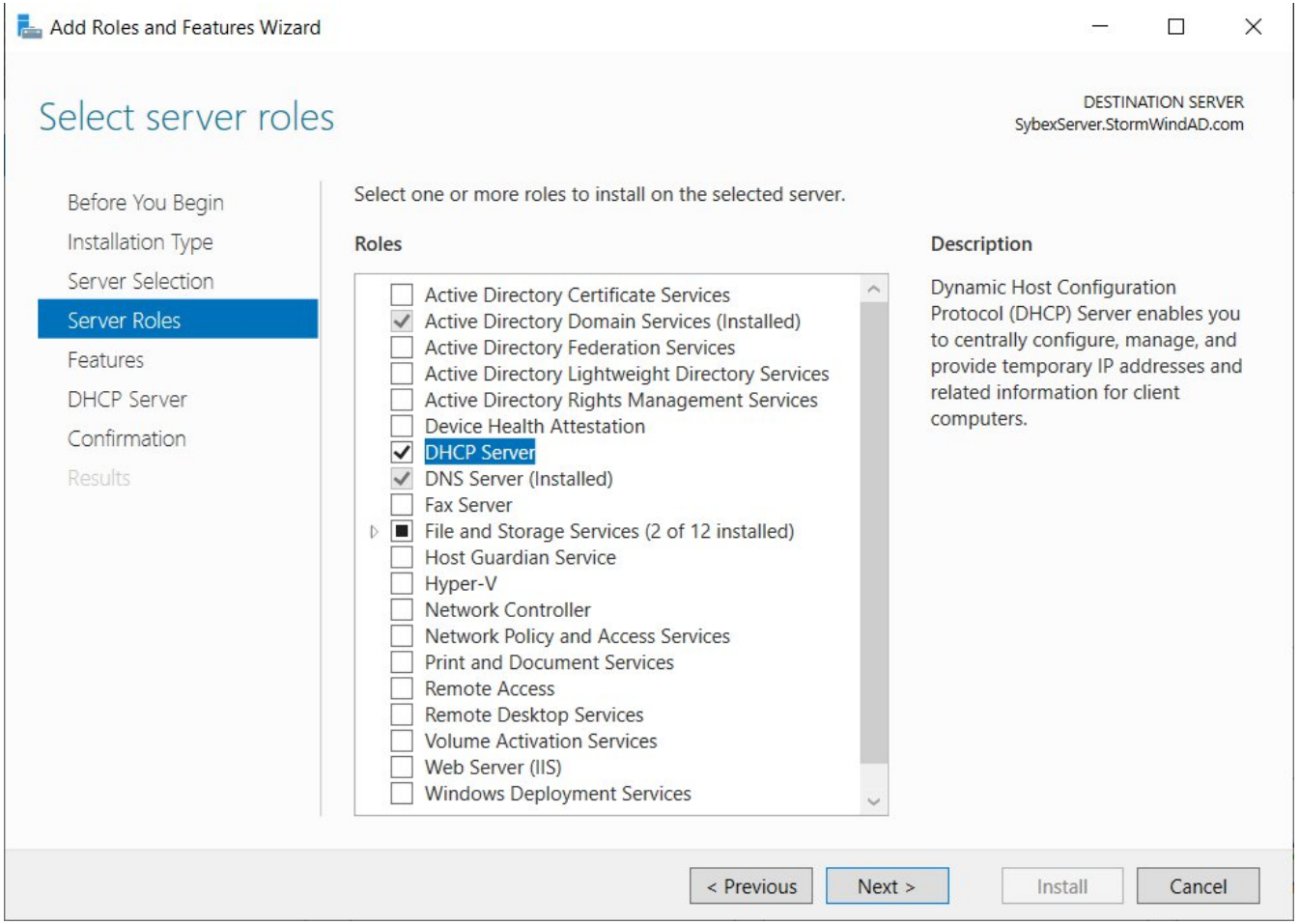
- By design, the DHCP protocol is intended to work only with clients and servers on a single IP network to communicate.

- If no DHCP server is available on the client's network can use a DHCP relay agent to forward DHCP broadcasts from the client's network to the DHCP server.

- The relay agent acts like a radio repeater, listening for DHCP client requests and retransmitting them through the router to the server.

SYBEX
A Wiley Brand

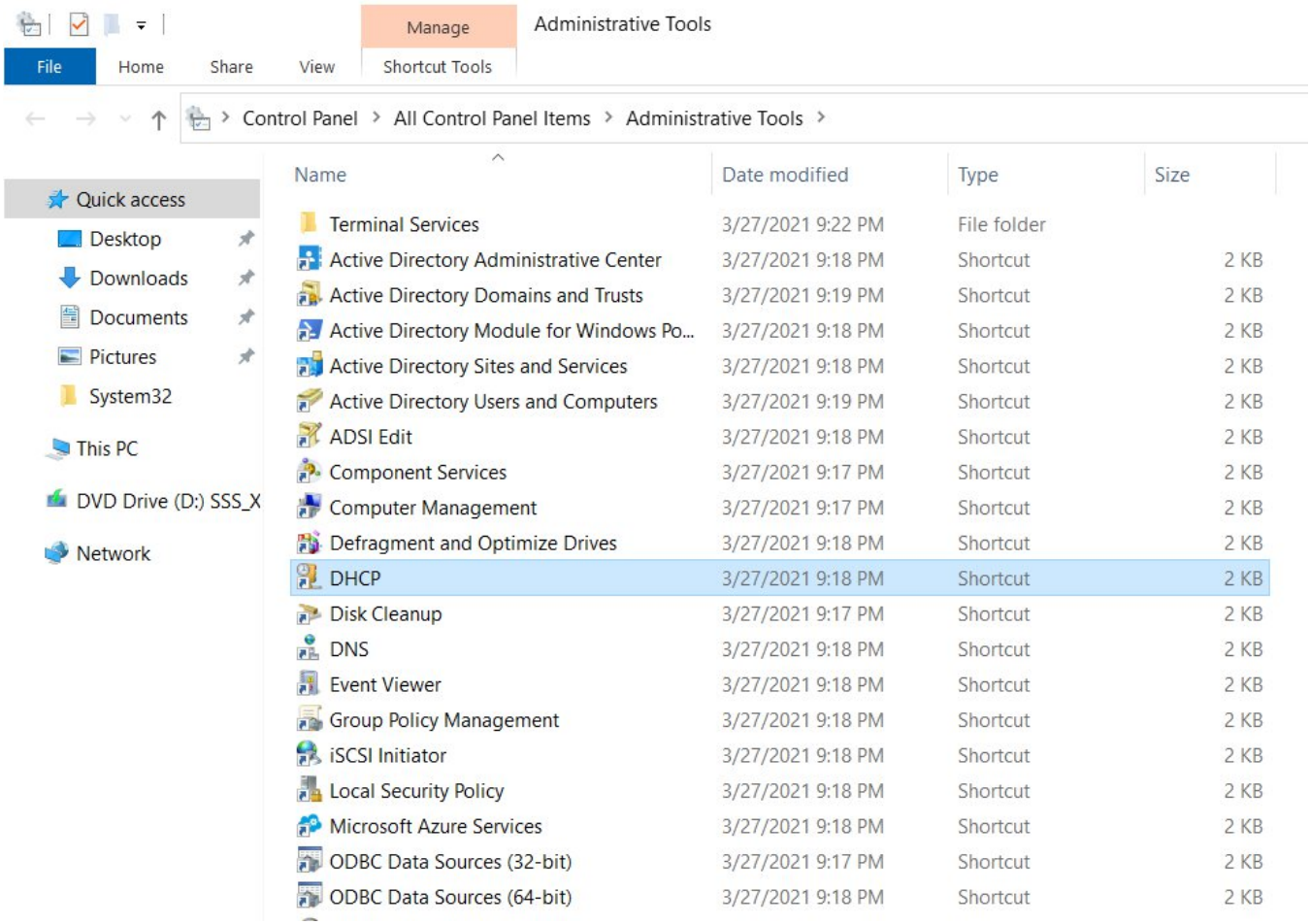
Installing the DHCP Service



WILEY

SYBEX
A Wiley Brand

DHCP Snap-In



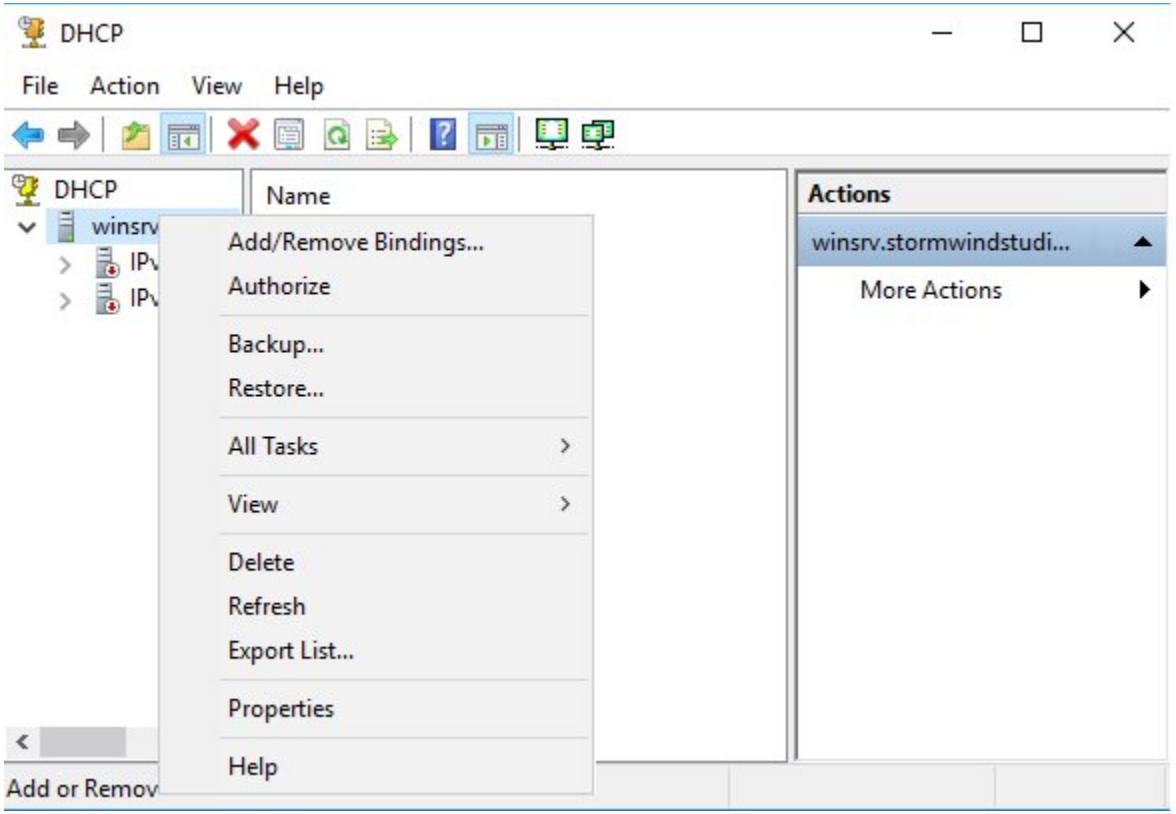
WILEY

Authorizing DHCP

- Authorization creates an Active Directory object representing the new server.
- It helps keep unauthorized servers off your network.
- Unauthorized servers can cause two kinds of problems.

SYBEX
A Wiley Brand

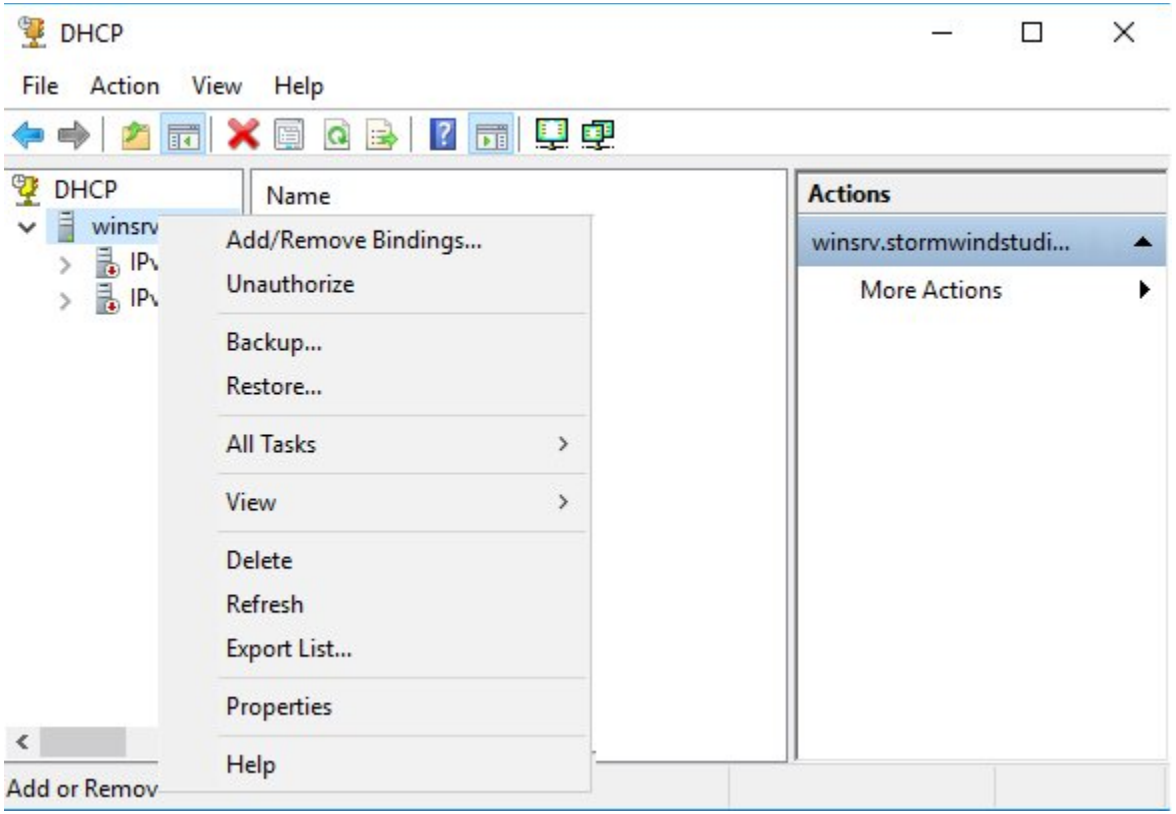
Authorizing a DHCP Server – Choosing Authorize



WILEY

SYBEX
A Wiley Brand

Authorizing a DHCP Server – Choosing Unauthorize



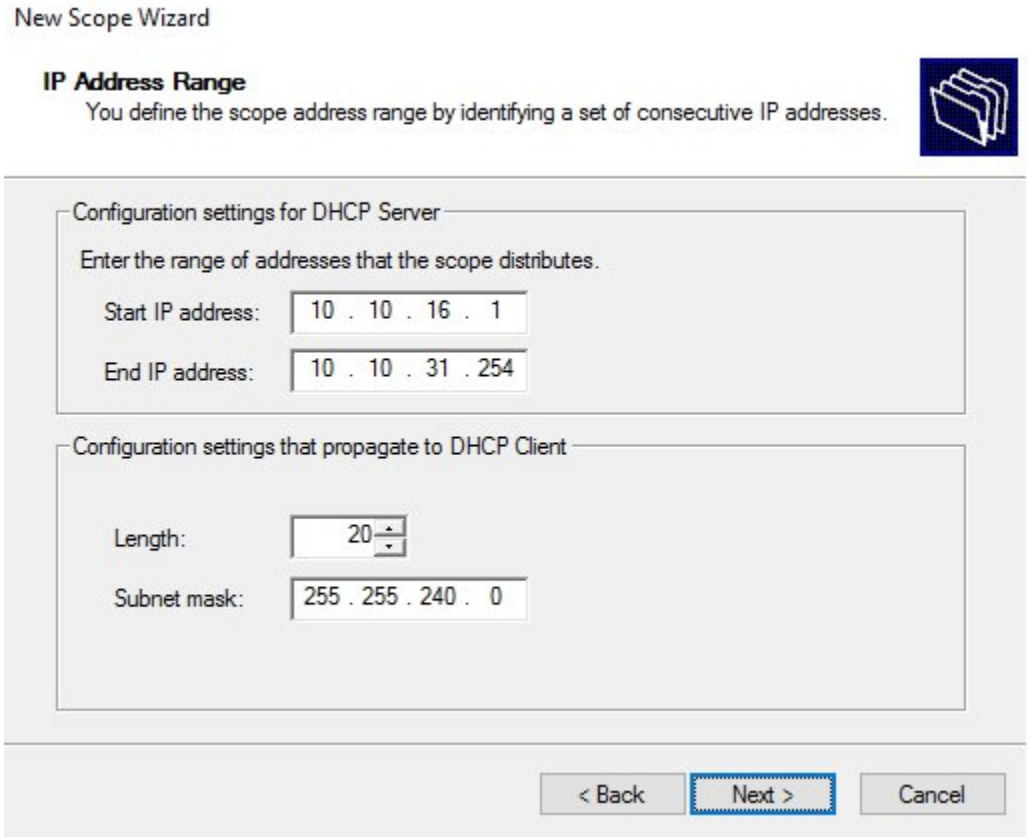
WILEY

Create and Manage DHCP Scopes

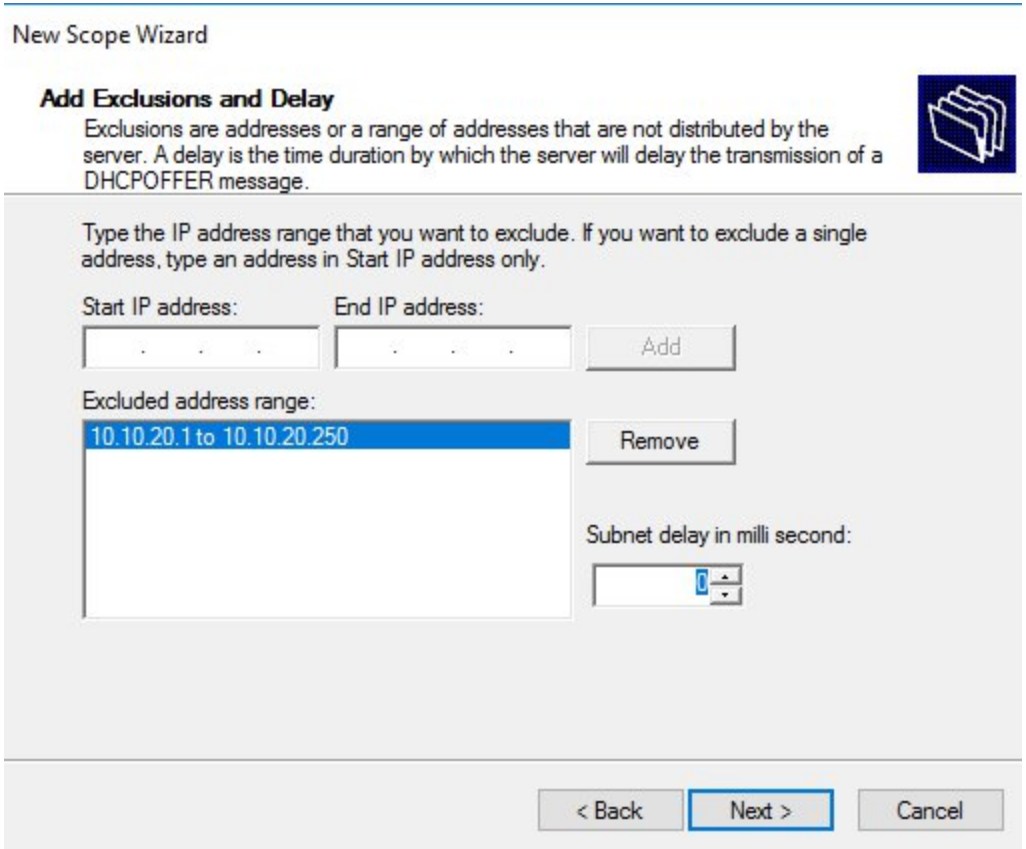
Can perform the following management tasks on DHCP scopes:

- Create a scope
- Configure scope properties
- Configure reservations and exclusions
- Set scope options
- Activate and deactivate scopes
- Create a superscope
- Create a multicast scope
- Integrate Dynamic DNS and DHCP

Creating Scopes
Scope Range and Subnet in IPv4

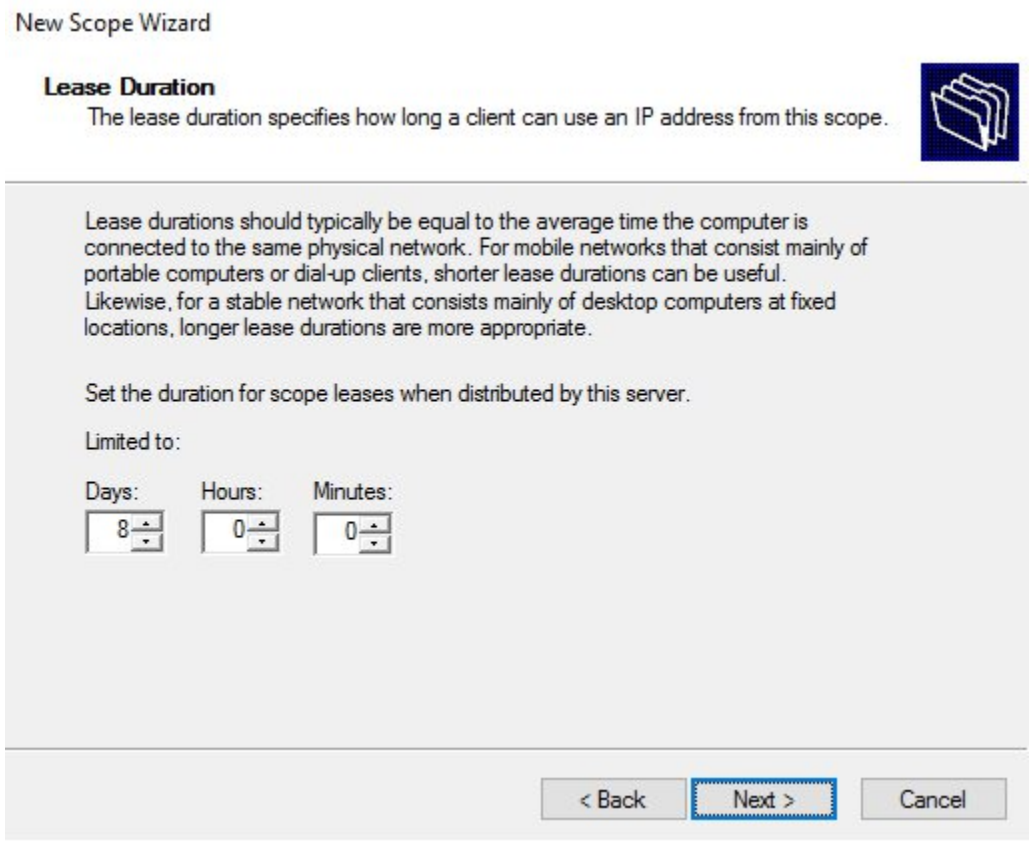


Creating Scopes Exclusions and Delay



SYBEX
A Wiley Brand

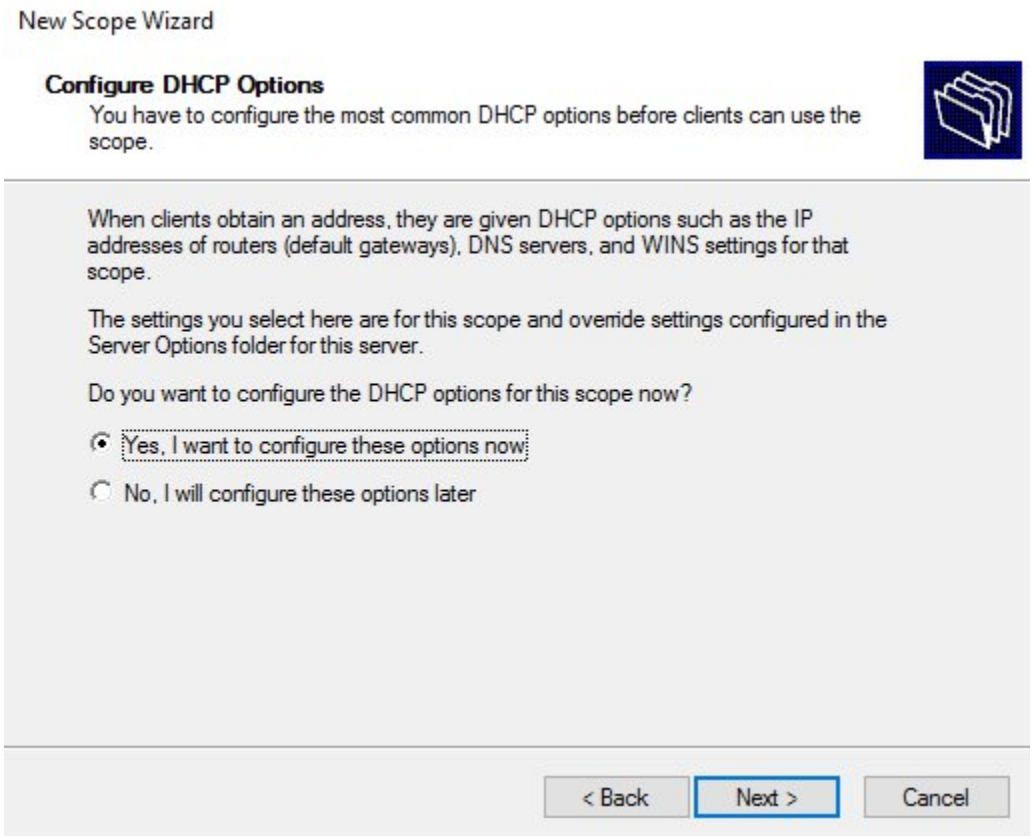
Setting a Lease Duration



WILEY

SYBEX
A Wiley Brand

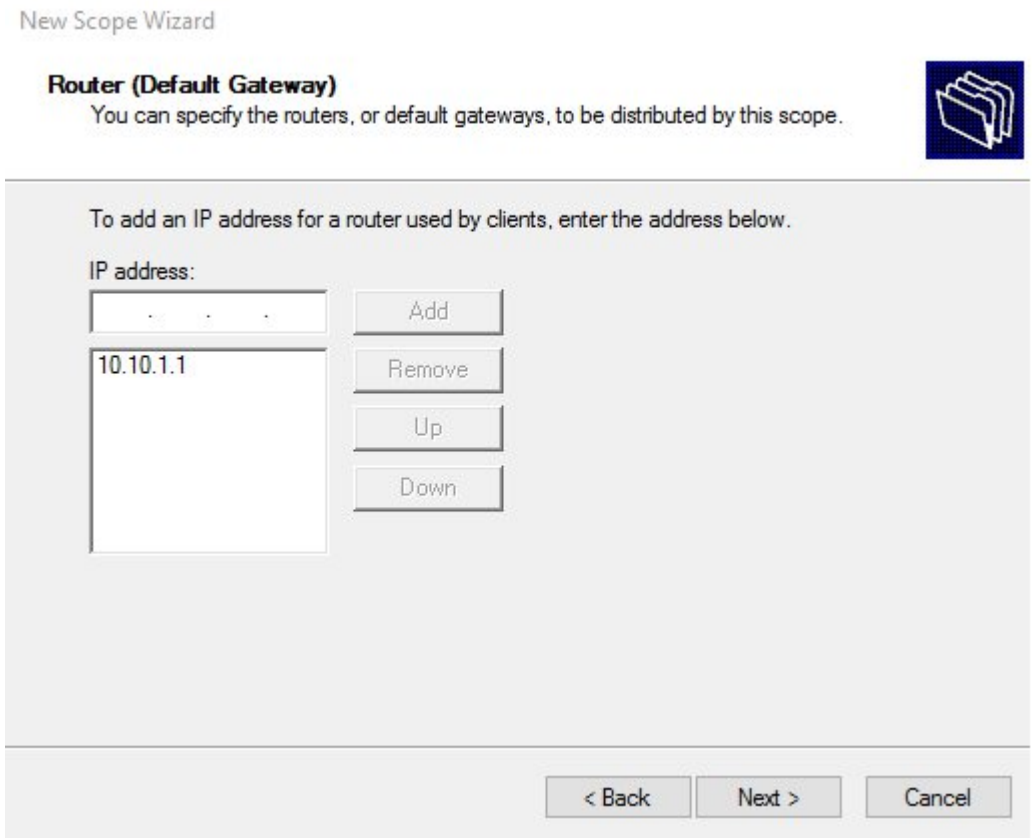
Configure Basic DHCP Options – Options Page



WILEY

SYBEX
A Wiley Brand

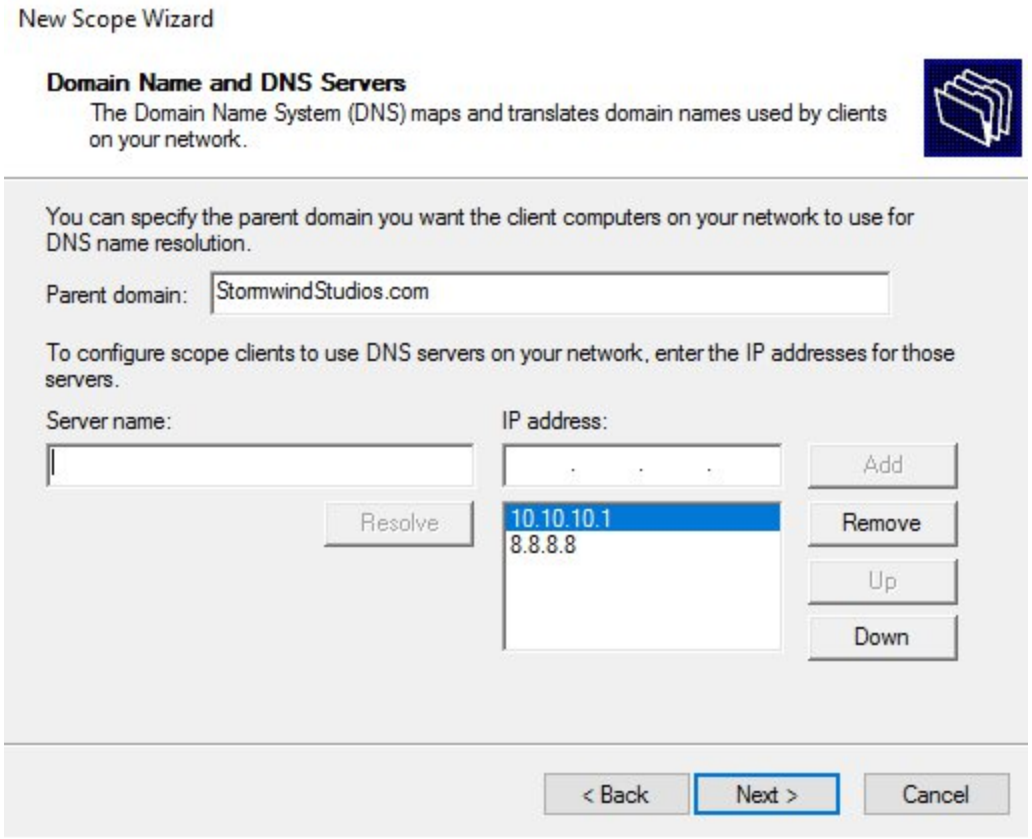
Configure Basic DHCP Options – Router (Default Gateway)



WILEY

SYBEX
A Wiley Brand

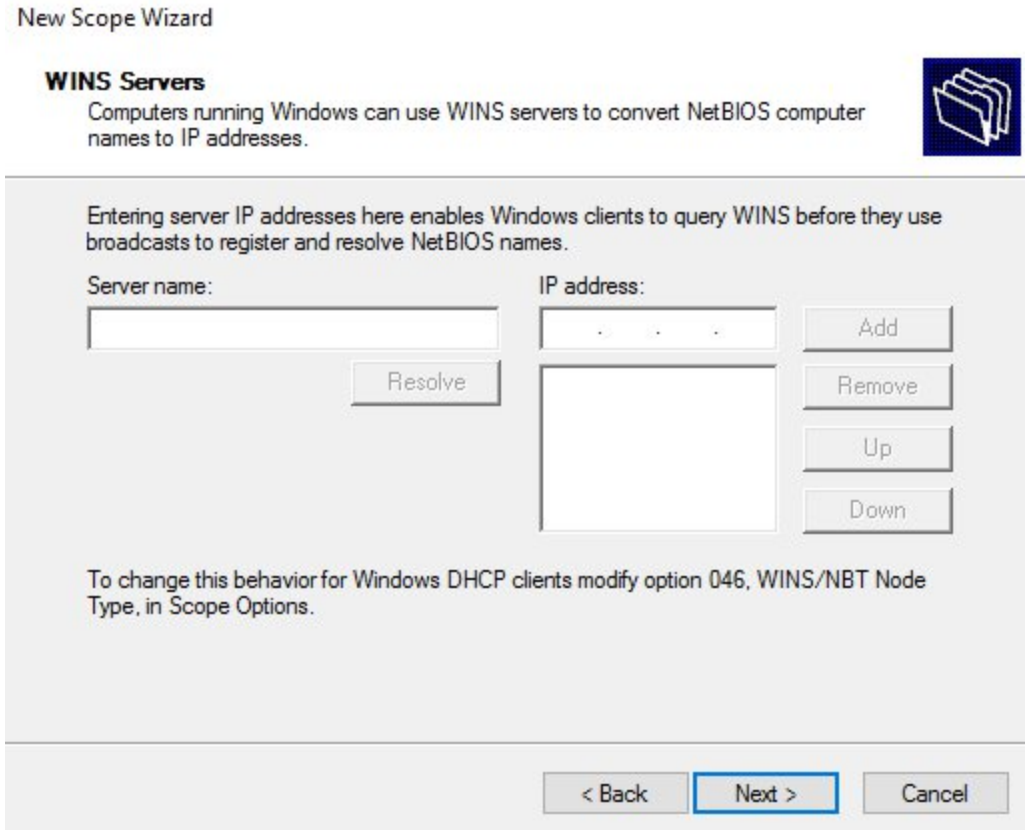
Configure Basic DHCP Options – Domain Name and DNS Servers



WILEY

SYBEX
A Wiley Brand

Configure Basic DHCP Options – WINS Server



WILEY

Creating Scopes
Common Scope Options

003 Router Used to provide a list of available routers or default gateways on the same subnet.

006 DNS Servers Used to provide a list of DNS servers.

015 DNS Domain Name Used to provide the DNS suffix.

028 Broadcast Address Used to configure the broadcast address, if different than the default, based on the subnet mask.

44 WINS/NBNS Servers Used to configure the IP addresses of WINS servers.

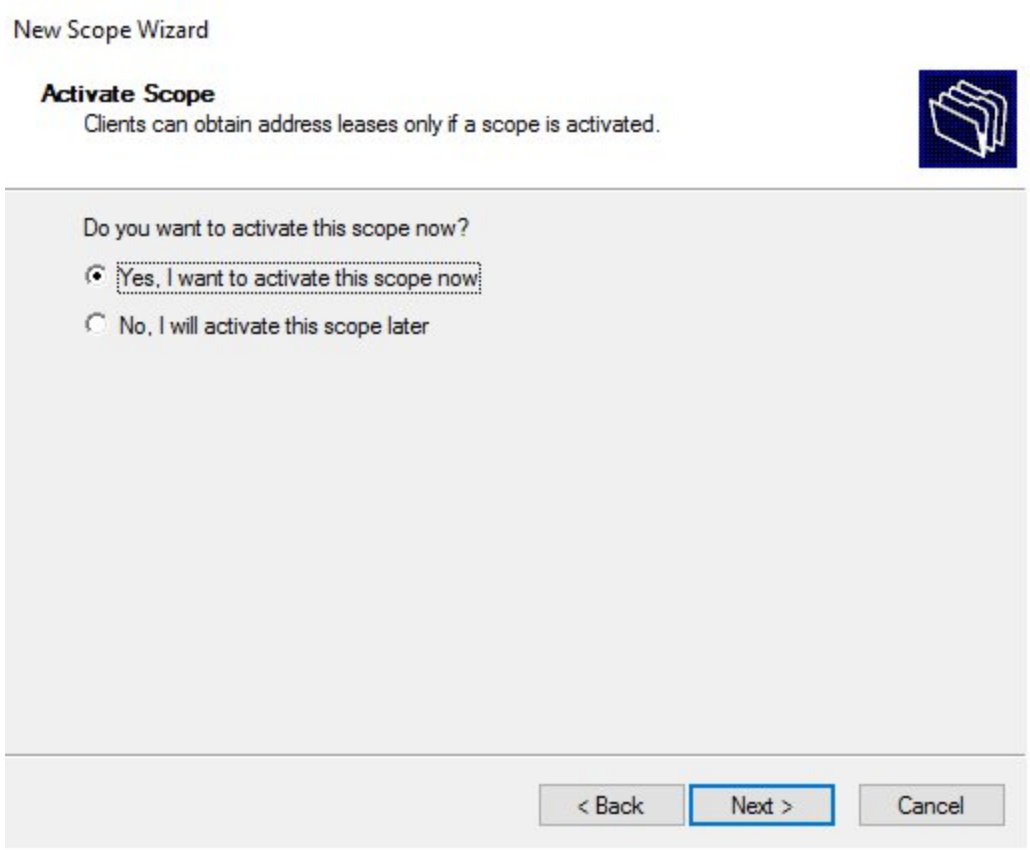
46 WINS/NBT Node Type Used to configure the preferred NetBIOS name resolution method. There are four settings for node type:

- **B node (0x1)** Broadcast for NetBIOS resolution
- **P node (0x2)** Peer-to-peer (WINS) server for NetBIOS resolution
- **M node (0x4)** Mixed node (does a B node and then a P node)
- **H node (0x8)** Hybrid node (does a P node and then a B node)

051 Lease Used to configure a special lease duration.

SYBEX
A Wiley Brand

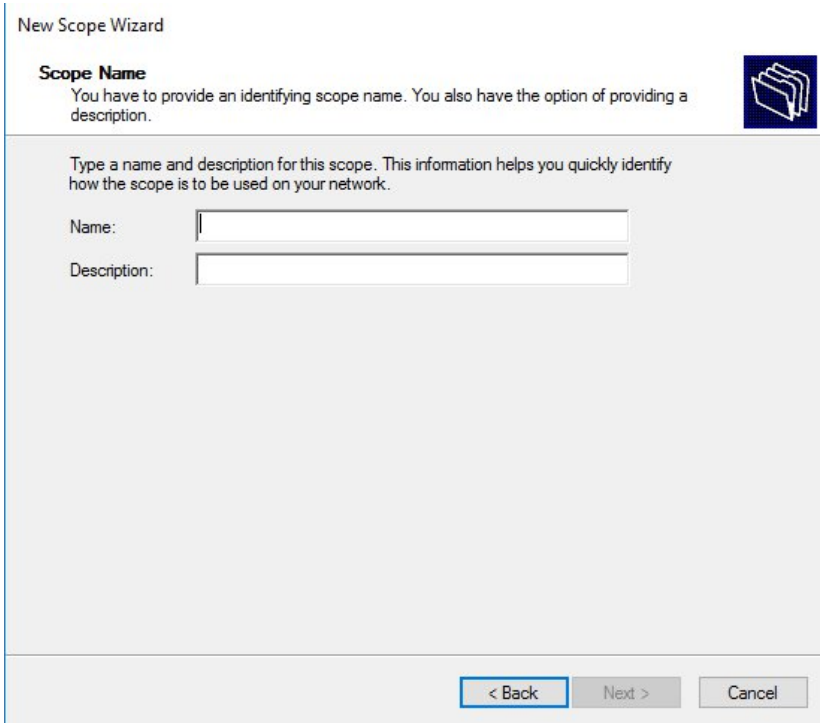
Activating the Scope



WILEY

Creating a New Scope in IPv6

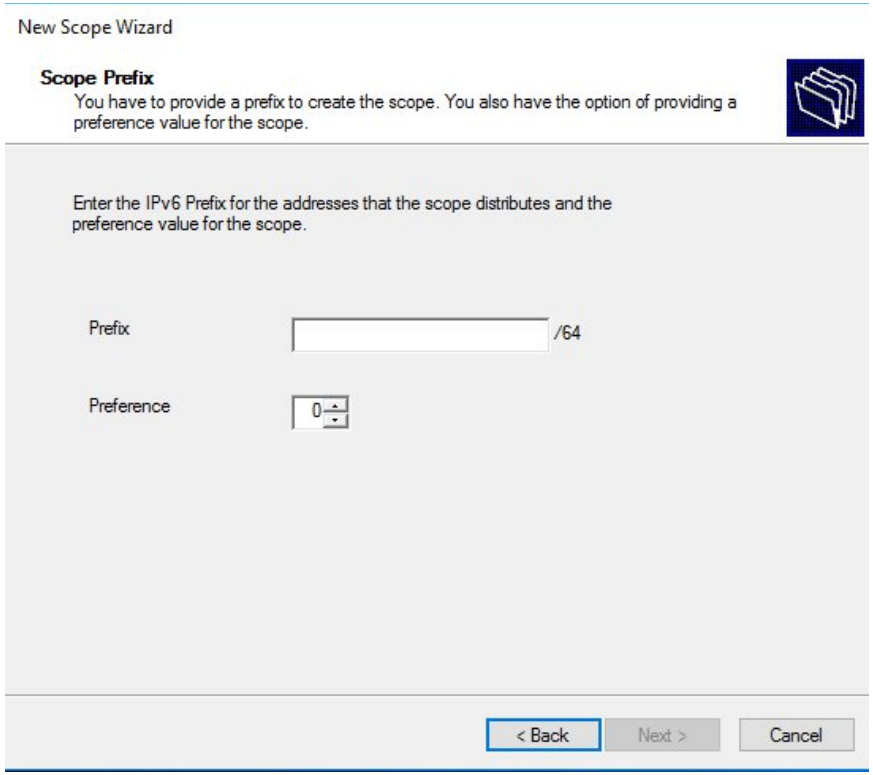
- To create a scope, right-click the IPv6 option in the DHCP snap-in under the server name and select the Action ➢ New Scope command.



Scope Prefix in IPv6

IPv6 has three types of addresses:

- Unicast
- Multicast
- Anycast



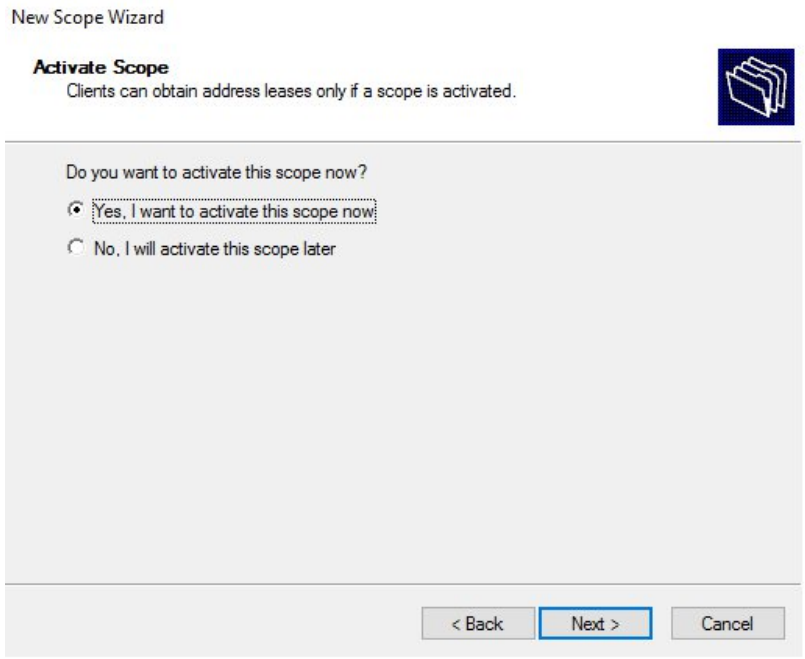
Other Options to Set

There are a few other options that you can set when setting up a DHCP scope. They are:

- Add Exclusions - the Add Exclusions page allows you to create exclusion ranges.
- Scope Lease - allows you to set how long a device gets to use an assigned IP address before it has to renew its lease.

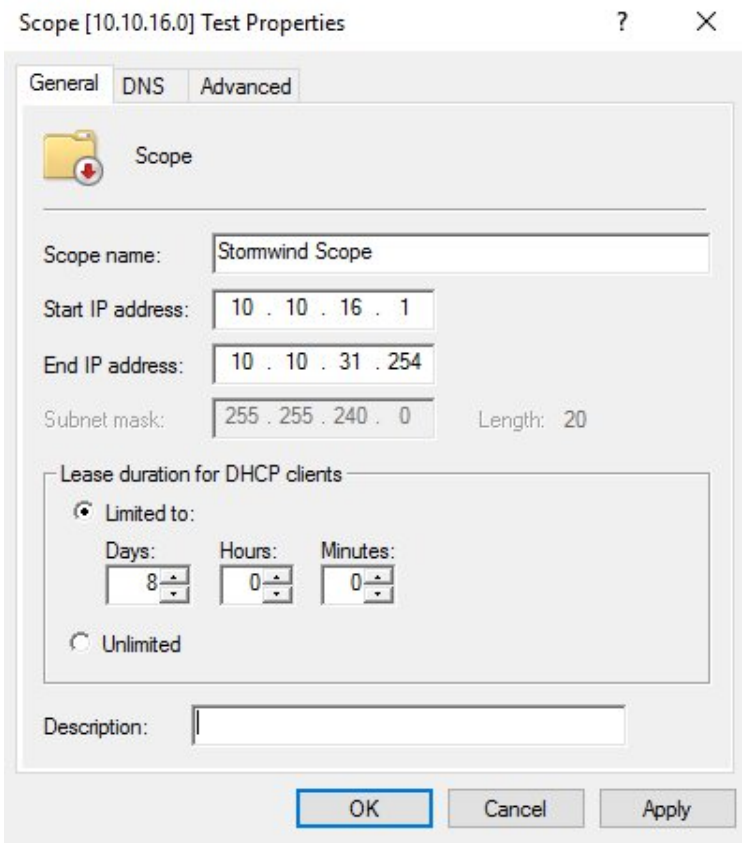
Activating a New Scope in IPv6

- By default, the wizard will assume you want the scope activated. If you want to wait to activate the scope, choose No in the Activate Scope Now box.



SYBEX
A Wiley Brand

Changing Scope Properties – General Tab (for an IPv4 Scope)



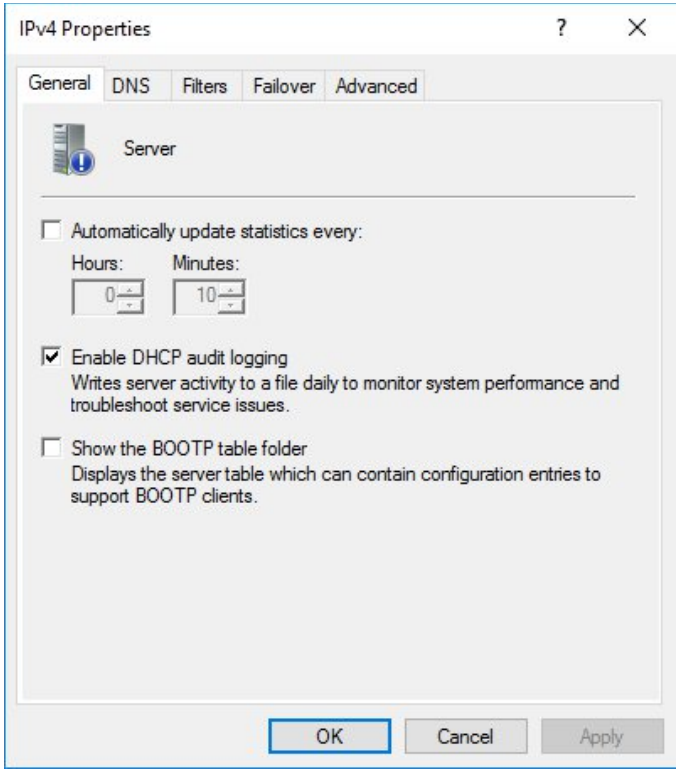
WILEY

Changing Server Properties

You access the server properties by right-clicking the IPv4 or IPv6 object within the DHCP management console and selecting Properties.

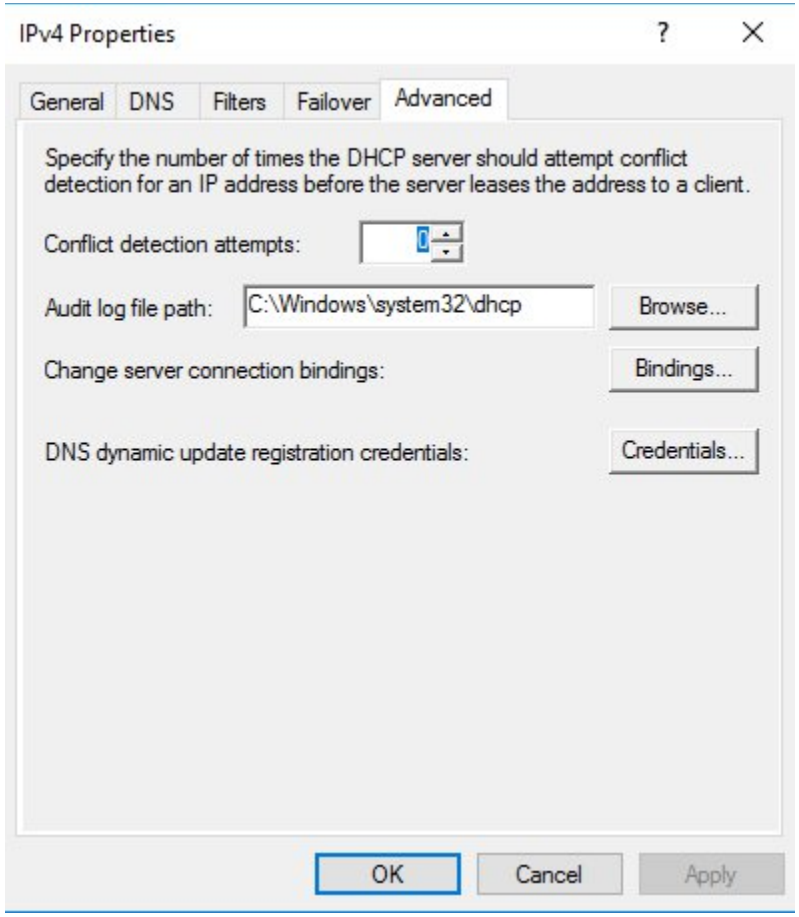
Tabs include:

- General
- DNS
- Filters
- Failover
- Advanced



SYBEX
A Wiley Brand

IPv4 Properties – Advanced Tab Dialog Box



WILEY

IPv6 Server Properties

The IPv6 Properties dialog box for the server has two tabs:

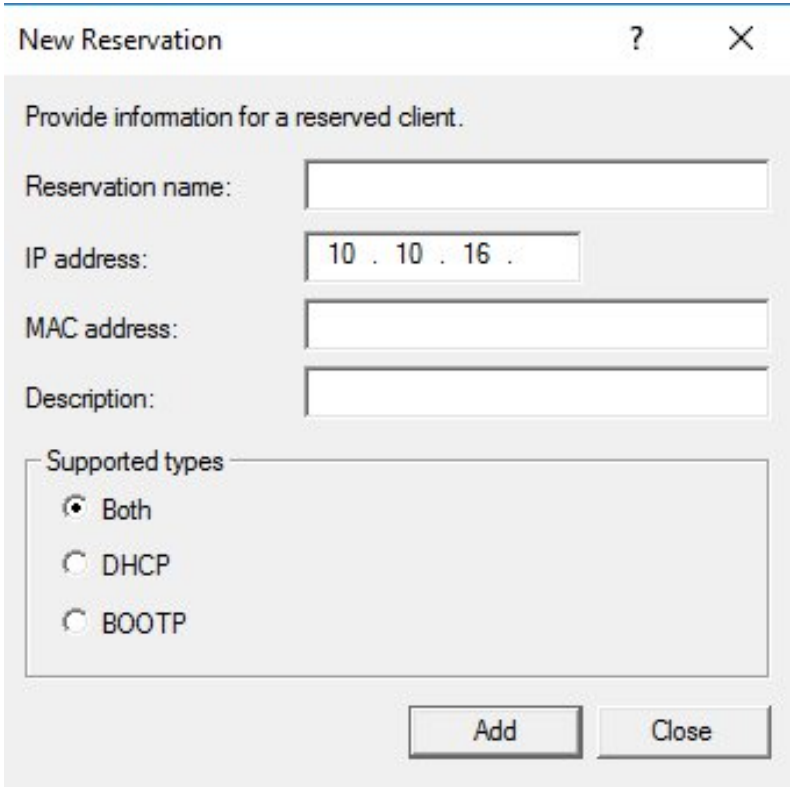
- General tab:
  - Frequency with which statistics are updated
  - DHCP auditing
- The Advanced
  - Database path for the audit log file path.
  - Connection bindings.
  - Registration credentials for dynamic DNS. The registration credential is the user account that DHCP will use to register clients with Active Directory.

Removing an Exclusion Range

- To remove an exclusion, just right-click it and choose the Delete command.
- After confirming your command, the snap-in removes the excluded range and the addresses become immediately available for issuance.

SYBEX
A Wiley Brand

Adding Reservations



WILEY

Setting Scope Options for IPv4

Option Assignment:

- Predefined Options
- Server Options
- Scope Options
- Class Options
- Client Options

Creating IPv4 Multicast Scopes

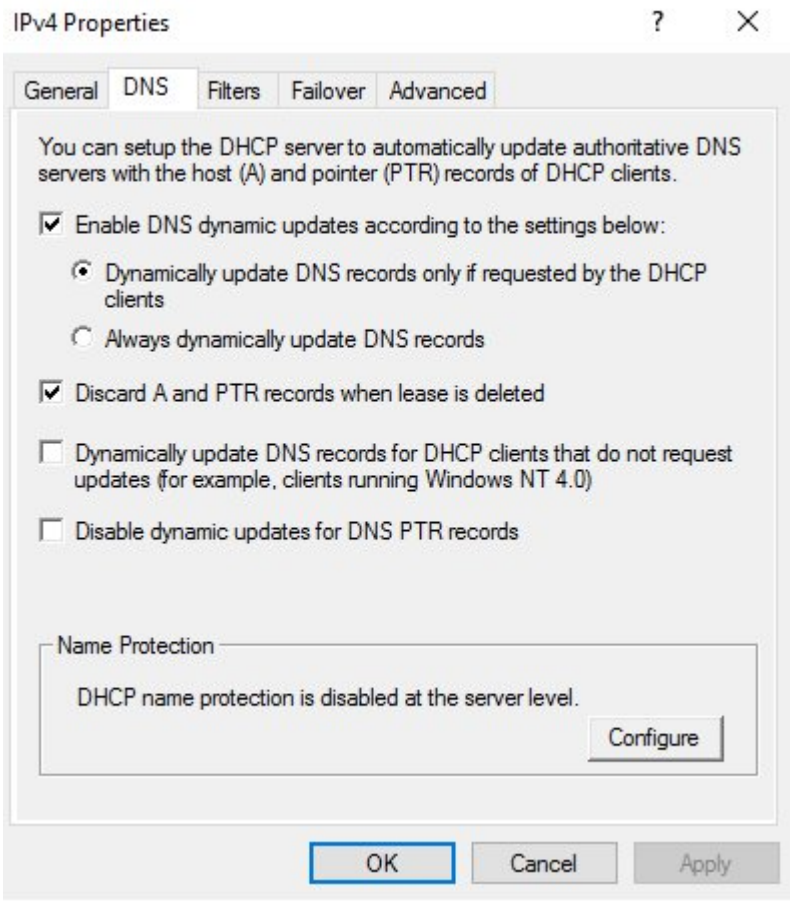
- *Multicasting* occurs when one machine communicates to a network of subscribed computers rather than specifically addressing each computer on the destination network.
- Multicast Address Dynamic Client Allocation Protocol (MADCAP) is the protocol that controls multicasting.

Integrating Dynamic DNS and IPv4 DHCP

- Can pass addresses to DHCP clients while still maintaining the integrity of your DNS services.
- The DNS server can be updated in two ways.
  - One way is for the DHCP client to tell the DNS server its address.
  - Another way is for the DHCP server to tell the DNS server when it registers a new client.

SYBEX
A Wiley Brand

IPv4 Properties – DNS Tab



WILEY

Using DHCP Failover Architecture

- DHCP can become a single point of failure within a network if there is only one DHCP server.
- If that server becomes unavailable, clients will not be able to obtain new leases or renew existing leases.
- It is recommended to have more than one DHCP server in the network.
- Microsoft recommends the 80/20 rule for redundancy of DHCP services in a network.

DHCP Load Sharing

- Load sharing is the normal default way that you use multiple DHCP servers.
- Both servers cover the same subnets simultaneously, and both servers assign IP addresses and options to clients on the assigned subnets.

DHCP Hot Standby

- In a DHCP hot standby situation, the two DHCP servers operate in a failover relationship where one server acts as an active server and is responsible for leasing IP addresses to all clients in a scope or subnet.
- The secondary DHCP server assumes the standby role, and it is ready to go in the event that the primary DHCP server becomes unavailable.

DHCP Database Files (1/2)

- DHCP uses a set of database files to maintain its knowledge of scopes, superscopes, and client leases.
- These files, reside in the *systemroot*\System32\DHCP folder, are always open when the DHCP service is running.
- DHCP servers use Joint Engine Technology (JET) databases to maintain their records.

DHCP Database Files (2/2)

The primary database file is dhcp.mdb—it has all of the scope data in it. The following files are also part of the DHCP database:

- Dhcp.tmp - This is a backup copy of the database file created during reindexing of the database.
- J50.log - This file (plus a number of files named J50xxxxx.log, where xxxxx stands for 00001, 00002, 00003, and so on) is a log file that stores changes before they're written to the database.
- J50.chk - This is a checkpoint file that tells the DHCP engine which log files it still needs to recover.

Removing the DHCP Database Files

1. Stop the DHCP service by typing **net stop dhcpserver** at the command prompt.
2. Remove all of the files from the *systemroot*\system32\DHCP folder.
3. Restart the service (at command prompt type **net start dhcpserver**).
4. Reconcile the scope.

Changing Database Backup Interval

- By default, the DHCP service backs up its databases every 60 minutes.
- Can adjust this setting by editing the Backup Interval value under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters.

Compacting the DHCP Database Files

- Microsoft has a utility called jetpack.exe that allows you to compact the JET database. Microsoft JET databases are used for WINS and DHCP databases. If you wanted to use the jetpack command, the proper syntax is:

```
JETPACK.EXE <database name><temp database name>
```

- After you compact the database, you rename the temp database to dhcp.mdb.

Implement DHCPv6

- Administrators can create and manage both IPv4 and IPv6 DHCP scopes for their organization. Even though they are managed separately, they have the same capabilities of being able to configure reservations, exclusions, and other DHCP options.
- DHCPv6 client uses a device unique identifier (DUID) instead of a MAC address to get an IP address from the DHCP server.
- DHCPv6 supports both stateful address configuration and stateless address configuration.

DHCP Failover

- *DHCP failover* provides load balancing and redundancy for DHCP services, enabling administrators to deploy a highly resilient DHCP service for their organization.

- Benefits:
  - Multisite
  - Flexibility
  - Seamless
  - Simplicity

Configuring DHCP Failover

1. Open the DHCP Management Console.
2. Right-click IPv4 and choose the Configure Failover command to launch the Configure Failover Wizard. Click Next on the Introduction page.
3. On the Specify The Partner Server To Use For Failover page, select your partner DHCP server from the drop-down menu or by browsing the Add Server directory. Click Next.
4. On the Create A New Failover Relationship page, provide a relationship name, select the Load Balance mode from the drop-down, and provide a shared secret password that will be used to authenticate the DHCP failover relationship between the two servers in the failover cluster. Click Next.

Configuring DHCP Failover - Continued

5. Review your configuration settings and click the Finish button to configure your new DHCP failover configuration. Click Close upon successful completion.
6. After the wizard successfully completes on the primary DHCP server, verify that the new failover scope has been created and activated on the secondary DHCP server in the DHCP Management Console.

DHCP Name Protection

- *DHCP name protection* is an additional configuration option that administrators should consider when working DHCP within their environment.
- Name protection protects a DHCP leased machine's name from being overwritten by another machine with the same name during DNS dynamic updates.

IP Address Management (IPAM) Administration

- IPAM is a built-in utility that allows administrators to discover, monitor, audit, and manage the TCP/IP schema used on the network.
- Ability to observe and administer the servers that are running DHCP and DNS.
- 3 main methods to deploy an IPAM server are Distributed, Centralized or Hybrid.

IPAM Advantages

Includes the following advantages:

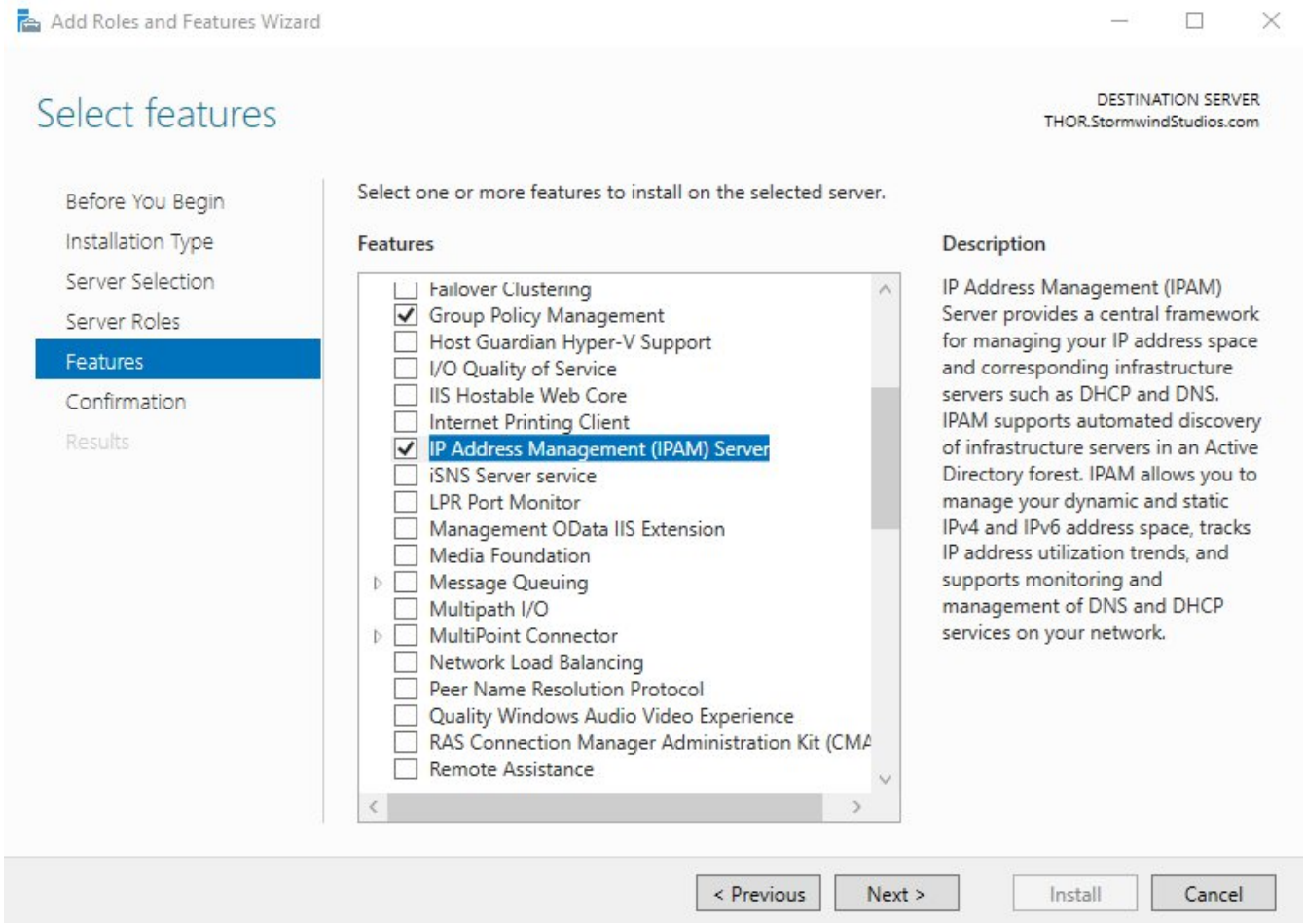
- Automatic IP Address Infrastructure Discovery
- Management of DHCP and DNS Services
- Custom IP address Management
- Multiple Active Directory Forest Support
- Purge Utilization Data
- Auditing and Tracking of IP address
- PowerShell Support

IPAM Hardware/Software Requirements

- IPAM must be loaded onto a Windows Server.
- Before the IPAM client can be used, must first install the Remote Server Administration Tools (RSAT).
- The network needs to be part of a domain but it can't be a domain controller.
- IPAM will work on both an IPv4 and IPv6 network.
- You should ***NOT*** put the IPAM server on a server with other network services like DNS or DHCP.

SYBEX
A Wiley Brand

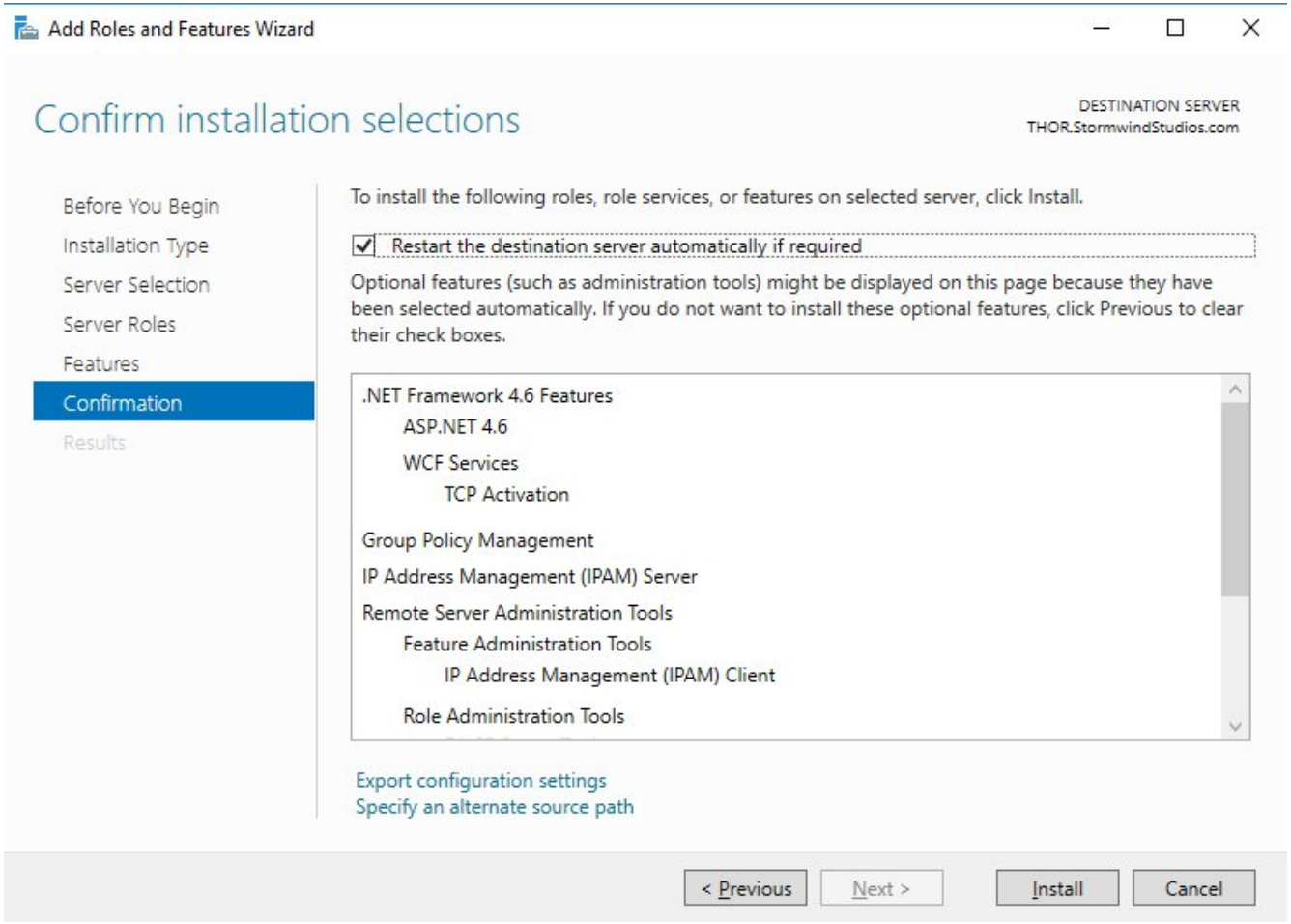
Installing the IPAM Feature



WILEY

SYBEX
A Wiley Brand

Installing IPAM - Confirmation



WILEY

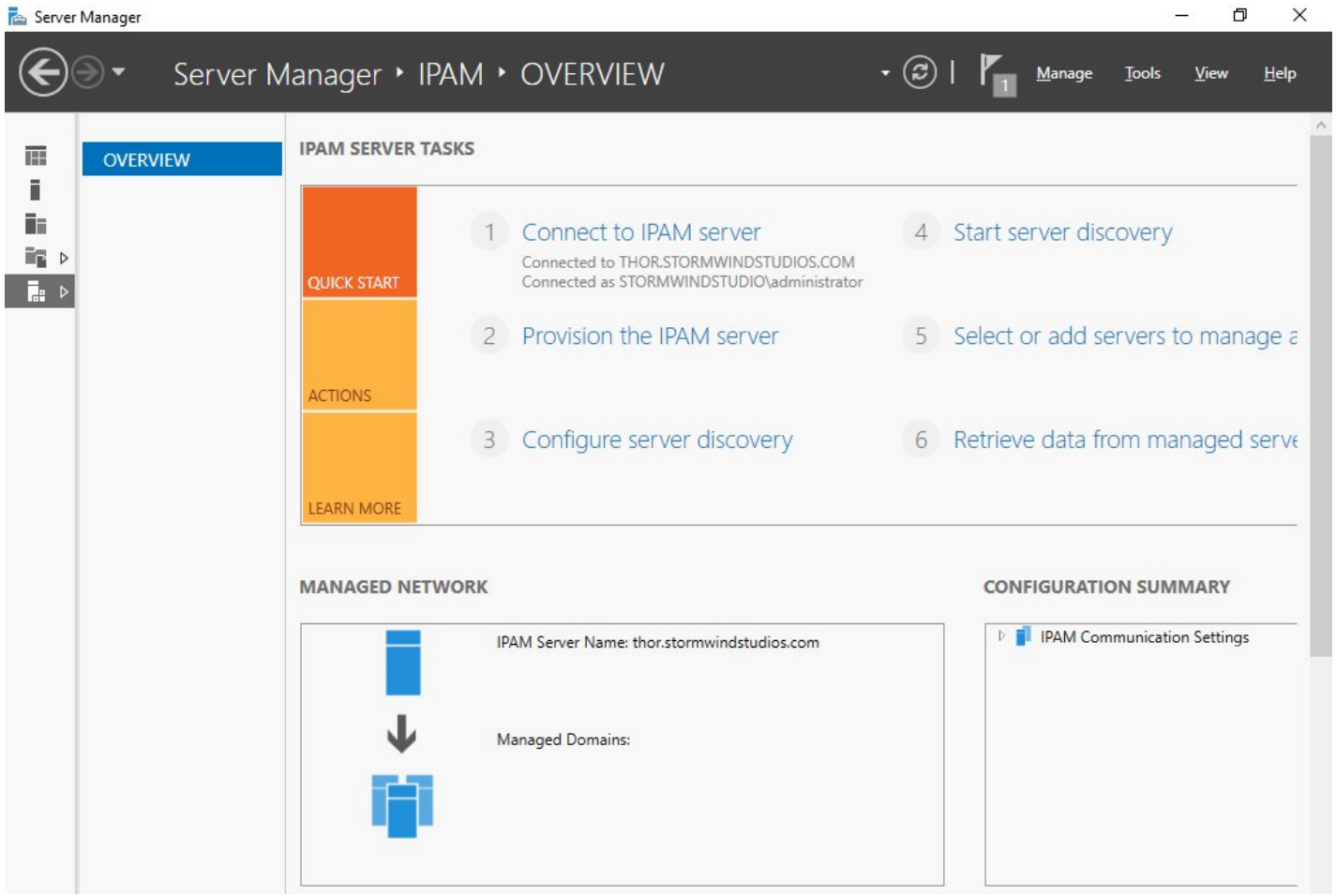
Provisioning IPAM

- When setting up an IPAM server, you must determine how the IPAM server will communicate with your other servers. This is called IPAM provisioning.

- IPAM provisioning can be setup two ways:
  - Manually
  - Using GPOs

SYBEX
A Wiley Brand

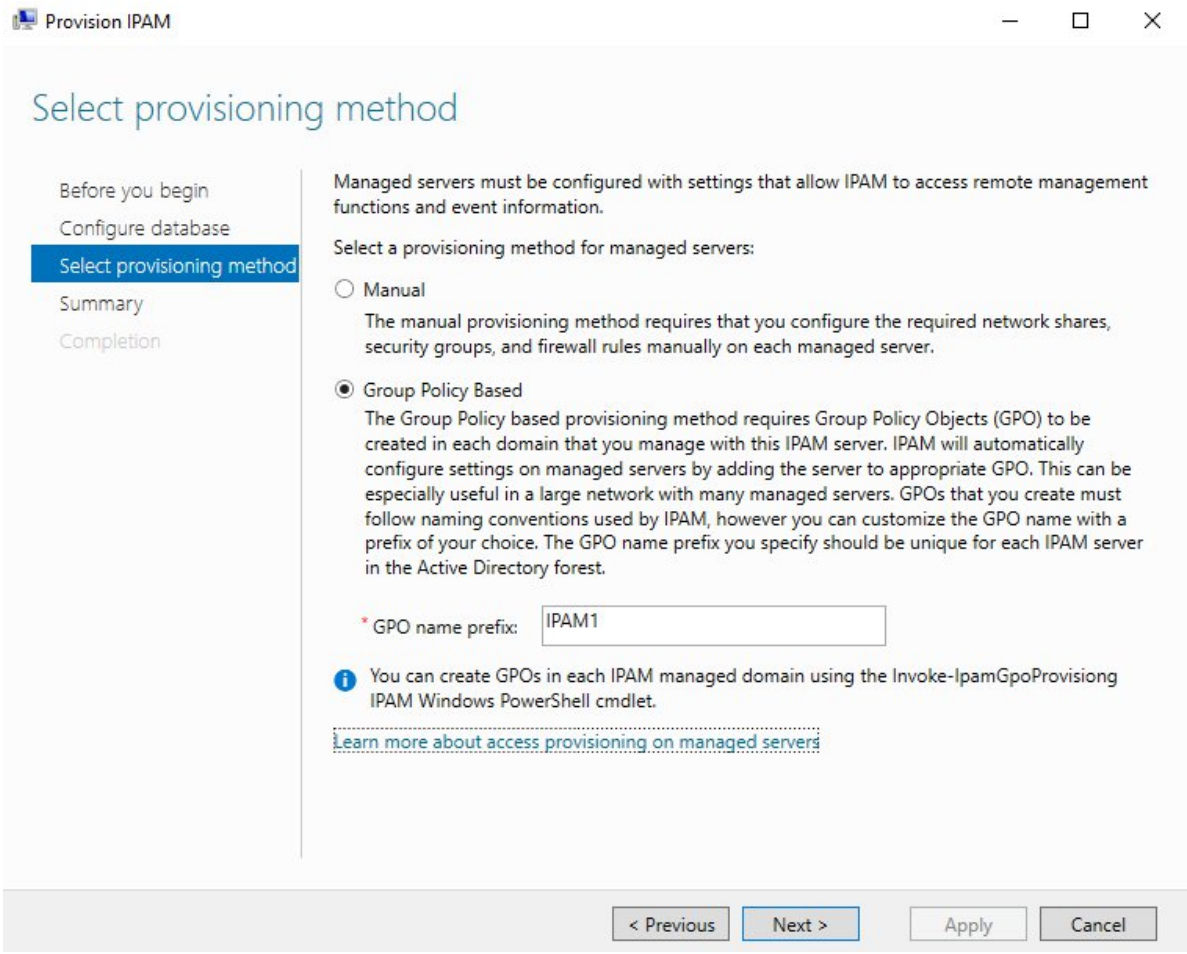
IPAM Provisioning - Overview Screen



WILEY

SYBEX
A Wiley Brand

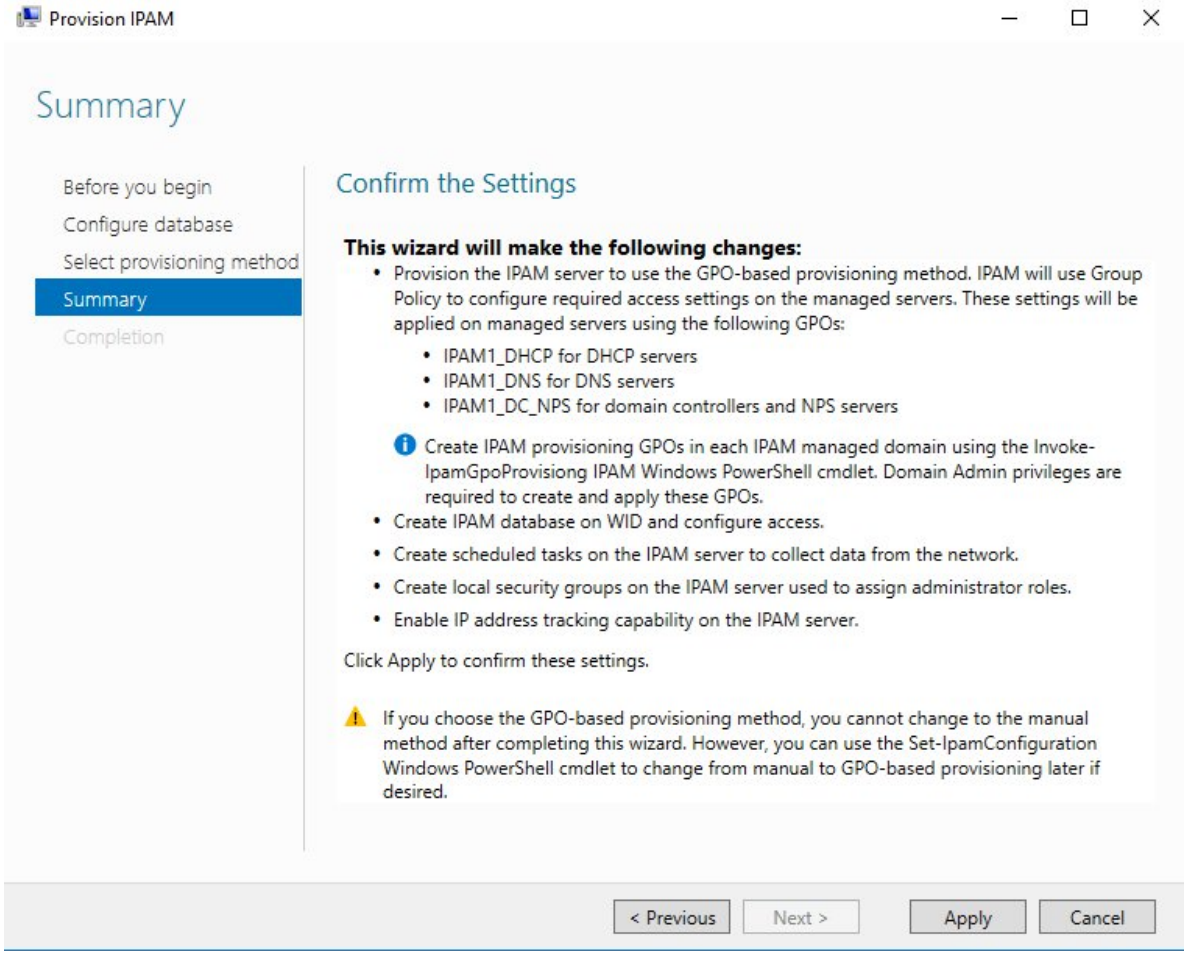
Provisioning IPAM – Select Method



WILEY

SYBEX
A Wiley Brand

Provisioning IPAM – Summary



WILEY

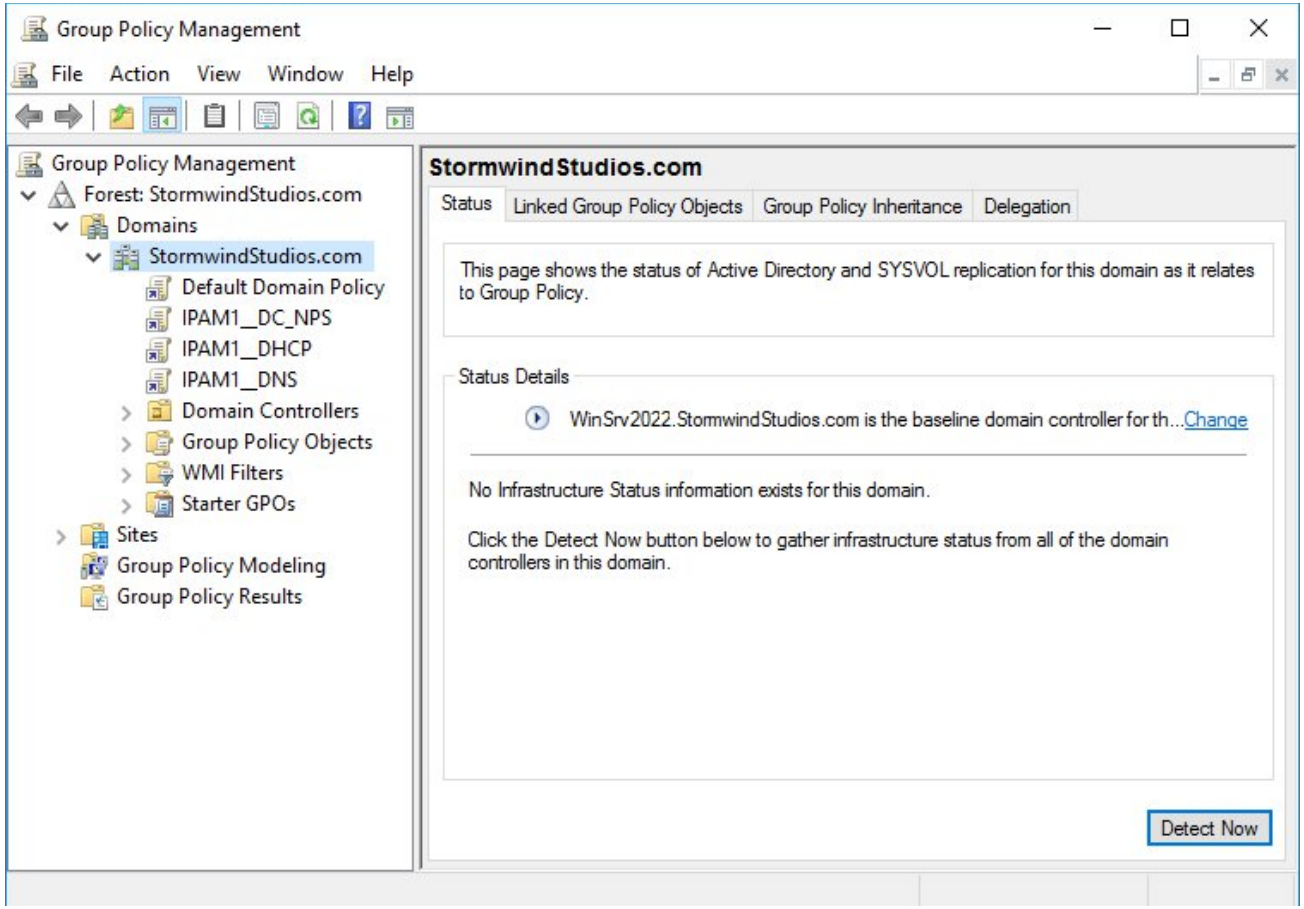
Provisioned GPOs

- To create provisioned GPOs automatically, need to use the Invoke-IpamGpoProvisioning cmdlet at an elevated Windows PowerShell prompt.
- The following is an example of the Invoke-IpamGpoProvisioning command:

```
Invoke-IpamGPOProvioning -Domain
StormWindStudios.com -GpoPrefixName IPAM1
-IpamServerFqdn
IPAMServer.StormWindStudios.com -Force
```

SYBEX
A Wiley Brand

Viewing the New GPOs



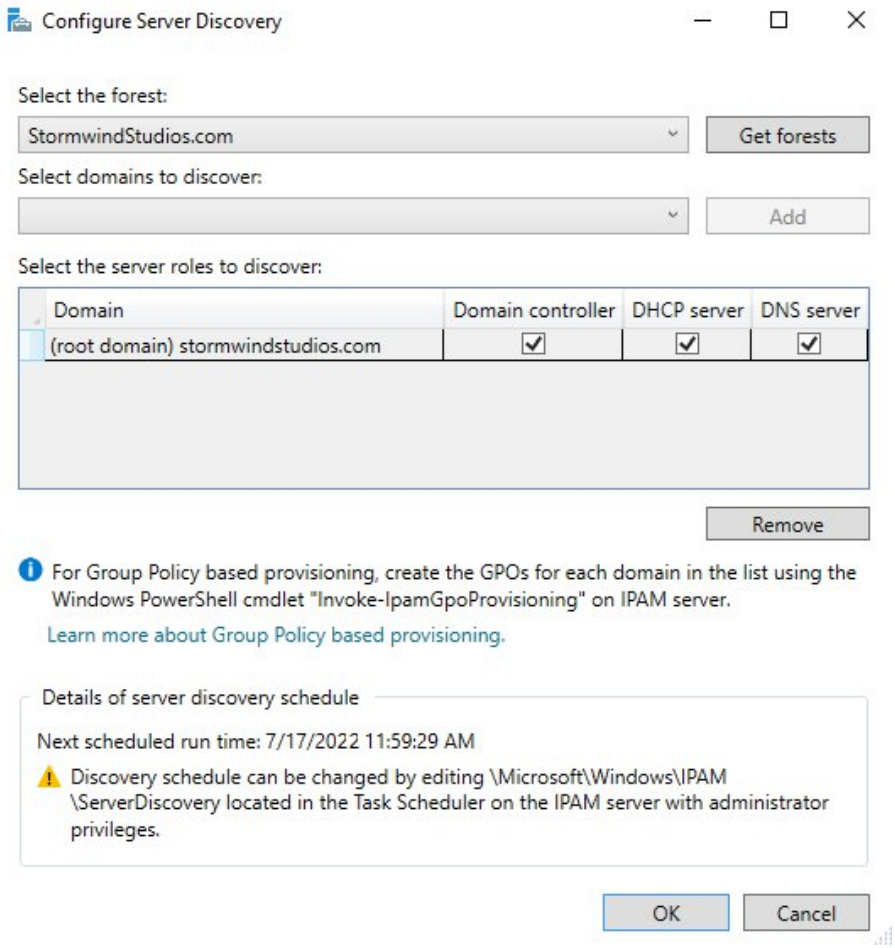
WILEY

Configure IPAM Server Discovery

- Once you have successfully installed and provisioned the IPAM feature on your Windows Server 2022 machine, you can begin server discovery.
- Server discovery will automatically search for all of the machines running on the specified domain.
- Administrator privileges are required for the domain against which you are running server discovery.

SYBEX
A Wiley Brand

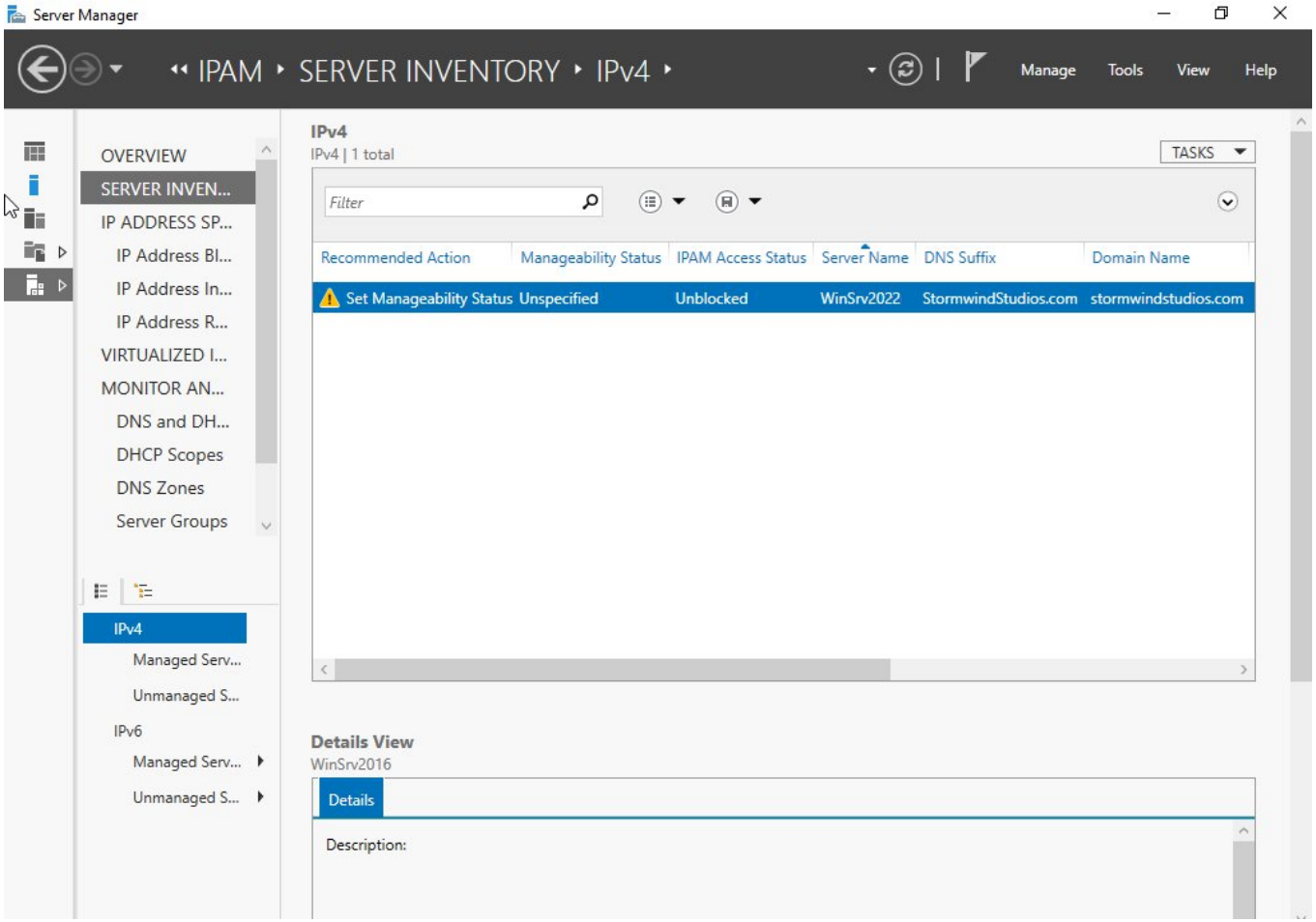
Configure Server Discovery



WILEY

SYBEX
A Wiley Brand

Server Inventory Screen



WILEY

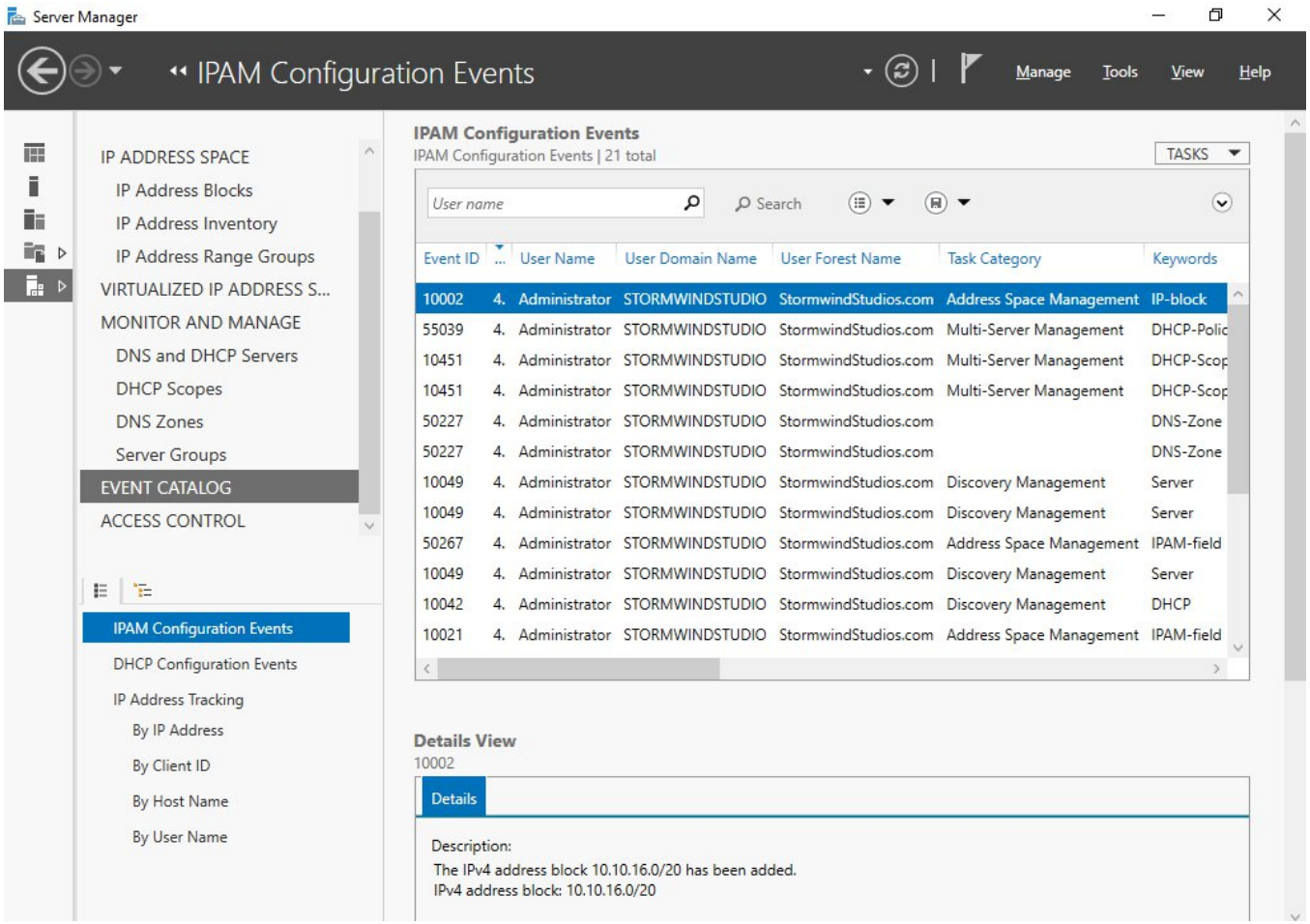
IP Blocks and Ranges

- In IPAM, IP address space is divided into:
  - IP Addresses
  - IP Address Ranges
  - IP Address Blocks

- When you have an IPAM managed DHCP server, the IP address ranges found within the scopes of that DHCP server are automatically entered into the IPAM database during the discover process. Individual IP addresses and IP blocks are not automatically added to the IPAM database.

SYBEX
A Wiley Brand

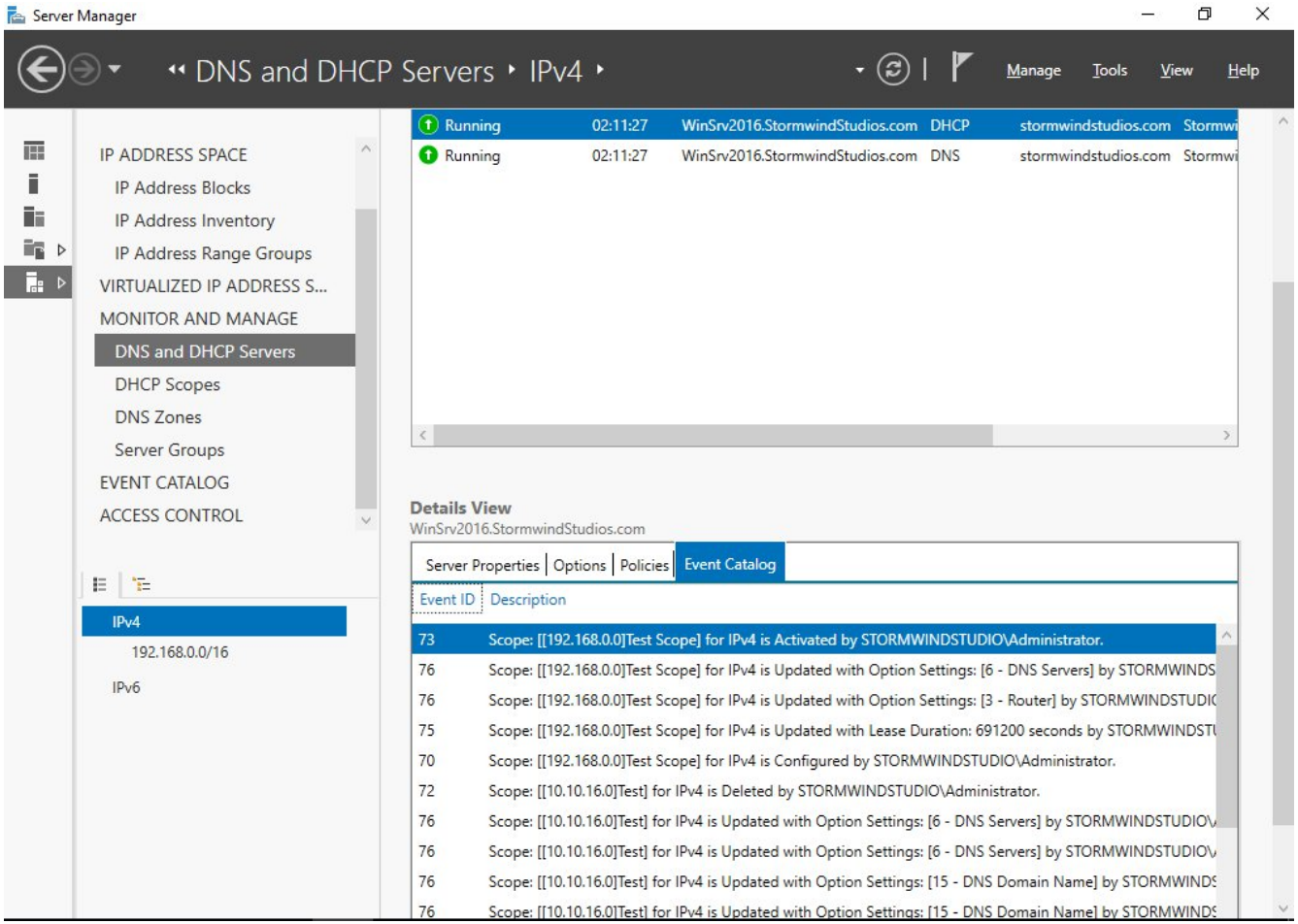
Auditing IPAM - Event Catalog



WILEY

SYBEX
A Wiley Brand

DHCP Event Catalog



WILEY

Configuring Auditing

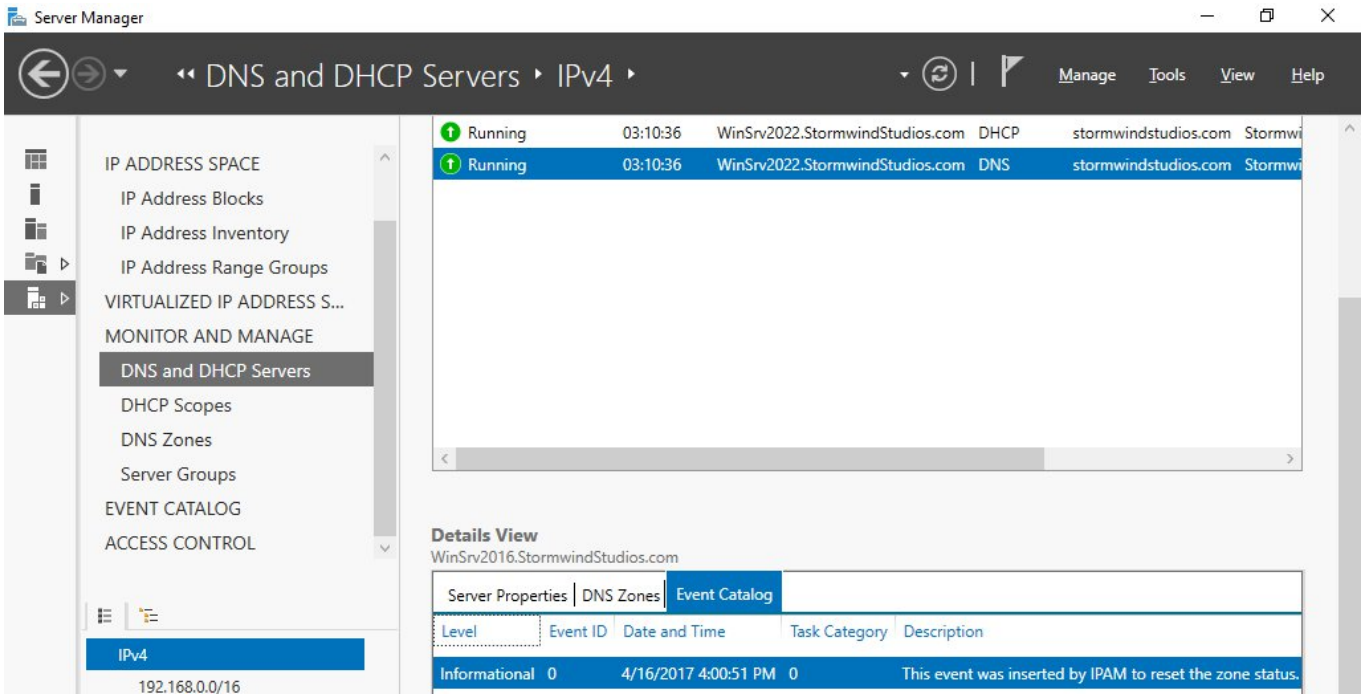
1. Open Server Manager and click on IPAM.
2. Click Event Catalog in the navigation window. In the right hand side under IPAM Configuration Event, you will see all of the IPAM configuration events that have been logged.
3. In the lower window, click on DHCP configuration events. This will show you any configuration changes made to the DHCP servers.
4. Now click on IP address tracking. This allows you to audit the IP address usage.
5. Under the Monitor and Manage section, click on DNS and DHCP servers. In the right hand windows, click either of the two servers and then choose Event Catalog under the Details View.

Configuring Auditing - Continued

6. Under the Monitor and Manage section, you can choose any server that you want to monitor, including your domain controllers. Just click on the server and then choose Event Catalog under the Details View.
7. Once you are finished looking at all of the different servers you have in IPAM, close Server Manager.

SYBEX
A Wiley Brand

DNS Event Catalog



WILEY

SYBEX
A Wiley Brand

DHCP PowerShell Commands

Command	Description
`Add-DhcpServerInDC`	Allows an administrator to authorize the DHCP server services in Active Directory.
`Add-DhcpServerv4Class`	Allows an administrator to add an IPv4 vendor or user class.
`Add-DhcpServerv4ExclusionRange`	Administrators can use this command to add an exclusion range to an IPv4 scope.
`Add-DhcpServerv4Failover`	Administrators can use this command to add an IPv4 failover.
`Add-DhcpServerv4Lease`	This command allows an administrator to add a new IPv4 address lease.
`Add-DhcpServerv4MulticastScope`	Administrators use this command to add a multicast scope server.
`Add-DhcpServerv4OptionDefinition`	This command allows an administrator to add a DHCPv4 option definition.
`Add-DhcpServerv4Policy`	Admins can use this command to add a new policy to either the server or scope level.
`Add-DhcpServerv4Reservation`	This command allows an admin to reserve a client IPv4 address in the scope.
`Add-DhcpServerv4Scope`	This command adds an IPv4 scope.
`Add-DhcpServerv6Class`	This command allows an administrator to add an IPv6 vendor or user class.

WILEY

DHCP PowerShell Commands – Continued (1/2)

Command	Description
`Add-DhcpServerv6ExclusionRange`	Administrators can use this command to add an exclusion range to an IPv6 scope.
`Add-DhcpServerv6Lease`	This command allows an administrator to add a new IPv6 address lease.
`Add-DhcpServerv6OptionDefinition`	This command allows an administrator to add a DHCPv6 option definition.
`Add-DhcpServerv6Reservation`	This command allows an admin to reserve a client IPv6 address in the scope.
`Add-DhcpServerv6Scope`	This command adds an IPv6 scope.
`Backup-DhcpServer`	Administrators can use this command to back up the DHCP database.
`Export-DhcpServer`	This command allows an administrator to Export the DHCP server configuration and lease data.
`Get-DhcpServerAuditLog`	This command shows you the audit log for the DHCP configuration.
`Get-DhcpServerDatabase`	Administrators can use this command to view the configuration parameters of the DHCP database.
`Get-DhcpServerSetting`	This command allows an admin to view the configuration parameters of the DHCP database.

DHCP PowerShell Commands – Continued (2/2)

Command	Description
`Get-DhcpServerv4Class`	Administrators use this command to view the IPv4 vendor or user class settings.
`Set-DhcpServerDatabase`	Allows an administrator to modify configuration settings of the DHCP DB.
`Set-DhcpServerDnsCredential`	Administrators can set the credentials of the DHCP Server service which help register or deregister client records.
`Set-DhcpServerSetting`	This command allows an administrator to configure the server level settings.
`Set-DhcpServerv4Class`	Allows an administrator to configure the IPv4 vendor class or user class settings.
`Set-DhcpServerv4Failover`	Allows an admin to configure the settings for an existing failover relationship.
`Set-DhcpServerv4Policy`	Administrators can use this command to configure the settings of a DHCP policy.
`Set-DhcpServerv4Reservation`	This command allows an administrator to configure an IPv4 reservation.
`Set-DhcpServerv4Scope`	Admins can use this command to configure the settings of an existing IPv4 scope.
`Set-DhcpServerv6Reservation`	This command allows an administrator to configure an IPv4 reservation.
`Set-DhcpServerv6Scope`	Admins can use this command to configure the settings of an existing IPv6 scope.

SYBEX
A Wiley Brand

PowerShell Commands for IPAM

Command	Description
Add-IpamAddress	This command allows an administrator to add an IP address to IPAM.
Add-IpamAddressSpace	This command allows an administrator to add an address space to IPAM.
Add-IpamBlock	Administrators can use this command to add an IP address block to IPAM.
Add-IpamCustomField	This command is used to add a custom field to IPAM.
Add-IpamCustomValue	Administrators can use this command to add a IPAM value to a custom field.
Add-IpamDiscoveryDomain	This command allows an administrator to add a new domain in which IPAM discovers infrastructure servers.
Add-IpamRange	Administrators can use this command to add an IP address range to an IPAM server.
Disable-IpamCapability	This command allows an administrator to disable an IPAM optional capability.
Enable-IpamCapability	This command allows an administrator to enable an IPAM optional capability.
Export-IpamAddress	Administrators can use this command to export IP addresses from an IPAM server.
Export-IpamRange	Administrators can use this command to export all of the IP address ranges.
Export-IpamSubnet	This command allows an administrator to export the subnets of an IP address.
Find-IpamFreeAddress	This command will show you the available subnets for allocation, given an IP block, prefix length, and number of requested subnets.
Get-IpamAddress	This command shows an administrator a requested IP addresses from IPAM.
Get-IpamAddressSpace	This command shows an administrator an address spaces in IPAM.
Get-IpamBlock	This command shows an administrator a set of address blocks from IPAM.
Get-IpamDatabase	Administrators can use this command to view the IPAM database configuration settings.
Get-IpamDhcpScope	Administrators can use this command to view DHCP scopes on an IPAM server.
Get-IpamDhcpServer	This command allows an administrator to view DHCP server information from IPAM database.

WILEY

SYBEX
A Wiley Brand

PowerShell Commands for IPAM - Continued

Command	Description
Get-IpamDnsResourceRecord	Use this command to view DNS resource records in an IPAM database.
Get-IpamDnsServer	Allows an administrator to view DNS server information from IPAM database.
Get-IpamDnsZone	Allows an administrator to view DNS zone information from IPAM database.
Get-IpamIpAddressAuditEvent	Use this command to view IP address audit events in IPAM.
Import-IpamAddress	Allows an admin to import an IP address into the IPAM server.
Import-IpamRange	Allows an admin to import an IP address range into the IPAM server.
Import-IpamSubnet	Allows an admin to import an IP address subnet into the IPAM server.
Invoke-IpamGpoProvisioning	Administrators can create and links IPAM group policies (GPOs) for provisioning.
Move-IpamDatabase	Allows an admin to move an IPAM database to a SQL server database.
Remove-IpamAddress	Administrators use this command on an IPAM server to remove a set of IP addresses.
Remove-IpamAddressSpace	Administrators use this command on an IPAM server to remove a set of IP address spaces.
Set-IpamAccessScope	This command allows an administrator to set up an IPAM access scope.
Set-IpamAddress	Administrators can use this command to configure an IP address in IPAM.
Set-IpamAddressSpace	Administrators can use this command to configure an IP address space in IPAM.
Set-IpamBlock	Administrators can use this command to configure an IP address block in IPAM.
Set-IpamConfiguration	Administrators can adjust the configuration of a computer that hosts the IPAM server.
Set-IpamDatabase	This command allows an administrator to change the settings on how IPAM connects to the IPAM database.
Set-IpamDiscoveryDomain	Administrators use this command to change the IPAM discovery configuration.
Set-IpamRange	This command is used to modify an existing IP address range.
Set-IpamSubnet	This command is used to modify an existing IP subnet.
Update-IpamServer	Administrators can use this command to update the IPAM server after an operating system upgrade.

WILEY