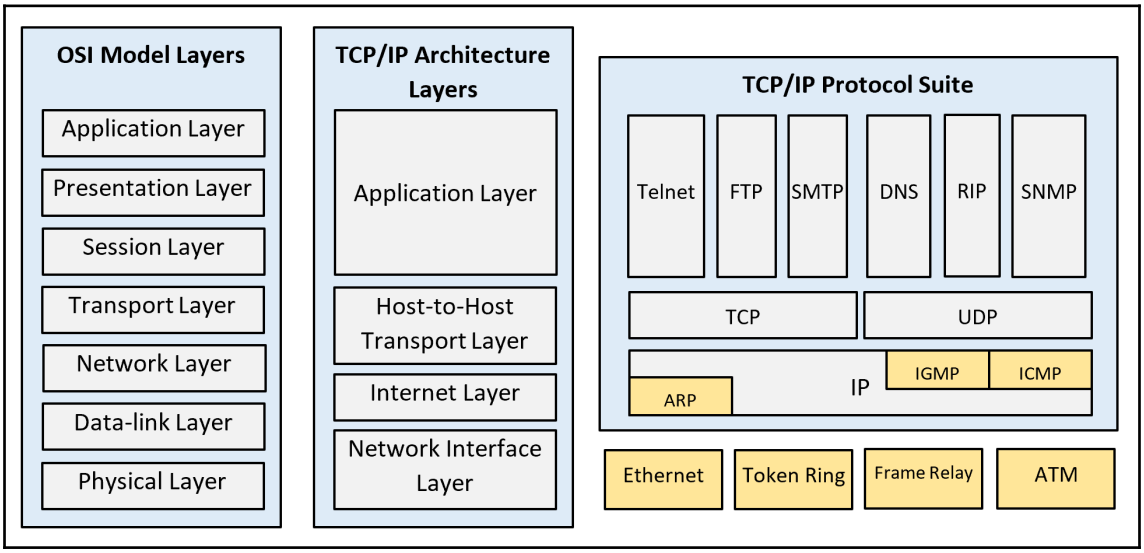
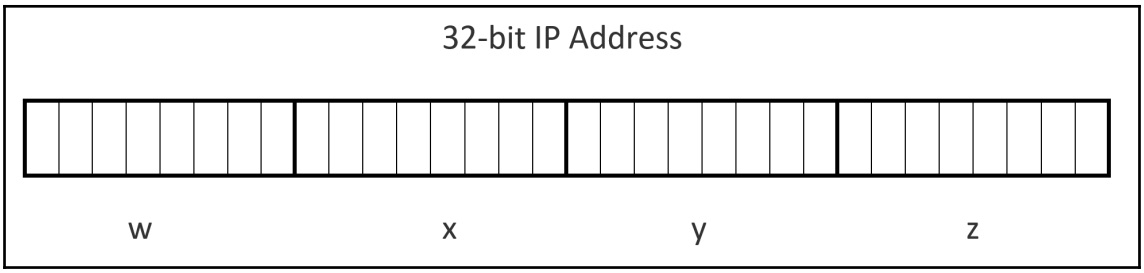
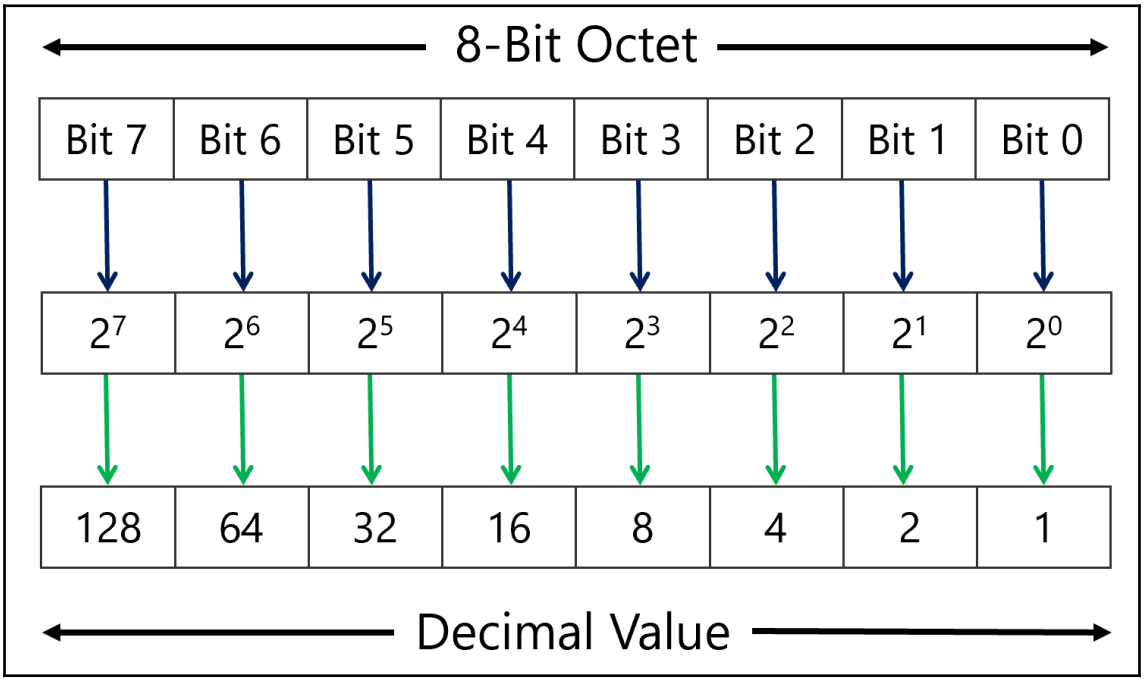
Chapter 1: Configuring Core Networking



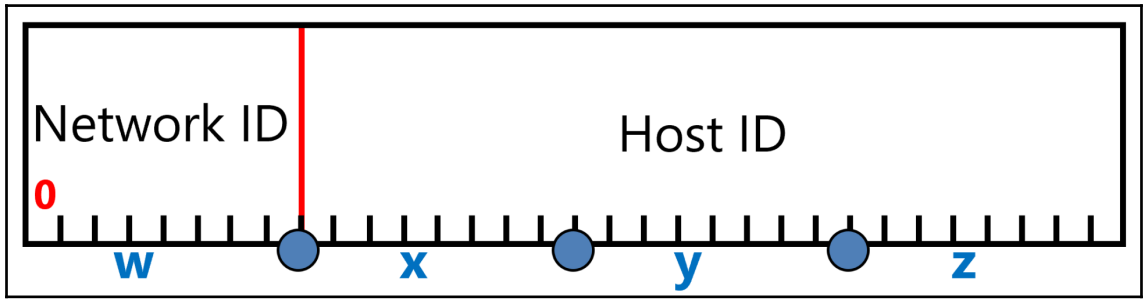
Protocol	Port	Function
HTTP	80	Web
HTTPS	443	Web (Secure)
FTP	20, 21	File transfer
SFTP	22	File transfer (Secure)
FTPS	989, 990	File transfer (Secure)
SIP	5060	VoIP (Internet phone)
DNS	53	Name resolution
SMTP	25	Mail
POP3	110	POP mailbox
IMAP	143	IMAP mailbox
Telnet	23	Remote login
SSH	122	Remote login (Secure)
NNTP	119	Usenet
NNTPS	563	Usenet (Secure)
IRC	194	Chat
NTP	123	Network time
SNMP	161, 162	Network management
Kerberos	88	Authentication

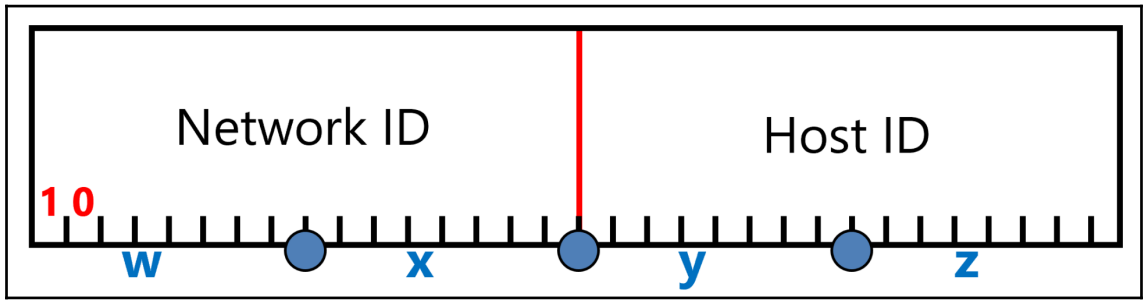


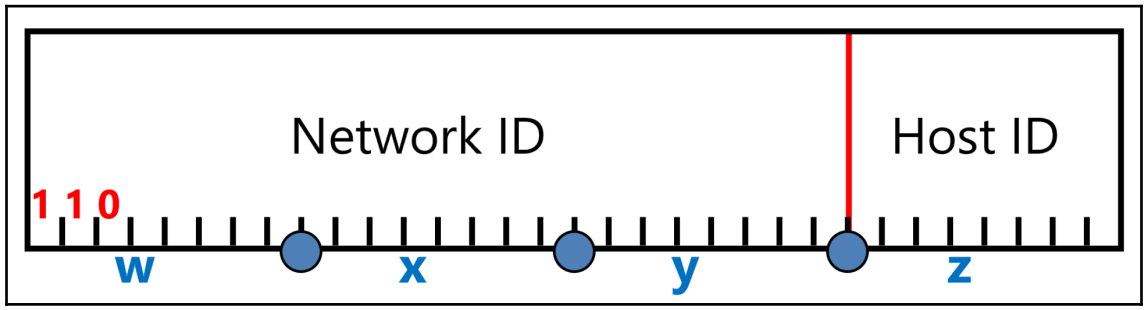


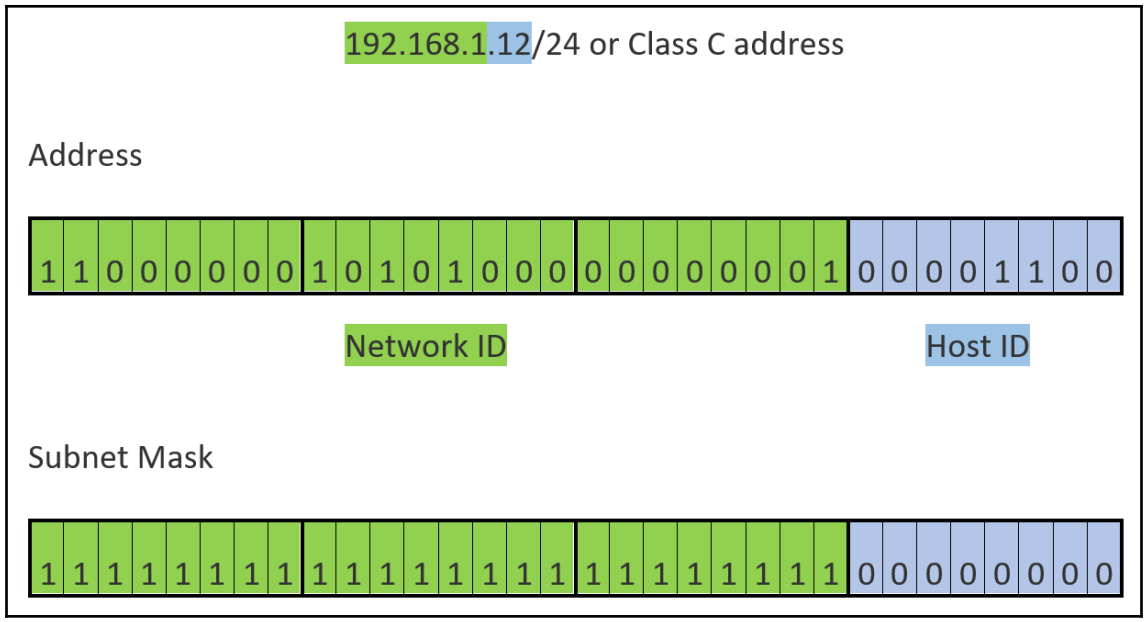
	w	x	y	z
Binary format	11000000	10101000	00000001	00001100
Decimal number	192	168	1	12

Address Class	Network (n) and Host (h) address octet layout	Default subnet mask	Number of networks	Number of hosts
Class A	n.h.h.h	255.0.0.0	128	16,777,216
Class B	n.n.h.h	255.255.0.0.	16,384	65,536
Class C	n.n.n.h	255.255.255.0	2,097,152	256



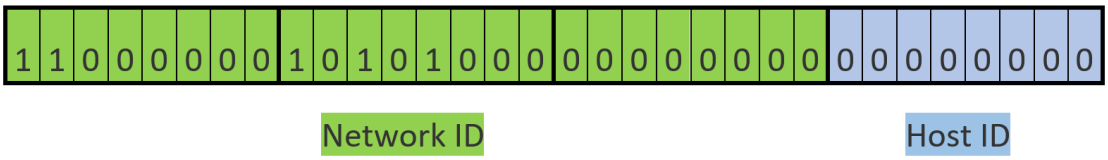




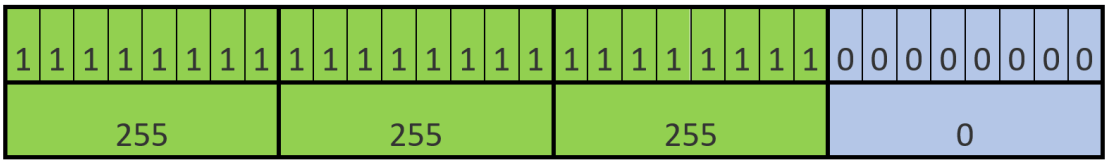

192.168.1.12/24 or Class C address
Address
1 1 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 1 0 0
Network ID
Host ID
Subnet Mask
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0

CIDR block address format	Subnet mask	Number of hosts/nodes
/32	255.255.255.255	1
/31	255.255.255.254	2
/30	255.255.255.252	4
/29	255.255.255.248	8
/28	255.255.255.240	16
/27	255.255.255.224	32
/26	255.255.255.192	64
/25	255.255.255.128	128
/24	255.255.255.0	256
/23	255.255.254.0	512
/22	255.255.252.0	1,024
/21	255.255.248.0	2,048
/20	255.255.240.0	4,096
/19	255.255.224.0	8,192
/18	255.255.192.0	16,384
/17	255.255.128.0	32,768
/16	255.255.0.0	65,536
/15	255.254.0.0	131,072
/14	255.252.0.0	262,144
/13	255.248.0.0	524,288
/12	255.240.0.0	1,048,576
/11	255.224.0.0	2,097,152
/10	255.192.0.0	4,194,304
/9	255.128.0.0	8,388,608
/8	255.0.0.0	16,777,216
/7	254.0.0.0	33,554,432
/6	252.0.0.0	67,108,864
/5	248.0.0.0	134,217,728
/4	240.0.0.0	268,435,456
/3	224.0.0.0	536,870,912
/2	192.0.0.0	1,073,741,824
/1	128.0.0.0	2,147,483,648
/0	0.0.0.0	4,294,967,296

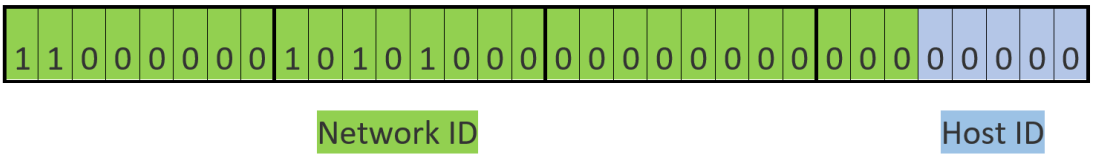
192.168.0.0/24 network and addresses



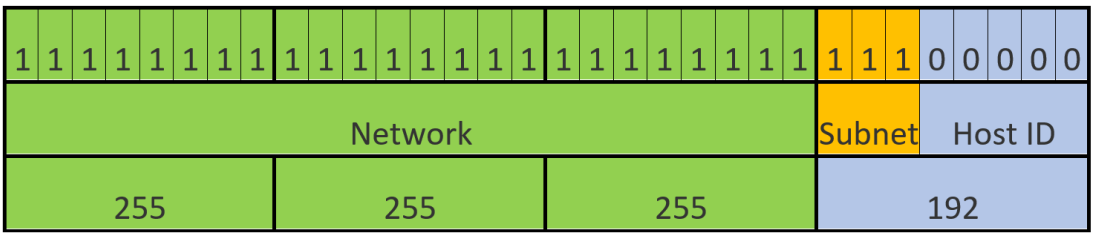
Subnet Mask 255.255.255.0



192.168.0.0/27 network and addresses



Subnet Mask 255.255.255.192



Number of Subnets needed	Number of Subnet or Host Bits to “borrow”
1-2	1
3-4	2
5-8	3
9-16	4
17-32	5
33-64	6
65-128	7
129-256	8
257-512	9
513-1,024	10
1,025-2,048	11
2,049-4,096	12
4,097-8,192	13
8,193-16,384	14
16,385-32,768	15
32,769-65,536	16

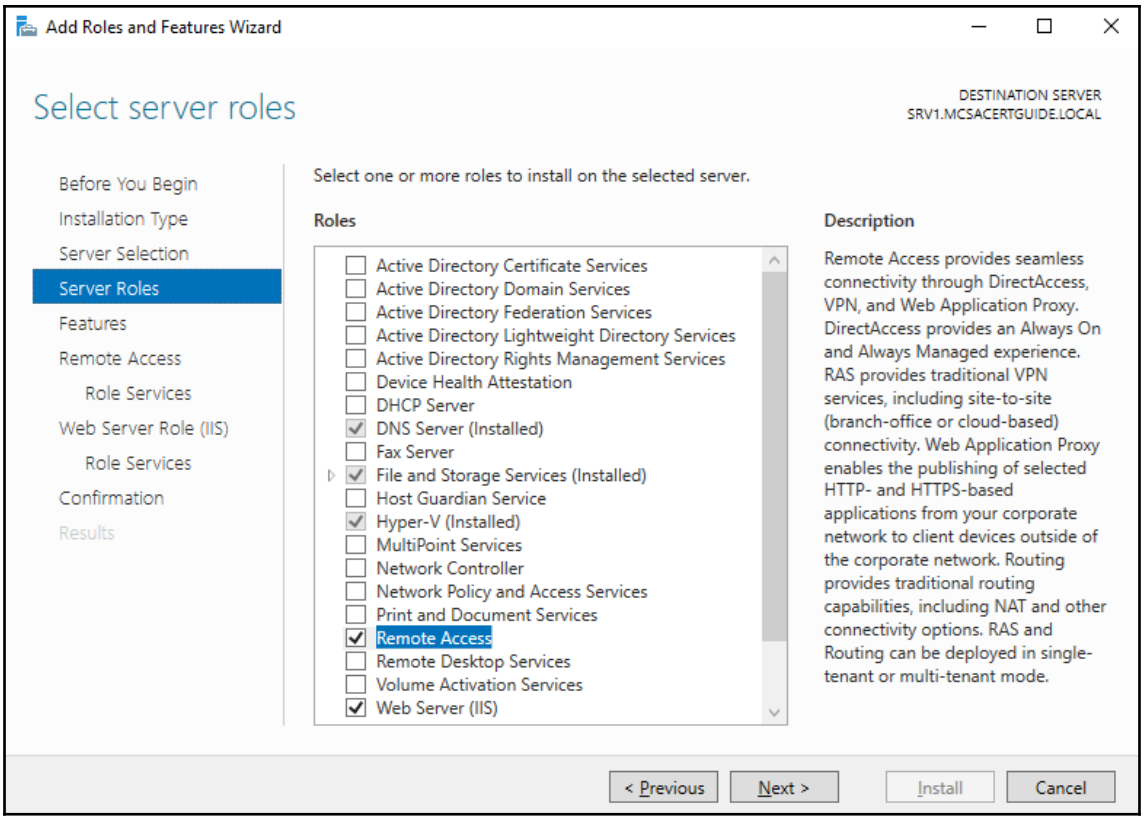
Subnet	Binary Representation	Subnet Address Prefix
1	11000000.10101000.00000000.**000**00000	192.168.0.0/27
2	11000000.10101000.00000000 **001**00000	192.168.0.32/27
3	11000000.10101000.00000000.**010**00000	192.168.0.64/27
4	11000000.10101000.00000000.**011**00000	192.168.0.96/27
5	11000000.10101000.00000000.**100**00000	192.168.0.128/27
6	11000000.10101000.00000000.**101**00000	192.168.0.160/27
7	11000000.10101000.00000000.**110**00000	192.168.0.192/27
8	11000000.10101000.00000000.**111**00000	192.168.0.224/27

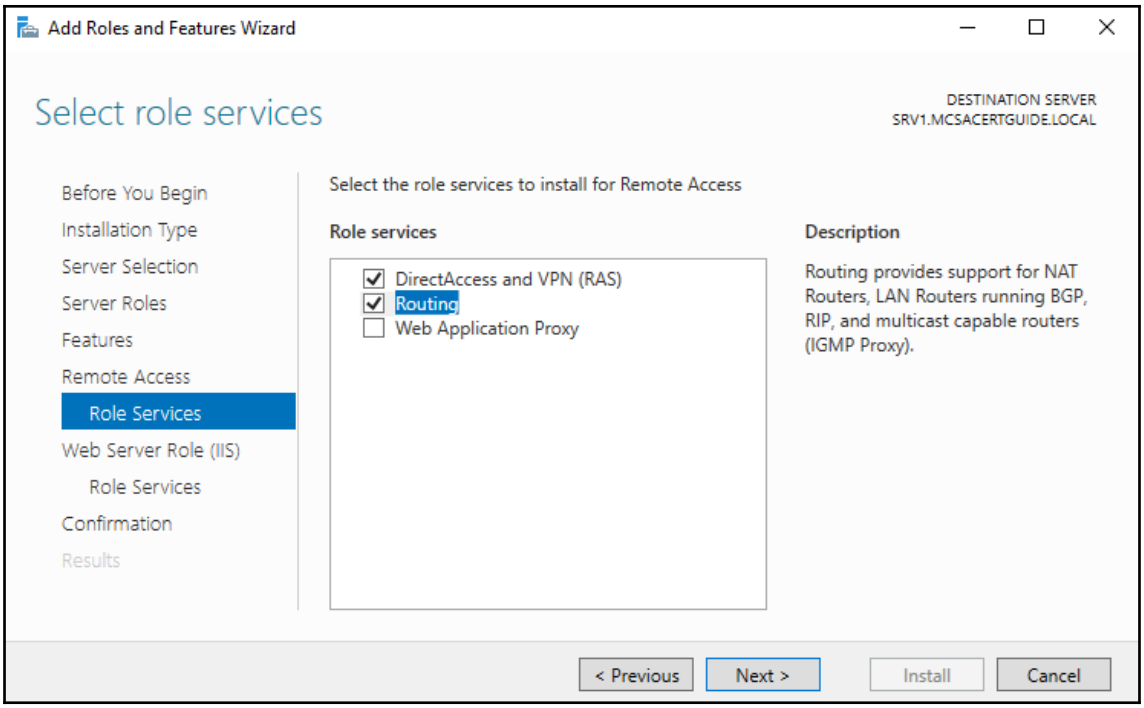
Subnet	Network ID	First Host ID	Last Host ID	Broadcast address
1	192.168.0.0/27	192.168.0.1	192.168.0.30	192.168.0.31
2	192.168.0.32/27	192.168.0.33	192.168.0.62	192.168.0.63
3	192.168.0.64/27	192.168.0.65	192.168.0.94	192.168.0.95
4	192.168.0.96/27	192.168.0.97	192.168.0.126	192.168.0.127
5	192.168.0.128/27	192.168.0.129	192.168.0.158	192.168.0.159
6	192.168.0.160/27	192.168.0.161	192.168.0.190	192.168.0.191
7	192.168.0.192/27	192.168.0.193	192.168.0.222	192.168.0.223
8	192.168.0.224/27	192.168.0.225	192.168.0.254	192.168.0.255

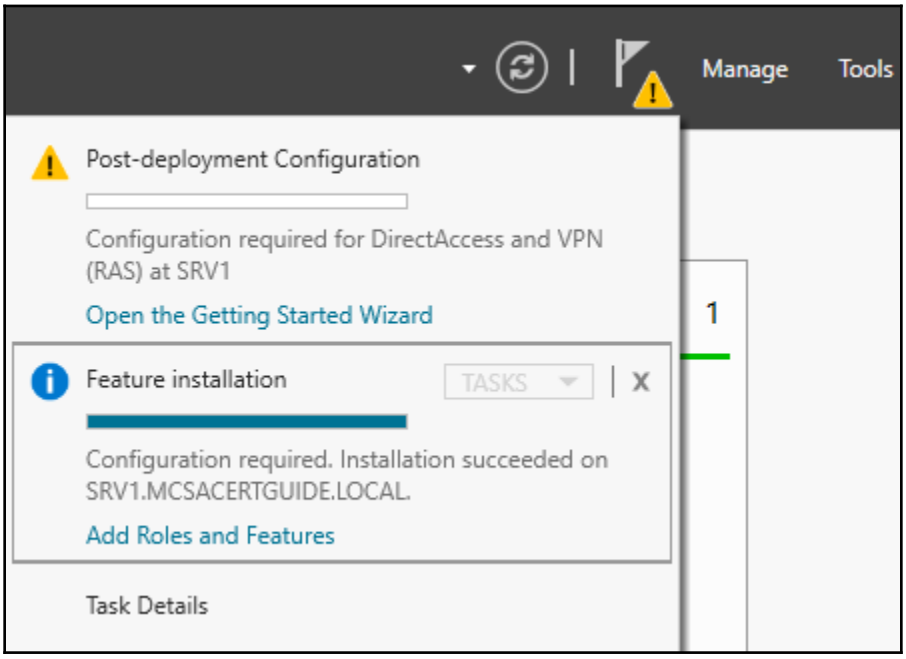
Network Class	Network	Range
A	10.0.0.0/8	10.0.0.0 – 10.255.255.255
B	172.16.0.0/12	172.16.0.0 –172.31.255.255
C	192.168.0.0/16	192.168.0.0 – 192.168.255.255

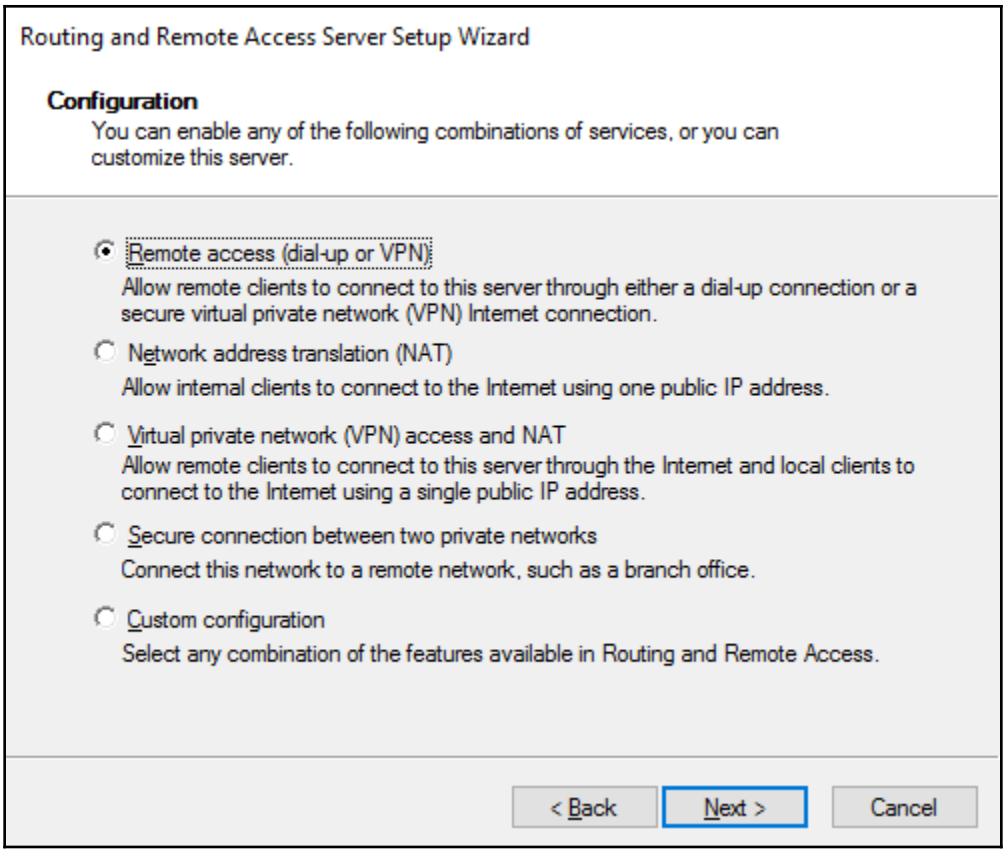
Decimal	Hexadecimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

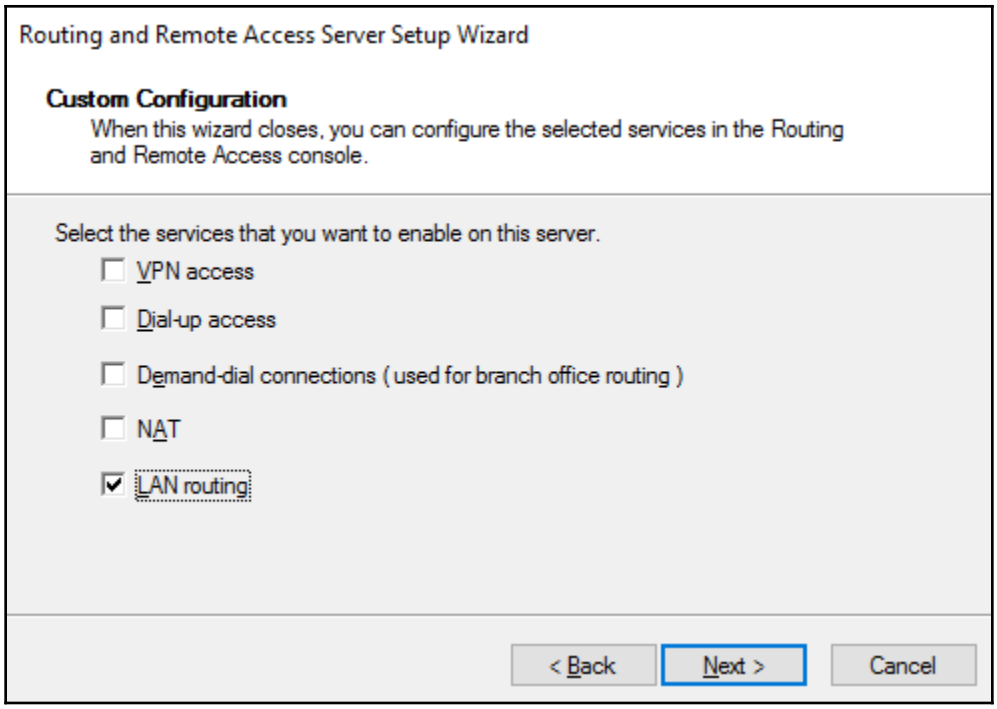
IPv4 Address	IPv6 Address
Internet address classes	No such classes in IPv6
IPv4 multicast addresses (224.0.0.0/4)	IPv6 multicast addresses (FF00::/8)
Broadcast addresses: network broadcast, subnet broadcast, all-subnets directed broadcast, limited broadcast	No such addresses in IPv6
Unspecified address is 0.0.0.0	Unspecified address is ::
Loopback address is 127.0.0.1	Loopback address is ::1
Public IPv4 addresses	Global unicast addresses
Private IPv4 addresses (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16)	Site-local addresses (FEC0::/10)
APIPA addresses (169.254.0.0/16)	Link-local addresses (FE80::/64)
Address syntax: dotted decimal notation	Address syntax: colon hexadecimal format with suppression of leading zeros and zero compression. Embedded IPv4 addresses are expressed in dotted decimal notation.
Address prefix syntax: prefix length or dotted decimal (subnet mask) notation	Address prefix syntax: prefix length notation only

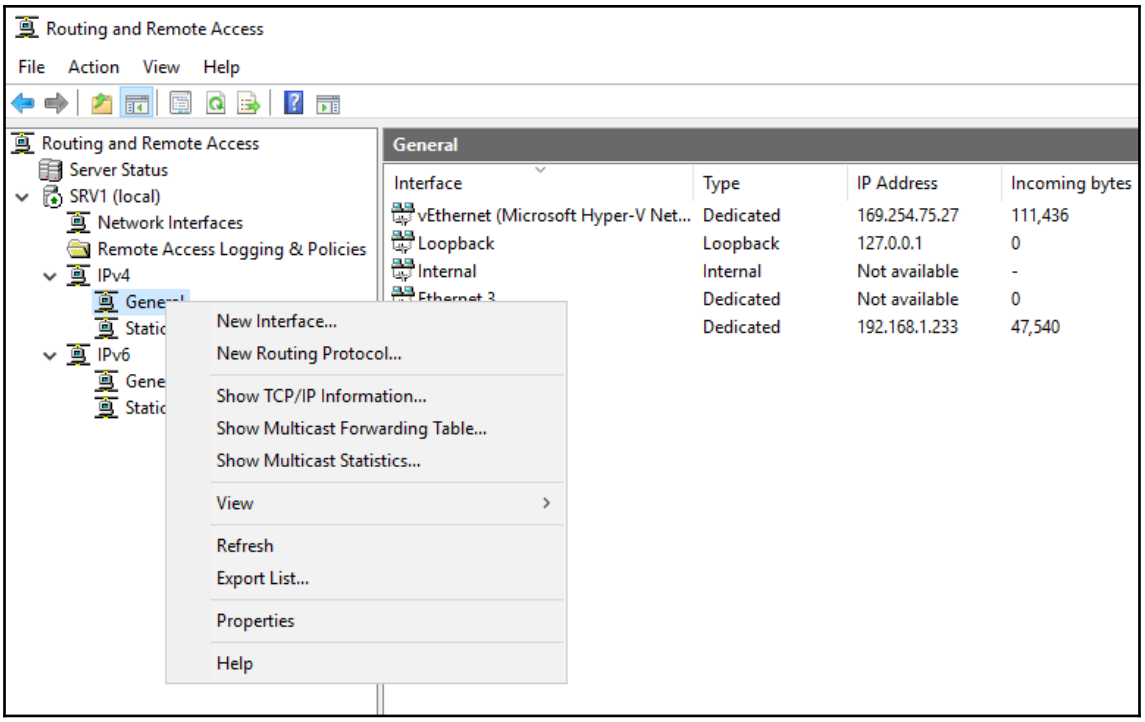

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
SRV1.MCSACERTGUIDE.LOCAL
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server (Installed)
Fax Server
File and Storage Services (Installed)
Host Guardian Service
Hyper-V (Installed)
MultiPoint Services
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Description
Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience. RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.
< Previous
Next >
Install
Cancel

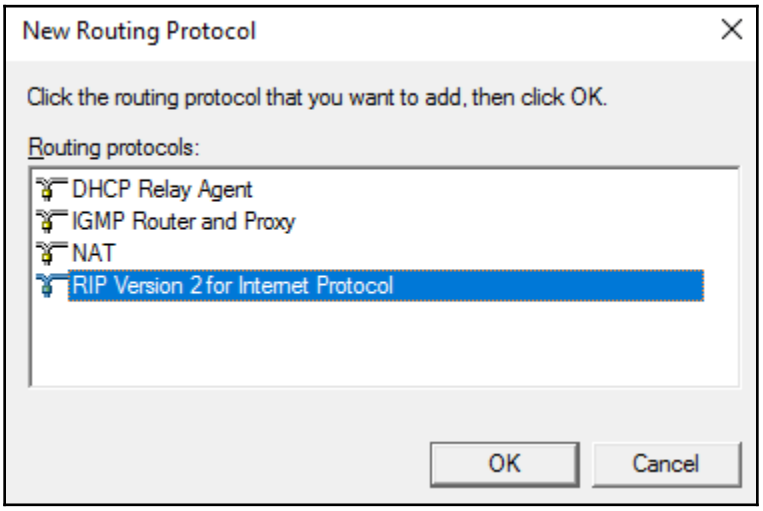

Add Roles and Features Wizard
Select role services
DESTINATION SERVER
SRV1.MCSACERTGUIDE.LOCAL
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Remote Access
Role services
DirectAccess and VPN (RAS)
Routing
Web Application Proxy
Description
Routing provides support for NAT Routers, LAN Routers running BGP, RIP, and multicast capable routers (IGMP Proxy).
< Previous
Next >
Install
Cancel


Manage
Tools
Post-deployment Configuration
Configuration required for DirectAccess and VPN (RAS) at SRV1
Open the Getting Started Wizard
Feature installation
TASKS
Configuration required. Installation succeeded on SRV1.MCSACERTGUIDE.LOCAL.
Add Roles and Features
Task Details
1

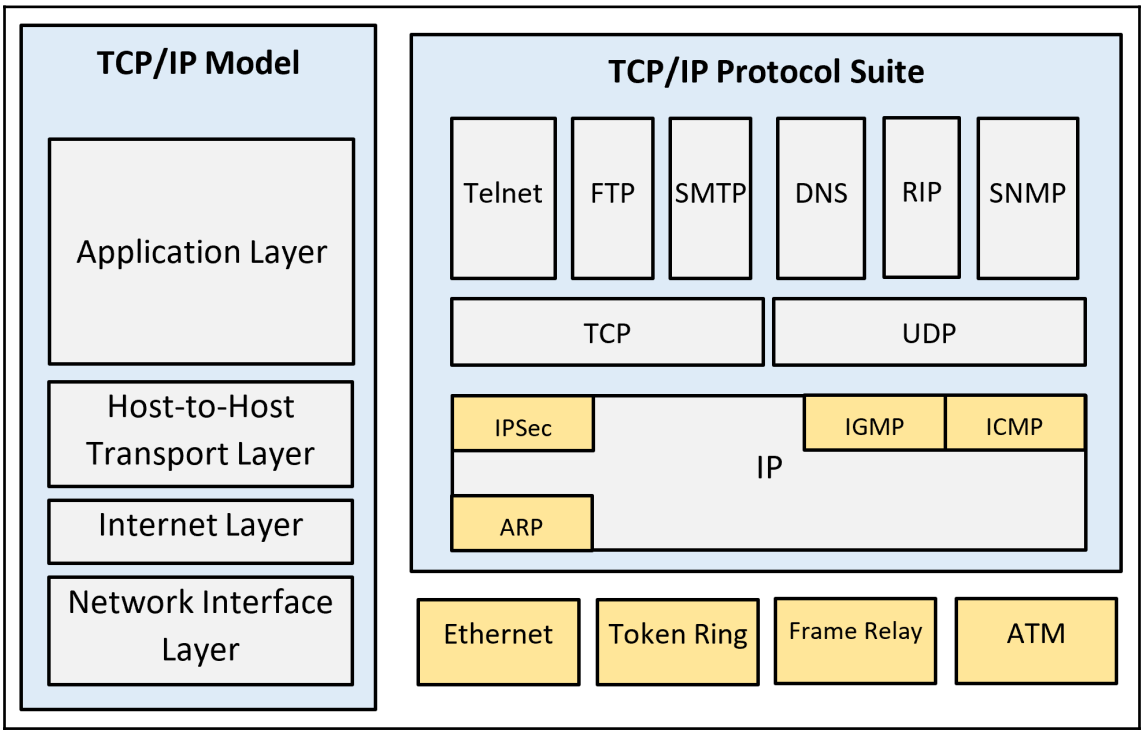

Routing and Remote Access Server Setup Wizard
Configuration
You can enable any of the following combinations of services, or you can customize this server.
Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
Custom configuration
Select any combination of the features available in Routing and Remote Access.
< Back
Next >
Cancel

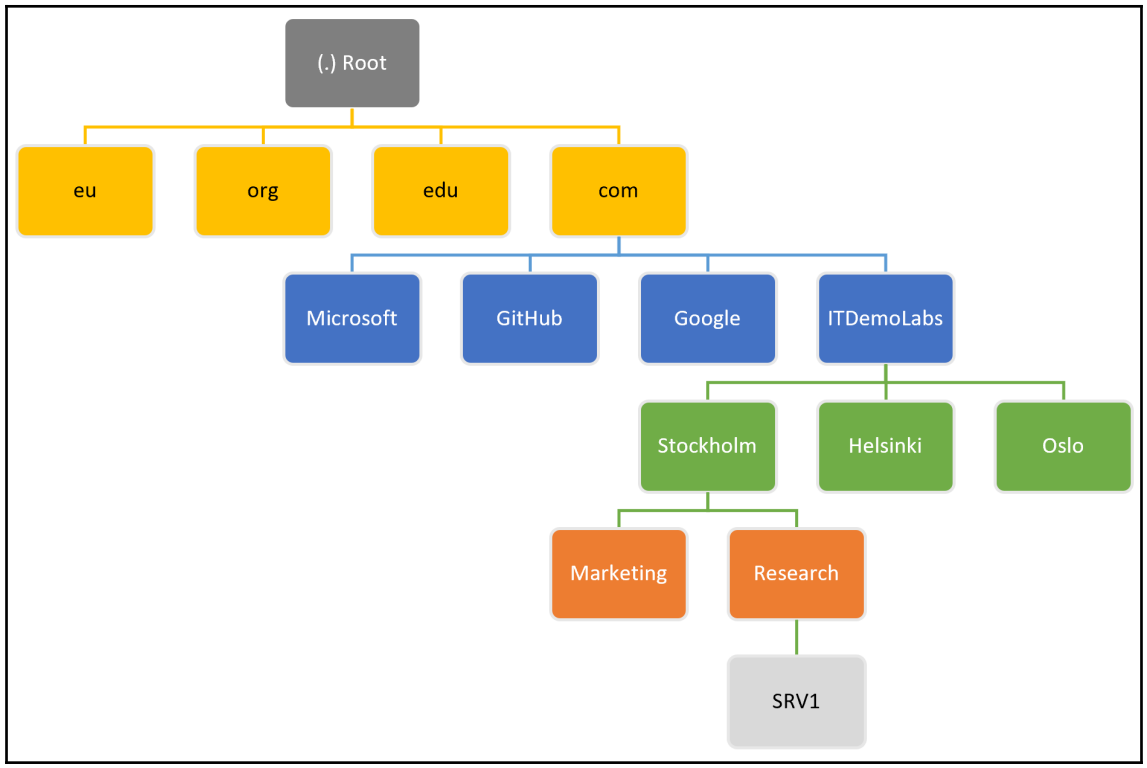

Routing and Remote Access Server Setup Wizard
Custom Configuration
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.
Select the services that you want to enable on this server.
VPN access
Dial-up access
Demand-dial connections (used for branch office routing)
NAT
LAN routing
< Back
Next >
Cancel

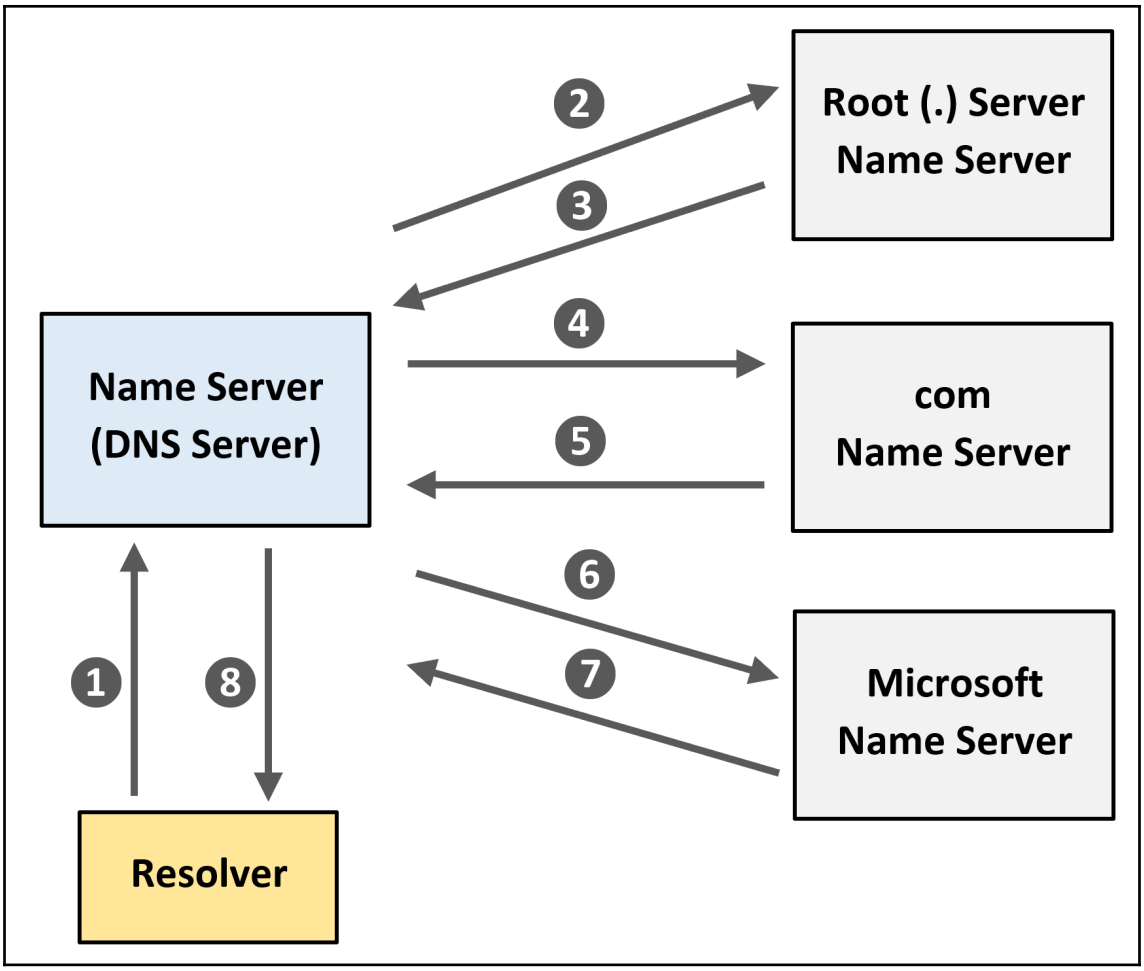

Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
SRV1 (local)
Network Interfaces
Remote Access Logging & Policies
IPv4
IPv6
General
Interface
Type
IP Address
Incoming bytes
vEthernet (Microsoft Hyper-V Net...
Dedicated
169.254.75.27
111,436
Loopback
Loopback
127.0.0.1
0
Internal
Internal
Not available
-
Dedicated
Not available
0
Dedicated
192.168.1.233
47,540
New Interface...
New Routing Protocol...
Show TCP/IP Information...
Show Multicast Forwarding Table...
Show Multicast Statistics...
View
Refresh
Export List...
Properties
Help

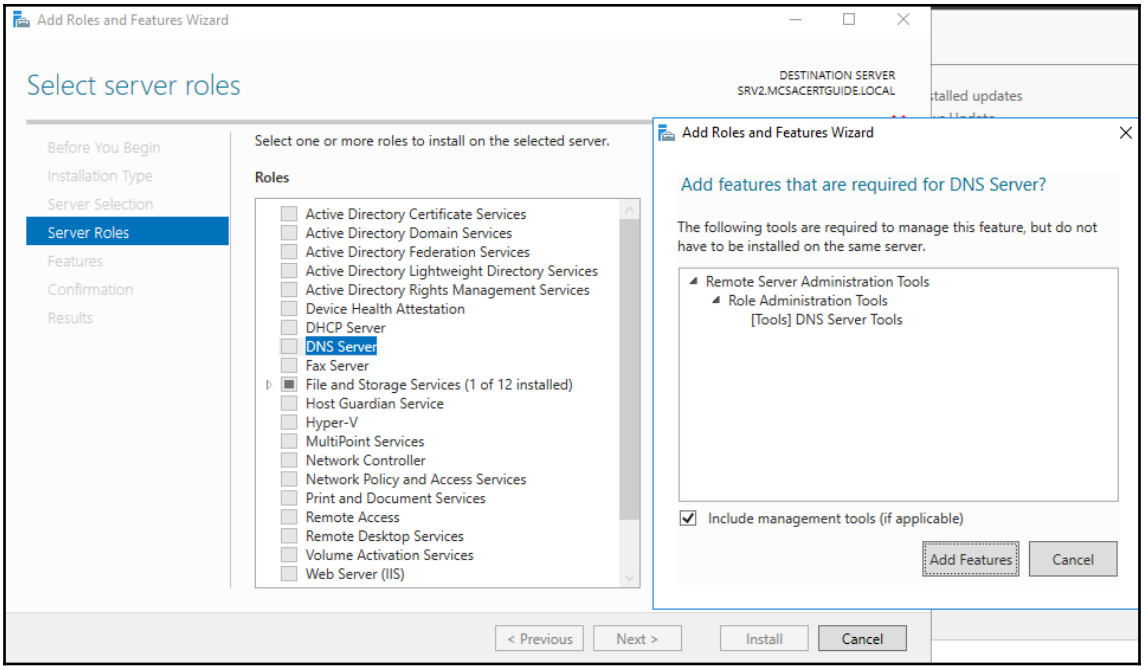

New Routing Protocol
Click the routing protocol that you want to add, then click OK.
Routing protocols:
DHCP Relay Agent
IGMP Router and Proxy
NAT
RIP Version 2 for Internet Protocol
OK
Cancel

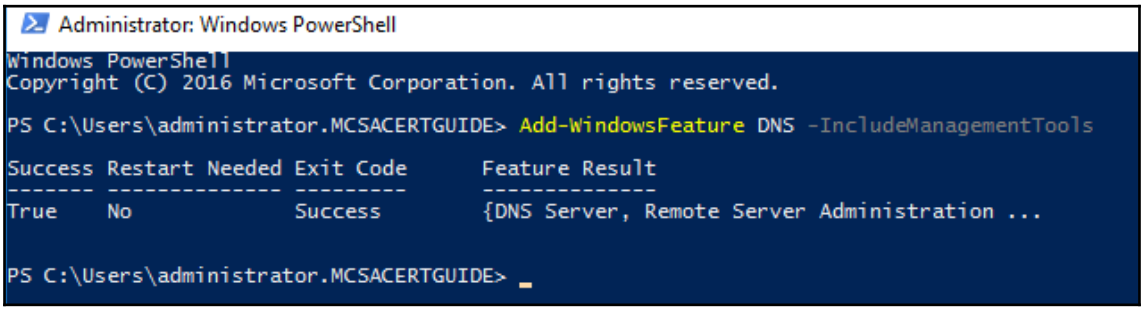
Chapter 2: Configuring DNS

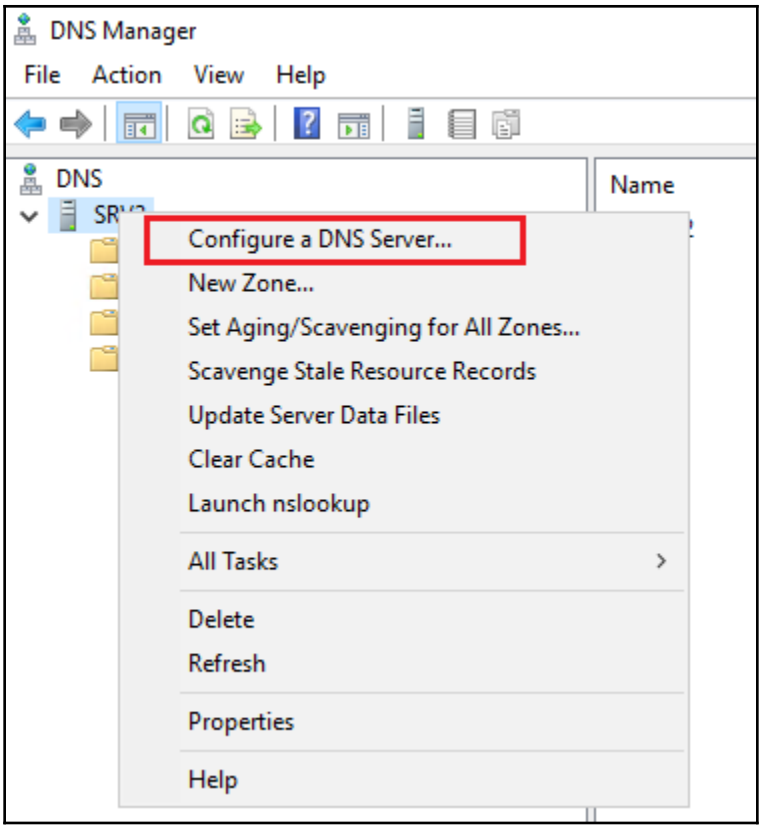


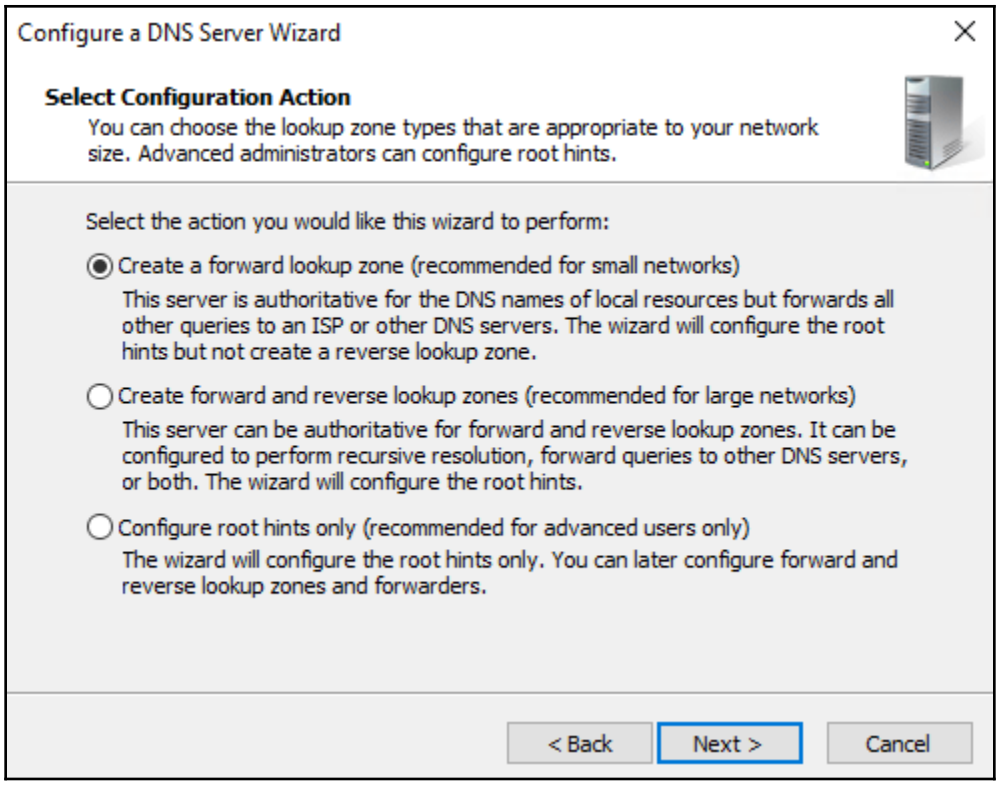

(.) Root
eu
org
edu
com
Microsoft
GitHub
Google
ITDemoLabs
Stockholm
Helsinki
Oslo
Marketing
Research
SRV1

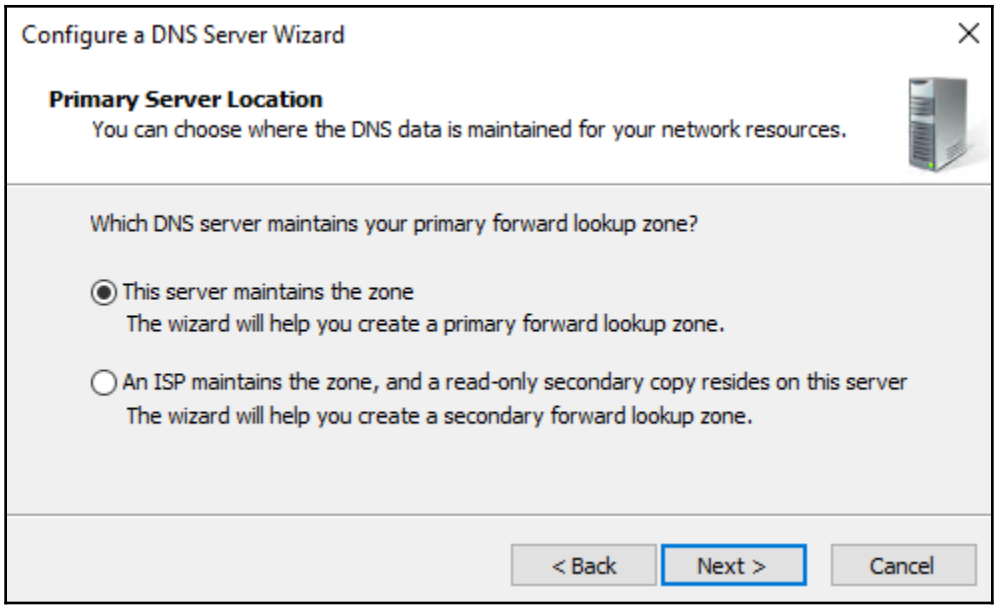

Root (.) Server
Name Server
2
3
Name Server
(DNS Server)
4
com
Name Server
5
6
1
8
7
Microsoft
Name Server
Resolver

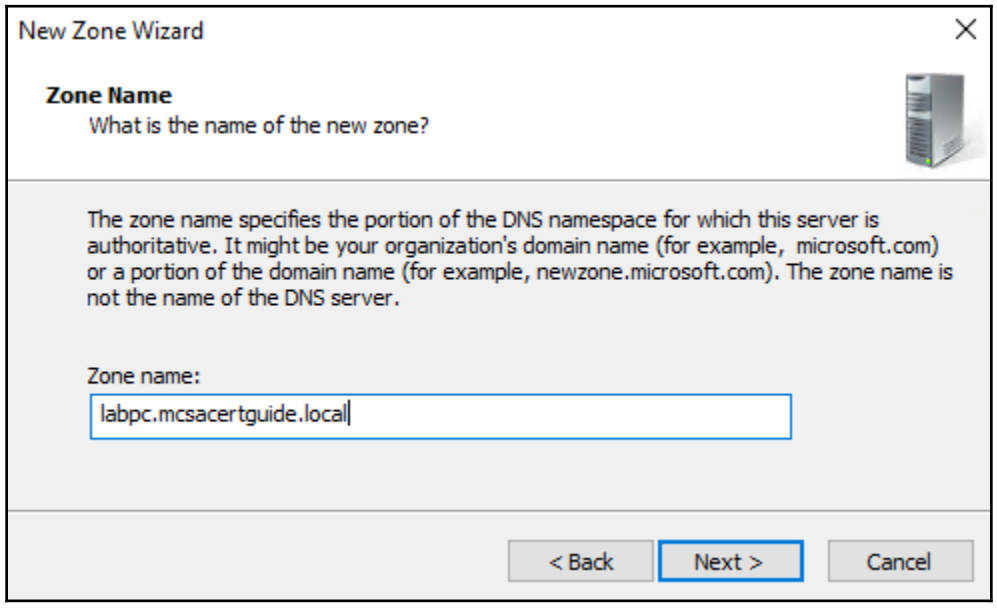

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
SRV2.MCSACERTGUIDE.LOCAL
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
< Previous
Next >
Install
Cancel
Add Roles and Features Wizard
Add features that are required for DNS Server?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] DNS Server Tools
Include management tools (if applicable)
Add Features
Cancel

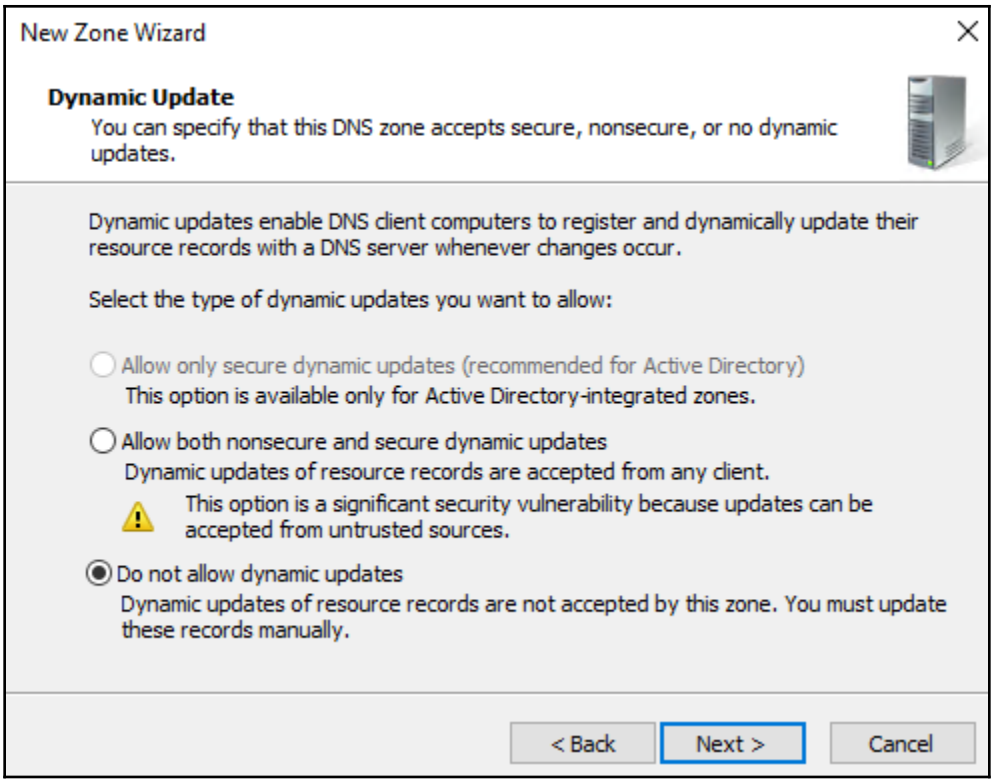

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\administrator.MCSACERTGUIDE> Add-WindowsFeature DNS -IncludeManagementTools
Success Restart Needed Exit Code Feature Result
------- -------------- --------- --------------
True No Success {DNS Server, Remote Server Administration ...
PS C:\Users\administrator.MCSACERTGUIDE>

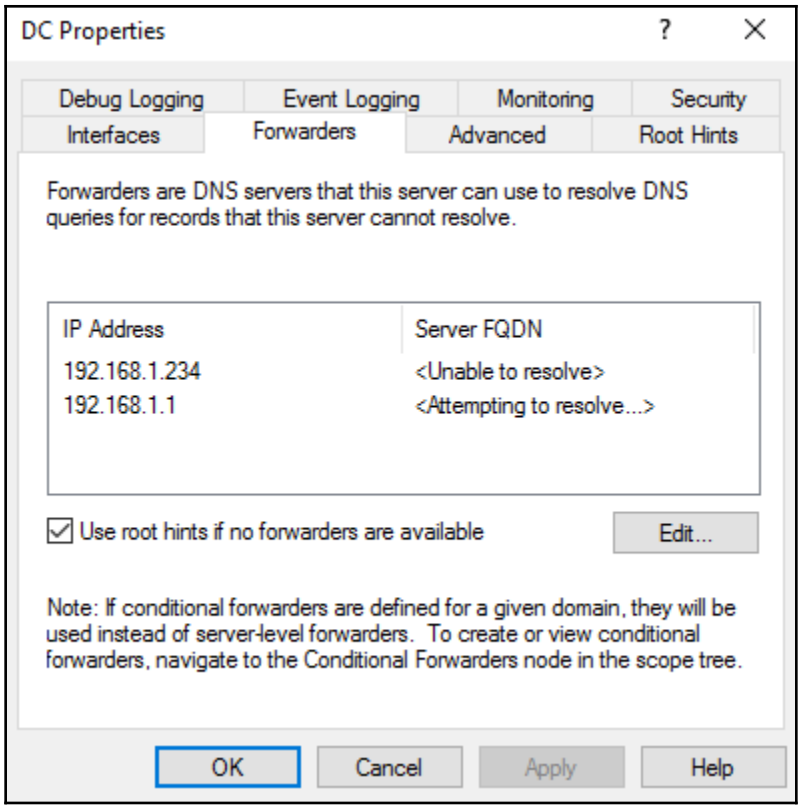

DNS Manager
File
Action
View
Help
DNS
Name
Configure a DNS Server...
New Zone...
Set Aging/Scavenging for All Zones...
Scavenge Stale Resource Records
Update Server Data Files
Clear Cache
Launch nslookup
All Tasks
Delete
Refresh
Properties
Help

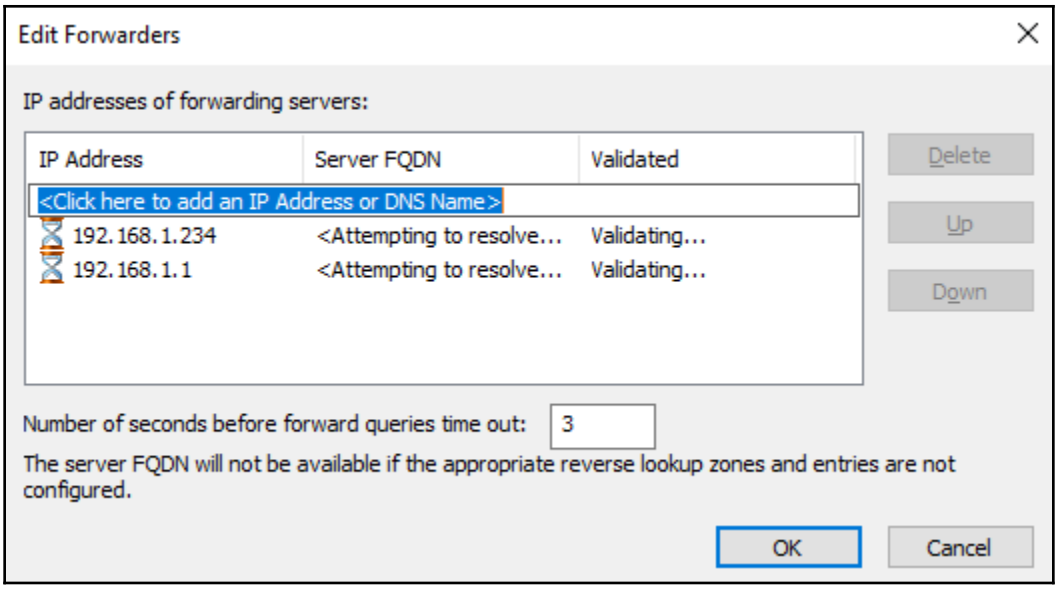

Configure a DNS Server Wizard
Select Configuration Action
You can choose the lookup zone types that are appropriate to your network size. Advanced administrators can configure root hints.
Select the action you would like this wizard to perform:
Create a forward lookup zone (recommended for small networks)
This server is authoritative for the DNS names of local resources but forwards all other queries to an ISP or other DNS servers. The wizard will configure the root hints but not create a reverse lookup zone.
Create forward and reverse lookup zones (recommended for large networks)
This server can be authoritative for forward and reverse lookup zones. It can be configured to perform recursive resolution, forward queries to other DNS servers, or both. The wizard will configure the root hints.
Configure root hints only (recommended for advanced users only)
The wizard will configure the root hints only. You can later configure forward and reverse lookup zones and forwarders.
< Back
Next >
Cancel

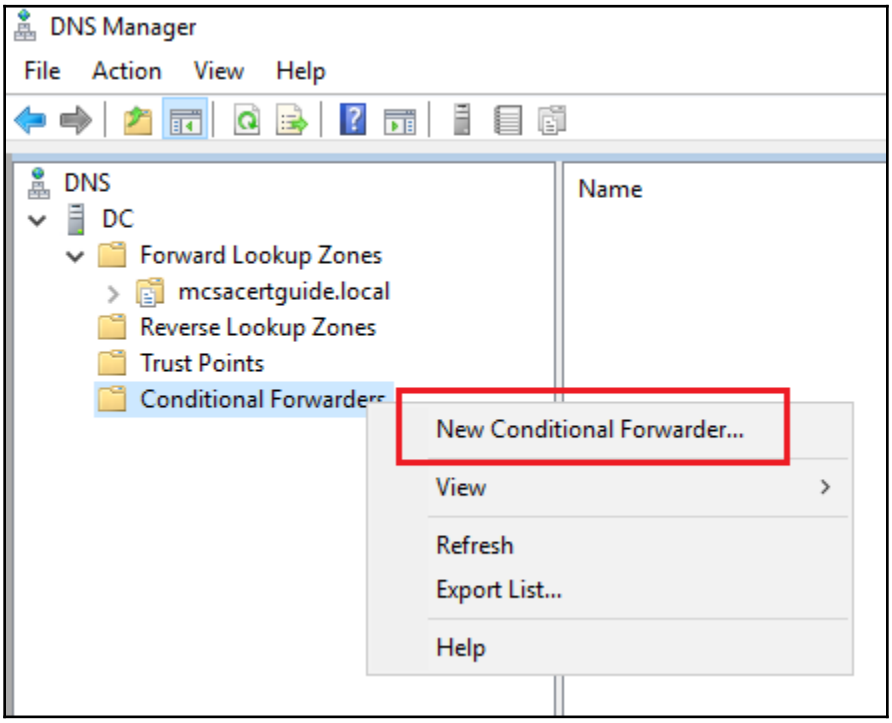

Configure a DNS Server Wizard
Primary Server Location
You can choose where the DNS data is maintained for your network resources.
Which DNS server maintains your primary forward lookup zone?
This server maintains the zone
The wizard will help you create a primary forward lookup zone.
An ISP maintains the zone, and a read-only secondary copy resides on this server
The wizard will help you create a secondary forward lookup zone.
< Back
Next >
Cancel

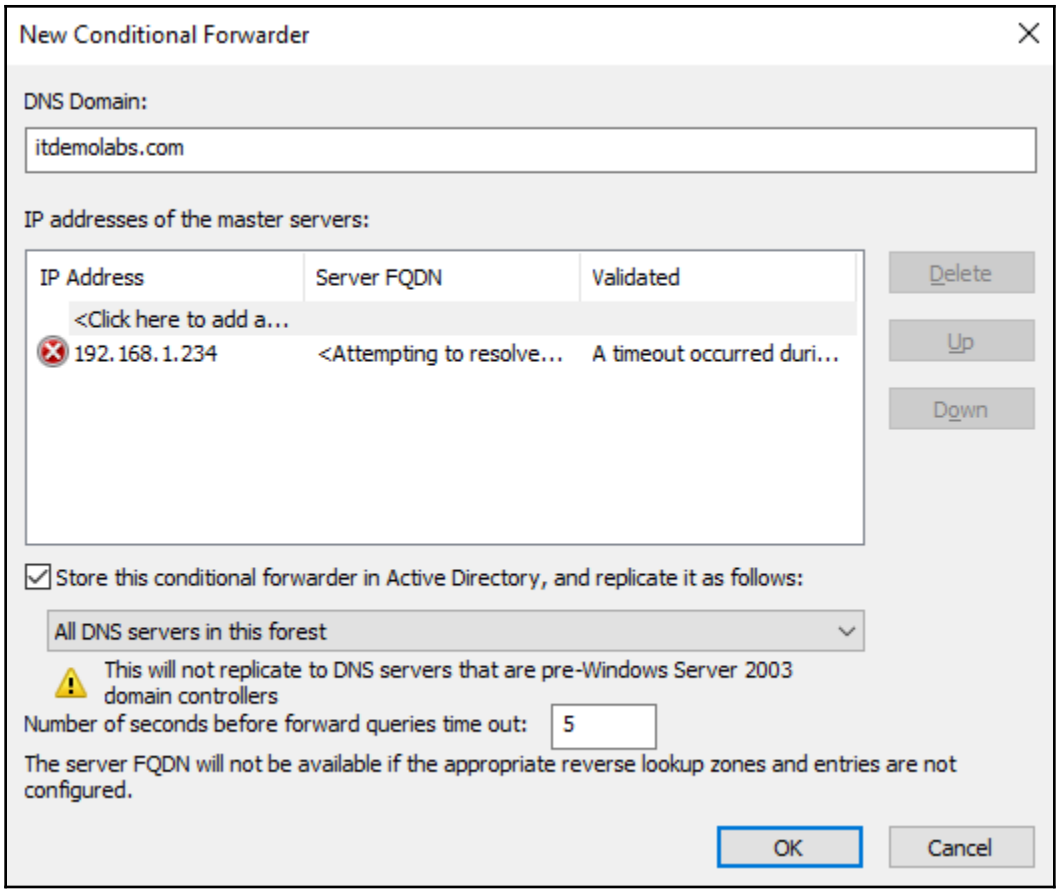

New Zone Wizard
Zone Name
What is the name of the new zone?
The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.
Zone name:
labpc.mcsacertguide.local
< Back
Next >
Cancel

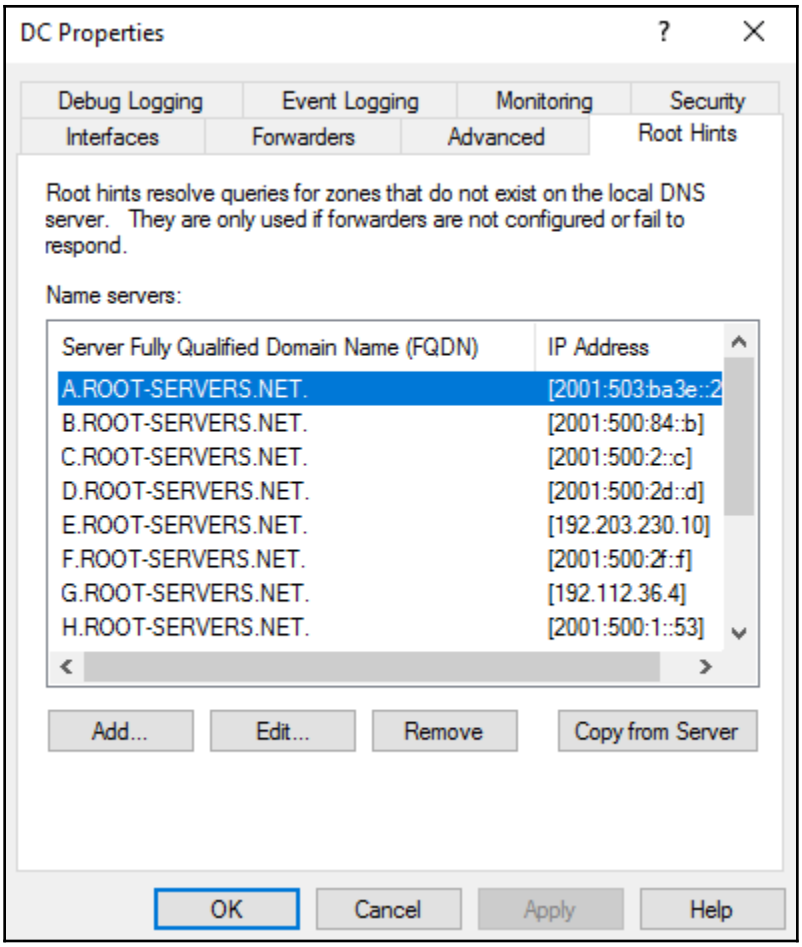

New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back
Next >
Cancel

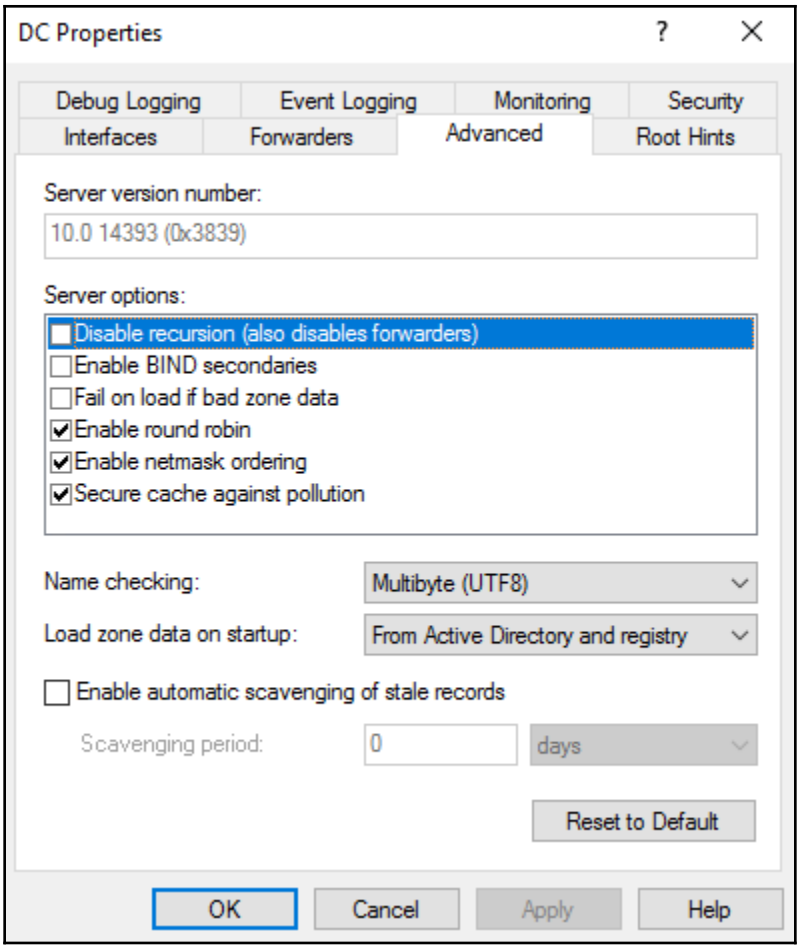

DC Properties
Debug Logging
Event Logging
Monitoring
Security
Interfaces
Forwarders
Advanced
Root Hints
Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.
IP Address
Server FQDN
192.168.1.234
<Unable to resolve>
192.168.1.1
<Attempting to resolve...>
Use root hints if no forwarders are available
Edit...
Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.
OK
Cancel
Apply
Help

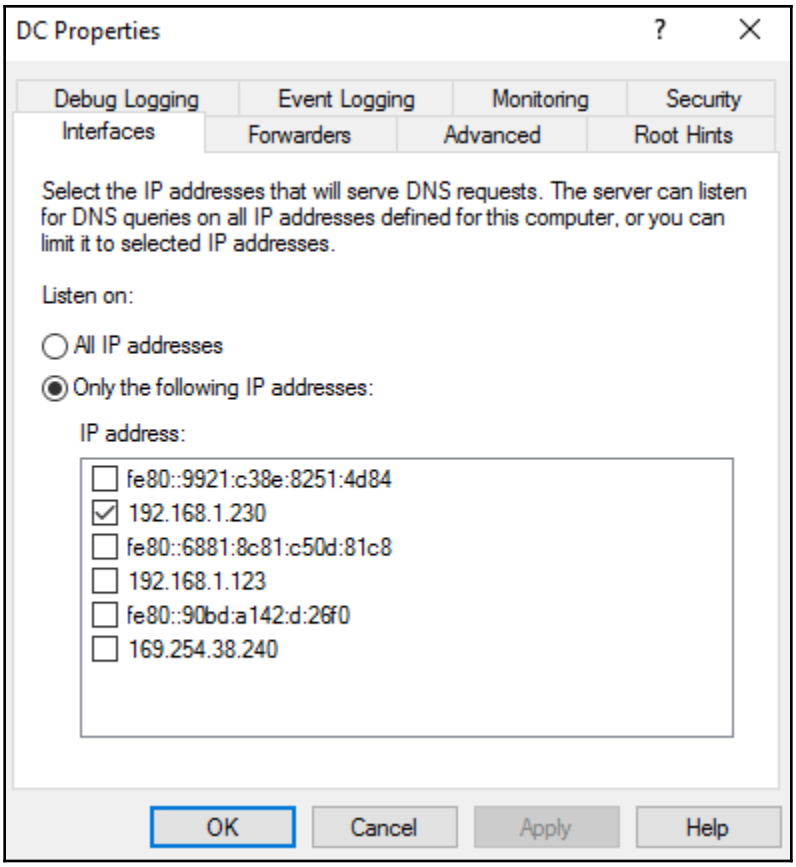

Edit Forwarders
IP addresses of forwarding servers:
IP Address
Server FQDN
Validated
<Click here to add an IP Address or DNS Name>
192.168.1.234
<Attempting to resolve...
Validating...
192.168.1.1
<Attempting to resolve...
Validating...
Delete
Up
Down
Number of seconds before forward queries time out:
3
The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.
OK
Cancel

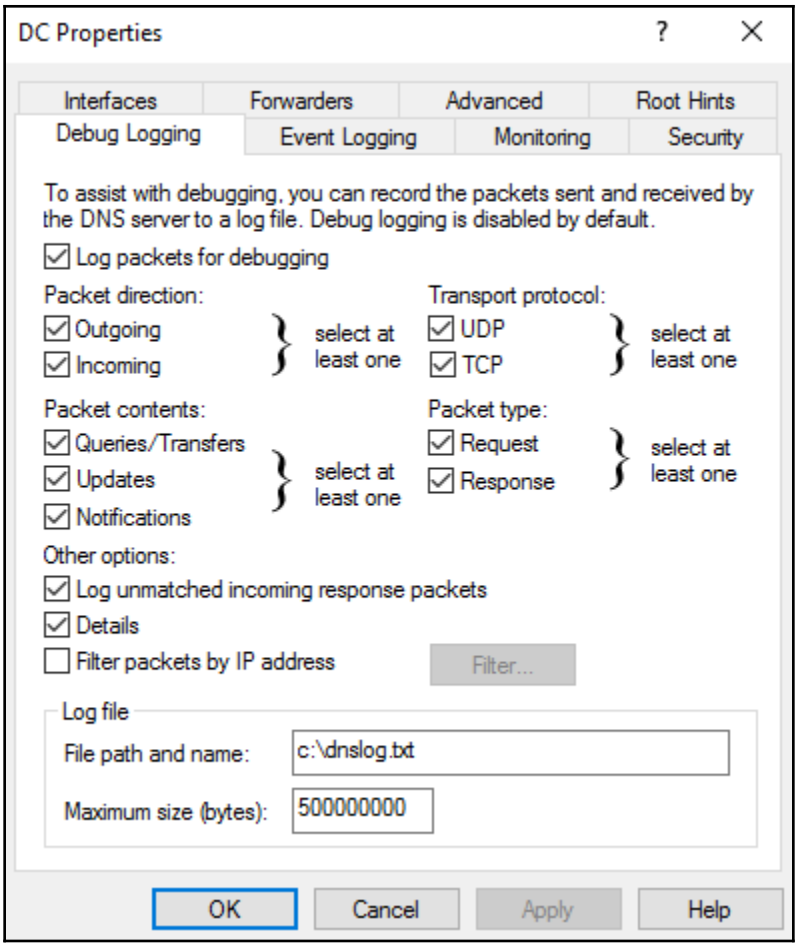

DNS Manager
File
Action
View
Help
DNS
DC
Forward Lookup Zones
mcsacertguide.local
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Name
New Conditional Forwarder...
View
Refresh
Export List...
Help

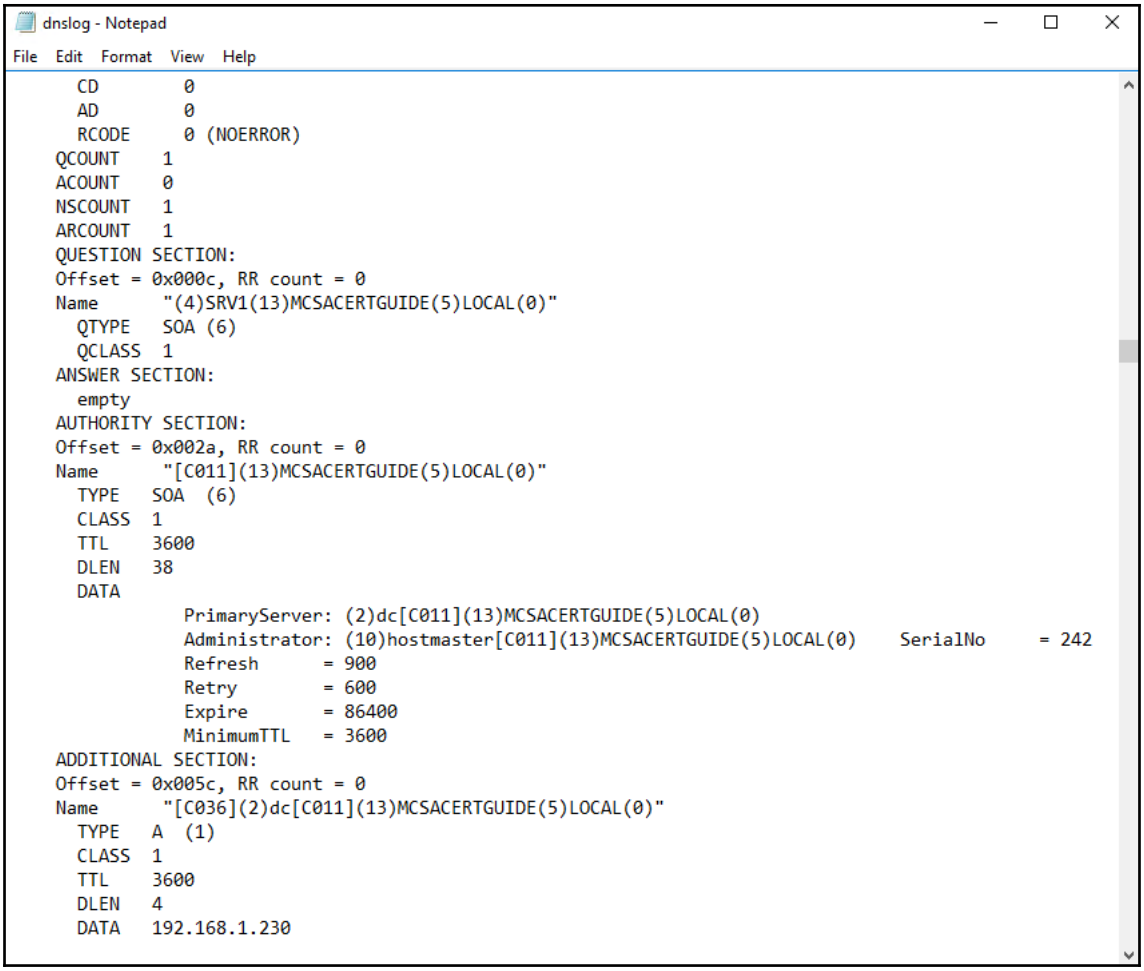

New Conditional Forwarder
DNS Domain:
itdemolabs.com
IP addresses of the master servers:
IP Address
Server FQDN
Validated
<Click here to add a...
192.168.1.234
<Attempting to resolve...
A timeout occurred duri...
Delete
Up
Down
Store this conditional forwarder in Active Directory, and replicate it as follows:
All DNS servers in this forest
This will not replicate to DNS servers that are pre-Windows Server 2003 domain controllers
Number of seconds before forward queries time out:
5
The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.
OK
Cancel

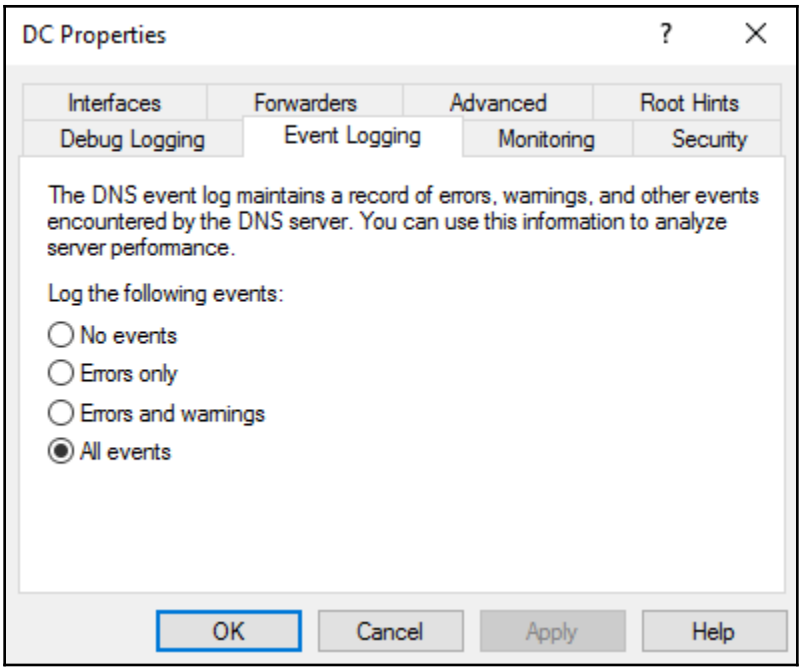

DC Properties
?
Debug Logging
Event Logging
Monitoring
Security
Interfaces
Forwarders
Advanced
Root Hints
Root hints resolve queries for zones that do not exist on the local DNS server. They are only used if forwarders are not configured or fail to respond.
Name servers:
Server Fully Qualified Domain Name (FQDN)
IP Address
A.ROOT-SERVERS.NET. [2001:503:ba3e::2
B.ROOT-SERVERS.NET. [2001:500:84::b]
C.ROOT-SERVERS.NET. [2001:500:2::c]
D.ROOT-SERVERS.NET. [2001:500:2d::d]
E.ROOT-SERVERS.NET. [192.203.230.10]
F.ROOT-SERVERS.NET. [2001:500:2f::f]
G.ROOT-SERVERS.NET. [192.112.36.4]
H.ROOT-SERVERS.NET. [2001:500:1::53]
Add...
Edit...
Remove
Copy from Server
OK
Cancel
Apply
Help

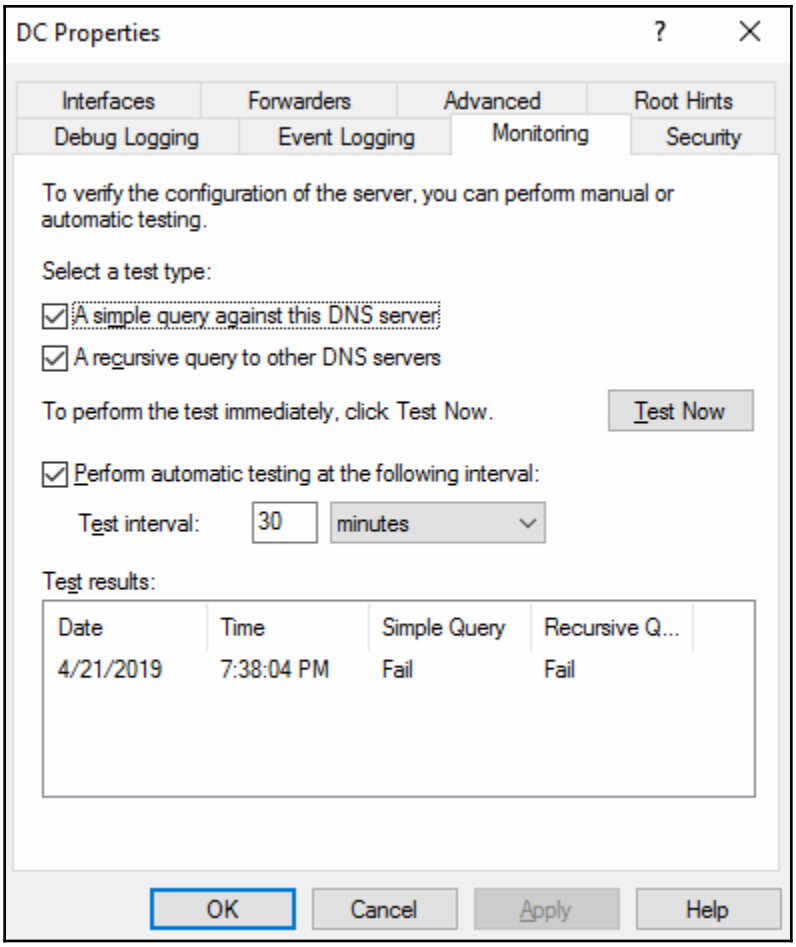

DC Properties
Debug Logging
Event Logging
Monitoring
Security
Interfaces
Forwarders
Advanced
Root Hints
Server version number:
10.0 14393 (0x3839)
Server options:
Disable recursion (also disables forwarders)
Enable BIND secondaries
Fail on load if bad zone data
Enable round robin
Enable netmask ordering
Secure cache against pollution
Name checking:
Multibyte (UTF8)
Load zone data on startup:
From Active Directory and registry
Enable automatic scavenging of stale records
Scavenging period:
0
days
Reset to Default
OK
Cancel
Apply
Help

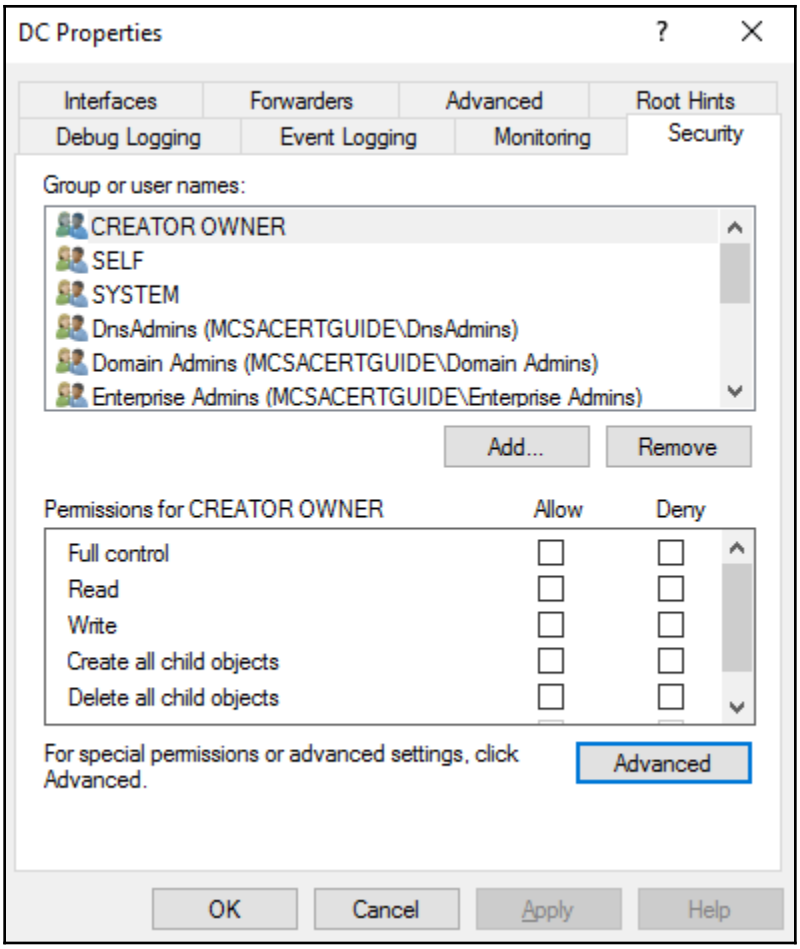

DC Properties
Debug Logging
Event Logging
Monitoring
Security
Interfaces
Forwarders
Advanced
Root Hints
Select the IP addresses that will serve DNS requests. The server can listen for DNS queries on all IP addresses defined for this computer, or you can limit it to selected IP addresses.
Listen on:
All IP addresses
Only the following IP addresses:
IP address:
fe80::9921:c38e:8251:4d84
192.168.1.230
fe80::6881:8c81:c50d:81c8
192.168.1.123
fe80::90bd:a142:d:26f0
169.254.38.240
OK
Cancel
Apply
Help

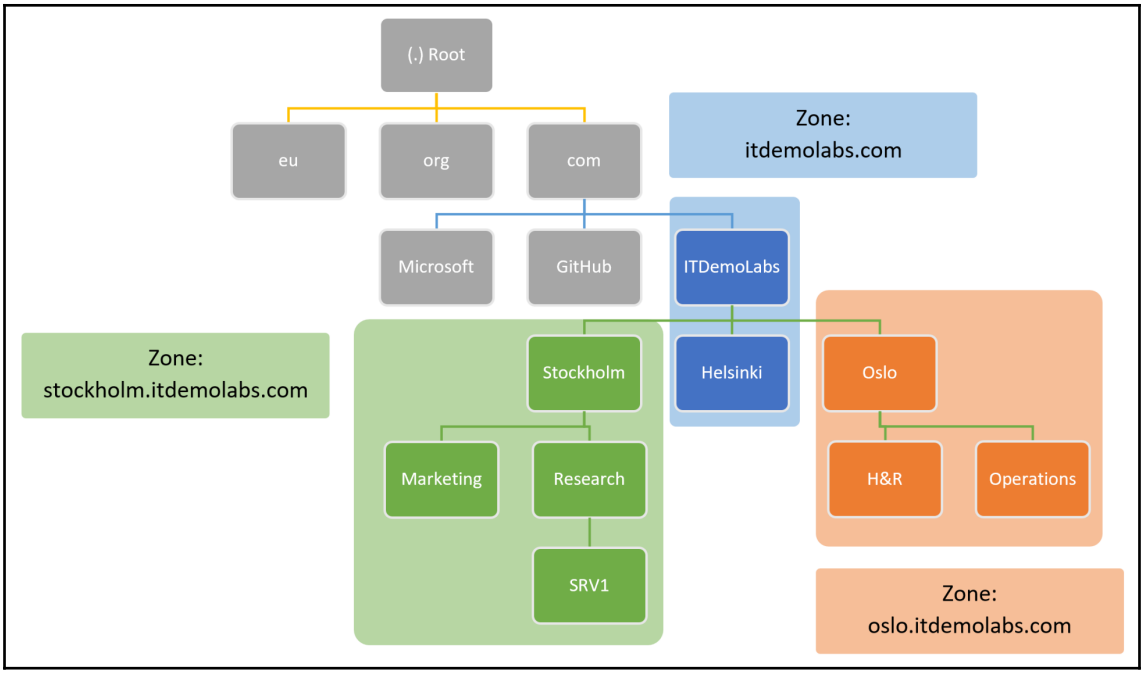

DC Properties
Interfaces
Forwarders
Advanced
Root Hints
Debug Logging
Event Logging
Monitoring
Security
To assist with debugging, you can record the packets sent and received by the DNS server to a log file. Debug logging is disabled by default.
Log packets for debugging
Packet direction:
Outgoing
Incoming
select at least one
Transport protocol:
UDP
TCP
select at least one
Packet contents:
Queries/Transfers
Updates
Notifications
select at least one
Packet type:
Request
Response
select at least one
Other options:
Log unmatched incoming response packets
Details
Filter packets by IP address
Filter...
Log file
File path and name:
c:\dnslog.txt
Maximum size (bytes):
500000000
OK
Cancel
Apply
Help

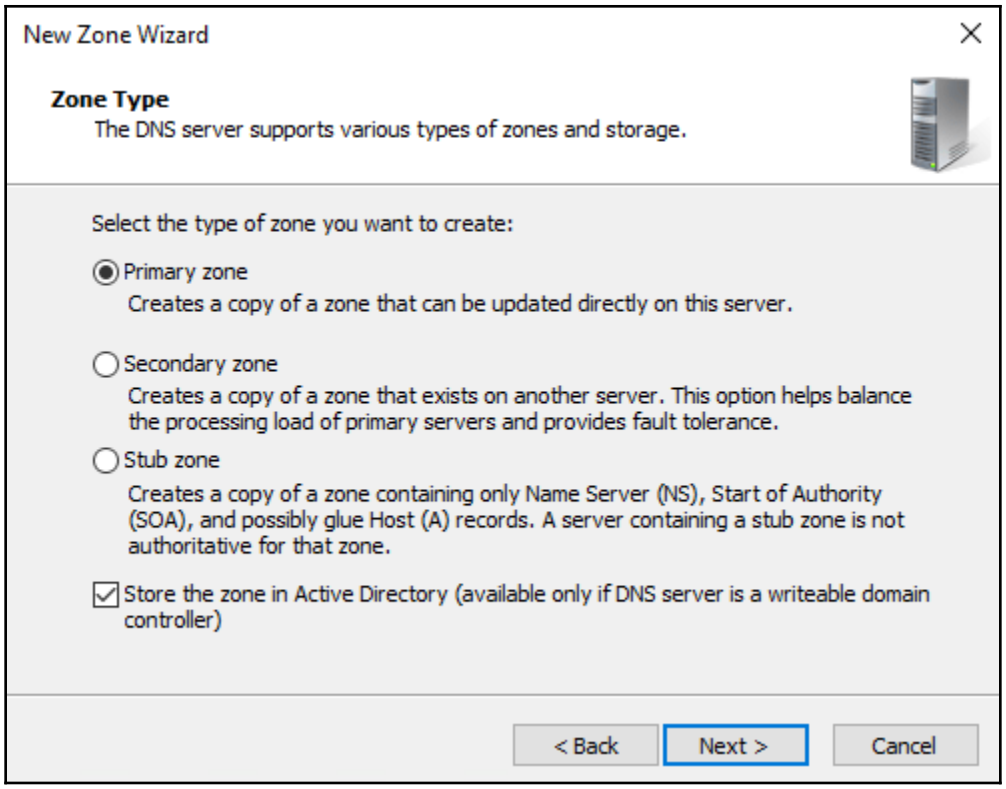

dnslog - Notepad
File Edit Format View Help
CD 0
AD 0
RCODE 0 (NOERROR)
QCOUNT 1
ACOUNT 0
NSCOUNT 1
ARCOUNT 1
QUESTION SECTION:
Offset = 0x000c, RR count = 0
Name "(4)SRV1(13)MCSACERTGUIDE(5)LOCAL(0)"
QTYPE SOA (6)
QCLASS 1
ANSWER SECTION:
empty
AUTHORITY SECTION:
Offset = 0x002a, RR count = 0
Name "[C011](13)MCSACERTGUIDE(5)LOCAL(0)"
TYPE SOA (6)
CLASS 1
TTL 3600
DLEN 38
DATA
PrimaryServer: (2)dc[C011](13)MCSACERTGUIDE(5)LOCAL(0)
Administrator: (10)hostmaster[C011](13)MCSACERTGUIDE(5)LOCAL(0) SerialNo = 242
Refresh = 900
Retry = 600
Expire = 86400
MinimumTTL = 3600
ADDITIONAL SECTION:
Offset = 0x005c, RR count = 0
Name "[C036](2)dc[C011](13)MCSACERTGUIDE(5)LOCAL(0)"
TYPE A (1)
CLASS 1
TTL 3600
DLEN 4
DATA 192.168.1.230

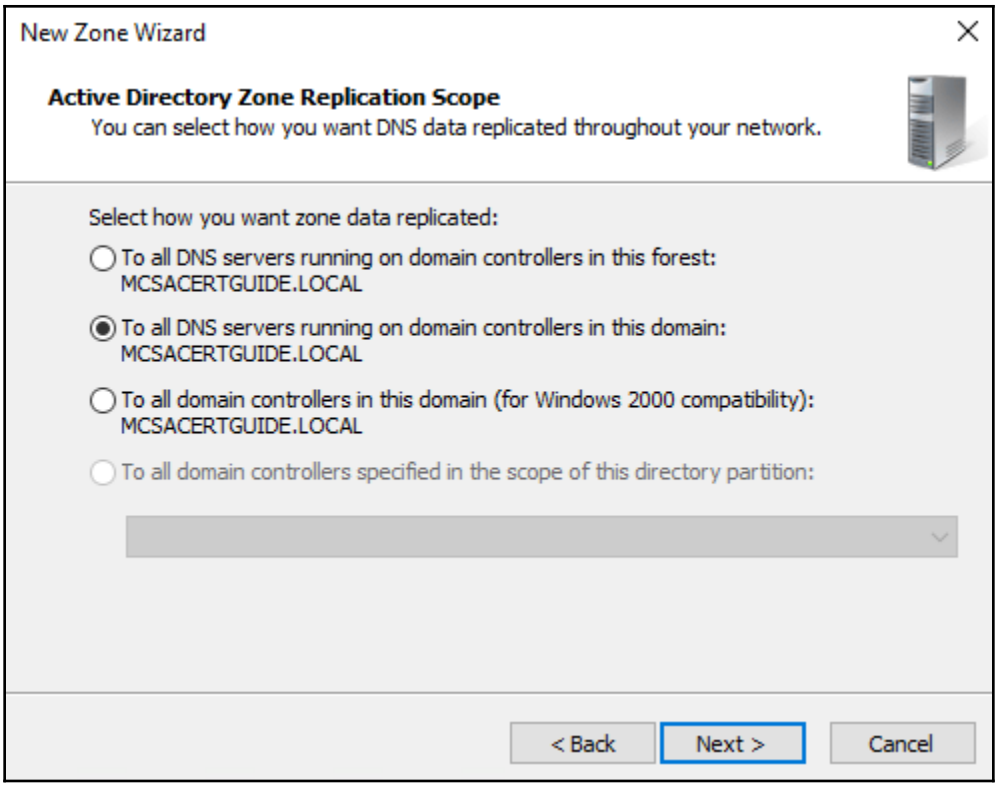

DC Properties
?
Interfaces
Forwarders
Advanced
Root Hints
Debug Logging
Event Logging
Monitoring
Security
The DNS event log maintains a record of errors, warnings, and other events encountered by the DNS server. You can use this information to analyze server performance.
Log the following events:
No events
Errors only
Errors and warnings
All events
OK
Cancel
Apply
Help

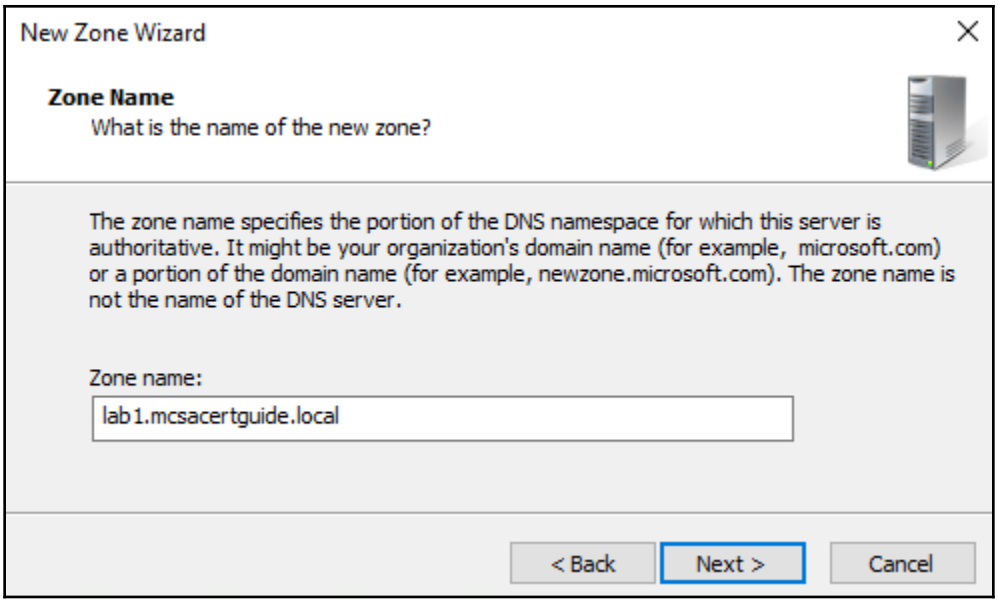

DC Properties
Interfaces
Forwarders
Advanced
Root Hints
Debug Logging
Event Logging
Monitoring
Security
To verify the configuration of the server, you can perform manual or automatic testing.
Select a test type:
A simple query against this DNS server
A recursive query to other DNS servers
To perform the test immediately, click Test Now.
Test Now
Perform automatic testing at the following interval:
Test interval:
30
minutes
Test results:
Date
Time
Simple Query
Recursive Q...
4/21/2019
7:38:04 PM
Fail
Fail
OK
Cancel
Apply
Help

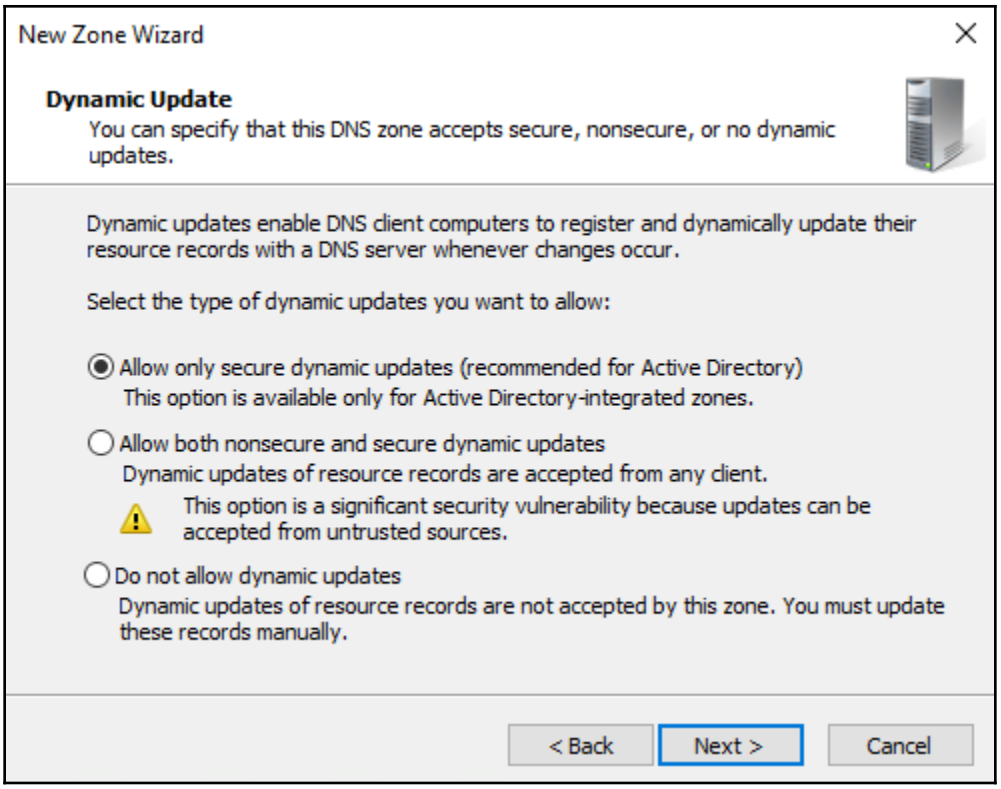

DC Properties
Interfaces
Forwarders
Advanced
Root Hints
Debug Logging
Event Logging
Monitoring
Security
Group or user names:
CREATOR OWNER
SELF
SYSTEM
DnsAdmins (MCSACERTGUIDE\DnsAdmins)
Domain Admins (MCSACERTGUIDE\Domain Admins)
Enterprise Admins (MCSACERTGUIDE\Enterprise Admins)
Add...
Remove
Permissions for CREATOR OWNER
Allow
Deny
Full control
Read
Write
Create all child objects
Delete all child objects
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help

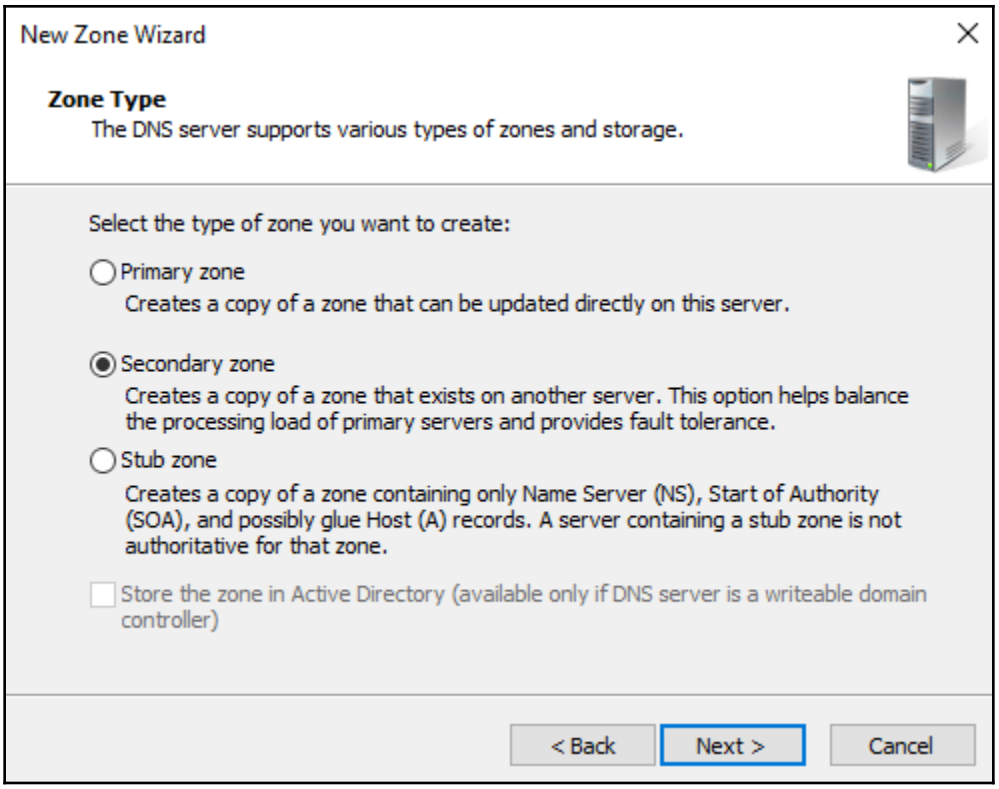

(.) Root
eu
org
com
Zone:
itdemolabs.com
Microsoft
GitHub
ITDemoLabs
Zone:
stockholm.itdemolabs.com
Stockholm
Helsinki
Oslo
Marketing
Research
H&R
Operations
SRV1
Zone:
oslo.itdemolabs.com

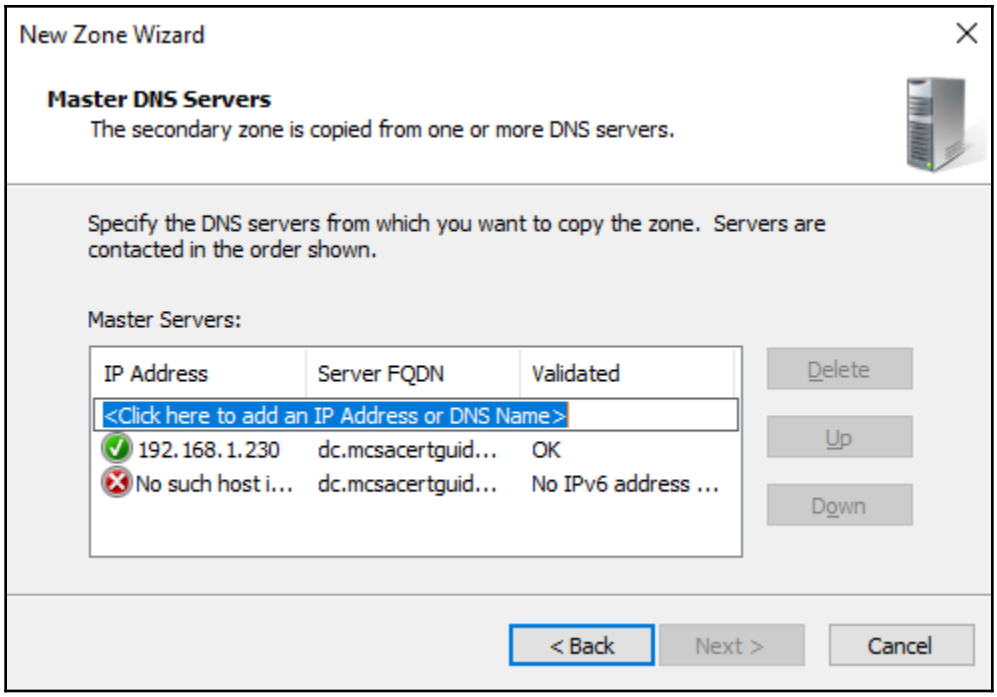

New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
< Back
Next >
Cancel

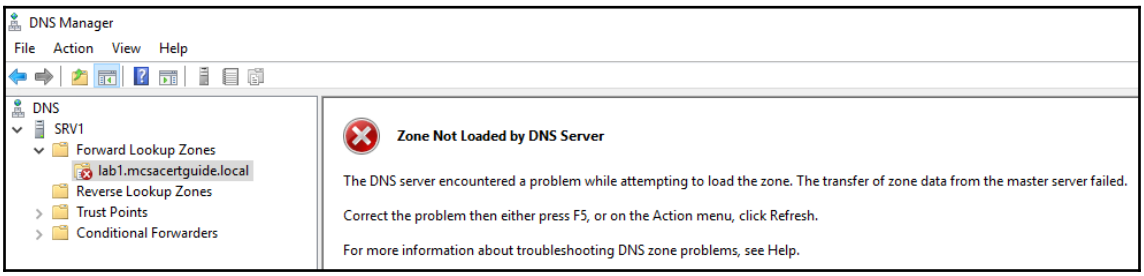

New Zone Wizard
Active Directory Zone Replication Scope
You can select how you want DNS data replicated throughout your network.
Select how you want zone data replicated:
To all DNS servers running on domain controllers in this forest:
MCSACERTGUIDE.LOCAL
To all DNS servers running on domain controllers in this domain:
MCSACERTGUIDE.LOCAL
To all domain controllers in this domain (for Windows 2000 compatibility):
MCSACERTGUIDE.LOCAL
To all domain controllers specified in the scope of this directory partition:
< Back
Next >
Cancel

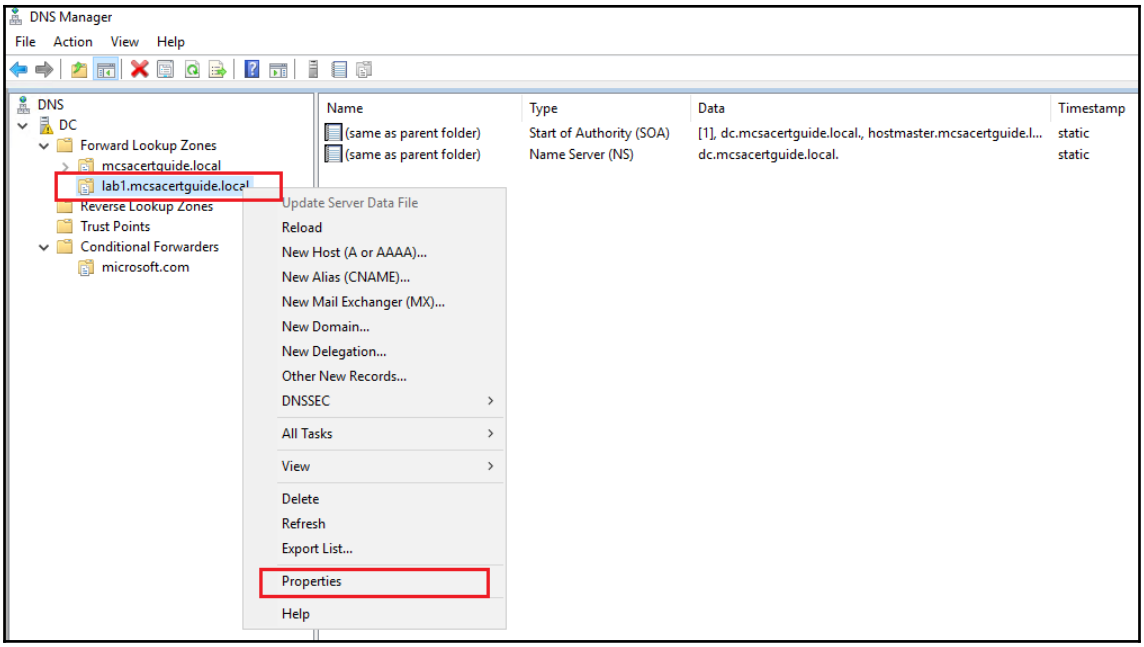

New Zone Wizard
Zone Name
What is the name of the new zone?
The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.
Zone name:
lab1.mcsacertguide.local
< Back
Next >
Cancel

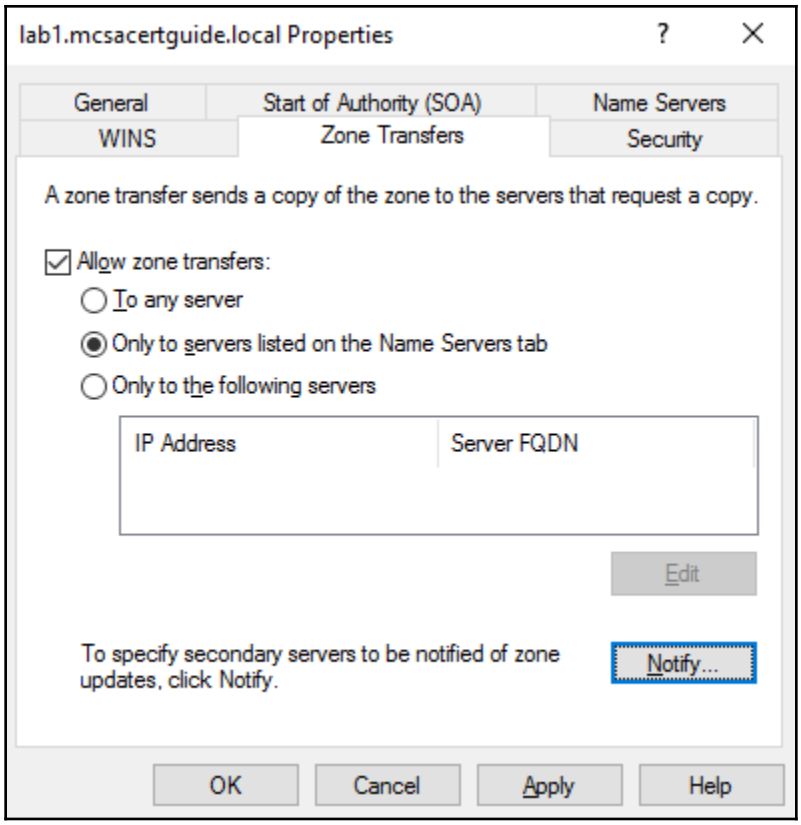

New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back
Next >
Cancel

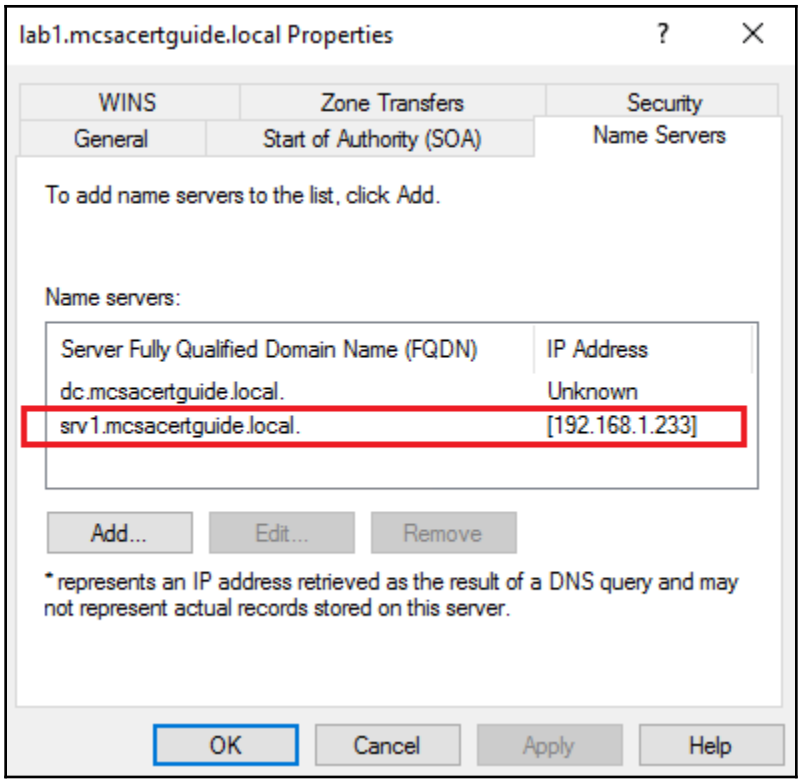

New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
< Back
Next >
Cancel

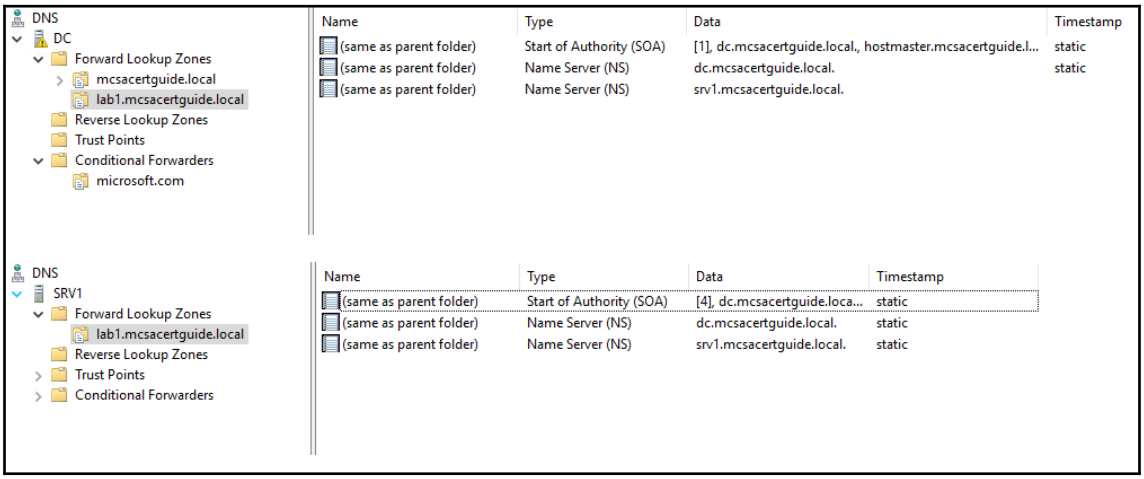

New Zone Wizard
Master DNS Servers
The secondary zone is copied from one or more DNS servers.
Specify the DNS servers from which you want to copy the zone. Servers are contacted in the order shown.
Master Servers:
IP Address
Server FQDN
Validated
<Click here to add an IP Address or DNS Name>
192.168.1.230
dc.mcsacertguid...
OK
No such host i...
dc.mcsacertguid...
No IPv6 address ...
Delete
Up
Down
< Back
Next >
Cancel


DNS Manager
File Action View Help
DNS
SRV1
Forward Lookup Zones
lab1.mcsacertguide.local
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Zone Not Loaded by DNS Server
The DNS server encountered a problem while attempting to load the zone. The transfer of zone data from the master server failed.
Correct the problem then either press F5, or on the Action menu, click Refresh.
For more information about troubleshooting DNS zone problems, see Help.

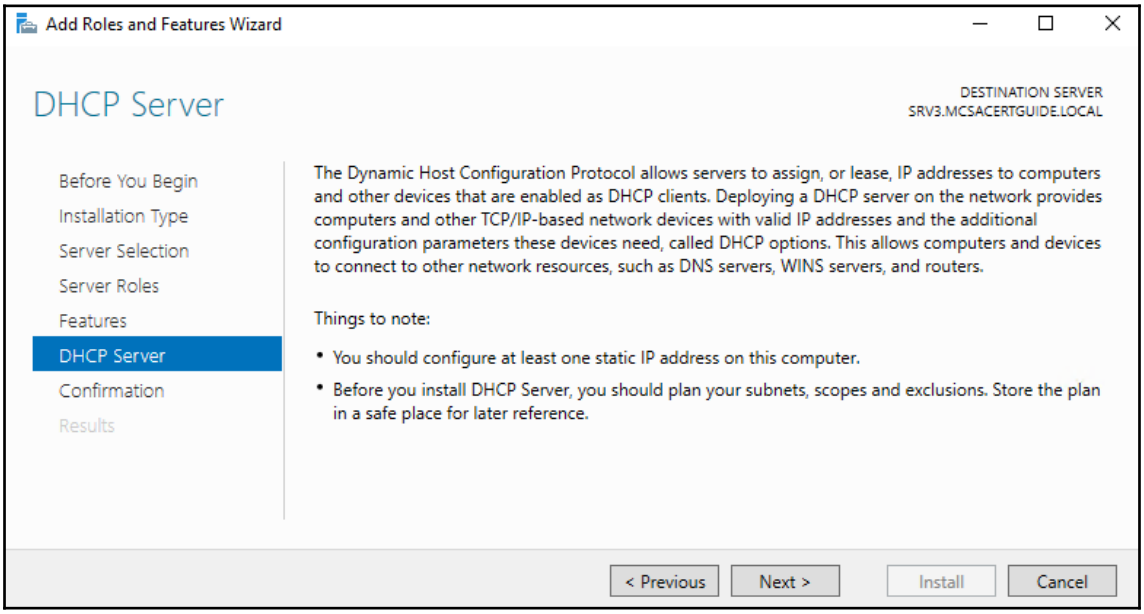

DNS Manager
File Action View Help
DNS
DC
Forward Lookup Zones
mcsacertguide.local
lab1.mcsacertguide.local
Reverse Lookup Zones
Trust Points
Conditional Forwarders
microsoft.com
Name
Type
Data
Timestamp
(same as parent folder)
Start of Authority (SOA)
[1], dc.mcsacertguide.local., hostmaster.mcsacertguide.l...
static
(same as parent folder)
Name Server (NS)
dc.mcsacertguide.local.
static
Update Server Data File
Reload
New Host (A or AAAA)...
New Alias (CNAME)...
New Mail Exchanger (MX)...
New Domain...
New Delegation...
Other New Records...
DNSSEC
All Tasks
View
Delete
Refresh
Export List...
Properties
Help

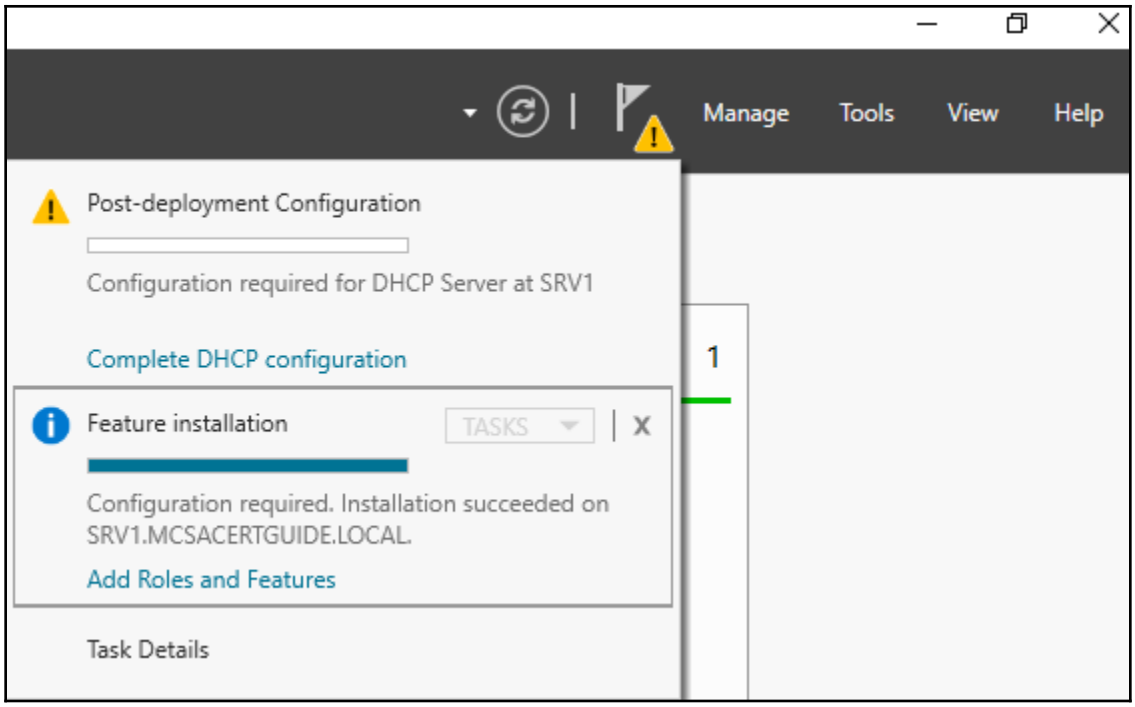

lab1.mcsacertguide.local Properties
General
Start of Authority (SOA)
Name Servers
WINS
Zone Transfers
Security
A zone transfer sends a copy of the zone to the servers that request a copy.
Allow zone transfers:
To any server
Only to servers listed on the Name Servers tab
Only to the following servers
IP Address
Server FQDN
Edit
To specify secondary servers to be notified of zone updates, click Notify.
Notify...
OK
Cancel
Apply
Help

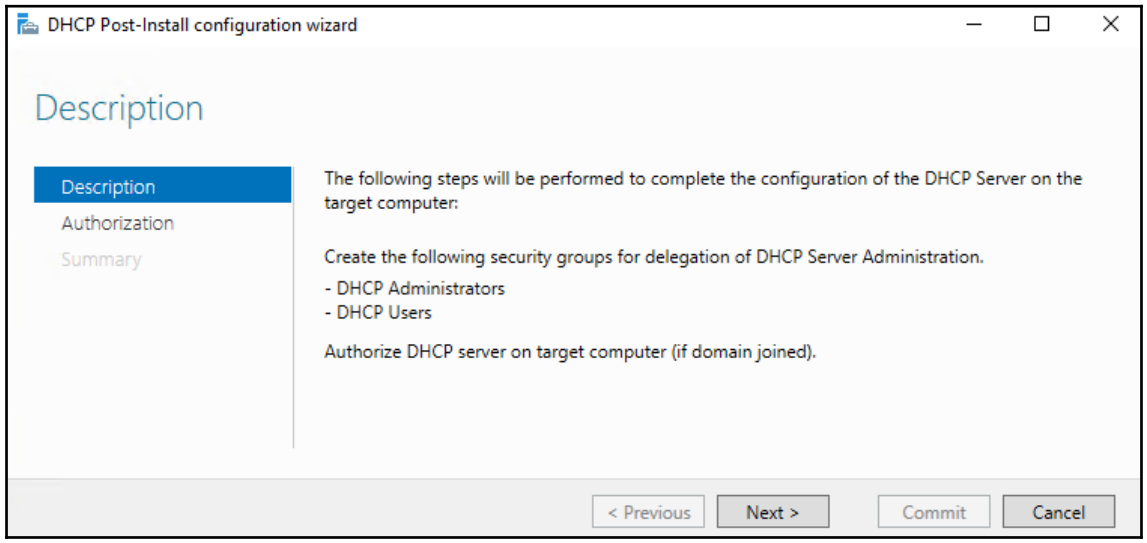

lab1.mcsacertguide.local Properties
WINS
Zone Transfers
Security
General
Start of Authority (SOA)
Name Servers
To add name servers to the list, click Add.
Name servers:
Server Fully Qualified Domain Name (FQDN)
IP Address
dc.mcsacertguide.local.
Unknown
srv1.mcsacertguide.local.
[192.168.1.233]
Add...
Edit...
Remove
* represents an IP address retrieved as the result of a DNS query and may not represent actual records stored on this server.
OK
Cancel
Apply
Help

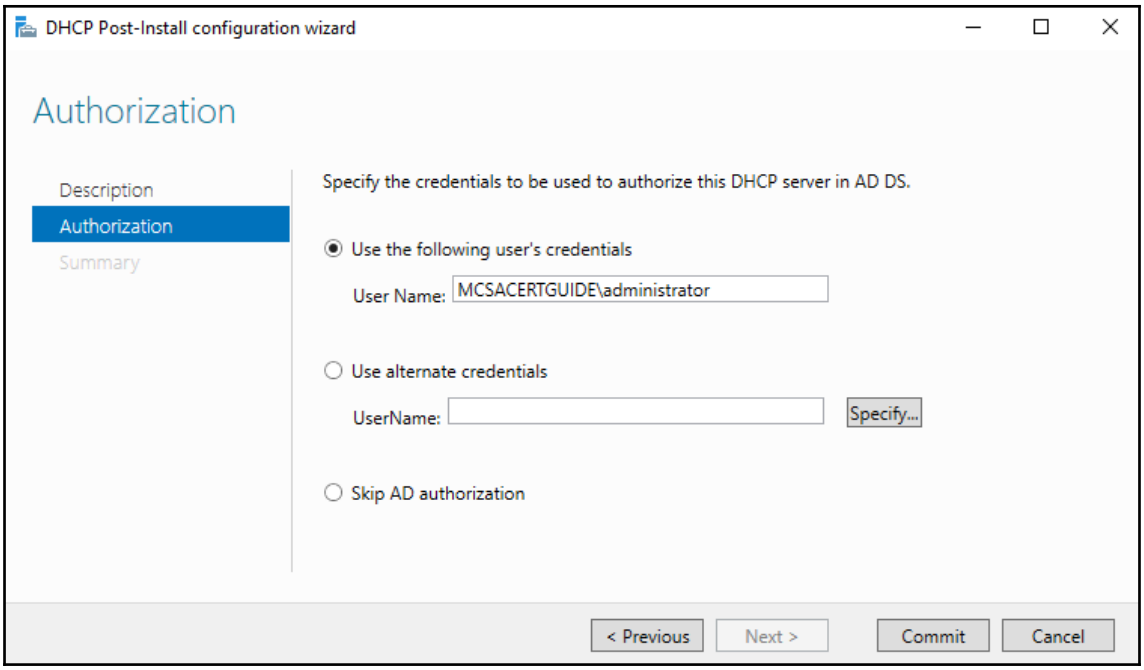

DNS
DC
Forward Lookup Zones
mcsacertguide.local
lab1.mcsacertguide.local
Reverse Lookup Zones
Trust Points
Conditional Forwarders
microsoft.com
Name
Type
Data
Timestamp
(same as parent folder)
Start of Authority (SOA)
[1], dc.mcsacertguide.local., hostmaster.mcsacertguide.l...
static
(same as parent folder)
Name Server (NS)
dc.mcsacertguide.local.
static
(same as parent folder)
Name Server (NS)
srv1.mcsacertguide.local.
DNS
SRV1
Forward Lookup Zones
lab1.mcsacertguide.local
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Name
Type
Data
Timestamp
(same as parent folder)
Start of Authority (SOA)
[4], dc.mcsacertguide.loca...
static
(same as parent folder)
Name Server (NS)
dc.mcsacertguide.local.
static
(same as parent folder)
Name Server (NS)
srv1.mcsacertguide.local.
static

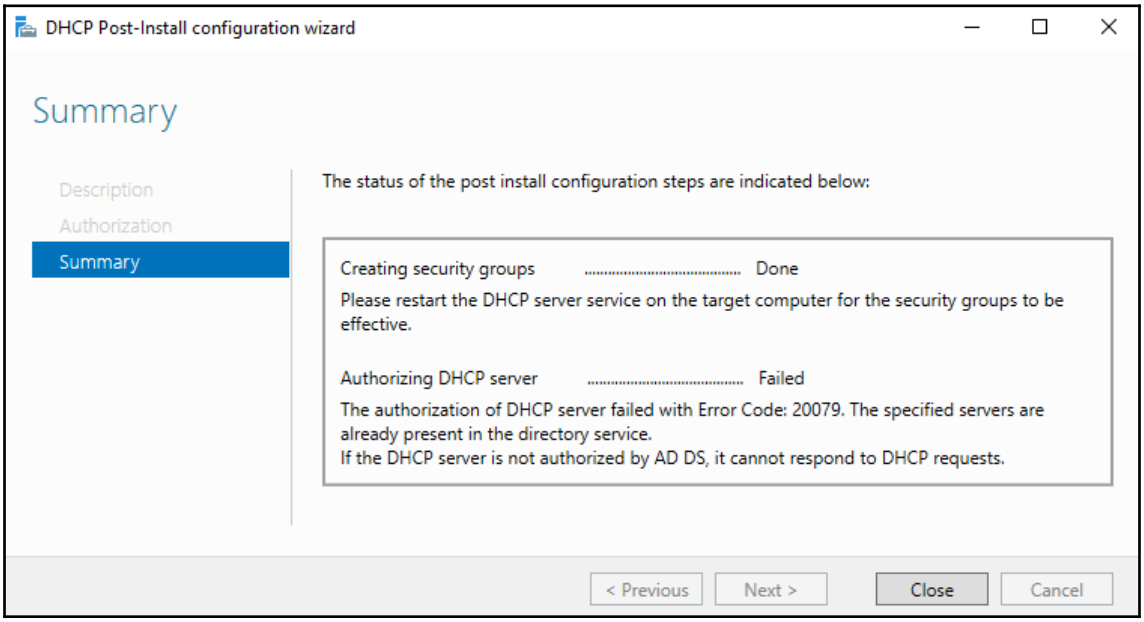
Chapter 3: Configuring DHCP

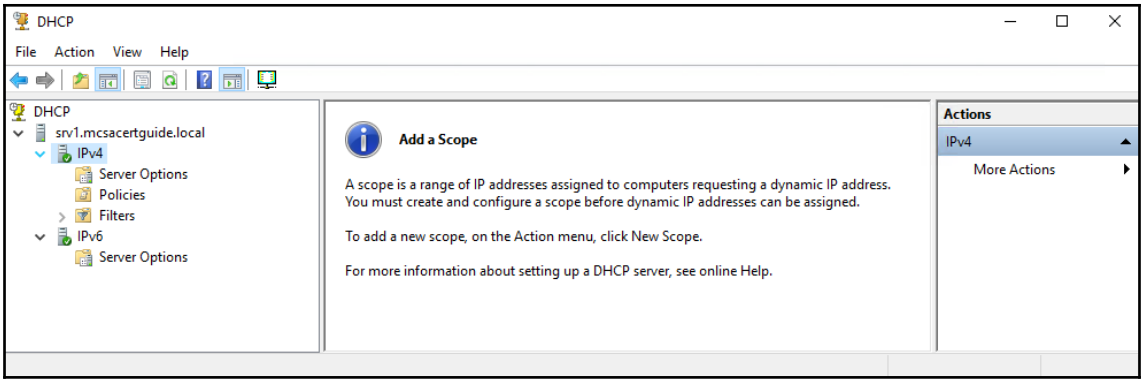


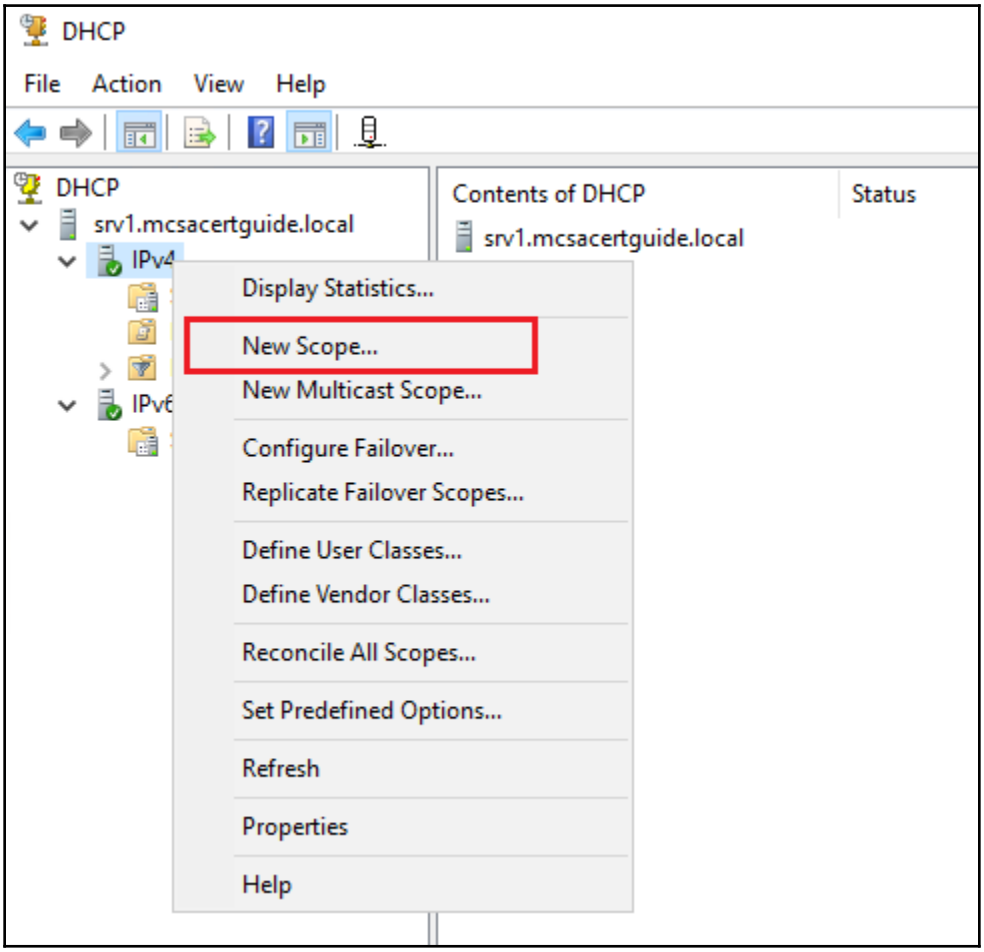

Manage
Tools
View
Help
Post-deployment Configuration
Configuration required for DHCP Server at SRV1
Complete DHCP configuration
Feature installation
TASKS
Configuration required. Installation succeeded on SRV1.MCSACERTGUIDE.LOCAL.
Add Roles and Features
Task Details
1

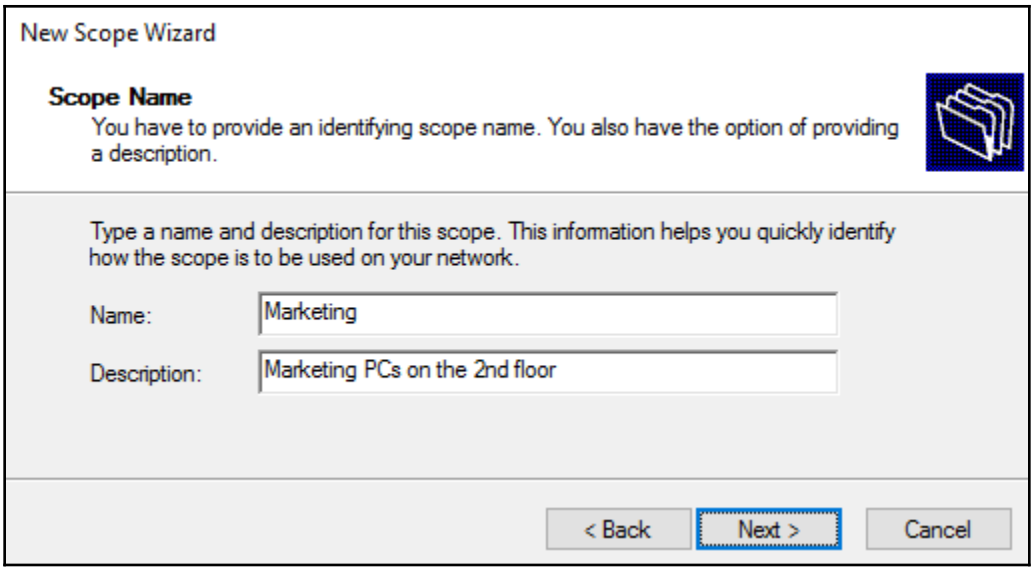

DHCP Post-Install configuration wizard
Description
Description
Authorization
Summary
The following steps will be performed to complete the configuration of the DHCP Server on the target computer:
Create the following security groups for delegation of DHCP Server Administration.
- DHCP Administrators
- DHCP Users
Authorize DHCP server on target computer (if domain joined).
< Previous
Next >
Commit
Cancel

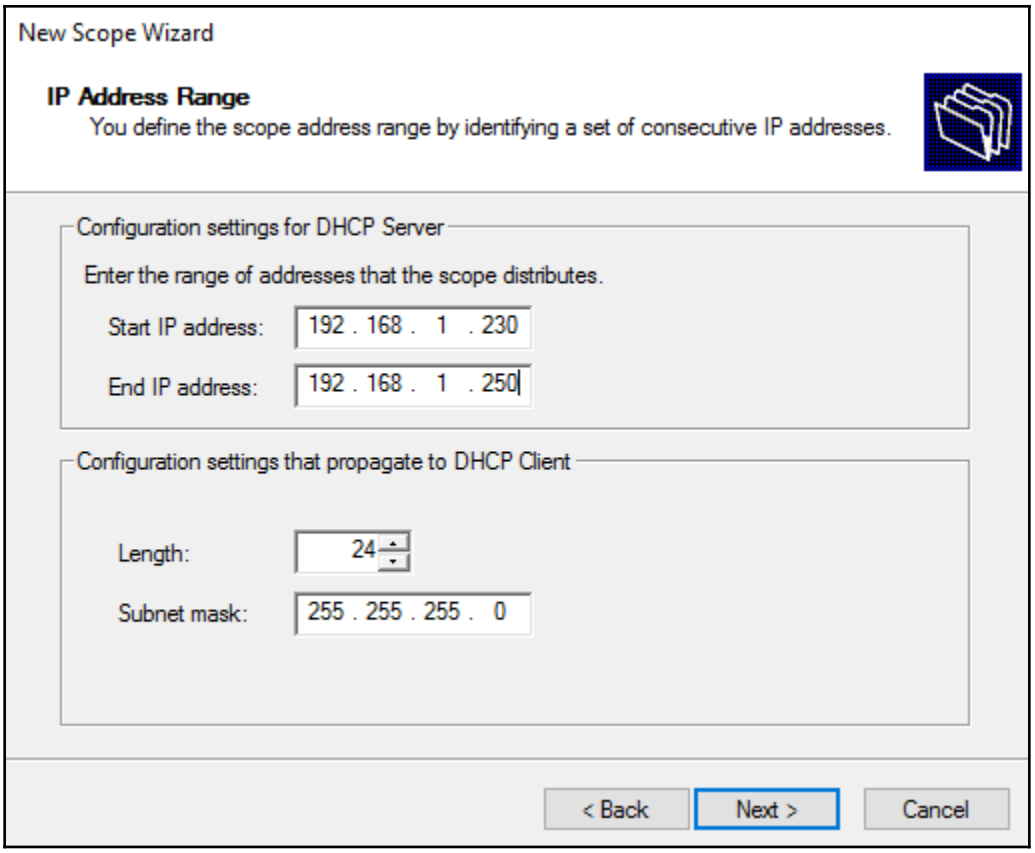

DHCP Post-Install configuration wizard
Authorization
Description
Authorization
Summary
Specify the credentials to be used to authorize this DHCP server in AD DS.
Use the following user's credentials
User Name: MCSACERTGUIDE\administrator
Use alternate credentials
UserName:
Specify...
Skip AD authorization
< Previous
Next >
Commit
Cancel

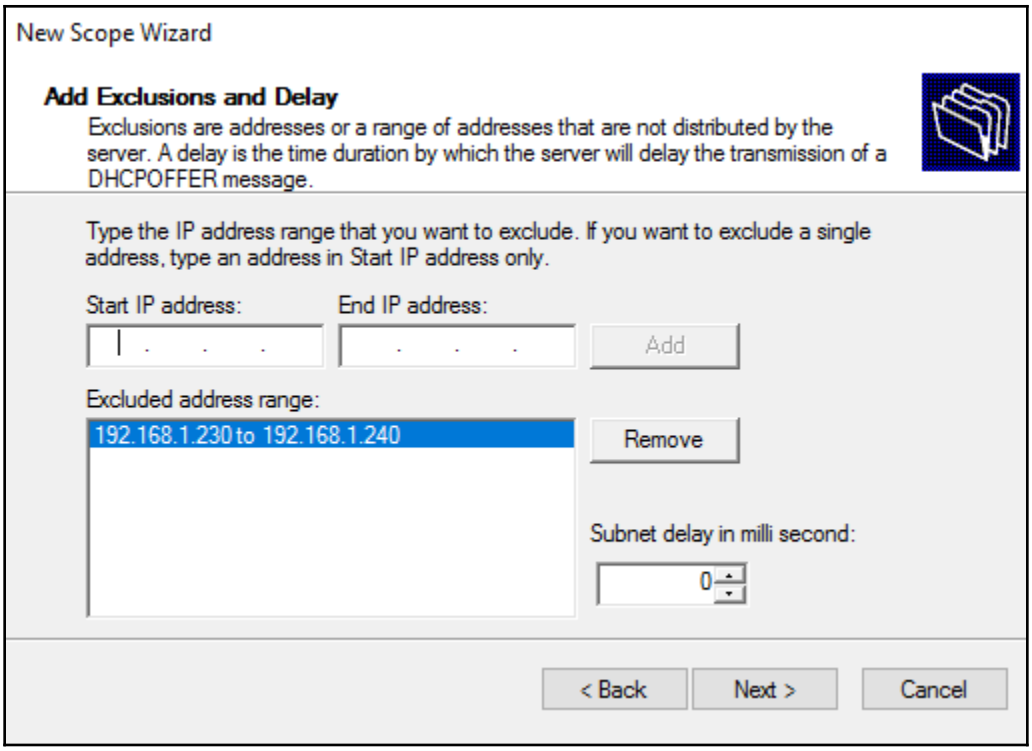

DHCP Post-Install configuration wizard
Summary
Description
Authorization
Summary
The status of the post install configuration steps are indicated below:
Creating security groups ..... Done
Please restart the DHCP server service on the target computer for the security groups to be effective.
Authorizing DHCP server ..... Failed
The authorization of DHCP server failed with Error Code: 20079. The specified servers are already present in the directory service.
If the DHCP server is not authorized by AD DS, it cannot respond to DHCP requests.
< Previous
Next >
Close
Cancel

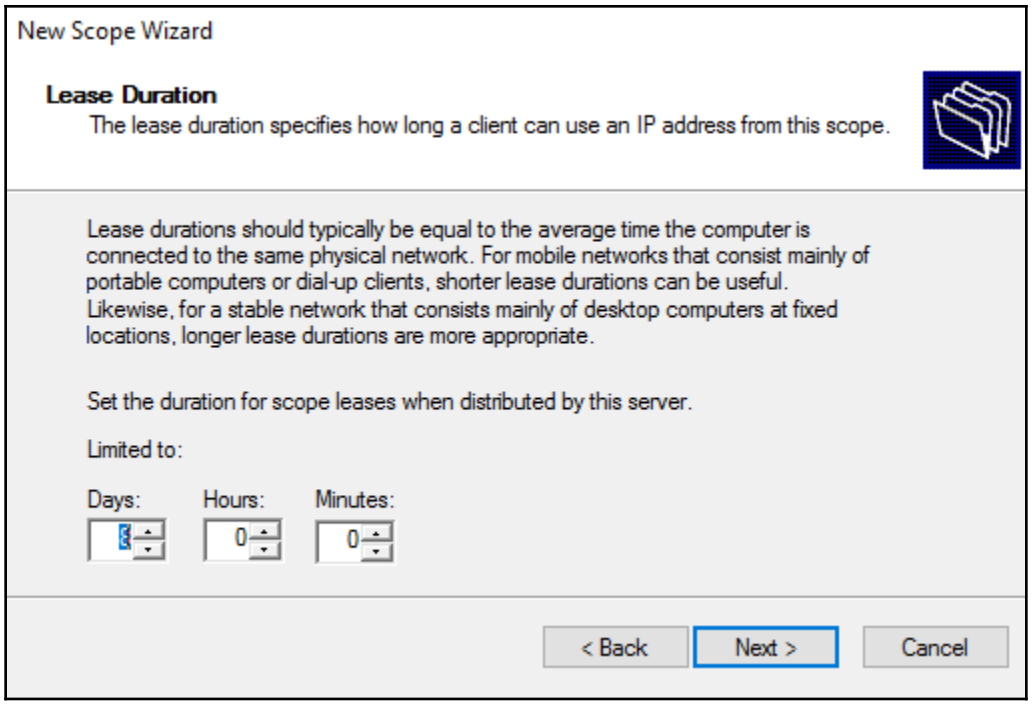

DHCP
File Action View Help
DHCP
srv1.mcsacertguide.local
IPv4
Server Options
Policies
Filters
IPv6
Server Options
Add a Scope
A scope is a range of IP addresses assigned to computers requesting a dynamic IP address. You must create and configure a scope before dynamic IP addresses can be assigned.
To add a new scope, on the Action menu, click New Scope.
For more information about setting up a DHCP server, see online Help.
Actions
IPv4
More Actions

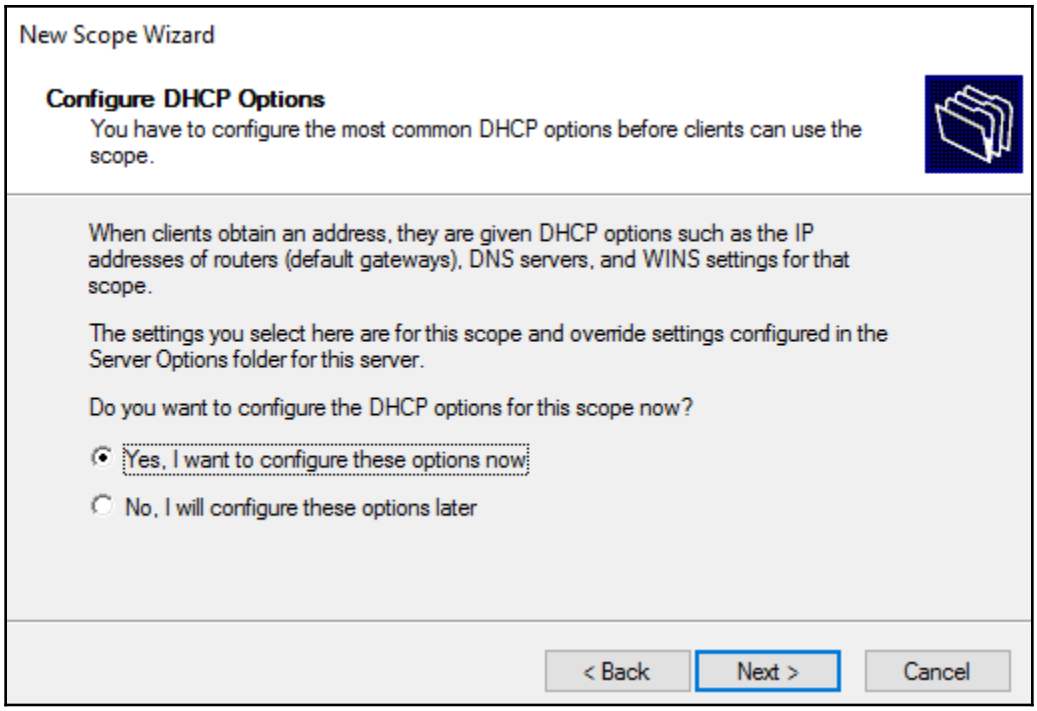

DHCP
File Action View Help
DHCP
srv1.mcsacertguide.local
IPv4
IPv6
Contents of DHCP
Status
srv1.mcsacertguide.local
Display Statistics...
New Scope...
New Multicast Scope...
Configure Failover...
Replicate Failover Scopes...
Define User Classes...
Define Vendor Classes...
Reconcile All Scopes...
Set Predefined Options...
Refresh
Properties
Help

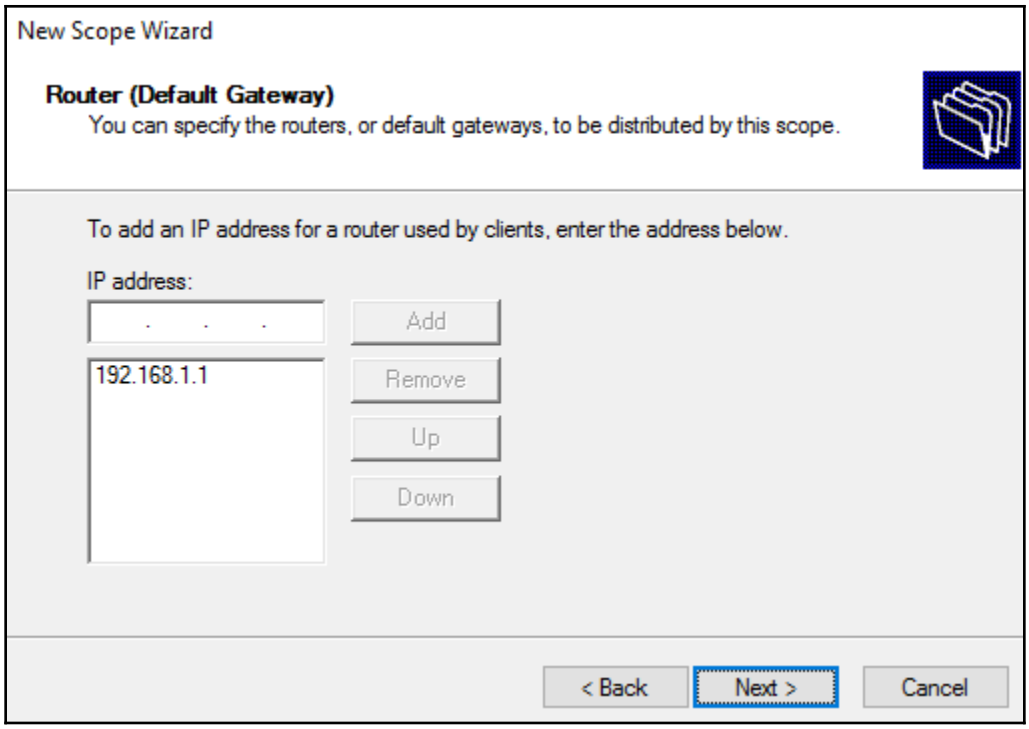

New Scope Wizard
Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.
Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.
Name:
Marketing
Description:
Marketing PCs on the 2nd floor
< Back
Next >
Cancel

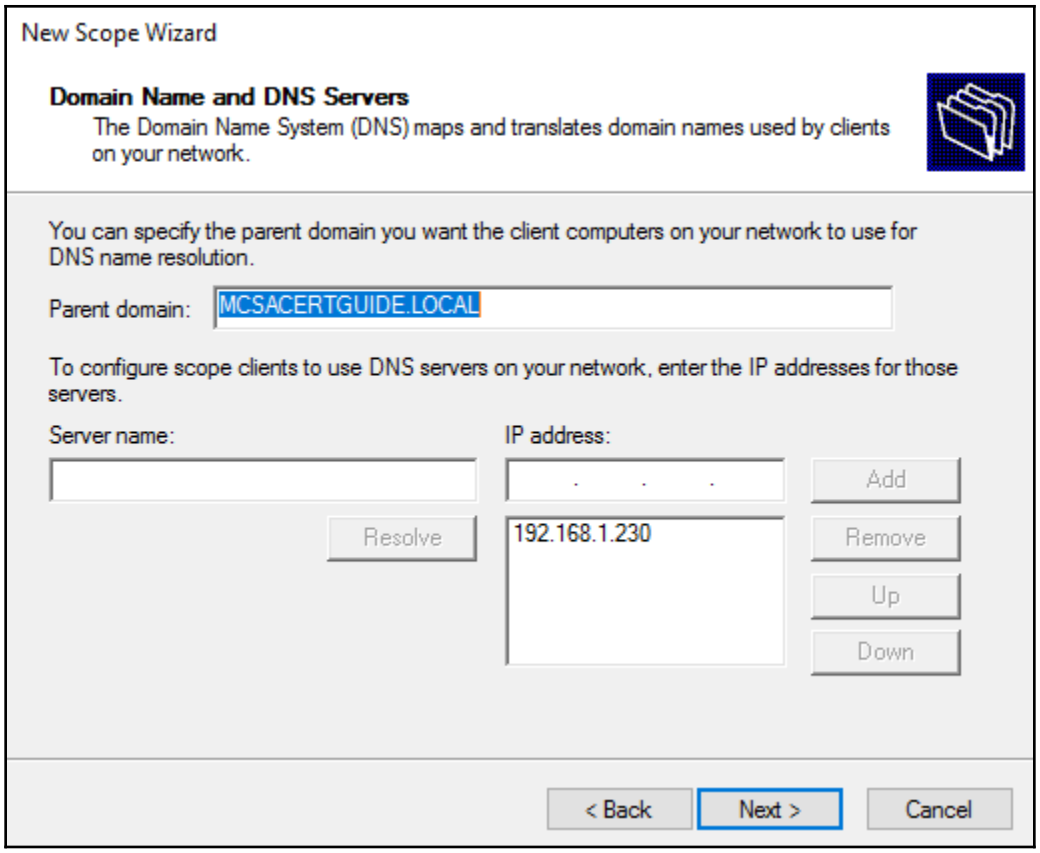

New Scope Wizard
IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.
Configuration settings for DHCP Server
Enter the range of addresses that the scope distributes.
Start IP address:
192 . 168 . 1 . 230
End IP address:
192 . 168 . 1 . 250
Configuration settings that propagate to DHCP Client
Length:
24
Subnet mask:
255 . 255 . 255 . 0
< Back
Next >
Cancel

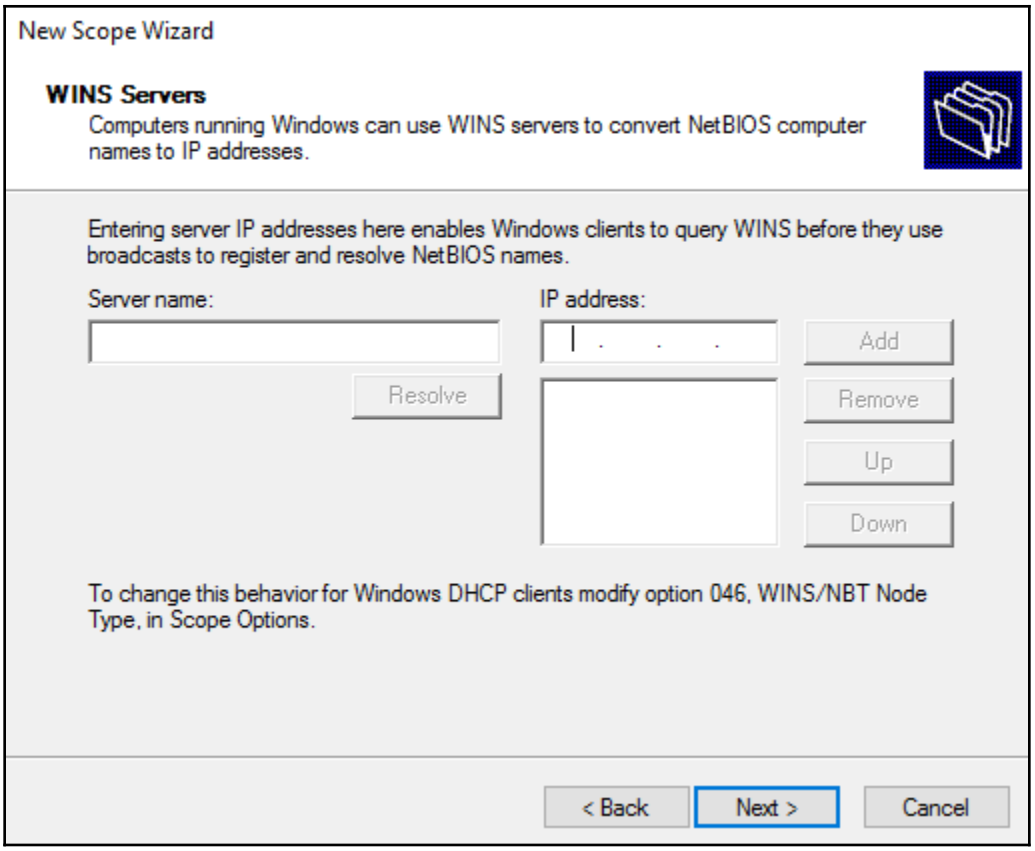

New Scope Wizard
Add Exclusions and Delay
Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCPOFFER message.
Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.
Start IP address:
End IP address:
Add
Excluded address range:
192.168.1.230 to 192.168.1.240
Remove
Subnet delay in milli second:
0
< Back
Next >
Cancel

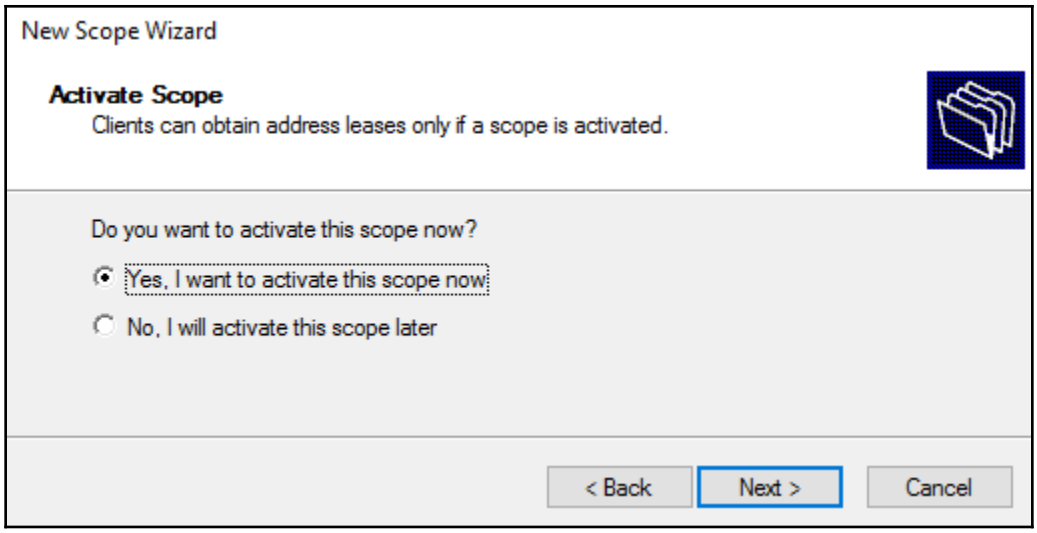

New Scope Wizard
Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.
Set the duration for scope leases when distributed by this server.
Limited to:
Days:
Hours:
Minutes:
8
0
0
< Back
Next >
Cancel

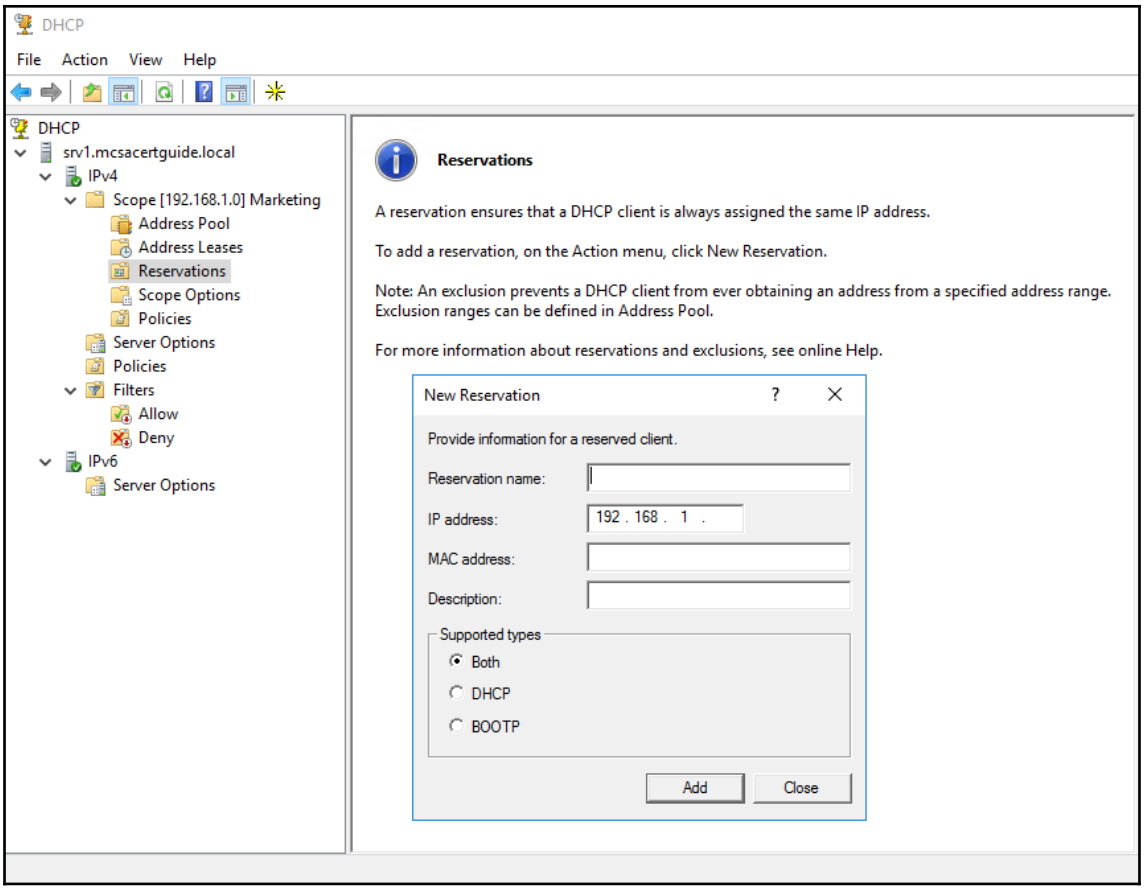

New Scope Wizard
Configure DHCP Options
You have to configure the most common DHCP options before clients can use the scope.
When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.
Do you want to configure the DHCP options for this scope now?
Yes, I want to configure these options now
No, I will configure these options later
< Back
Next >
Cancel

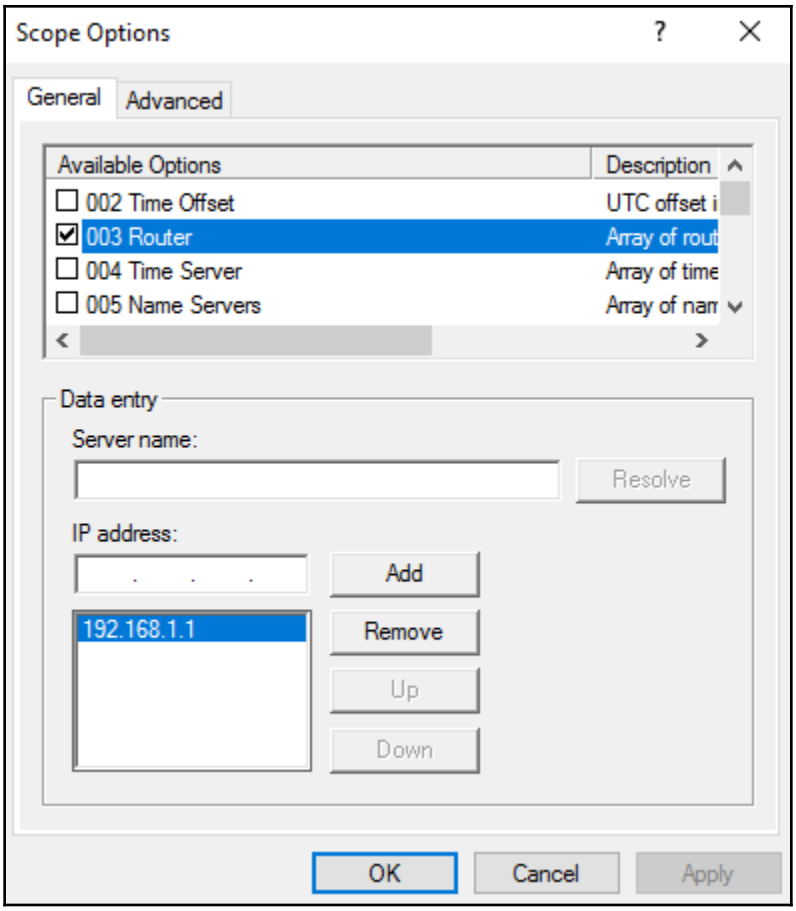

New Scope Wizard
Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.
To add an IP address for a router used by clients, enter the address below.
IP address:
Add
192.168.1.1
Remove
Up
Down
< Back
Next >
Cancel

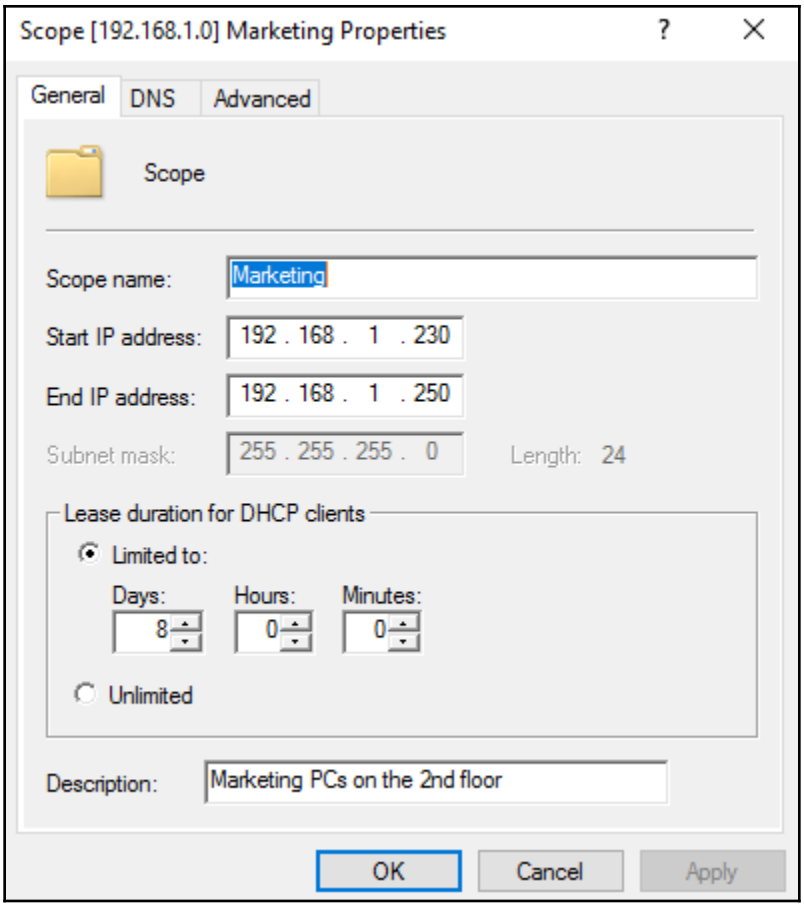

New Scope Wizard
Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.
You can specify the parent domain you want the client computers on your network to use for DNS name resolution.
Parent domain:
MCSACERTGUIDE.LOCAL
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.
Server name:
IP address:
Add
Resolve
192.168.1.230
Remove
Up
Down
< Back
Next >
Cancel

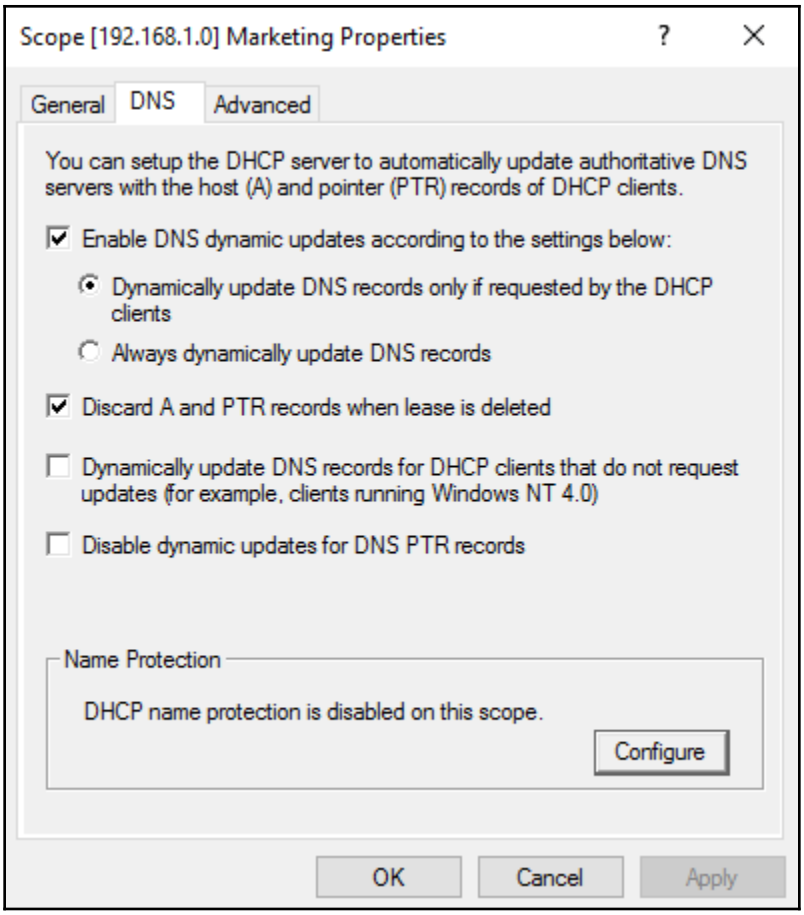

New Scope Wizard
WINS Servers
Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.
Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.
Server name:
IP address:
Add
Resolve
Remove
Up
Down
To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.
< Back
Next >
Cancel

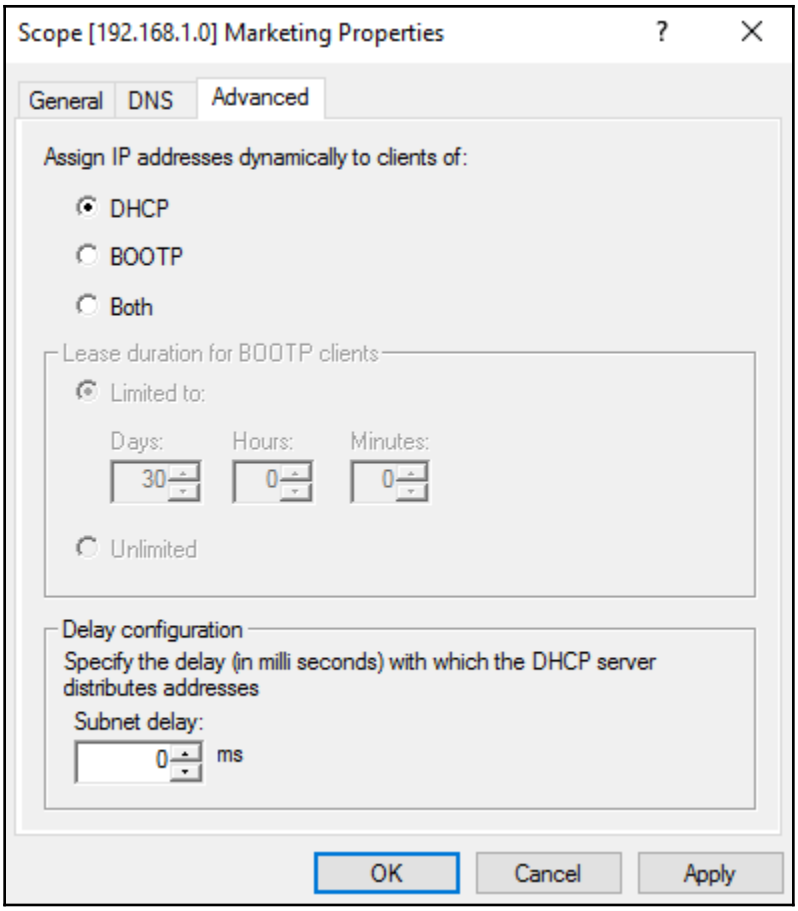

New Scope Wizard
Activate Scope
Clients can obtain address leases only if a scope is activated.
Do you want to activate this scope now?
Yes, I want to activate this scope now
No, I will activate this scope later
< Back
Next >
Cancel

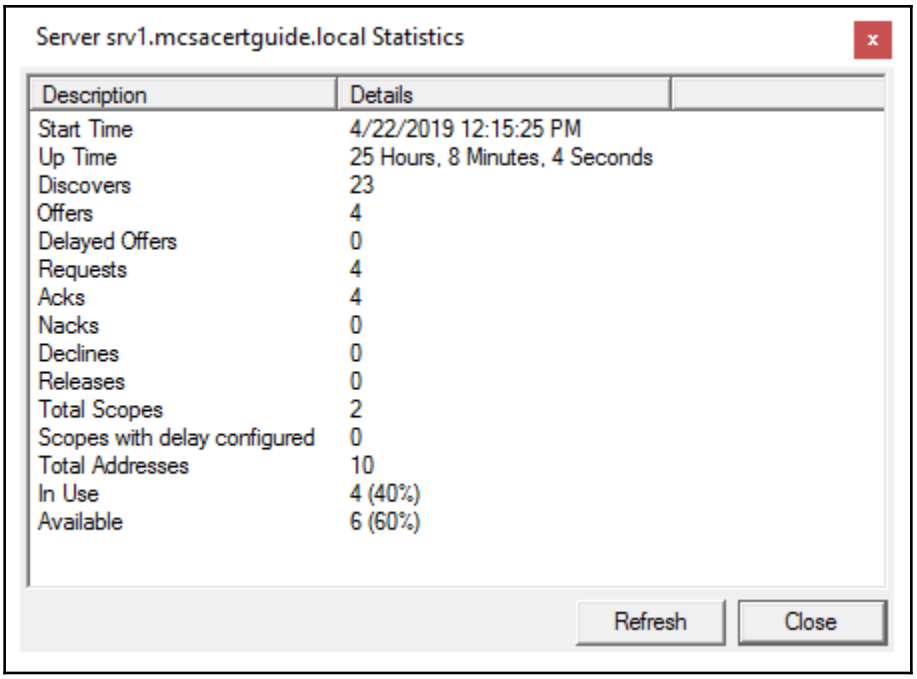

DHCP
File Action View Help
DHCP
srv1.mcsacertguide.local
IPv4
Scope [192.168.1.0] Marketing
Address Pool
Address Leases
Reservations
Scope Options
Policies
Server Options
Policies
Filters
Allow
Deny
IPv6
Server Options
Reservations
A reservation ensures that a DHCP client is always assigned the same IP address.
To add a reservation, on the Action menu, click New Reservation.
Note: An exclusion prevents a DHCP client from ever obtaining an address from a specified address range. Exclusion ranges can be defined in Address Pool.
For more information about reservations and exclusions, see online Help.
New Reservation
Provide information for a reserved client.
Reservation name:
IP address:
192 . 168 . 1 .
MAC address:
Description:
Supported types
Both
DHCP
BOOTP
Add
Close

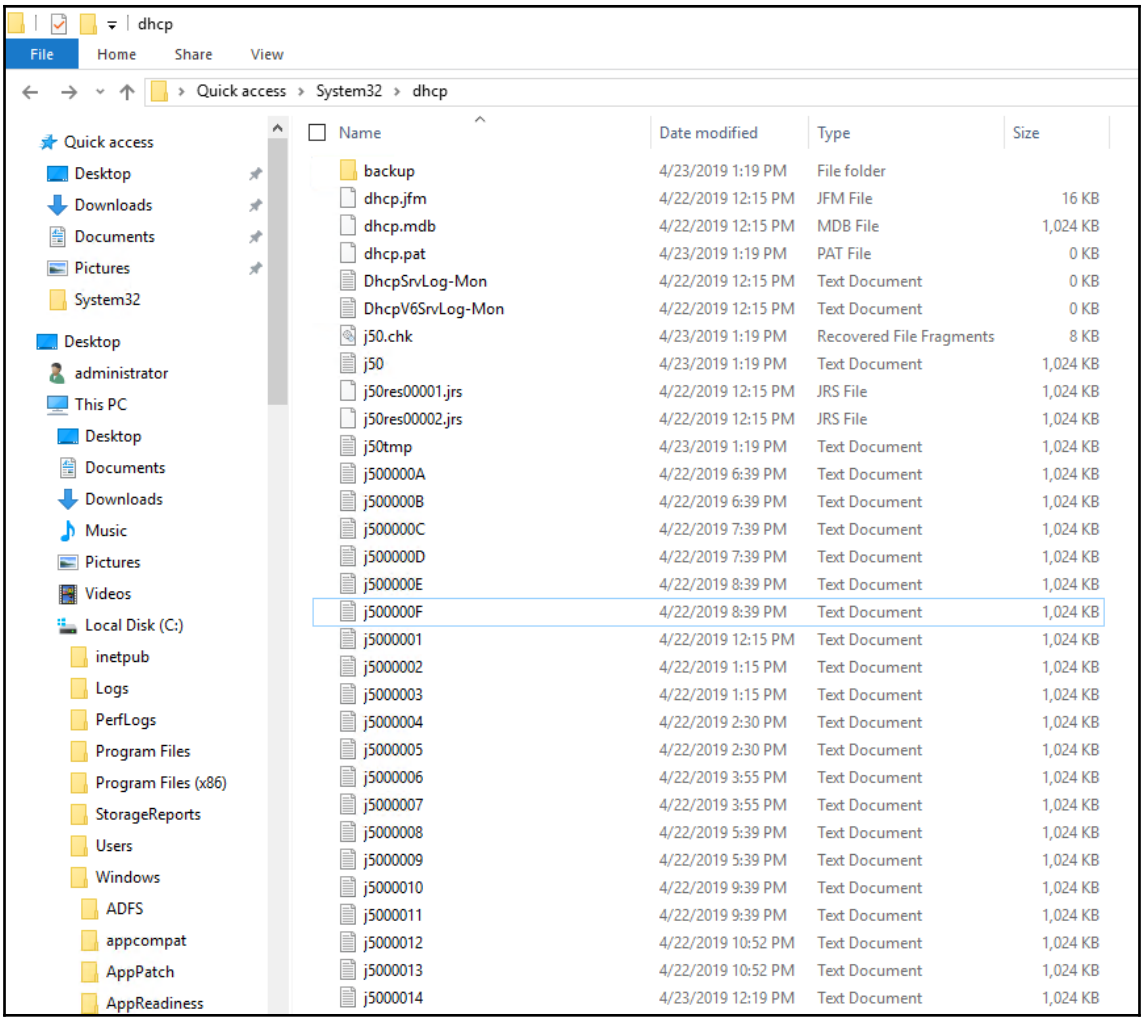

Scope Options
General
Advanced
Available Options
Description
002 Time Offset
UTC offset i
003 Router
Array of rout
004 Time Server
Array of time
005 Name Servers
Array of nam
Data entry
Server name:
Resolve
IP address:
Add
192.168.1.1
Remove
Up
Down
OK
Cancel
Apply

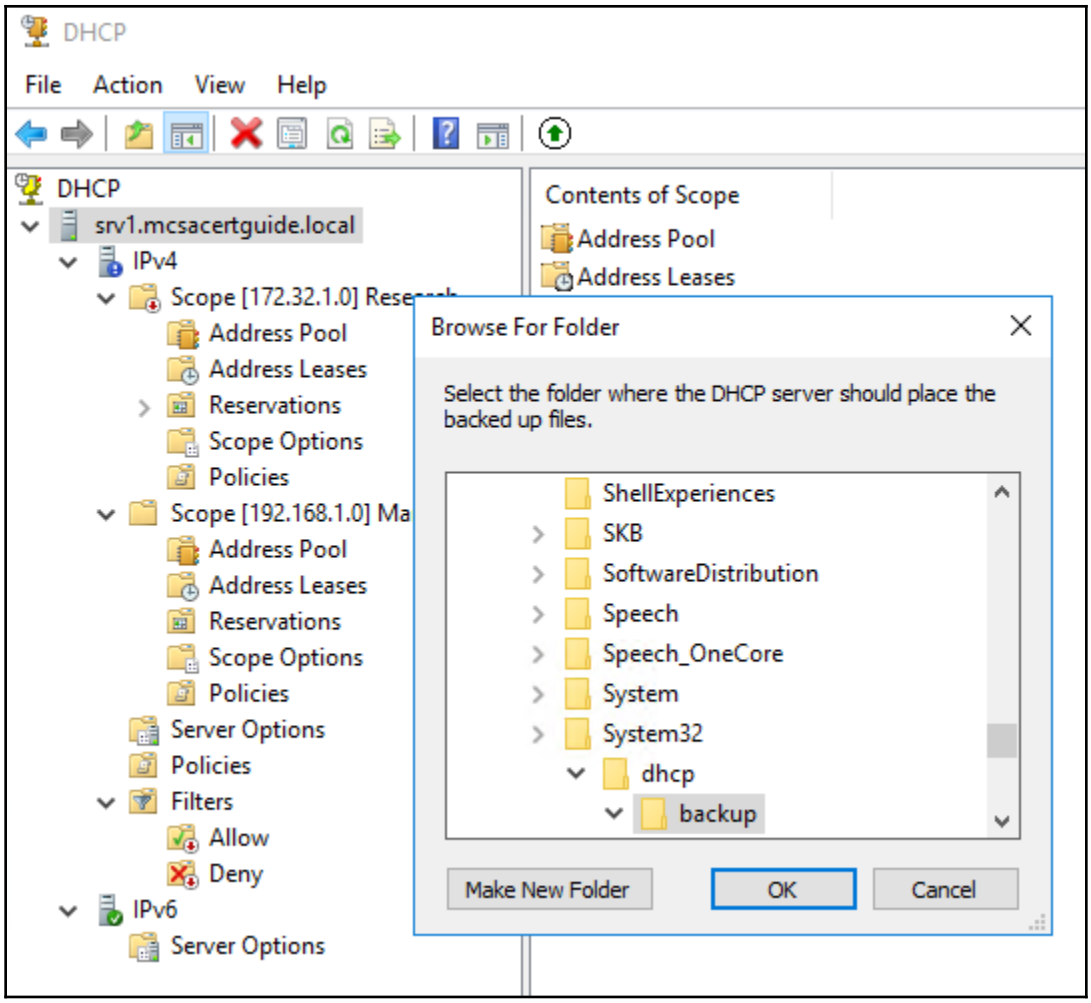

Scope [192.168.1.0] Marketing Properties
General
DNS
Advanced
Scope
Scope name:
Marketing
Start IP address:
192 . 168 . 1 . 230
End IP address:
192 . 168 . 1 . 250
Subnet mask:
255 . 255 . 255 . 0
Length: 24
Lease duration for DHCP clients
Limited to:
Days:
Hours:
Minutes:
8
0
0
Unlimited
Description:
Marketing PCs on the 2nd floor
OK
Cancel
Apply

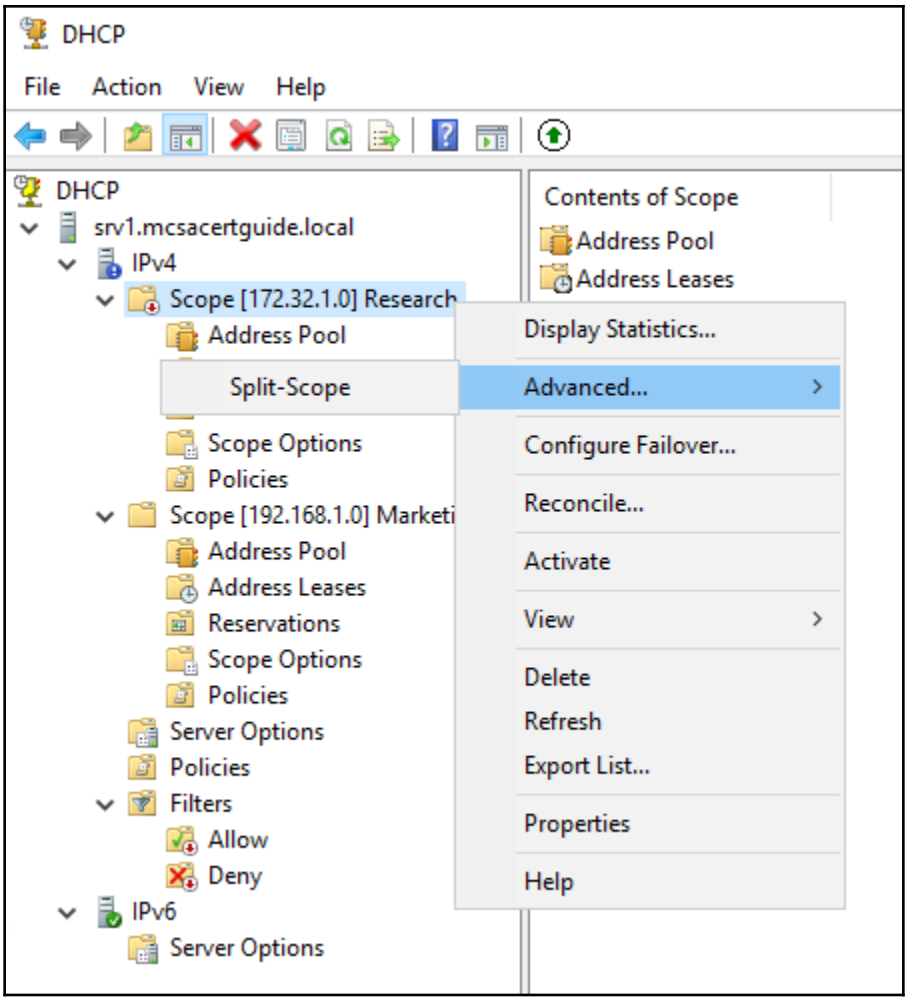

Scope [192.168.1.0] Marketing Properties
?
General
DNS
Advanced
You can setup the DHCP server to automatically update authoritative DNS servers with the host (A) and pointer (PTR) records of DHCP clients.
Enable DNS dynamic updates according to the settings below:
Dynamically update DNS records only if requested by the DHCP clients
Always dynamically update DNS records
Discard A and PTR records when lease is deleted
Dynamically update DNS records for DHCP clients that do not request updates (for example, clients running Windows NT 4.0)
Disable dynamic updates for DNS PTR records
Name Protection
DHCP name protection is disabled on this scope.
Configure
OK
Cancel
Apply

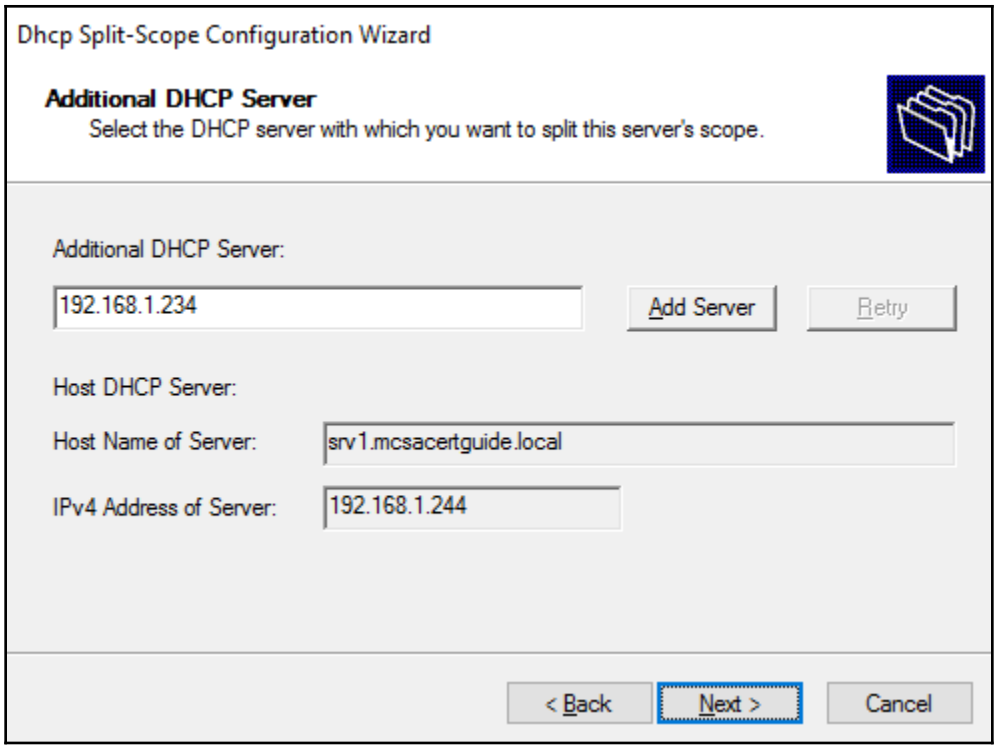

Scope [192.168.1.0] Marketing Properties
General
DNS
Advanced
Assign IP addresses dynamically to clients of:
DHCP
BOOTP
Both
Lease duration for BOOTP clients
Limited to:
Days:
30
Hours:
0
Minutes:
0
Unlimited
Delay configuration
Specify the delay (in milli seconds) with which the DHCP server distributes addresses
Subnet delay:
0
ms
OK
Cancel
Apply

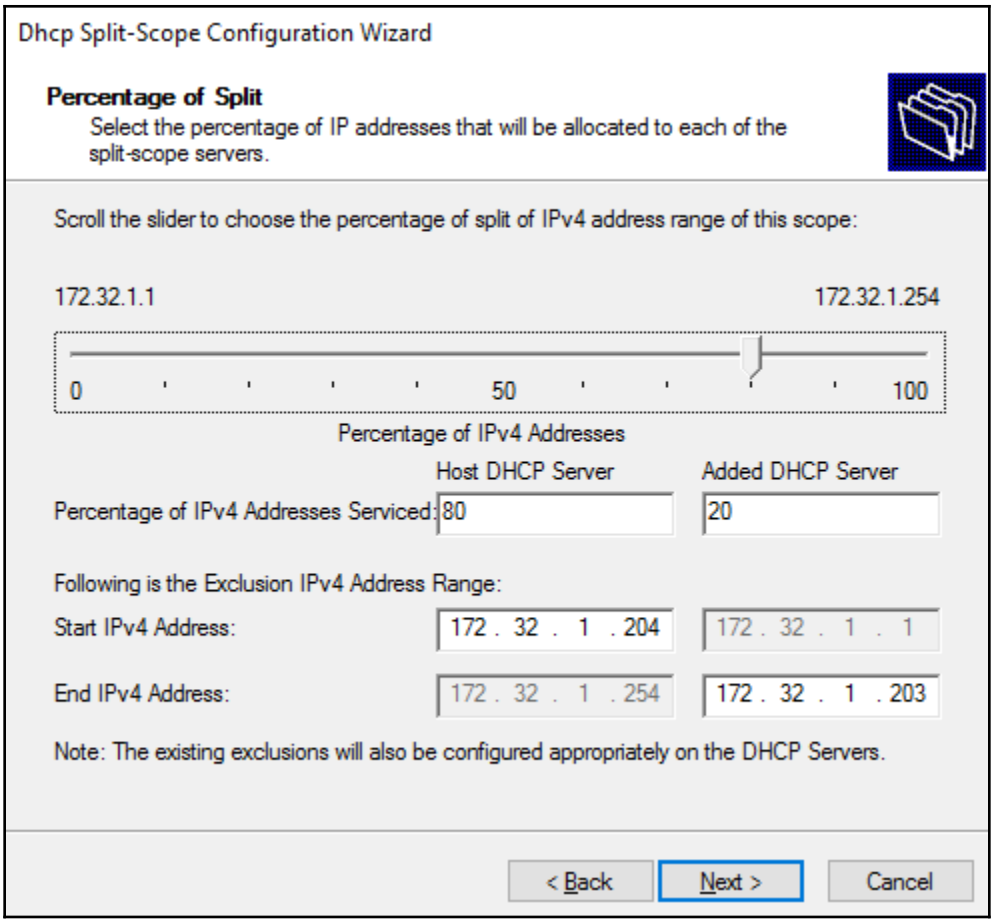

Server srv1.mcsacertguide.local Statistics
Description
Details
Start Time
4/22/2019 12:15:25 PM
Up Time
25 Hours, 8 Minutes, 4 Seconds
Discovers
23
Offers
4
Delayed Offers
0
Requests
4
Acks
4
Nacks
0
Declines
0
Releases
0
Total Scopes
2
Scopes with delay configured
0
Total Addresses
10
In Use
4 (40%)
Available
6 (60%)
Refresh
Close

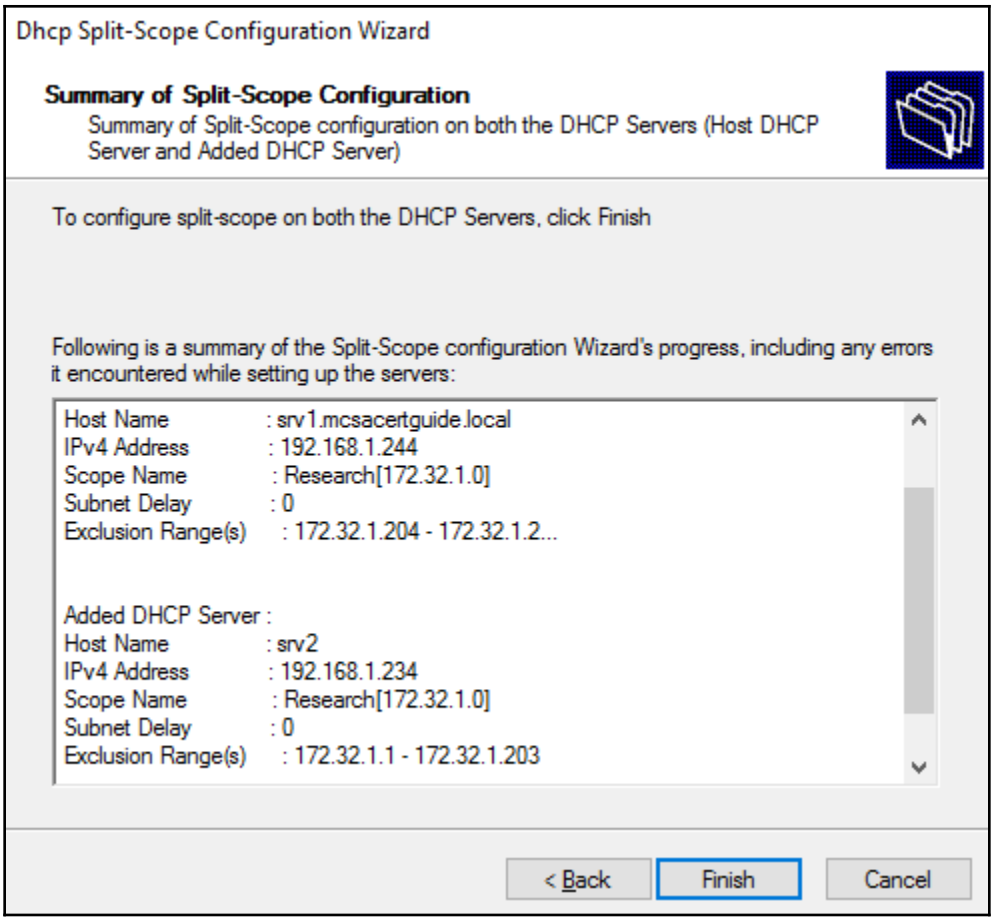

dhcp
File
Home
Share
View
Quick access
System32
dhcp
Quick access
Desktop
Downloads
Documents
Pictures
System32
Desktop
administrator
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
inetpub
Logs
PerfLogs
Program Files
Program Files (x86)
StorageReports
Users
Windows
ADFS
appcompat
AppPatch
AppReadiness
Name
Date modified
Type
Size
backup 4/23/2019 1:19 PM File folder
dhcp.jfm 4/22/2019 12:15 PM JFM File 16 KB
dhcp.mdb 4/22/2019 12:15 PM MDB File 1,024 KB
dhcp.pat 4/23/2019 1:19 PM PAT File 0 KB
DhcpSrvLog-Mon 4/22/2019 12:15 PM Text Document 0 KB
DhcpV6SrvLog-Mon 4/22/2019 12:15 PM Text Document 0 KB
j50.chk 4/23/2019 1:19 PM Recovered File Fragments 8 KB
j50 4/23/2019 1:19 PM Text Document 1,024 KB
j50res00001.jrs 4/22/2019 12:15 PM JRS File 1,024 KB
j50res00002.jrs 4/22/2019 12:15 PM JRS File 1,024 KB
j50tmp 4/23/2019 1:19 PM Text Document 1,024 KB
j500000A 4/22/2019 6:39 PM Text Document 1,024 KB
j500000B 4/22/2019 6:39 PM Text Document 1,024 KB
j500000C 4/22/2019 7:39 PM Text Document 1,024 KB
j500000D 4/22/2019 7:39 PM Text Document 1,024 KB
j500000E 4/22/2019 8:39 PM Text Document 1,024 KB
j500000F 4/22/2019 8:39 PM Text Document 1,024 KB
j5000001 4/22/2019 12:15 PM Text Document 1,024 KB
j5000002 4/22/2019 1:15 PM Text Document 1,024 KB
j5000003 4/22/2019 1:15 PM Text Document 1,024 KB
j5000004 4/22/2019 2:30 PM Text Document 1,024 KB
j5000005 4/22/2019 2:30 PM Text Document 1,024 KB
j5000006 4/22/2019 3:55 PM Text Document 1,024 KB
j5000007 4/22/2019 3:55 PM Text Document 1,024 KB
j5000008 4/22/2019 5:39 PM Text Document 1,024 KB
j5000009 4/22/2019 5:39 PM Text Document 1,024 KB
j5000010 4/22/2019 9:39 PM Text Document 1,024 KB
j5000011 4/22/2019 9:39 PM Text Document 1,024 KB
j5000012 4/22/2019 10:52 PM Text Document 1,024 KB
j5000013 4/22/2019 10:52 PM Text Document 1,024 KB
j5000014 4/23/2019 12:19 PM Text Document 1,024 KB

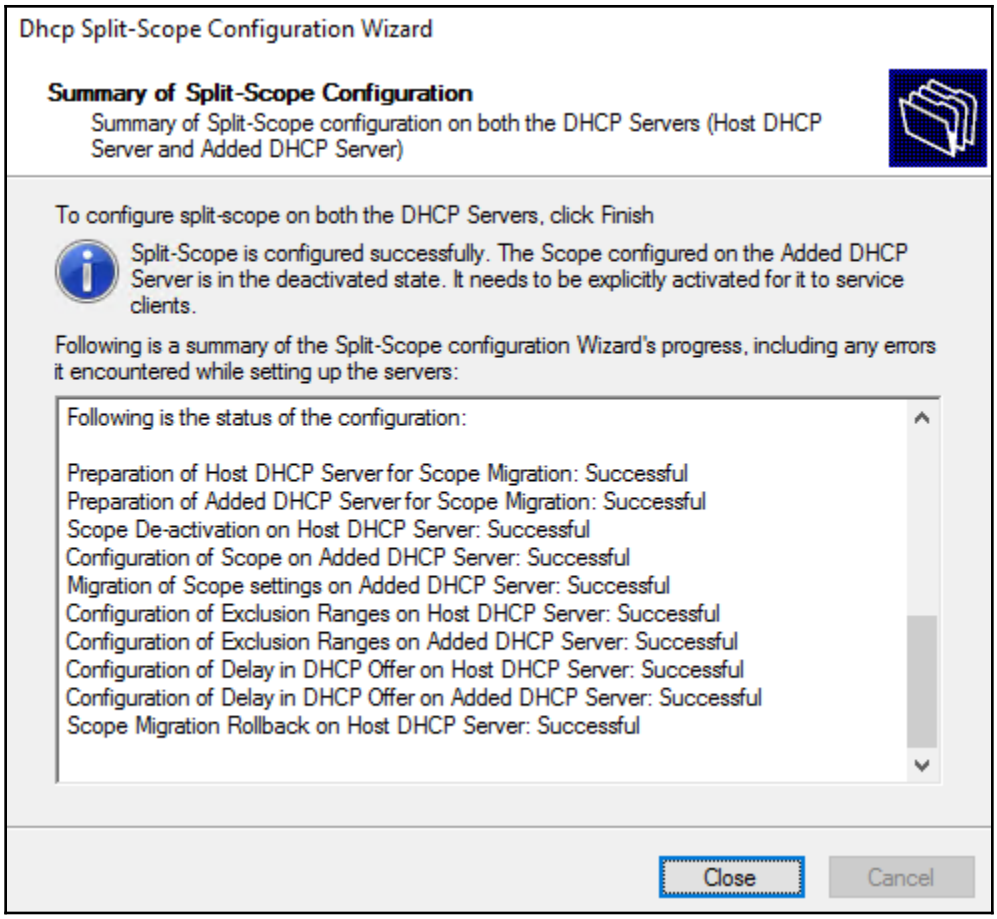

DHCP
File Action View Help
DHCP
srv1.mcsacertguide.local
IPv4
Scope [172.32.1.0] Reserach
Address Pool
Address Leases
Reservations
Scope Options
Policies
Scope [192.168.1.0] Ma
Address Pool
Address Leases
Reservations
Scope Options
Policies
Server Options
Policies
Filters
Allow
Deny
IPv6
Server Options
Contents of Scope
Address Pool
Address Leases
Browse For Folder
Select the folder where the DHCP server should place the backed up files.
ShellExperiences
SKB
SoftwareDistribution
Speech
Speech_OneCore
System
System32
dhcp
backup
Make New Folder
OK
Cancel

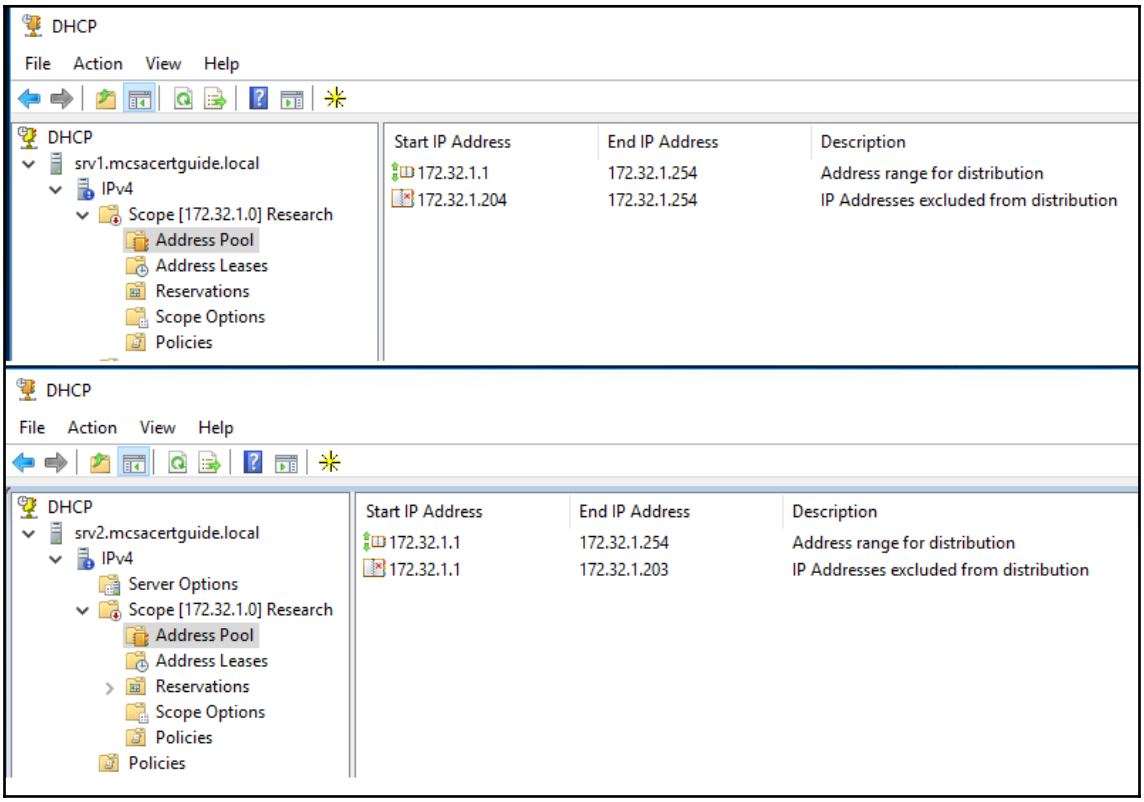

DHCP
File
Action
View
Help
DHCP
srv1.mcsacertguide.local
IPv4
Scope [172.32.1.0] Research
Address Pool
Split-Scope
Scope Options
Policies
Scope [192.168.1.0] Marketi
Address Pool
Address Leases
Reservations
Scope Options
Policies
Server Options
Policies
Filters
Allow
Deny
IPv6
Server Options
Contents of Scope
Address Pool
Address Leases
Display Statistics...
Advanced...
Configure Failover...
Reconcile...
Activate
View
Delete
Refresh
Export List...
Properties
Help

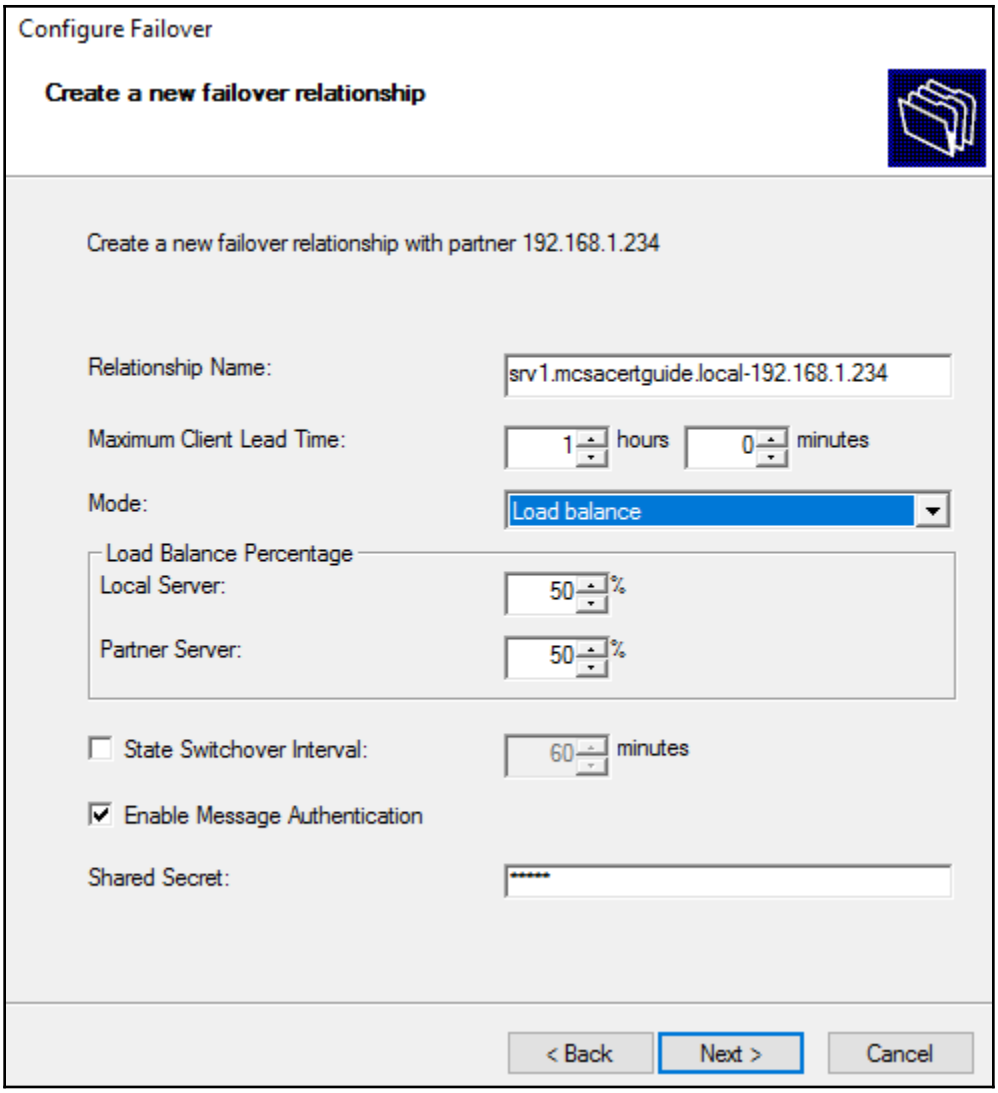

Dhcp Split-Scope Configuration Wizard
Additional DHCP Server
Select the DHCP server with which you want to split this server's scope.
Additional DHCP Server:
192.168.1.234
Add Server
Retry
Host DHCP Server:
Host Name of Server:
srv1.mcsacertguide.local
IPv4 Address of Server:
192.168.1.244
< Back
Next >
Cancel

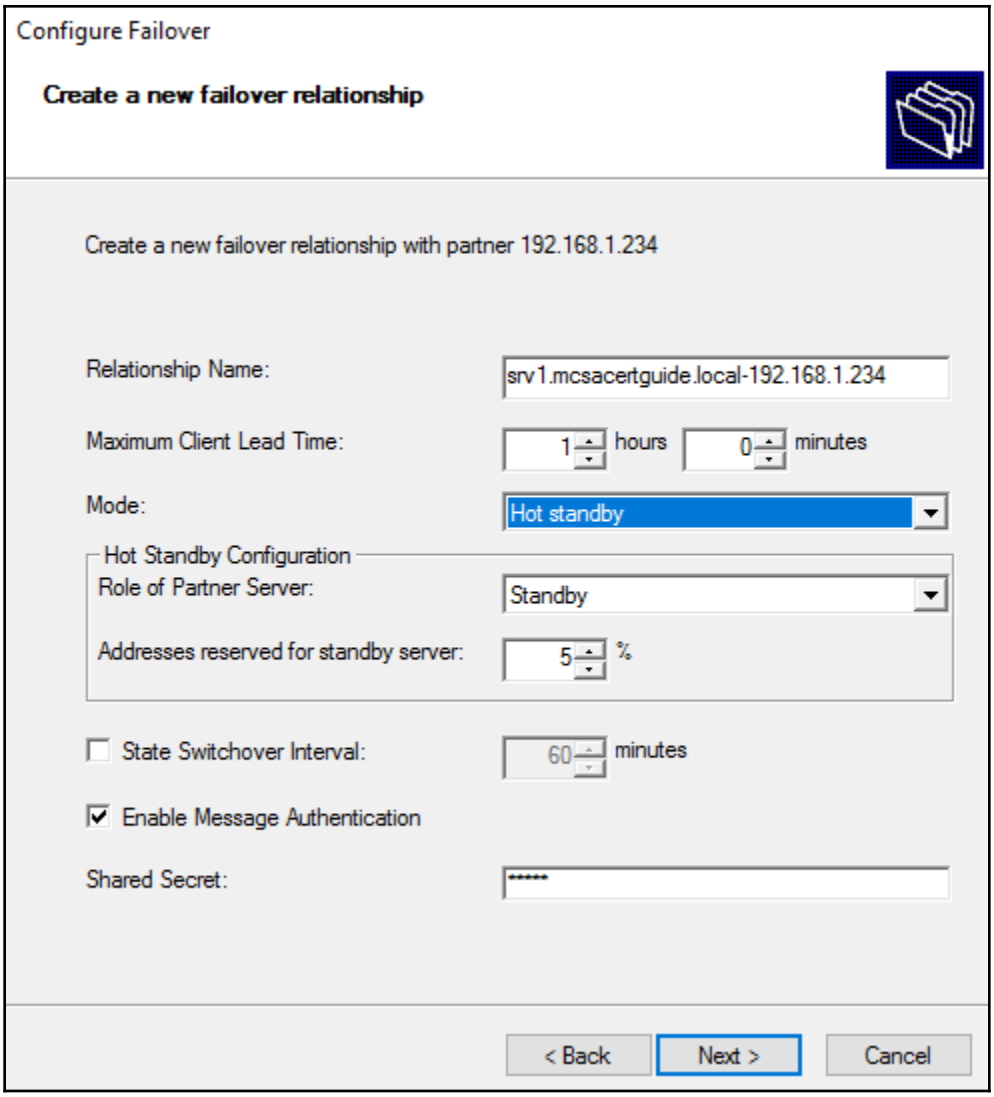

Dhcp Split-Scope Configuration Wizard
Percentage of Split
Select the percentage of IP addresses that will be allocated to each of the split-scope servers.
Scroll the slider to choose the percentage of split of IPv4 address range of this scope:
172.32.1.1
172.32.1.254
0
50
100
Percentage of IPv4 Addresses
Host DHCP Server
Added DHCP Server
Percentage of IPv4 Addresses Serviced:
80
20
Following is the Exclusion IPv4 Address Range:
Start IPv4 Address:
172 . 32 . 1 . 204
172 . 32 . 1 . 1
End IPv4 Address:
172 . 32 . 1 . 254
172 . 32 . 1 . 203
Note: The existing exclusions will also be configured appropriately on the DHCP Servers.
< Back
Next >
Cancel

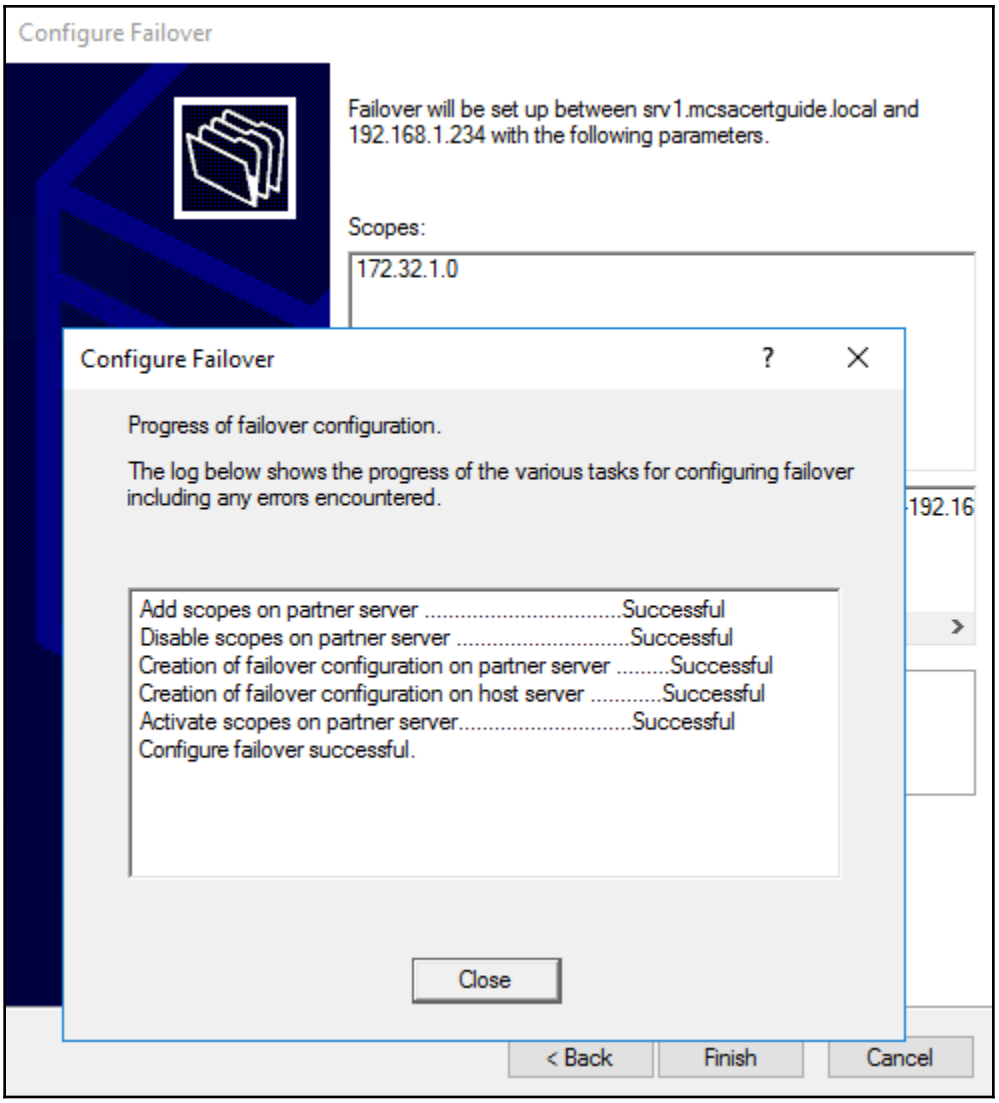

Dhcp Split-Scope Configuration Wizard
Summary of Split-Scope Configuration
Summary of Split-Scope configuration on both the DHCP Servers (Host DHCP Server and Added DHCP Server)
To configure split-scope on both the DHCP Servers, click Finish
Following is a summary of the Split-Scope configuration Wizard's progress, including any errors it encountered while setting up the servers:
Host Name : srv1.mcsacertguide.local
IPv4 Address : 192.168.1.244
Scope Name : Research[172.32.1.0]
Subnet Delay : 0
Exclusion Range(s) : 172.32.1.204 - 172.32.1.2...
Added DHCP Server :
Host Name : srv2
IPv4 Address : 192.168.1.234
Scope Name : Research[172.32.1.0]
Subnet Delay : 0
Exclusion Range(s) : 172.32.1.1 - 172.32.1.203
< Back
Finish
Cancel


Dhcp Split-Scope Configuration Wizard
Summary of Split-Scope Configuration
Summary of Split-Scope configuration on both the DHCP Servers (Host DHCP Server and Added DHCP Server)
To configure split-scope on both the DHCP Servers, click Finish
Split-Scope is configured successfully. The Scope configured on the Added DHCP Server is in the deactivated state. It needs to be explicitly activated for it to service clients.
Following is a summary of the Split-Scope configuration Wizard's progress, including any errors it encountered while setting up the servers:
Following is the status of the configuration:
Preparation of Host DHCP Server for Scope Migration: Successful
Preparation of Added DHCP Server for Scope Migration: Successful
Scope De-activation on Host DHCP Server: Successful
Configuration of Scope on Added DHCP Server: Successful
Migration of Scope settings on Added DHCP Server: Successful
Configuration of Exclusion Ranges on Host DHCP Server: Successful
Configuration of Exclusion Ranges on Added DHCP Server: Successful
Configuration of Delay in DHCP Offer on Host DHCP Server: Successful
Configuration of Delay in DHCP Offer on Added DHCP Server: Successful
Scope Migration Rollback on Host DHCP Server: Successful
Close
Cancel

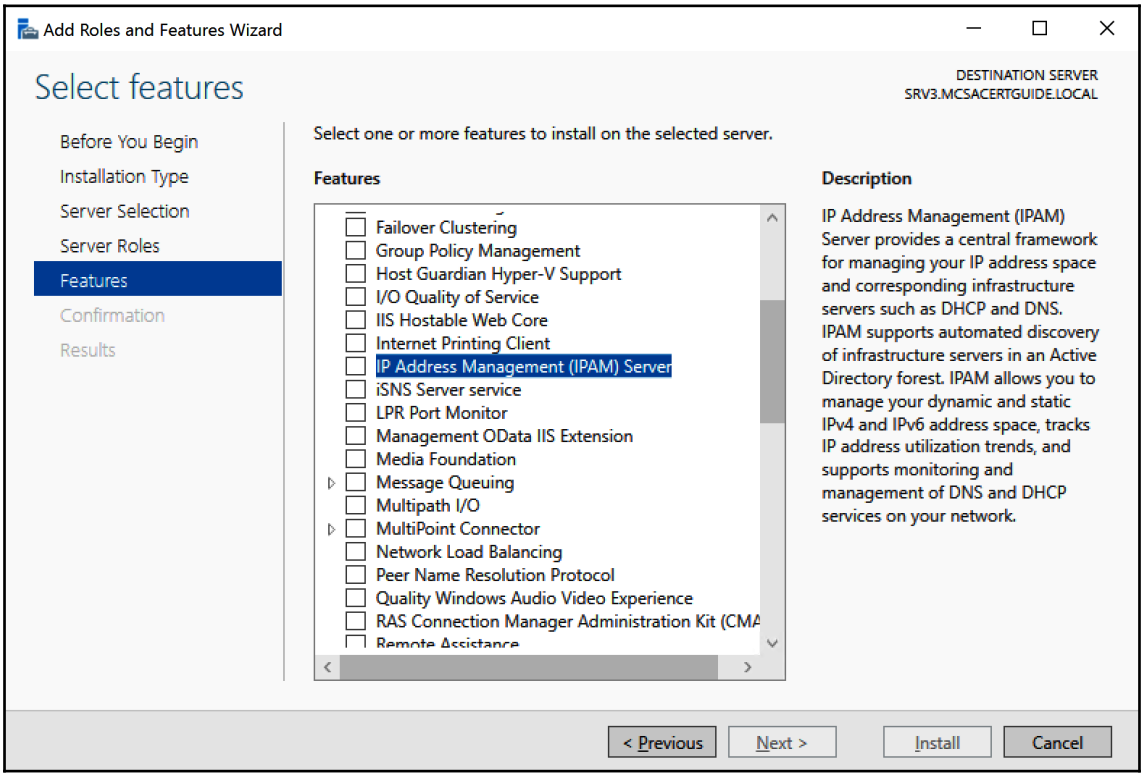

DHCP
File Action View Help
DHCP
srv1.mcsacertguide.local
IPv4
Scope [172.32.1.0] Research
Address Pool
Address Leases
Reservations
Scope Options
Policies
Start IP Address
End IP Address
Description
172.32.1.1
172.32.1.254
Address range for distribution
172.32.1.204
172.32.1.254
IP Addresses excluded from distribution
DHCP
File Action View Help
DHCP
srv2.mcsacertguide.local
IPv4
Server Options
Scope [172.32.1.0] Research
Address Pool
Address Leases
Reservations
Scope Options
Policies
Policies
Start IP Address
End IP Address
Description
172.32.1.1
172.32.1.254
Address range for distribution
172.32.1.1
172.32.1.203
IP Addresses excluded from distribution

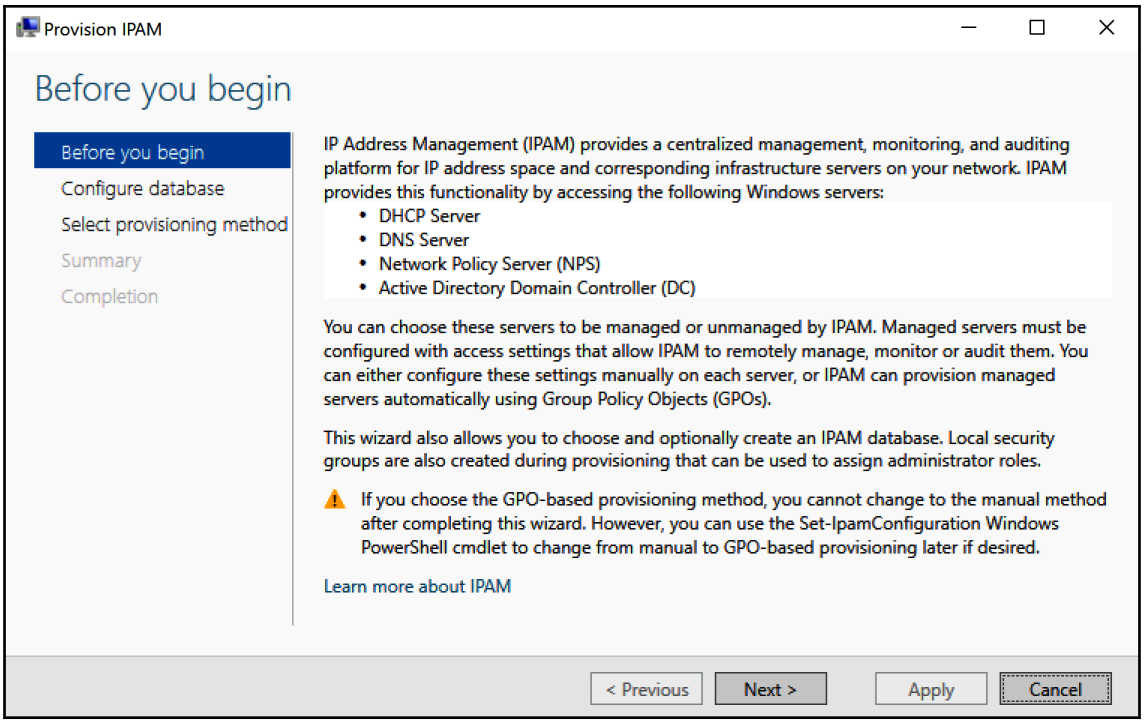

Configure Failover
Create a new failover relationship
Create a new failover relationship with partner 192.168.1.234
Relationship Name:
srv1.mcsacertguide.local-192.168.1.234
Maximum Client Lead Time:
1
hours
0
minutes
Mode:
Load balance
Load Balance Percentage
Local Server:
50
%
Partner Server:
50
%
State Switchover Interval:
60
minutes
Enable Message Authentication
Shared Secret:
< Back
Next >
Cancel

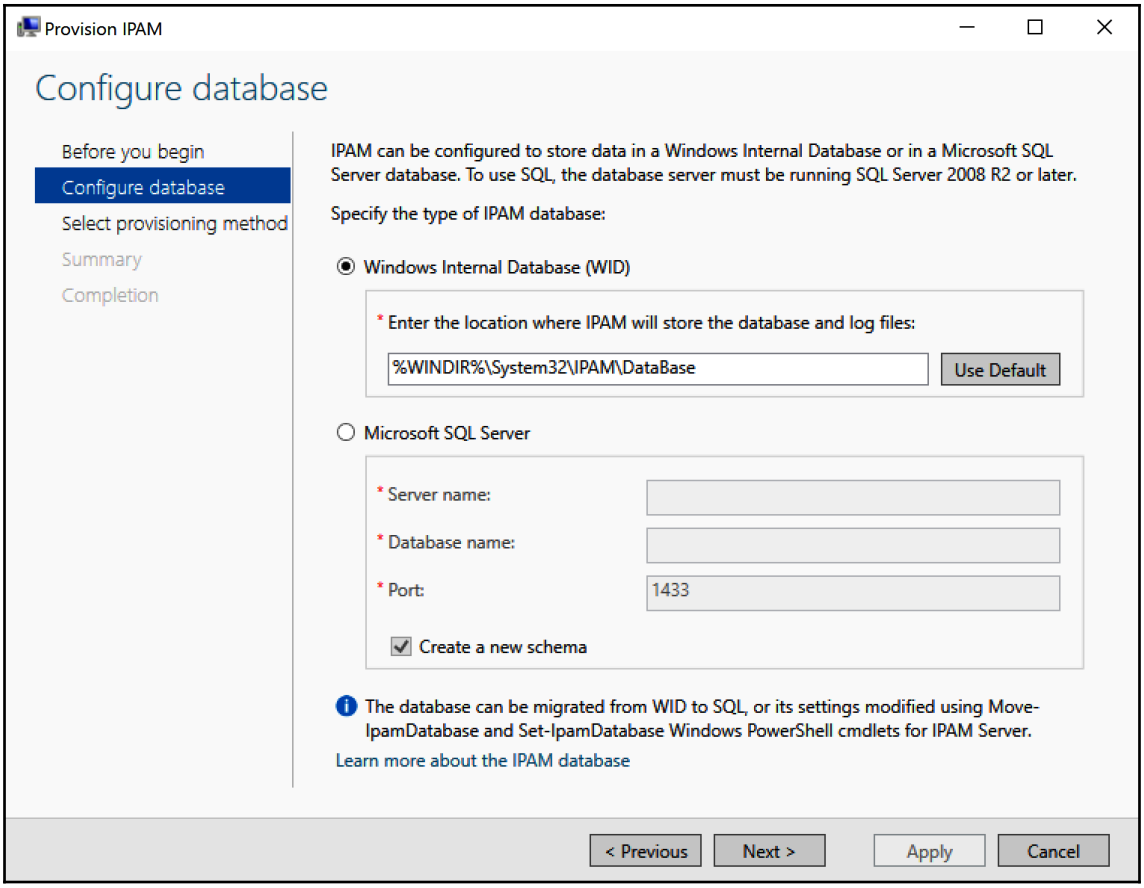

Configure Failover
Create a new failover relationship
Create a new failover relationship with partner 192.168.1.234
Relationship Name:
srv1.mcsacertguide.local-192.168.1.234
Maximum Client Lead Time:
1
hours
0
minutes
Mode:
Hot standby
Hot Standby Configuration
Role of Partner Server:
Standby
Addresses reserved for standby server:
5
%
State Switchover Interval:
60
minutes
Enable Message Authentication
Shared Secret:
*****
< Back
Next >
Cancel

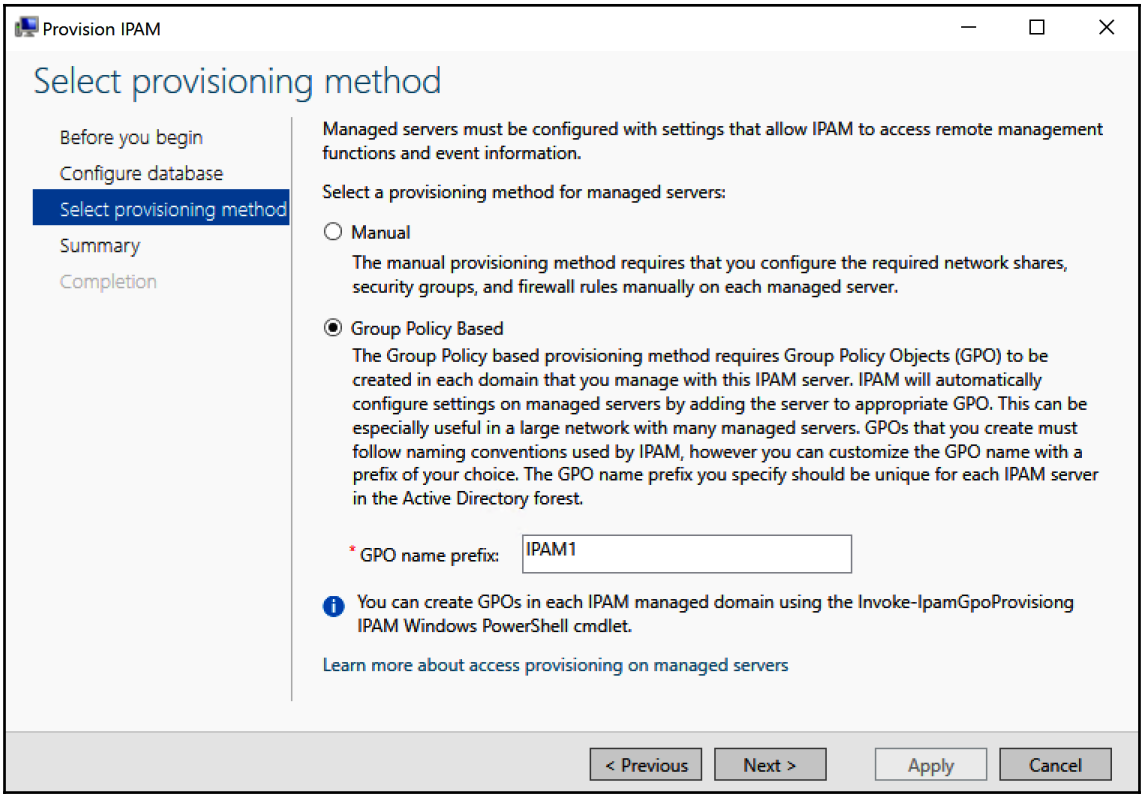

Configure Failover
Failover will be set up between srv1.mcsacertguide.local and 192.168.1.234 with the following parameters.
Scopes:
172.32.1.0
Configure Failover
Progress of failover configuration.
The log below shows the progress of the various tasks for configuring failover including any errors encountered.
Add scopes on partner server .....Successful
Disable scopes on partner server .....Successful
Creation of failover configuration on partner server .....Successful
Creation of failover configuration on host server .....Successful
Activate scopes on partner server.....Successful
Configure failover successful.
Close
< Back
Finish
Cancel

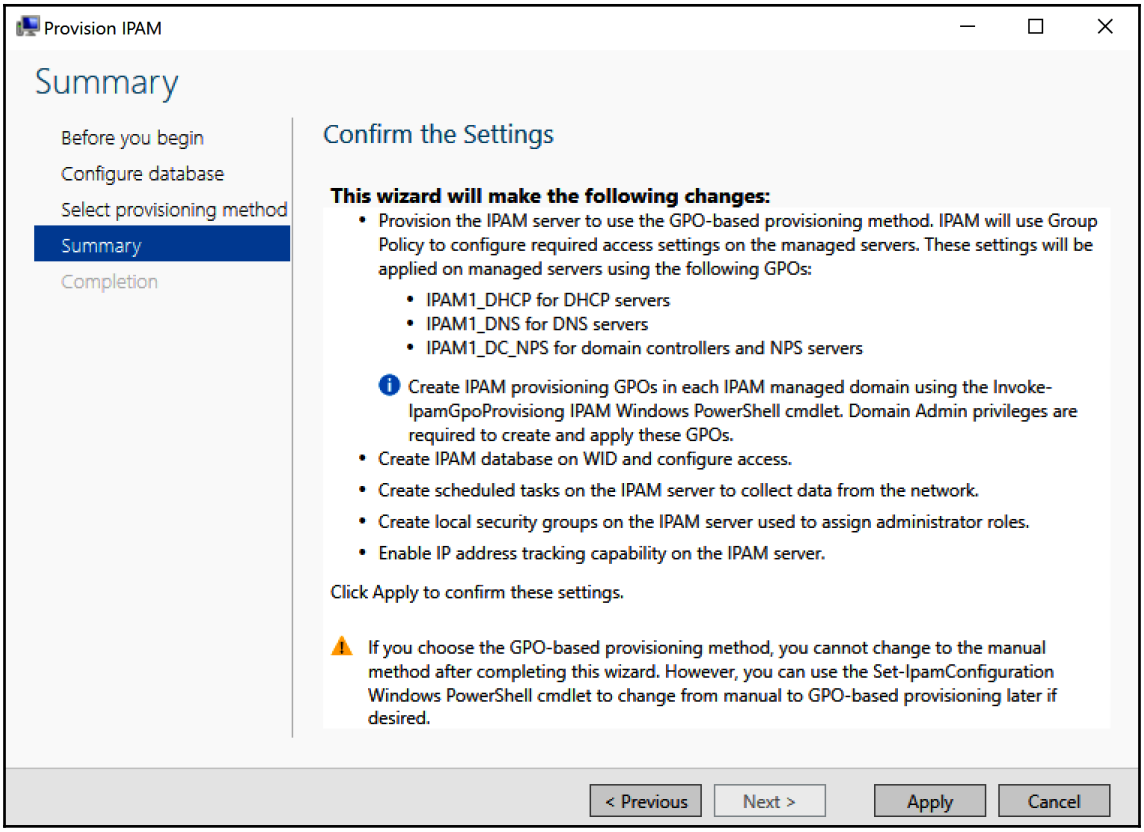
Chapter 4: Understanding IPAM

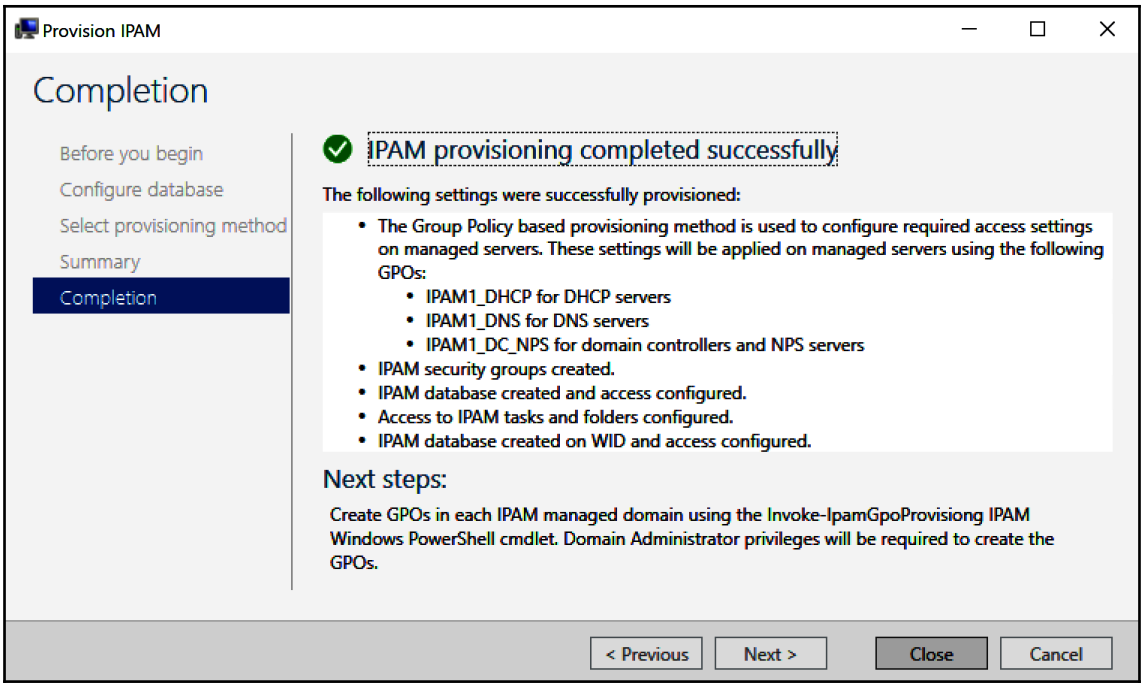


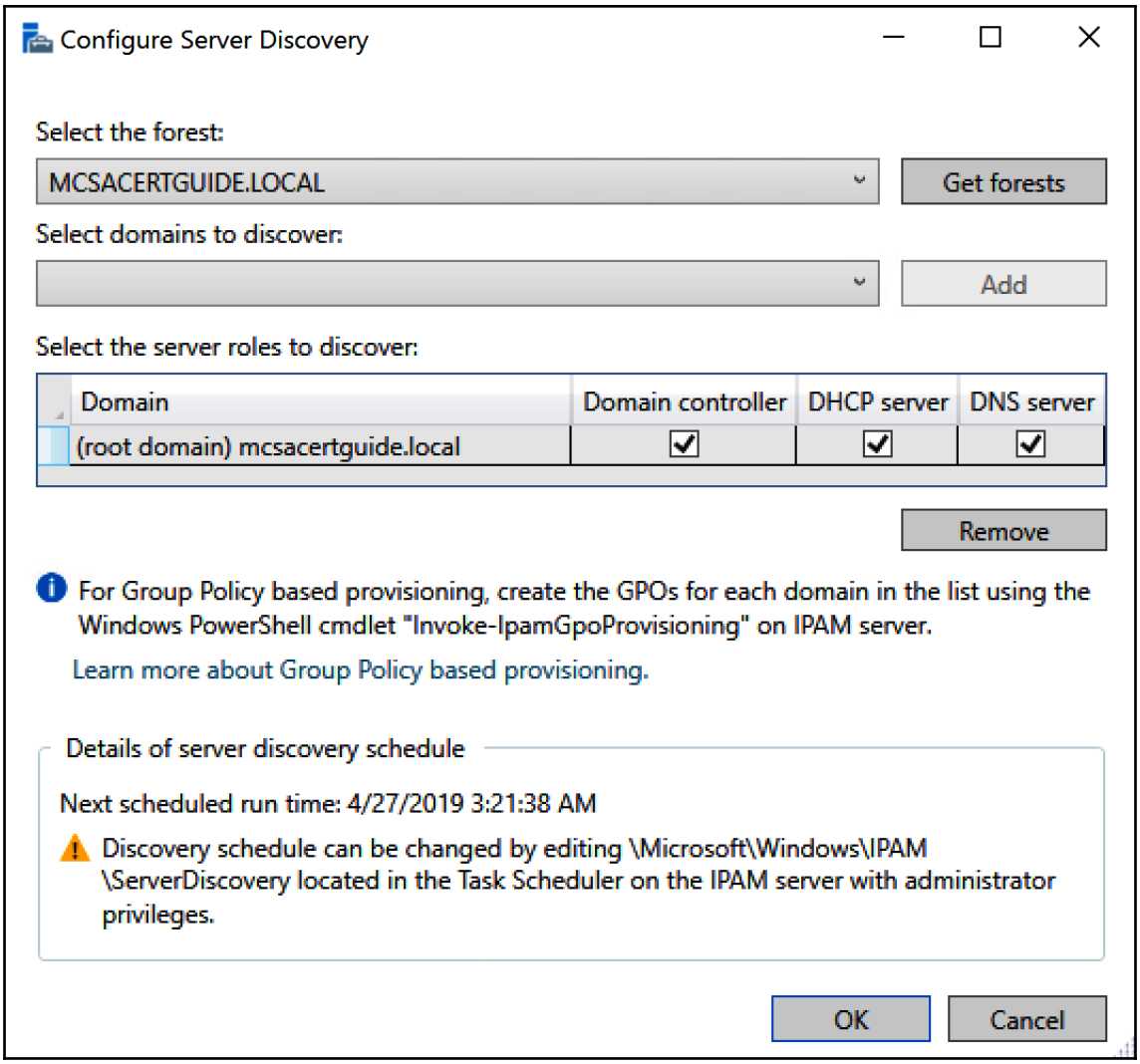

Provision IPAM
Before you begin
Before you begin
Configure database
Select provisioning method
Summary
Completion
IP Address Management (IPAM) provides a centralized management, monitoring, and auditing platform for IP address space and corresponding infrastructure servers on your network. IPAM provides this functionality by accessing the following Windows servers:
DHCP Server
DNS Server
Network Policy Server (NPS)
Active Directory Domain Controller (DC)
You can choose these servers to be managed or unmanaged by IPAM. Managed servers must be configured with access settings that allow IPAM to remotely manage, monitor or audit them. You can either configure these settings manually on each server, or IPAM can provision managed servers automatically using Group Policy Objects (GPOs).
This wizard also allows you to choose and optionally create an IPAM database. Local security groups are also created during provisioning that can be used to assign administrator roles.
If you choose the GPO-based provisioning method, you cannot change to the manual method after completing this wizard. However, you can use the Set-IpamConfiguration Windows PowerShell cmdlet to change from manual to GPO-based provisioning later if desired.
Learn more about IPAM
< Previous
Next >
Apply
Cancel

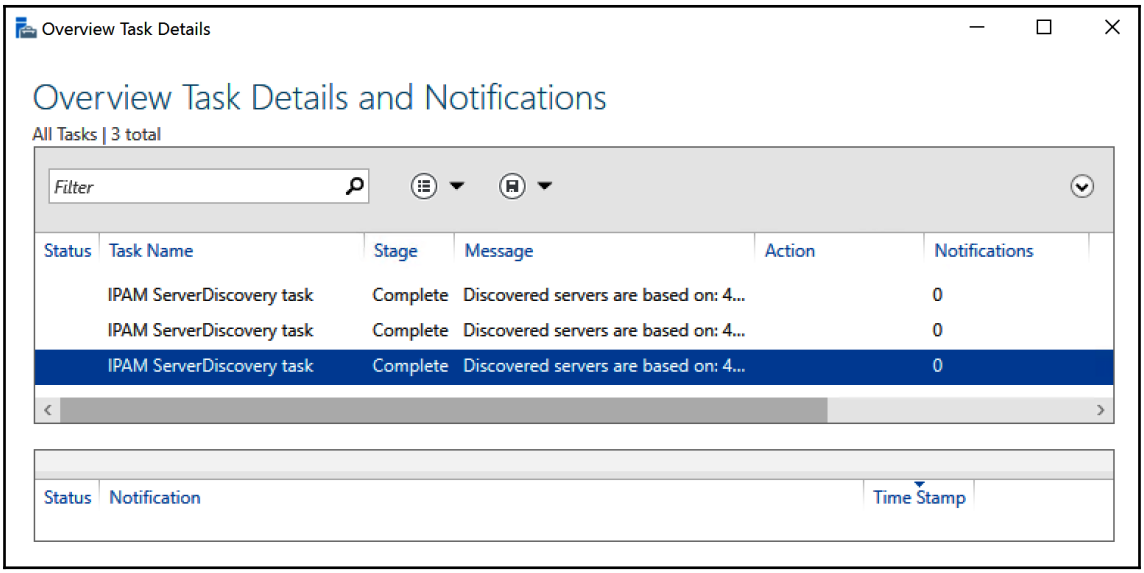

Provision IPAM
Configure database
Before you begin
Configure database
Select provisioning method
Summary
Completion
IPAM can be configured to store data in a Windows Internal Database or in a Microsoft SQL Server database. To use SQL, the database server must be running SQL Server 2008 R2 or later.
Specify the type of IPAM database:
Windows Internal Database (WID)
* Enter the location where IPAM will store the database and log files:
%WINDIR%\System32\IPAM\DataBase
Use Default
Microsoft SQL Server
* Server name:
* Database name:
* Port:
1433
Create a new schema
The database can be migrated from WID to SQL, or its settings modified using Move-IpamDatabase and Set-IpamDatabase Windows PowerShell cmdlets for IPAM Server.
Learn more about the IPAM database
< Previous
Next >
Apply
Cancel

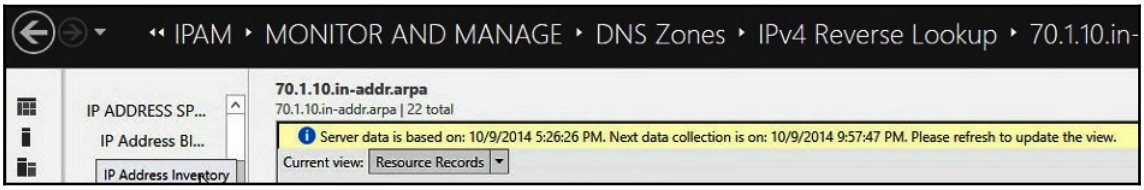

Provision IPAM
Select provisioning method
Before you begin
Configure database
Select provisioning method
Summary
Completion
Managed servers must be configured with settings that allow IPAM to access remote management functions and event information.
Select a provisioning method for managed servers:
Manual
The manual provisioning method requires that you configure the required network shares, security groups, and firewall rules manually on each managed server.
Group Policy Based
The Group Policy based provisioning method requires Group Policy Objects (GPO) to be created in each domain that you manage with this IPAM server. IPAM will automatically configure settings on managed servers by adding the server to appropriate GPO. This can be especially useful in a large network with many managed servers. GPOs that you create must follow naming conventions used by IPAM, however you can customize the GPO name with a prefix of your choice. The GPO name prefix you specify should be unique for each IPAM server in the Active Directory forest.
* GPO name prefix:
IPAM1
You can create GPOs in each IPAM managed domain using the Invoke-IpamGpoProvisiong IPAM Windows PowerShell cmdlet.
Learn more about access provisioning on managed servers
< Previous
Next >
Apply
Cancel

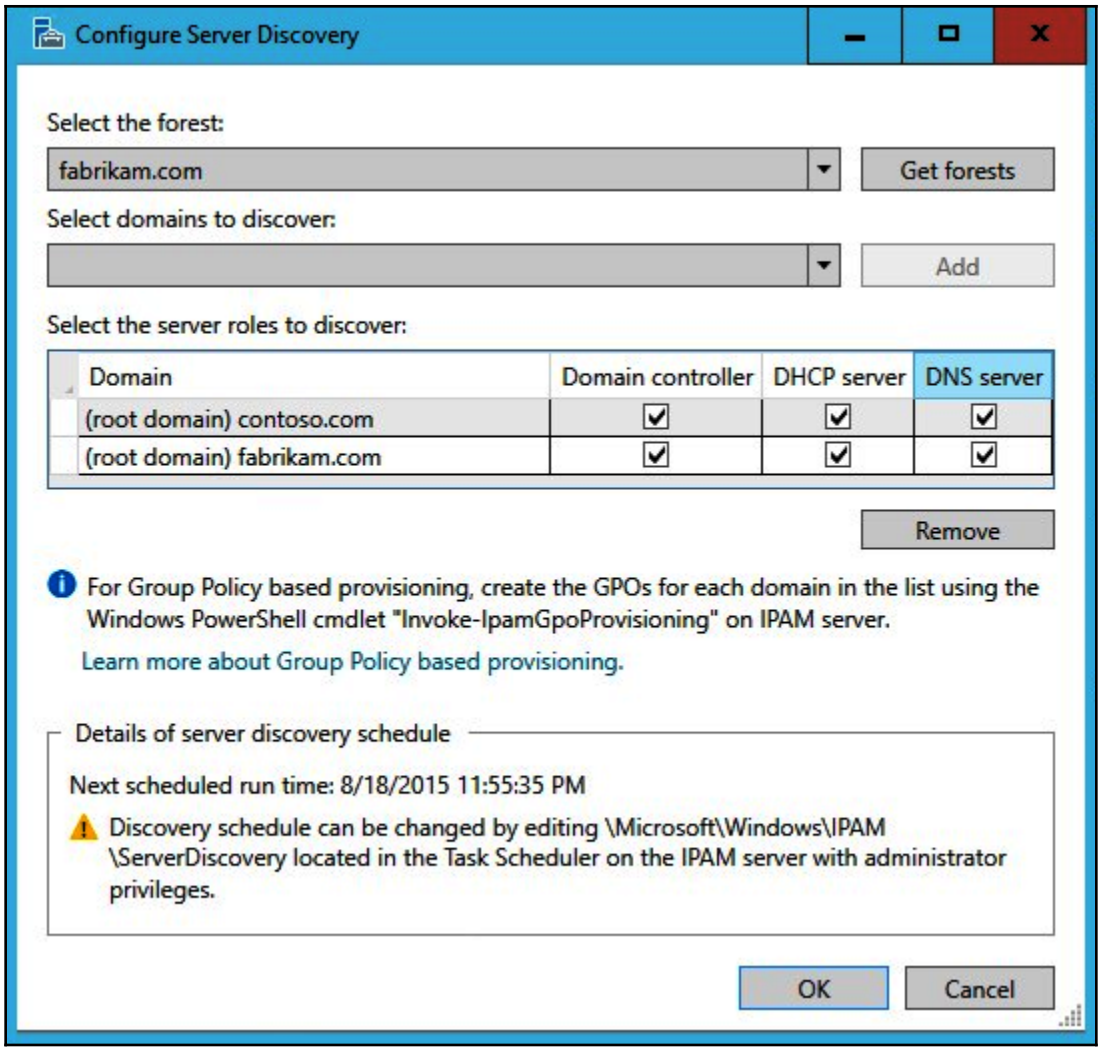

Provision IPAM
Summary
Before you begin
Configure database
Select provisioning method
Summary
Completion
Confirm the Settings
This wizard will make the following changes:
Provision the IPAM server to use the GPO-based provisioning method. IPAM will use Group Policy to configure required access settings on the managed servers. These settings will be applied on managed servers using the following GPOs:
IPAM1_DHCP for DHCP servers
IPAM1_DNS for DNS servers
IPAM1_DC_NPS for domain controllers and NPS servers
Create IPAM provisioning GPOs in each IPAM managed domain using the Invoke-IpamGpoProvisiong IPAM Windows PowerShell cmdlet. Domain Admin privileges are required to create and apply these GPOs.
Create IPAM database on WID and configure access.
Create scheduled tasks on the IPAM server to collect data from the network.
Create local security groups on the IPAM server used to assign administrator roles.
Enable IP address tracking capability on the IPAM server.
Click Apply to confirm these settings.
If you choose the GPO-based provisioning method, you cannot change to the manual method after completing this wizard. However, you can use the Set-IpamConfiguration Windows PowerShell cmdlet to change from manual to GPO-based provisioning later if desired.
< Previous
Next >
Apply
Cancel


Provision IPAM
Completion
Before you begin
Configure database
Select provisioning method
Summary
Completion
IPAM provisioning completed successfully
The following settings were successfully provisioned:
The Group Policy based provisioning method is used to configure required access settings on managed servers. These settings will be applied on managed servers using the following GPOs:
IPAM1_DHCP for DHCP servers
IPAM1_DNS for DNS servers
IPAM1_DC_NPS for domain controllers and NPS servers
IPAM security groups created.
IPAM database created and access configured.
Access to IPAM tasks and folders configured.
IPAM database created on WID and access configured.
Next steps:
Create GPOs in each IPAM managed domain using the Invoke-IpamGpoProvisiong IPAM Windows PowerShell cmdlet. Domain Administrator privileges will be required to create the GPOs.
< Previous
Next >
Close
Cancel

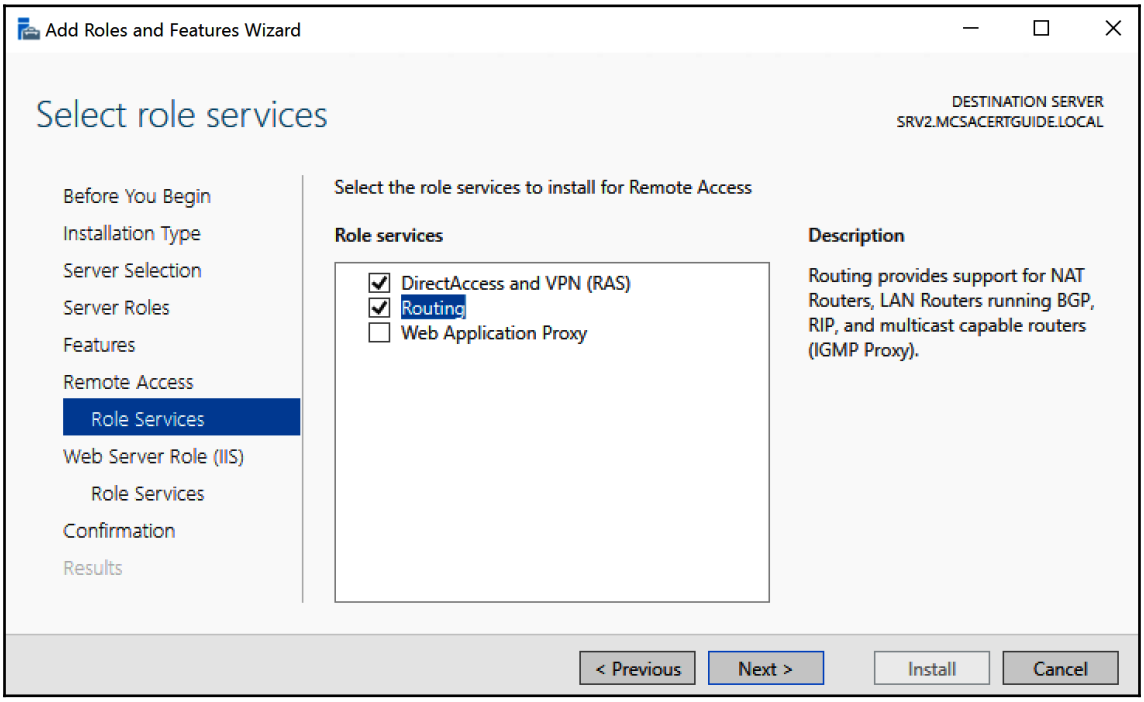

Configure Server Discovery
Select the forest:
MCSACERTGUIDE.LOCAL
Get forests
Select domains to discover:
Add
Select the server roles to discover:
Domain
Domain controller
DHCP server
DNS server
(root domain) mcsacertguide.local
Remove
For Group Policy based provisioning, create the GPOs for each domain in the list using the Windows PowerShell cmdlet "Invoke-IpamGpoProvisioning" on IPAM server.
Learn more about Group Policy based provisioning.
Details of server discovery schedule
Next scheduled run time: 4/27/2019 3:21:38 AM
Discovery schedule can be changed by editing \Microsoft\Windows\IPAM \ServerDiscovery located in the Task Scheduler on the IPAM server with administrator privileges.
OK
Cancel

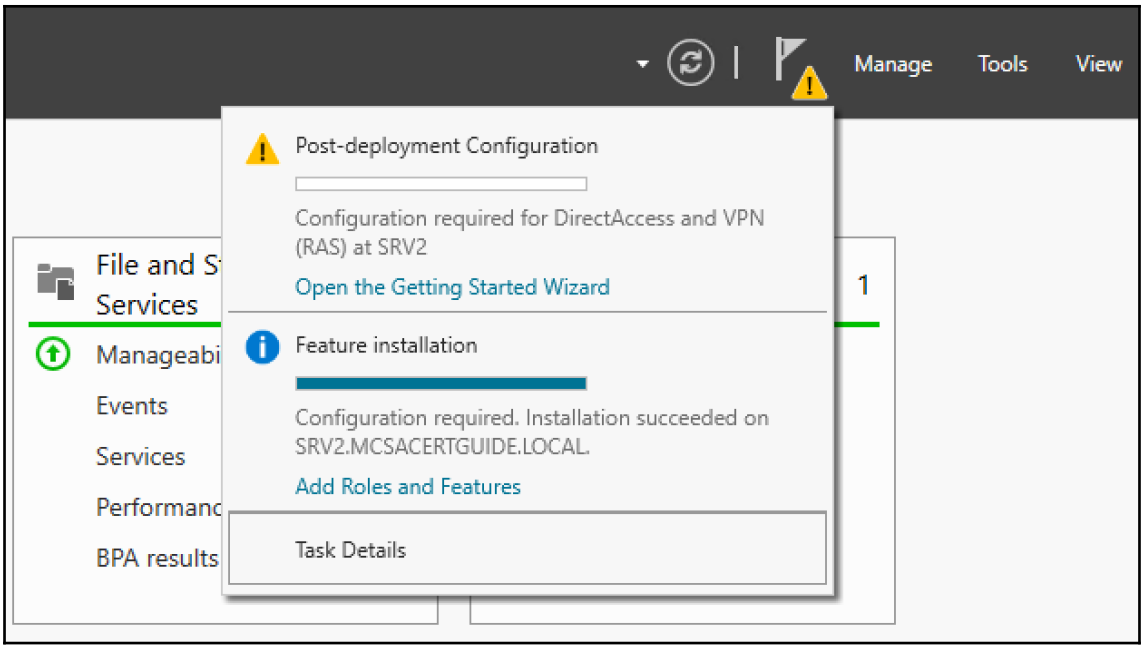

Overview Task Details
Overview Task Details and Notifications
All Tasks | 3 total
Filter
Status
Task Name
Stage
Message
Action
Notifications
IPAM ServerDiscovery task
Complete
Discovered servers are based on: 4...
0
IPAM ServerDiscovery task
Complete
Discovered servers are based on: 4...
0
IPAM ServerDiscovery task
Complete
Discovered servers are based on: 4...
0
Status
Notification
Time Stamp

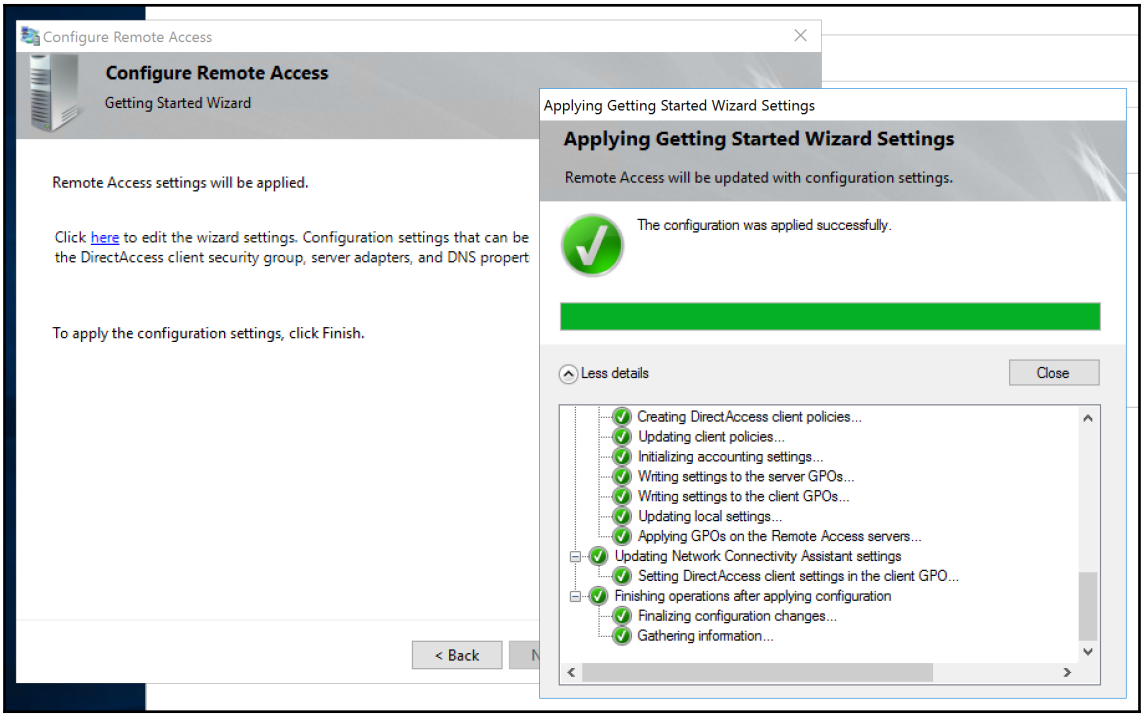

IPAM ▸ MONITOR AND MANAGE ▸ DNS Zones ▸ IPv4 Reverse Lookup ▸ 70.1.10.in-
IP ADDRESS SP...
IP Address Bl...
IP Address Inventory
70.1.10.in-addr.arpa
70.1.10.in-addr.arpa | 22 total
Server data is based on: 10/9/2014 5:26:26 PM. Next data collection is on: 10/9/2014 9:57:47 PM. Please refresh to update the view.
Current view:
Resource Records

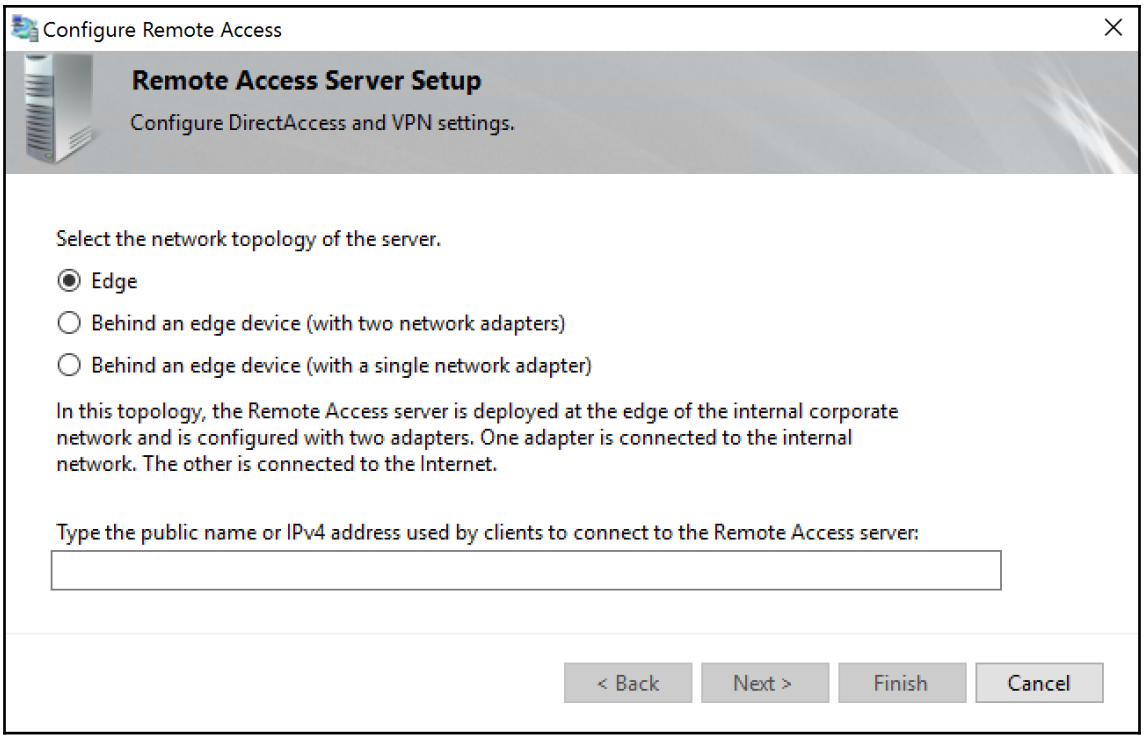

Configure Server Discovery
Select the forest:
fabrikam.com
Get forests
Select domains to discover:
Add
Select the server roles to discover:
Domain
Domain controller
DHCP server
DNS server
(root domain) contoso.com
(root domain) fabrikam.com
Remove
For Group Policy based provisioning, create the GPOs for each domain in the list using the Windows PowerShell cmdlet "Invoke-IpamGpoProvisioning" on IPAM server.
Learn more about Group Policy based provisioning.
Details of server discovery schedule
Next scheduled run time: 8/18/2015 11:55:35 PM
Discovery schedule can be changed by editing \Microsoft\Windows\IPAM \ServerDiscovery located in the Task Scheduler on the IPAM server with administrator privileges.
OK
Cancel

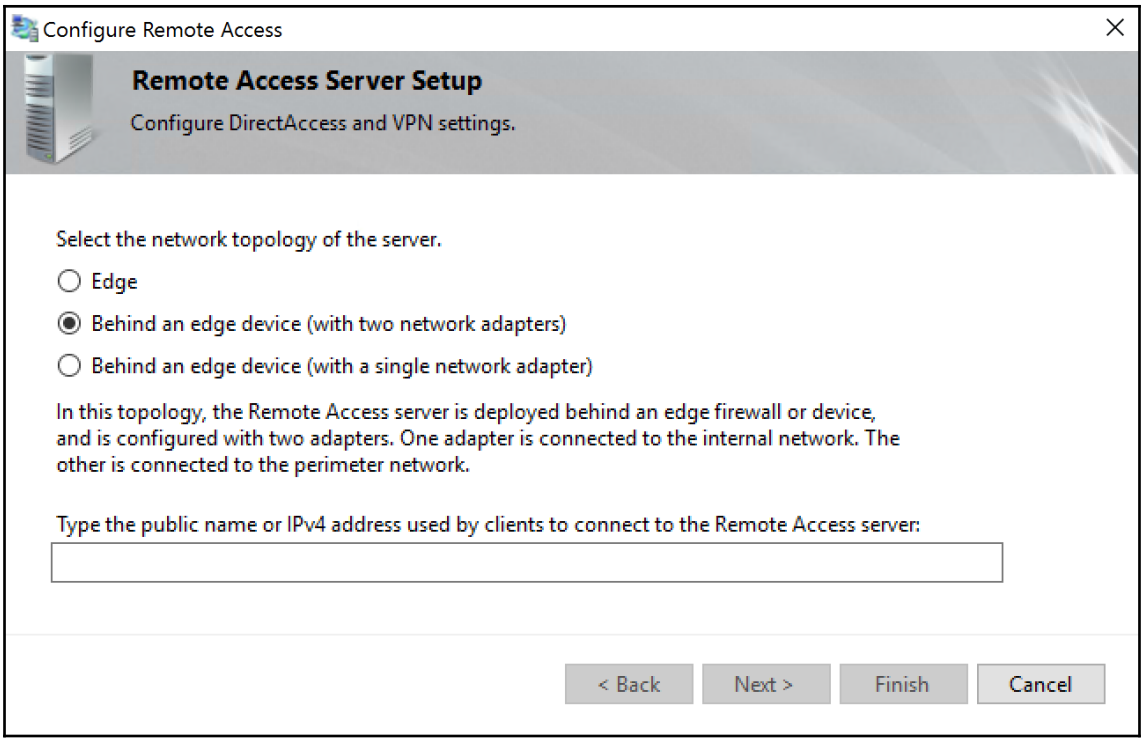
Chapter 5: Implementing Network Access

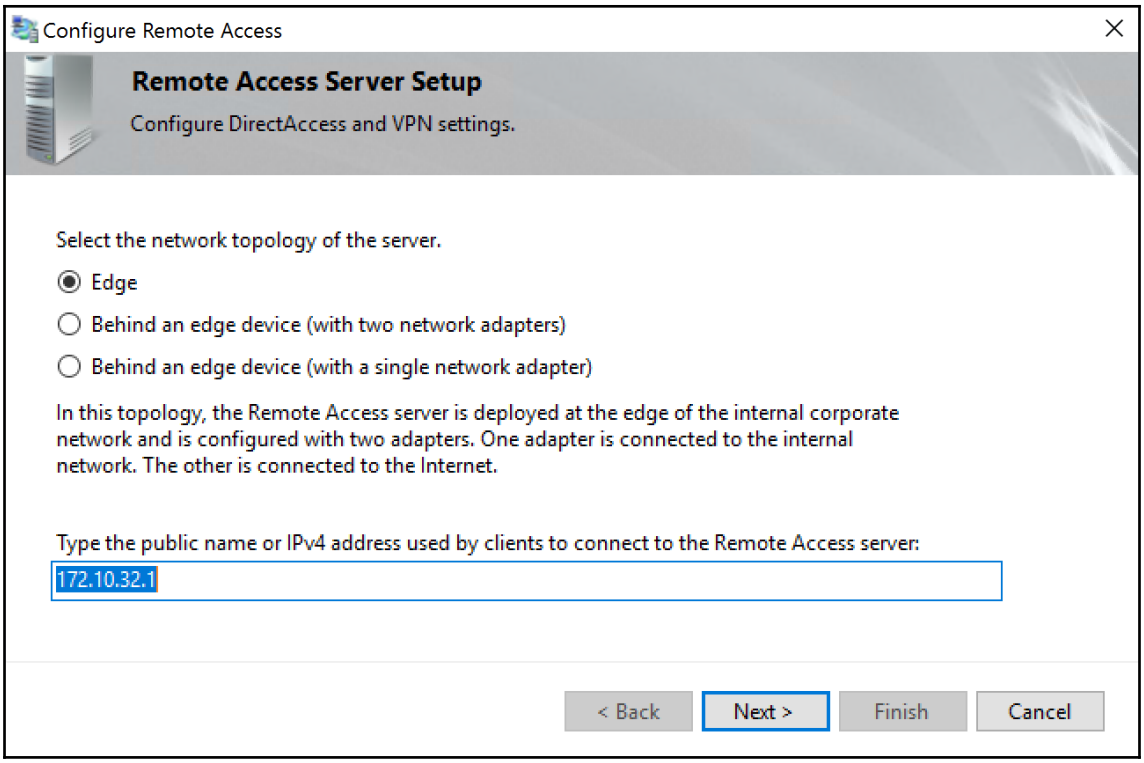


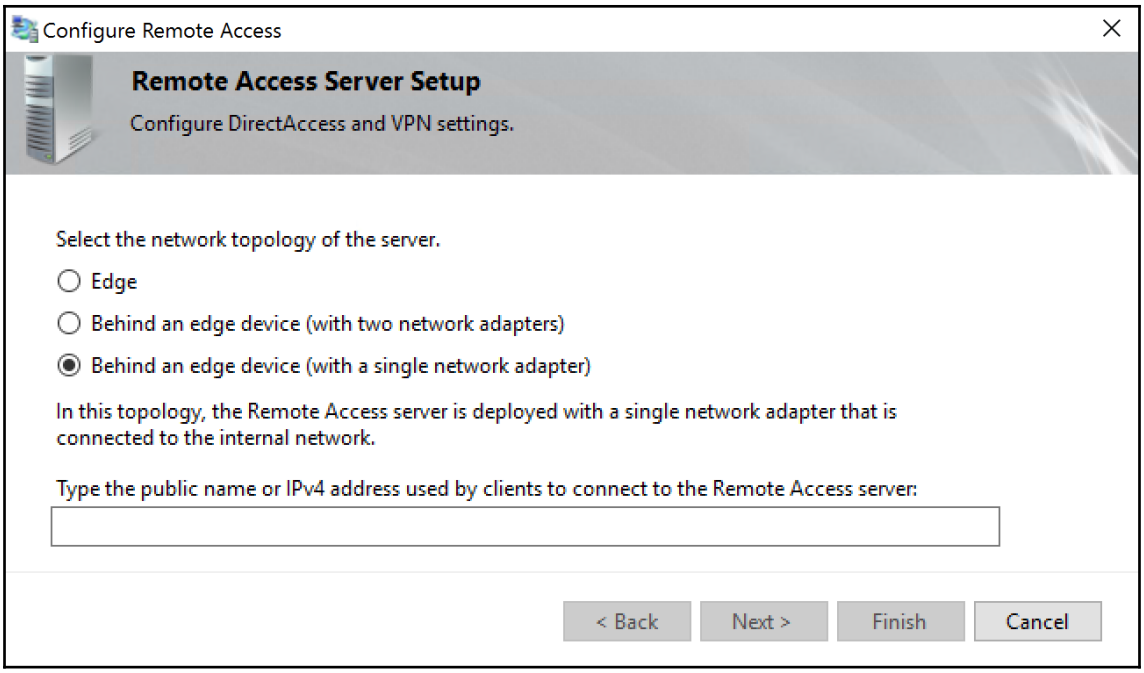

Manage
Tools
View
Post-deployment Configuration
Configuration required for DirectAccess and VPN (RAS) at SRV2
Open the Getting Started Wizard
Feature installation
Configuration required. Installation succeeded on SRV2.MCSACERTGUIDE.LOCAL.
Add Roles and Features
Task Details
File and S
Services
Manageabi
Events
Services
Performanc
BPA results
1

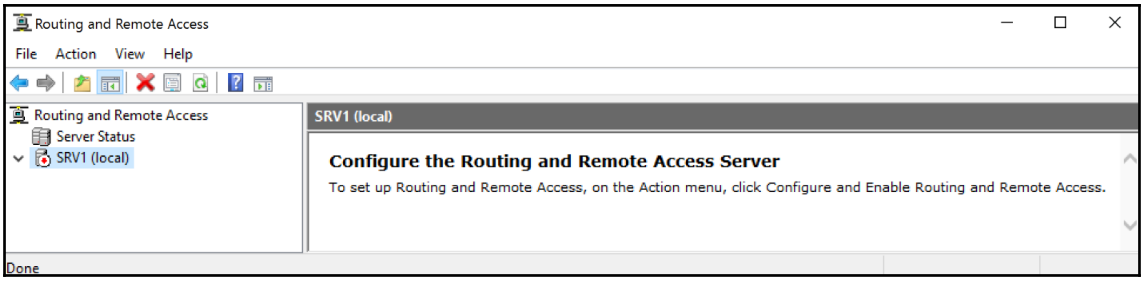

Configure Remote Access
Configure Remote Access
Getting Started Wizard
Remote Access settings will be applied.
Click here to edit the wizard settings. Configuration settings that can be
the DirectAccess client security group, server adapters, and DNS propert
To apply the configuration settings, click Finish.
< Back
Applying Getting Started Wizard Settings
Applying Getting Started Wizard Settings
Remote Access will be updated with configuration settings.
The configuration was applied successfully.
Less details
Close
Creating DirectAccess client policies...
Updating client policies...
Initializing accounting settings...
Writing settings to the server GPOs...
Writing settings to the client GPOs...
Updating local settings...
Applying GPOs on the Remote Access servers...
Updating Network Connectivity Assistant settings
Setting DirectAccess client settings in the client GPO...
Finishing operations after applying configuration
Finalizing configuration changes...
Gathering information...

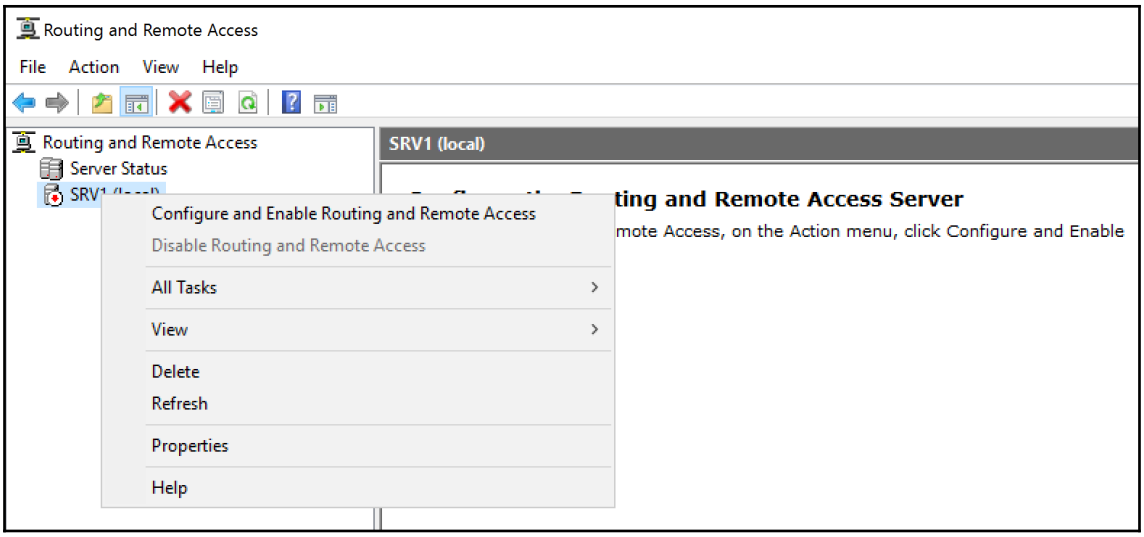

Configure Remote Access
Remote Access Server Setup
Configure DirectAccess and VPN settings.
Select the network topology of the server.
Edge
Behind an edge device (with two network adapters)
Behind an edge device (with a single network adapter)
In this topology, the Remote Access server is deployed at the edge of the internal corporate network and is configured with two adapters. One adapter is connected to the internal network. The other is connected to the Internet.
Type the public name or IPv4 address used by clients to connect to the Remote Access server:
< Back
Next >
Finish
Cancel

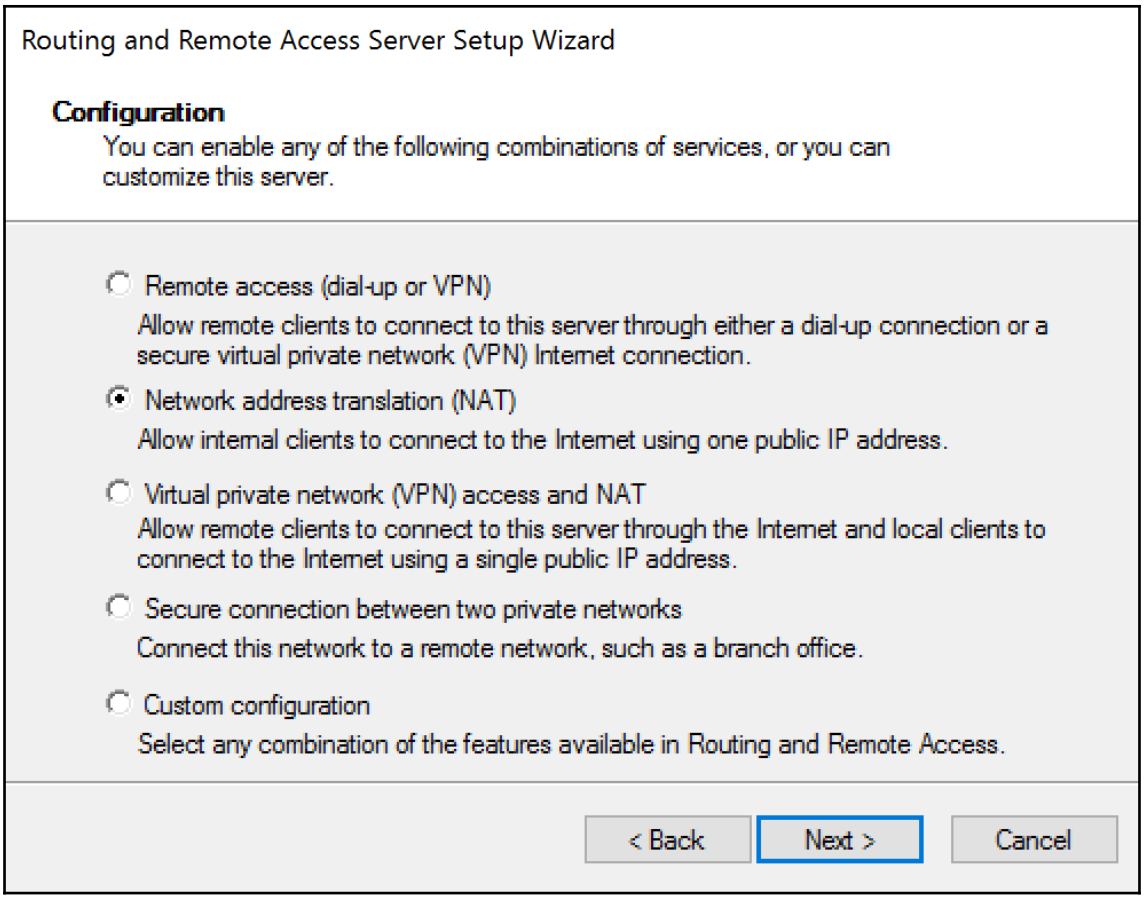

Configure Remote Access
Remote Access Server Setup
Configure DirectAccess and VPN settings.
Select the network topology of the server.
Edge
Behind an edge device (with two network adapters)
Behind an edge device (with a single network adapter)
In this topology, the Remote Access server is deployed behind an edge firewall or device, and is configured with two adapters. One adapter is connected to the internal network. The other is connected to the perimeter network.
Type the public name or IPv4 address used by clients to connect to the Remote Access server:
< Back
Next >
Finish
Cancel

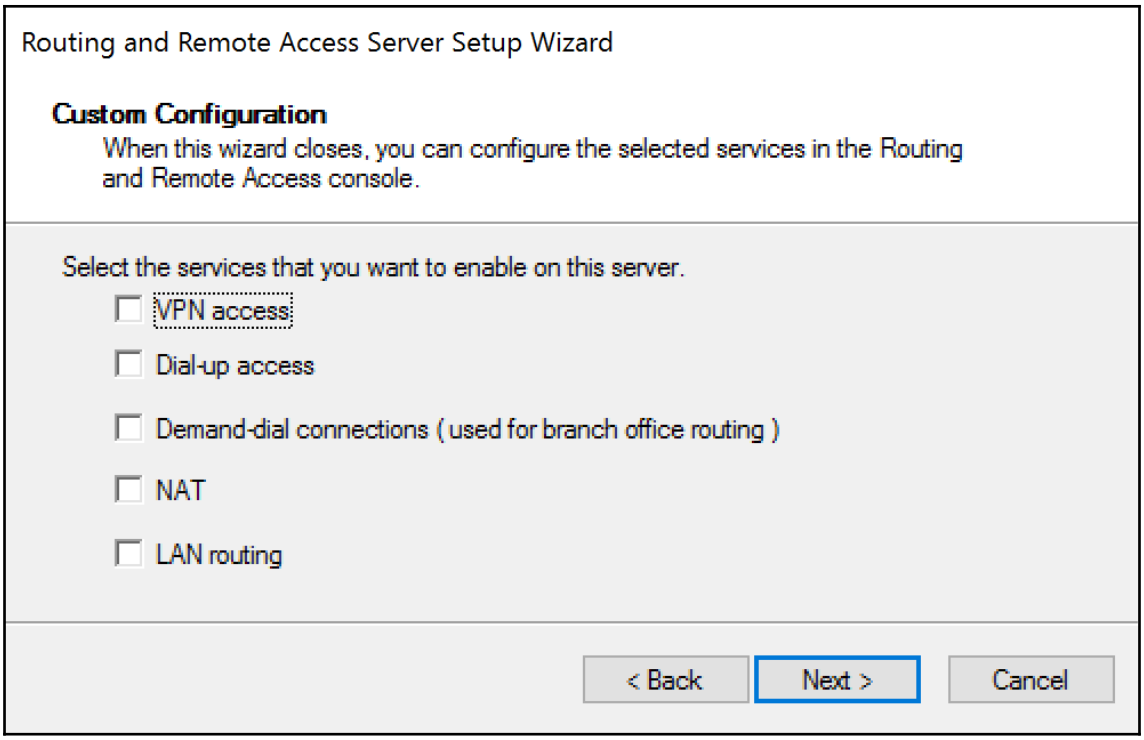

Configure Remote Access
Remote Access Server Setup
Configure DirectAccess and VPN settings.
Select the network topology of the server.
Edge
Behind an edge device (with two network adapters)
Behind an edge device (with a single network adapter)
In this topology, the Remote Access server is deployed at the edge of the internal corporate network and is configured with two adapters. One adapter is connected to the internal network. The other is connected to the Internet.
Type the public name or IPv4 address used by clients to connect to the Remote Access server:
172.10.32.1
< Back
Next >
Finish
Cancel

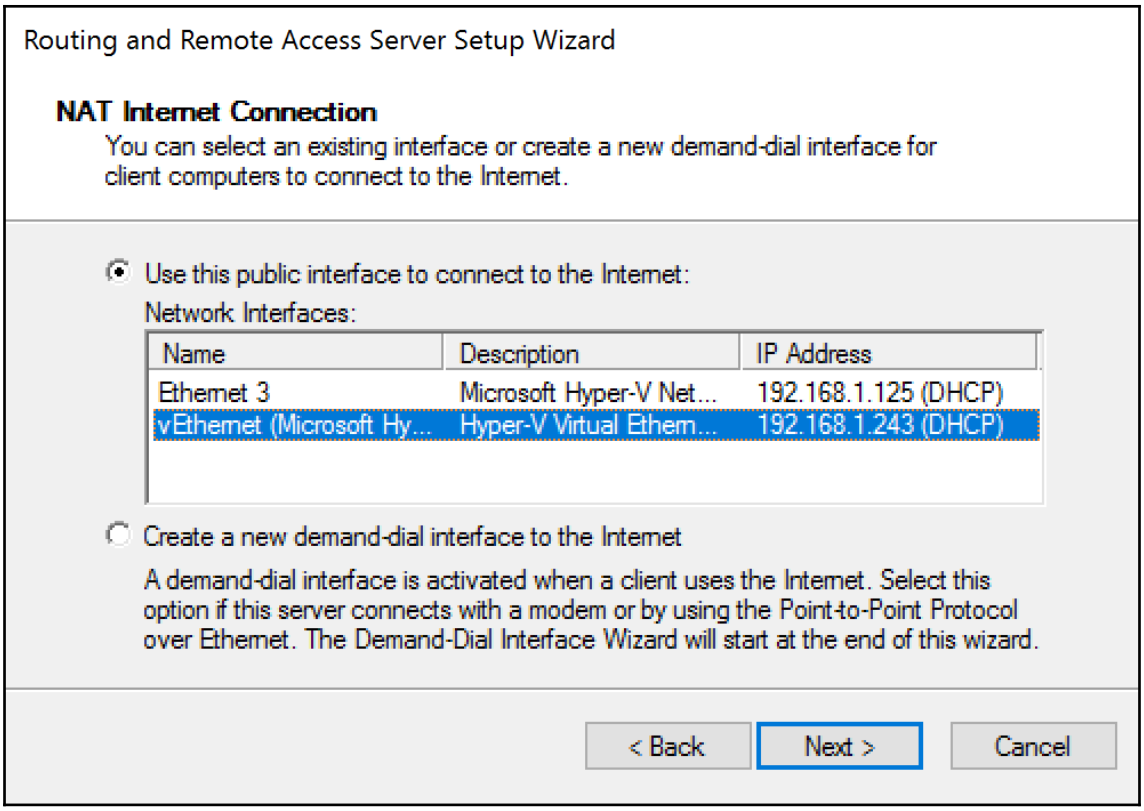

Configure Remote Access
Remote Access Server Setup
Configure DirectAccess and VPN settings.
Select the network topology of the server.
Edge
Behind an edge device (with two network adapters)
Behind an edge device (with a single network adapter)
In this topology, the Remote Access server is deployed with a single network adapter that is connected to the internal network.
Type the public name or IPv4 address used by clients to connect to the Remote Access server:
< Back
Next >
Finish
Cancel

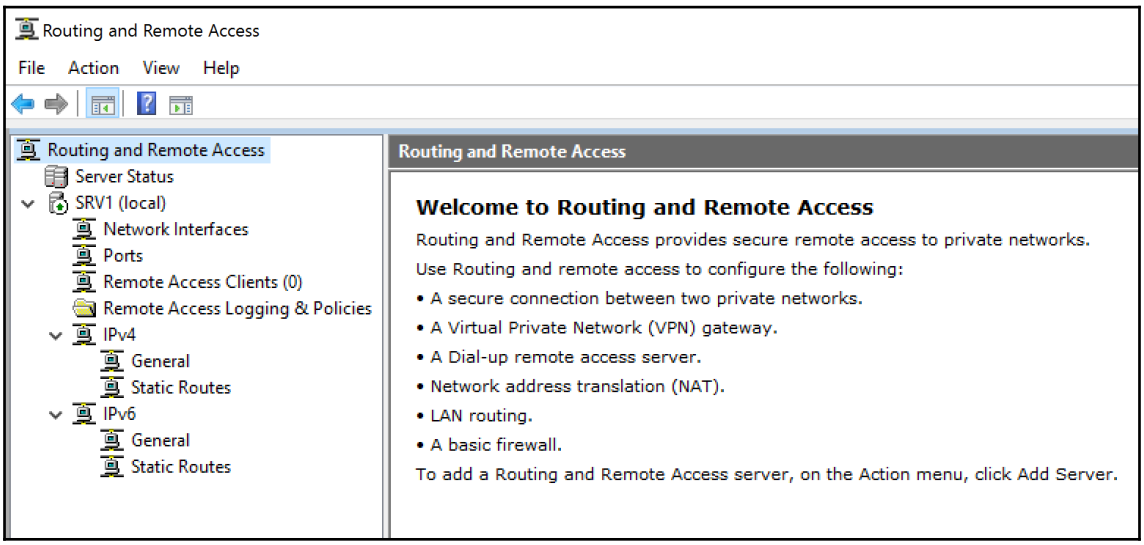

Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
SRV1 (local)
SRV1 (local)
Configure the Routing and Remote Access Server
To set up Routing and Remote Access, on the Action menu, click Configure and Enable Routing and Remote Access.
Done

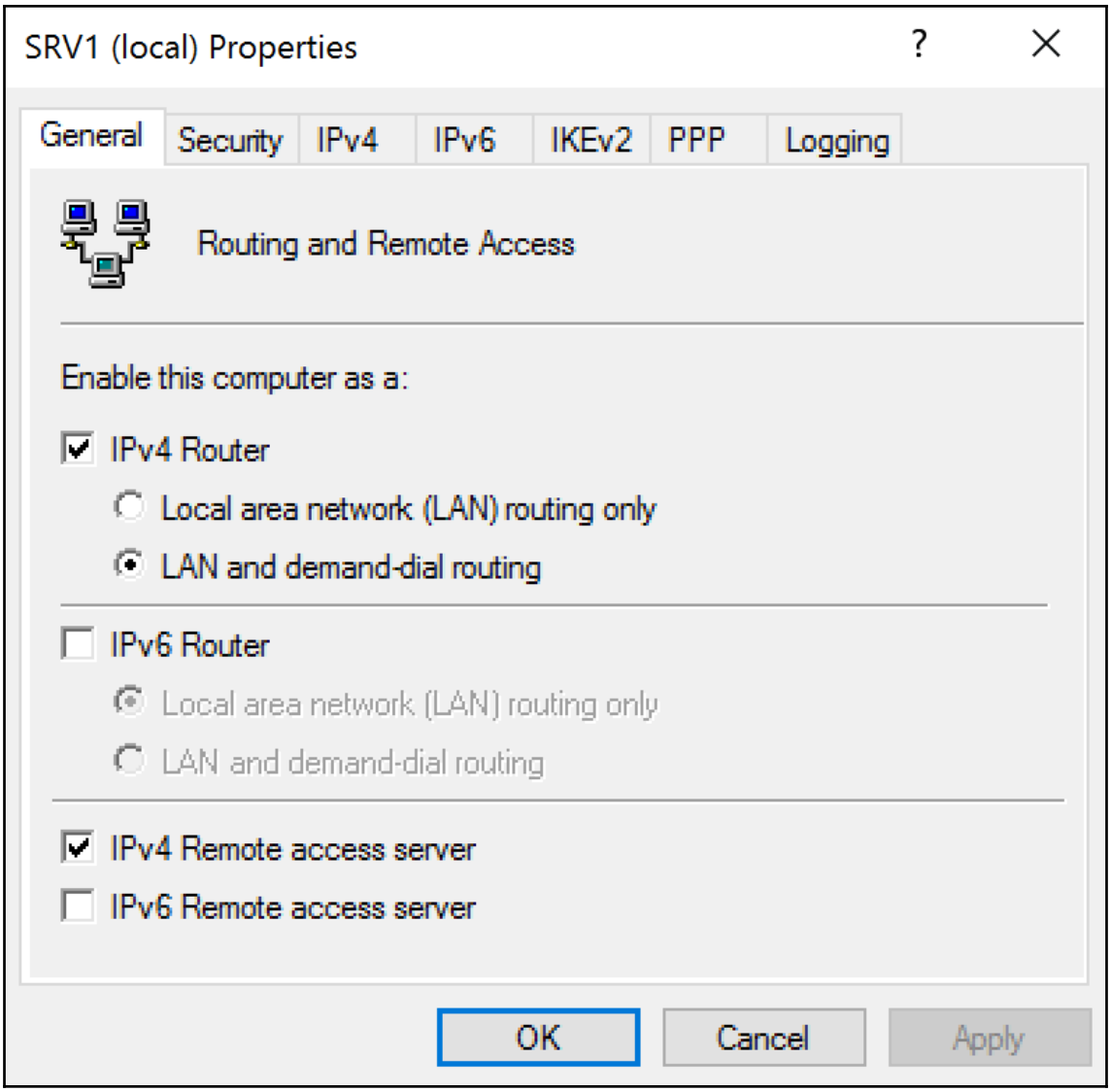

Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
SRV1 (local)
ting and Remote Access Server
mote Access, on the Action menu, click Configure and Enable
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
Delete
Refresh
Properties
Help

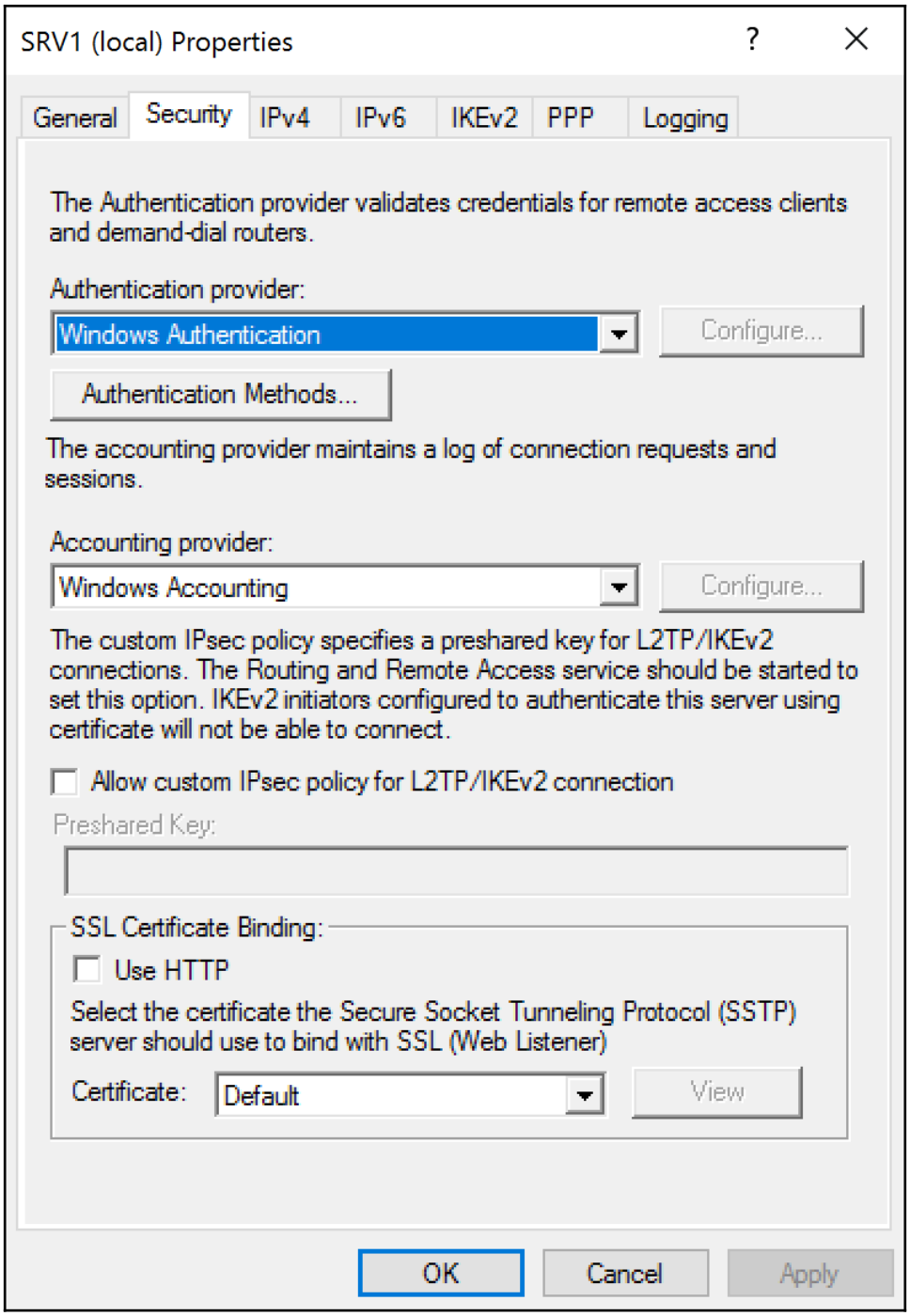

Routing and Remote Access Server Setup Wizard
Configuration
You can enable any of the following combinations of services, or you can customize this server.
Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
Custom configuration
Select any combination of the features available in Routing and Remote Access.
< Back
Next >
Cancel

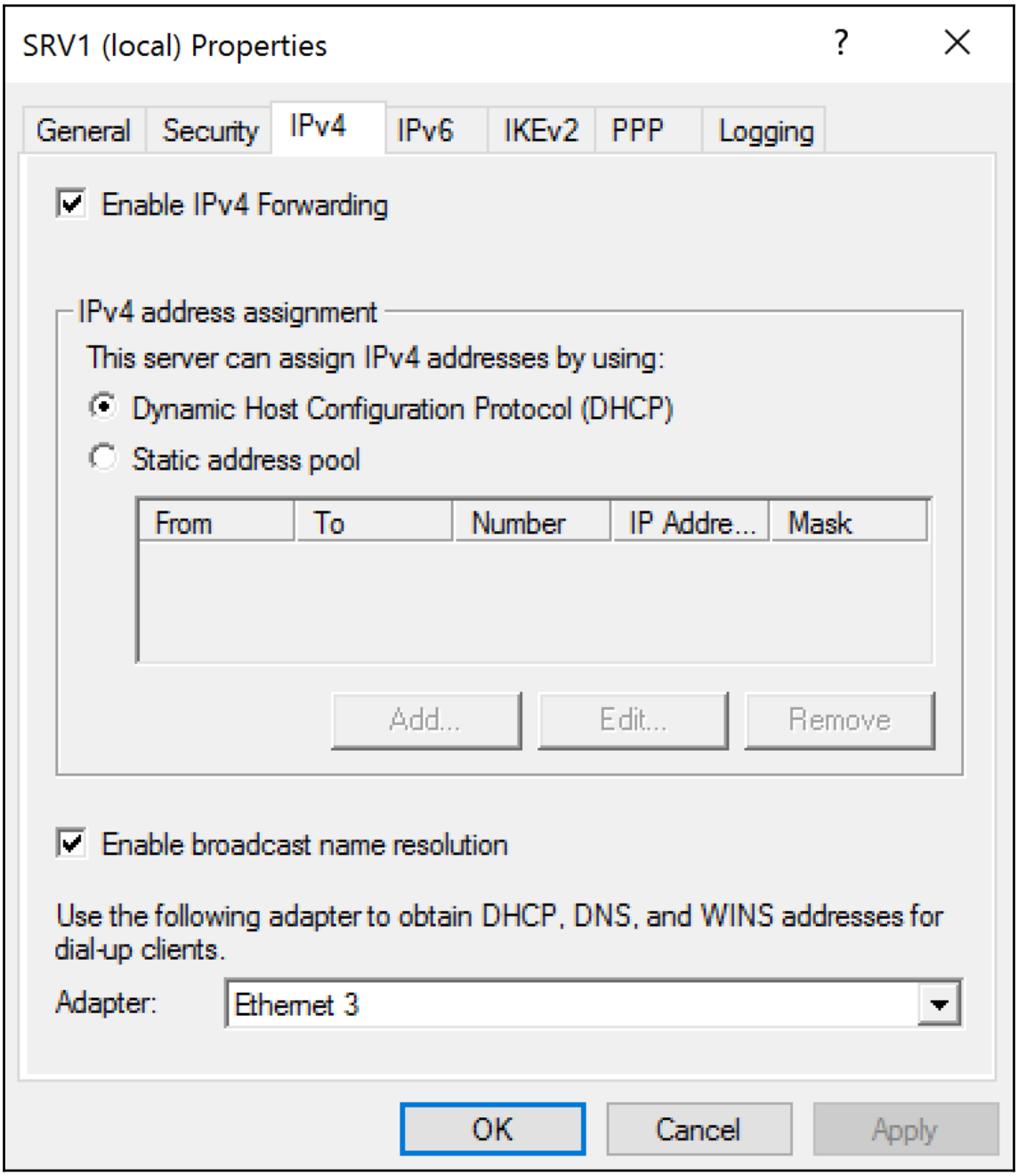

Routing and Remote Access Server Setup Wizard
Custom Configuration
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.
Select the services that you want to enable on this server.
VPN access
Dial-up access
Demand-dial connections (used for branch office routing)
NAT
LAN routing
< Back
Next >
Cancel

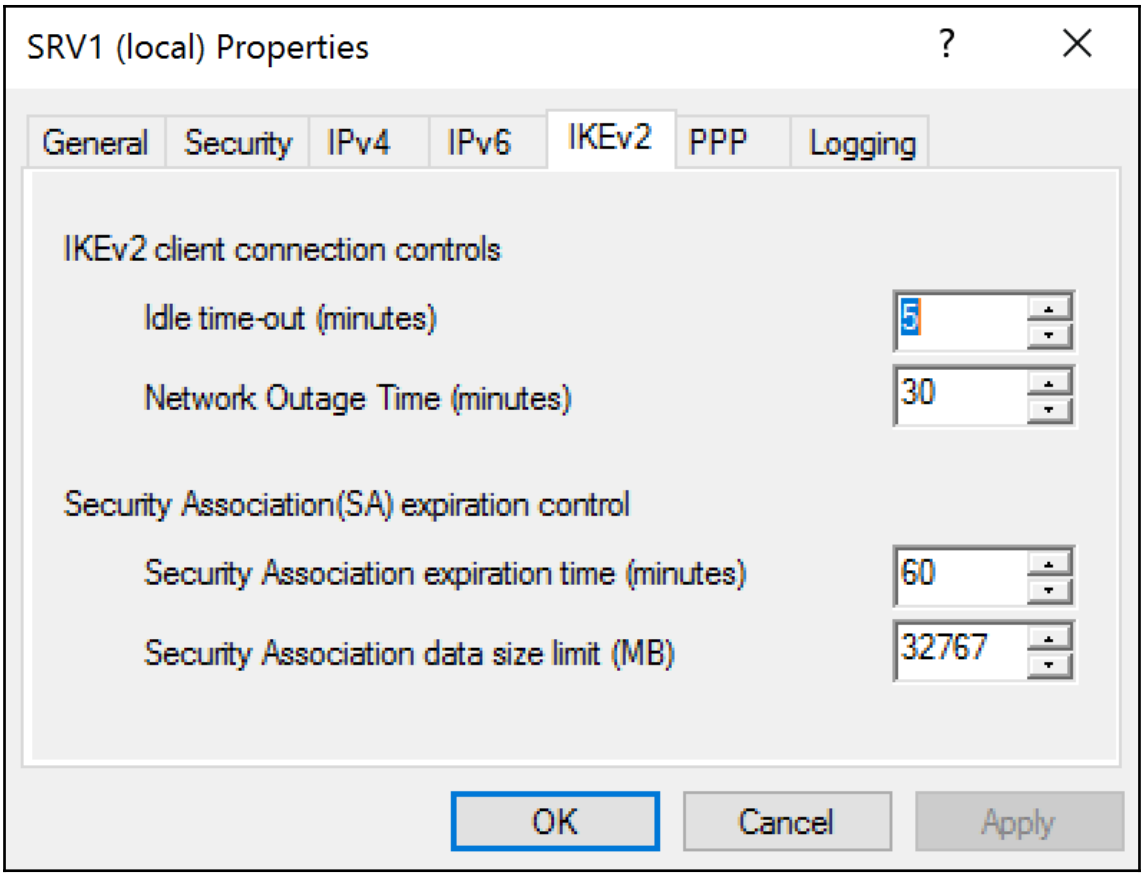

Routing and Remote Access Server Setup Wizard
NAT Internet Connection
You can select an existing interface or create a new demand-dial interface for client computers to connect to the Internet.
Use this public interface to connect to the Internet:
Network Interfaces:
Name
Description
IP Address
Ethernet 3
Microsoft Hyper-V Net...
192.168.1.125 (DHCP)
vEthernet (Microsoft Hy...
Hyper-V Virtual Ethern...
192.168.1.243 (DHCP)
Create a new demand-dial interface to the Internet
A demand-dial interface is activated when a client uses the Internet. Select this option if this server connects with a modem or by using the Point-to-Point Protocol over Ethernet. The Demand-Dial Interface Wizard will start at the end of this wizard.
< Back
Next >
Cancel

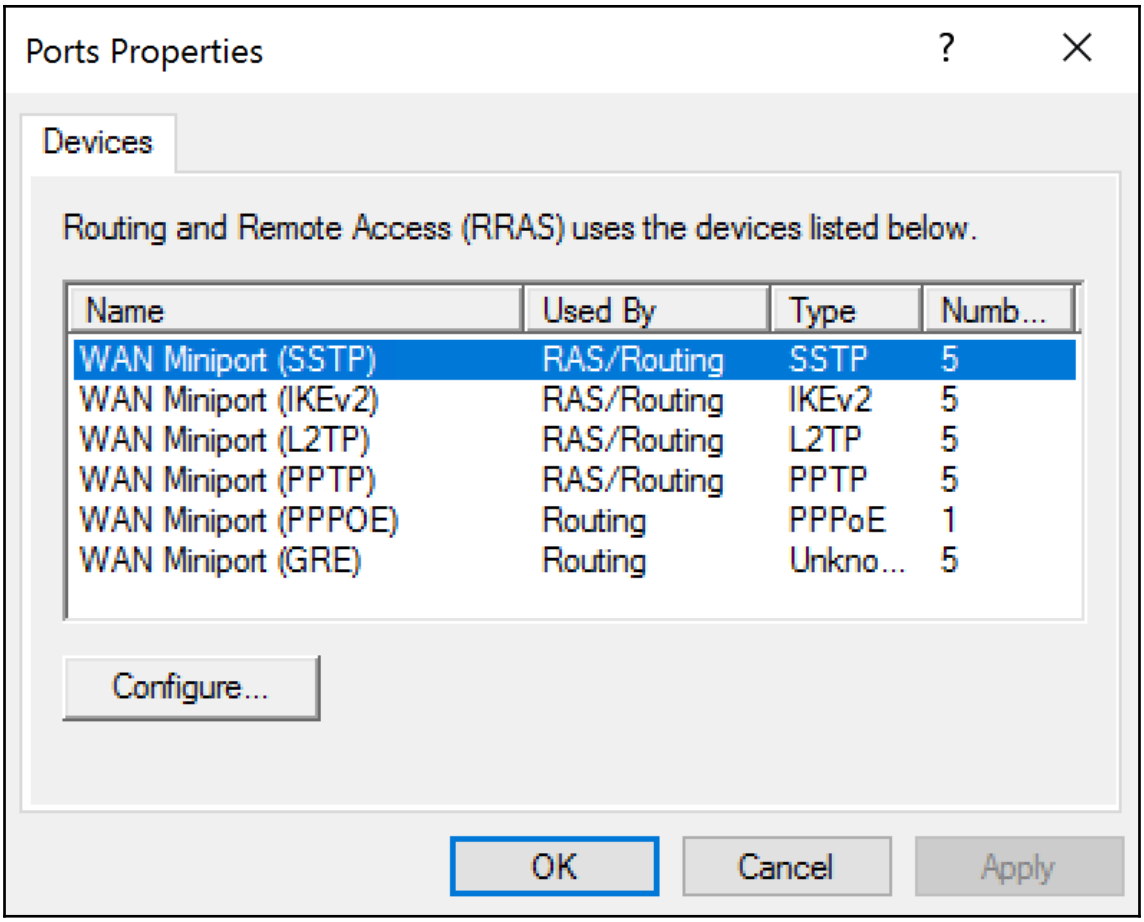

Routing and Remote Access
File
Action
View
Help
Routing and Remote Access
Server Status
SRV1 (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging & Policies
IPv4
General
Static Routes
IPv6
General
Static Routes
Routing and Remote Access
Welcome to Routing and Remote Access
Routing and Remote Access provides secure remote access to private networks.
Use Routing and remote access to configure the following:
• A secure connection between two private networks.
• A Virtual Private Network (VPN) gateway.
• A Dial-up remote access server.
• Network address translation (NAT).
• LAN routing.
• A basic firewall.
To add a Routing and Remote Access server, on the Action menu, click Add Server.

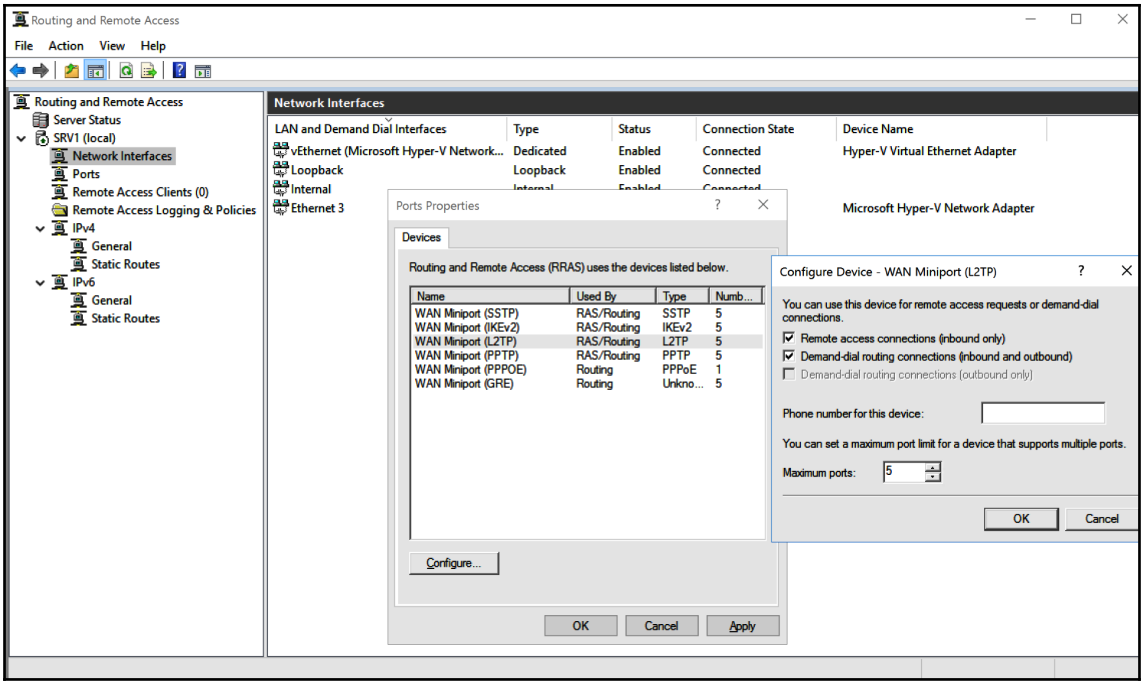

SRV1 (local) Properties
General
Security
IPv4
IPv6
IKEv2
PPP
Logging
Routing and Remote Access
Enable this computer as a:
IPv4 Router
Local area network (LAN) routing only
LAN and demand-dial routing
IPv6 Router
Local area network (LAN) routing only
LAN and demand-dial routing
IPv4 Remote access server
IPv6 Remote access server
OK
Cancel
Apply

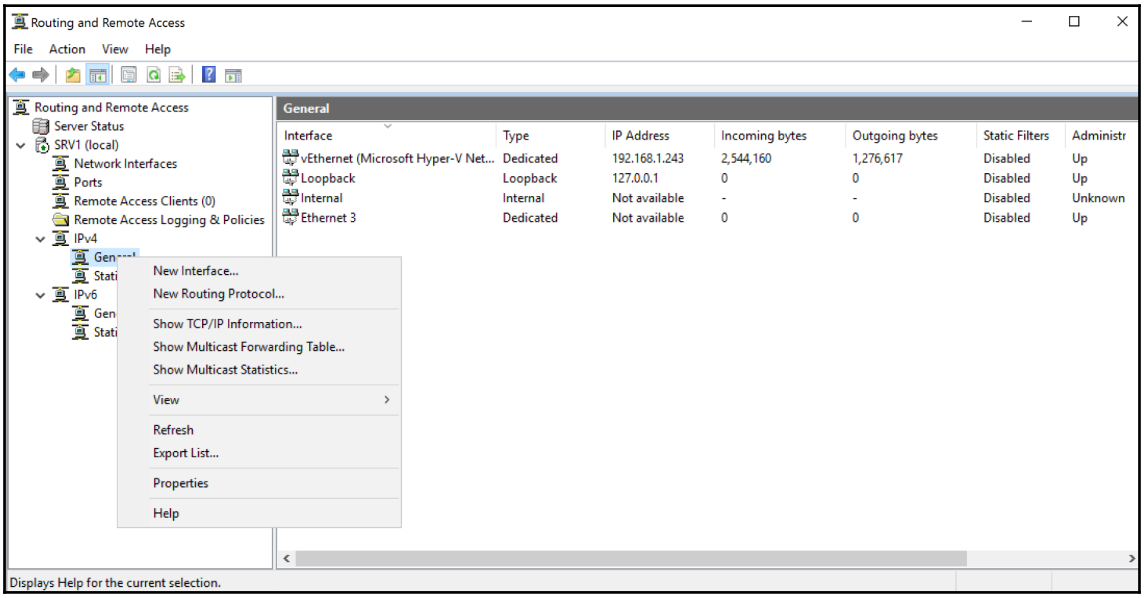

SRV1 (local) Properties
?
General
Security
IPv4
IPv6
IKEv2
PPP
Logging
The Authentication provider validates credentials for remote access clients and demand-dial routers.
Authentication provider:
Windows Authentication
Configure...
Authentication Methods...
The accounting provider maintains a log of connection requests and sessions.
Accounting provider:
Windows Accounting
Configure...
The custom IPsec policy specifies a preshared key for L2TP/IKEv2 connections. The Routing and Remote Access service should be started to set this option. IKEv2 initiators configured to authenticate this server using certificate will not be able to connect.
Allow custom IPsec policy for L2TP/IKEv2 connection
Preshared Key:
SSL Certificate Binding:
Use HTTP
Select the certificate the Secure Socket Tunneling Protocol (SSTP) server should use to bind with SSL (Web Listener)
Certificate:
Default
View
OK
Cancel
Apply

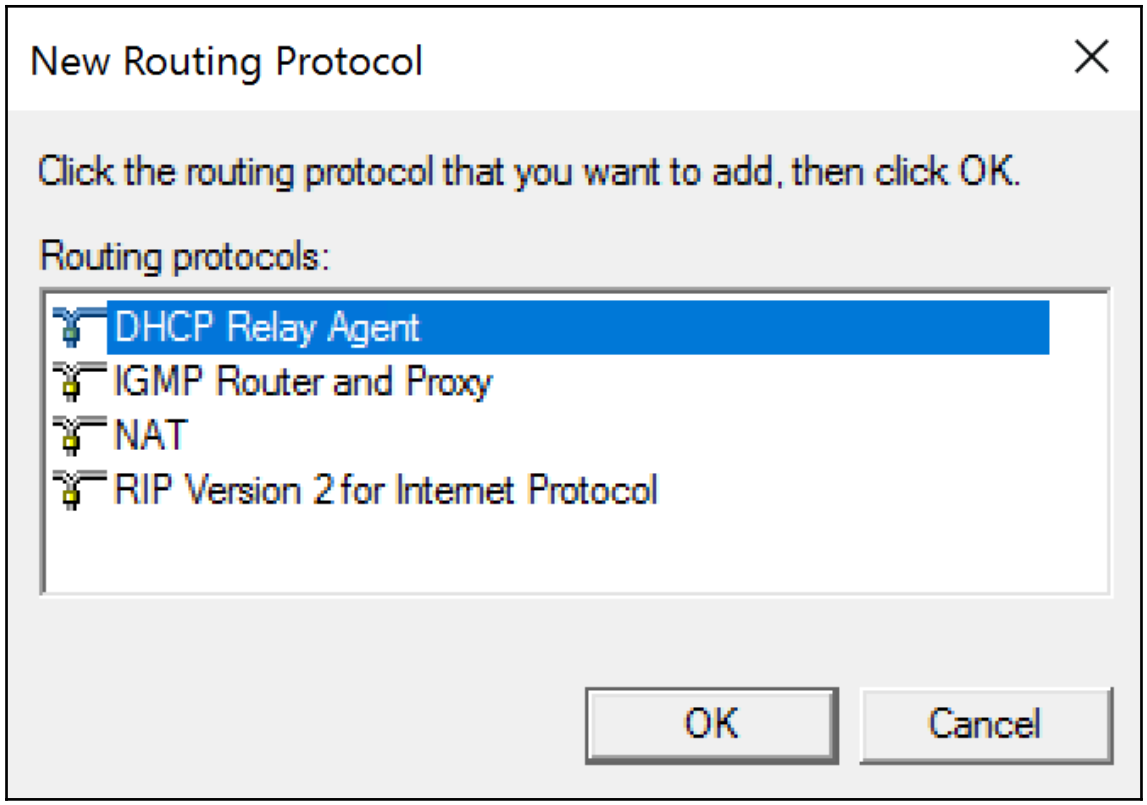

SRV1 (local) Properties
General
Security
IPv4
IPv6
IKEv2
PPP
Logging
Enable IPv4 Forwarding
IPv4 address assignment
This server can assign IPv4 addresses by using:
Dynamic Host Configuration Protocol (DHCP)
Static address pool
From
To
Number
IP Addre...
Mask
Add...
Edit...
Remove
Enable broadcast name resolution
Use the following adapter to obtain DHCP, DNS, and WINS addresses for dial-up clients.
Adapter:
Ethernet 3
OK
Cancel
Apply

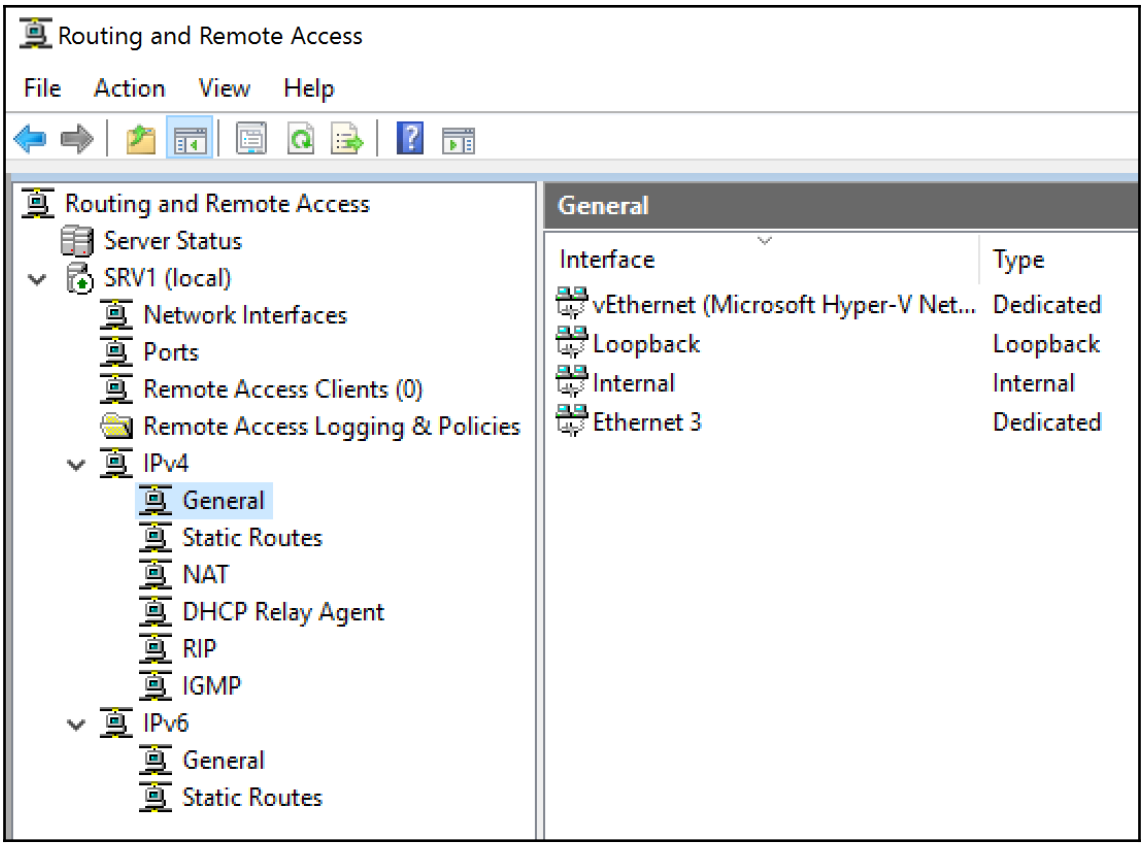

SRV1 (local) Properties
?
General
Security
IPv4
IPv6
IKEv2
PPP
Logging
IKEv2 client connection controls
Idle time-out (minutes)
5
Network Outage Time (minutes)
30
Security Association(SA) expiration control
Security Association expiration time (minutes)
60
Security Association data size limit (MB)
32767
OK
Cancel
Apply

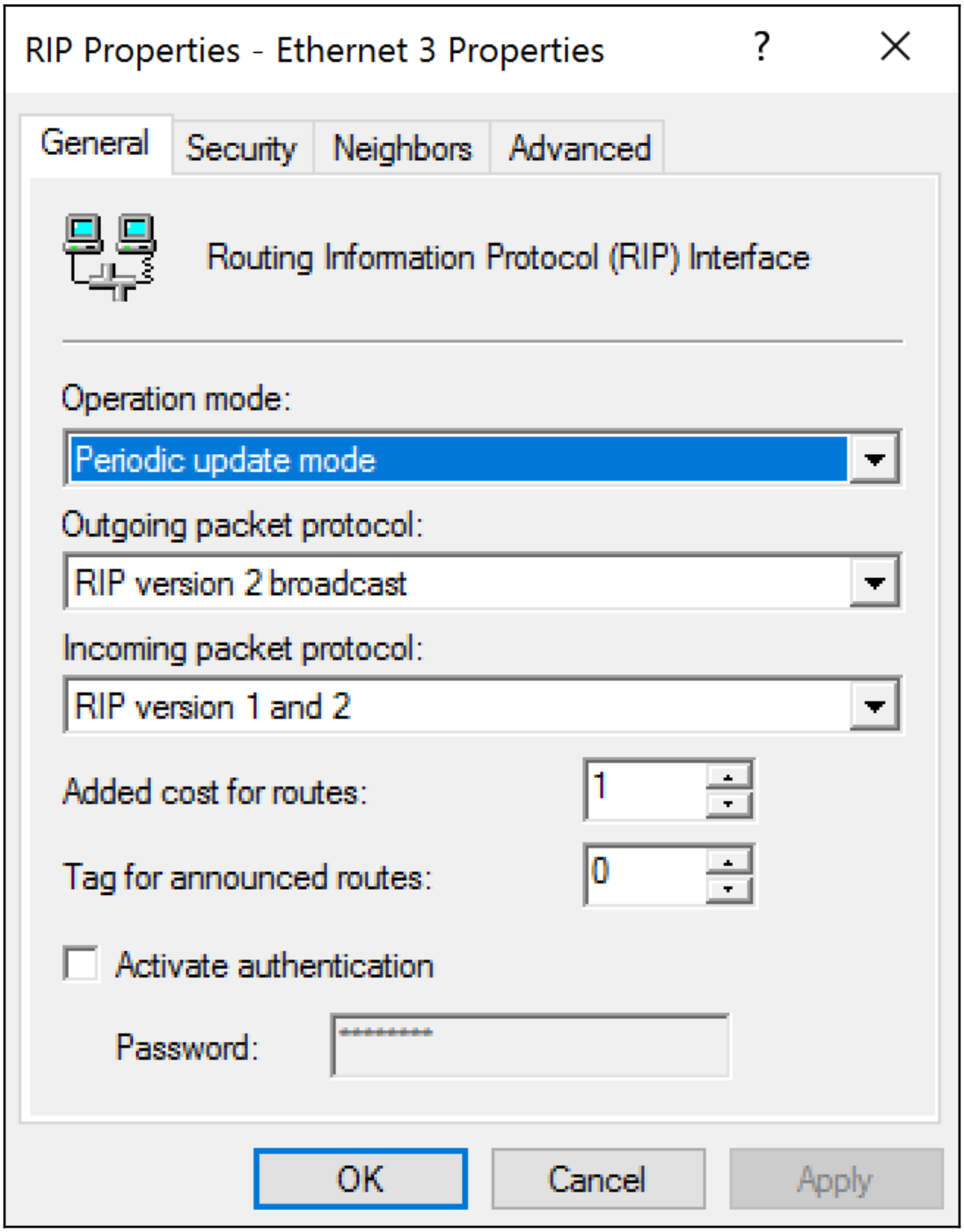

Ports Properties
?
Devices
Routing and Remote Access (RRAS) uses the devices listed below.
Name
Used By
Type
Numb...
WAN Miniport (SSTP)
RAS/Routing
SSTP
5
WAN Miniport (IKEv2)
RAS/Routing
IKEv2
5
WAN Miniport (L2TP)
RAS/Routing
L2TP
5
WAN Miniport (PPTP)
RAS/Routing
PPTP
5
WAN Miniport (PPPOE)
Routing
PPPoE
1
WAN Miniport (GRE)
Routing
Unkno...
5
Configure...
OK
Cancel
Apply

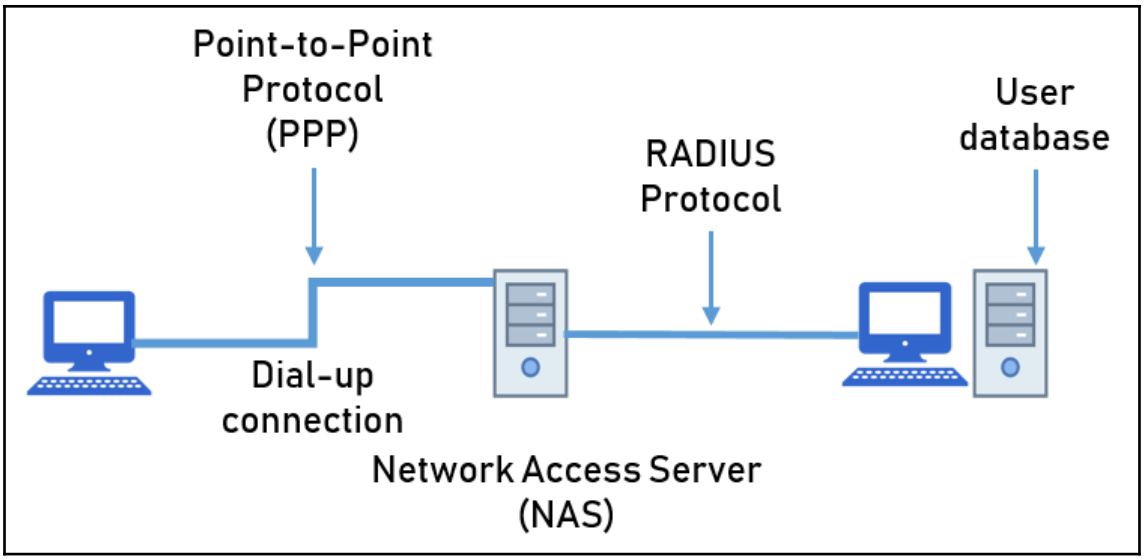

Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
SRV1 (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging & Policies
IPv4
General
Static Routes
IPv6
General
Static Routes
Network Interfaces
LAN and Demand Dial Interfaces
Type
Status
Connection State
Device Name
vEthernet (Microsoft Hyper-V Network...
Dedicated
Enabled
Connected
Hyper-V Virtual Ethernet Adapter
Loopback
Loopback
Enabled
Connected
Internal
Ethernet 3
Microsoft Hyper-V Network Adapter
Ports Properties
Devices
Routing and Remote Access (RRAS) uses the devices listed below.
Name
Used By
Type
Numb...
WAN Miniport (SSTP)
RAS/Routing
SSTP
5
WAN Miniport (IKEv2)
RAS/Routing
IKEv2
5
WAN Miniport (L2TP)
RAS/Routing
L2TP
5
WAN Miniport (PPTP)
RAS/Routing
PPTP
5
WAN Miniport (PPPOE)
Routing
PPPoE
1
WAN Miniport (GRE)
Routing
Unkno...
5
Configure...
OK
Cancel
Apply
Configure Device - WAN Miniport (L2TP)
You can use this device for remote access requests or demand-dial connections.
Remote access connections (inbound only)
Demand-dial routing connections (inbound and outbound)
Demand-dial routing connections (outbound only)
Phone number for this device:
You can set a maximum port limit for a device that supports multiple ports.
Maximum ports:
5
OK
Cancel


Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
SRV1 (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging & Policies
IPv4
IPv6
General
Interface
Type
IP Address
Incoming bytes
Outgoing bytes
Static Filters
Administr
vEthernet (Microsoft Hyper-V Net...
Dedicated
192.168.1.243
2,544,160
1,276,617
Disabled
Up
Loopback
Loopback
127.0.0.1
0
0
Disabled
Up
Internal
Internal
Not available
-
-
Disabled
Unknown
Ethernet 3
Dedicated
Not available
0
0
Disabled
Up
New Interface...
New Routing Protocol...
Show TCP/IP Information...
Show Multicast Forwarding Table...
Show Multicast Statistics...
View
Refresh
Export List...
Properties
Help
Displays Help for the current selection.

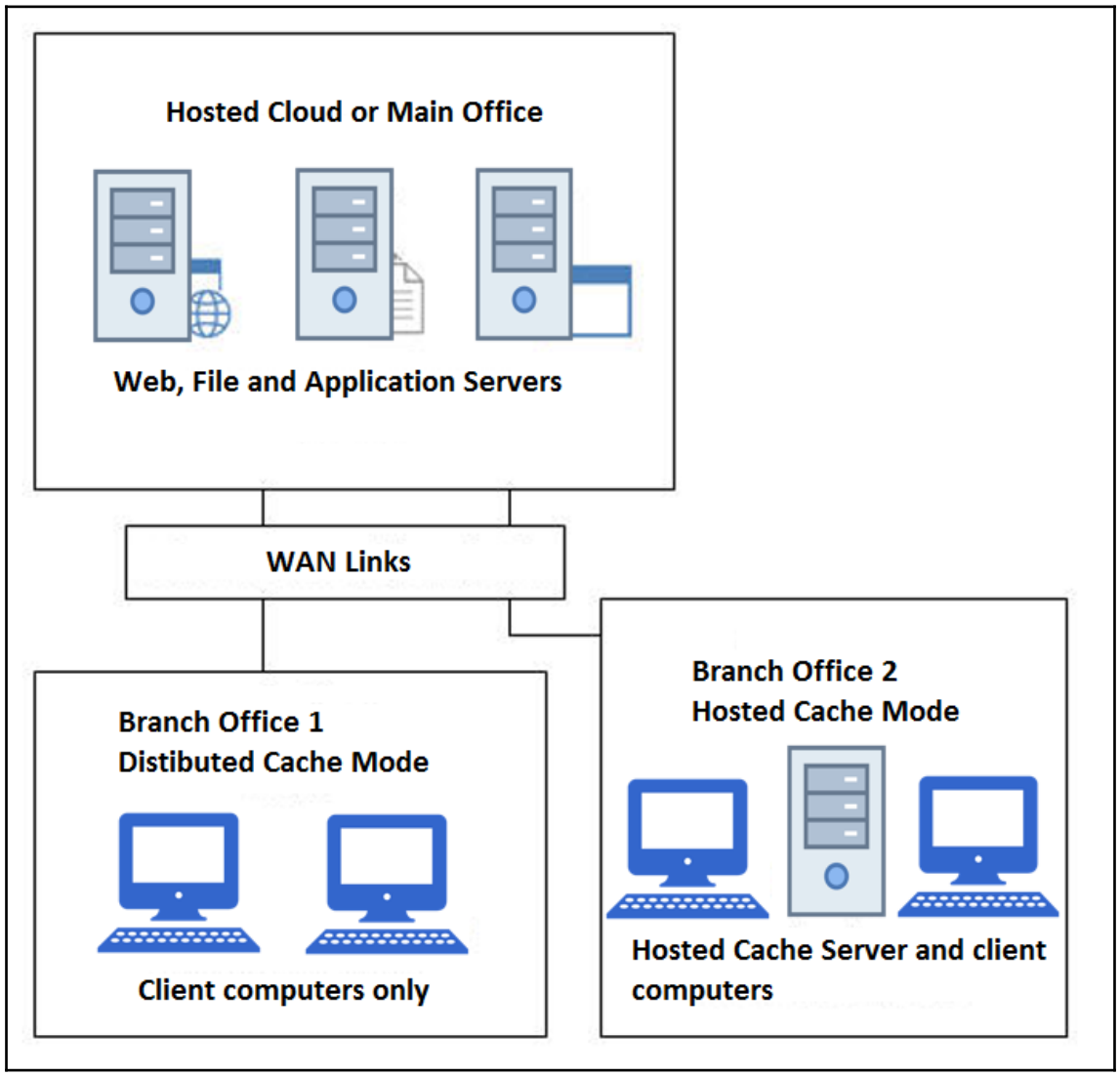

New Routing Protocol
Click the routing protocol that you want to add, then click OK.
Routing protocols:
DHCP Relay Agent
IGMP Router and Proxy
NAT
RIP Version 2 for Internet Protocol
OK
Cancel


Routing and Remote Access
File
Action
View
Help
Routing and Remote Access
Server Status
SRV1 (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging & Policies
IPv4
General
Static Routes
NAT
DHCP Relay Agent
RIP
IGMP
IPv6
General
Static Routes
General
Interface
Type
vEthernet (Microsoft Hyper-V Net...
Dedicated
Loopback
Loopback
Internal
Internal
Ethernet 3
Dedicated

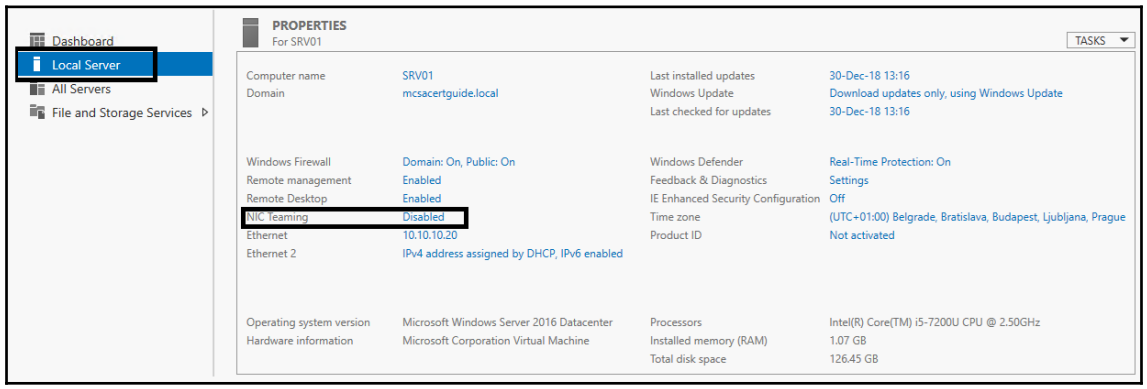

RIP Properties - Ethernet 3 Properties
General
Security
Neighbors
Advanced
Routing Information Protocol (RIP) Interface
Operation mode:
Periodic update mode
Outgoing packet protocol:
RIP version 2 broadcast
Incoming packet protocol:
RIP version 1 and 2
Added cost for routes:
1
Tag for announced routes:
0
Activate authentication
Password:
OK
Cancel
Apply

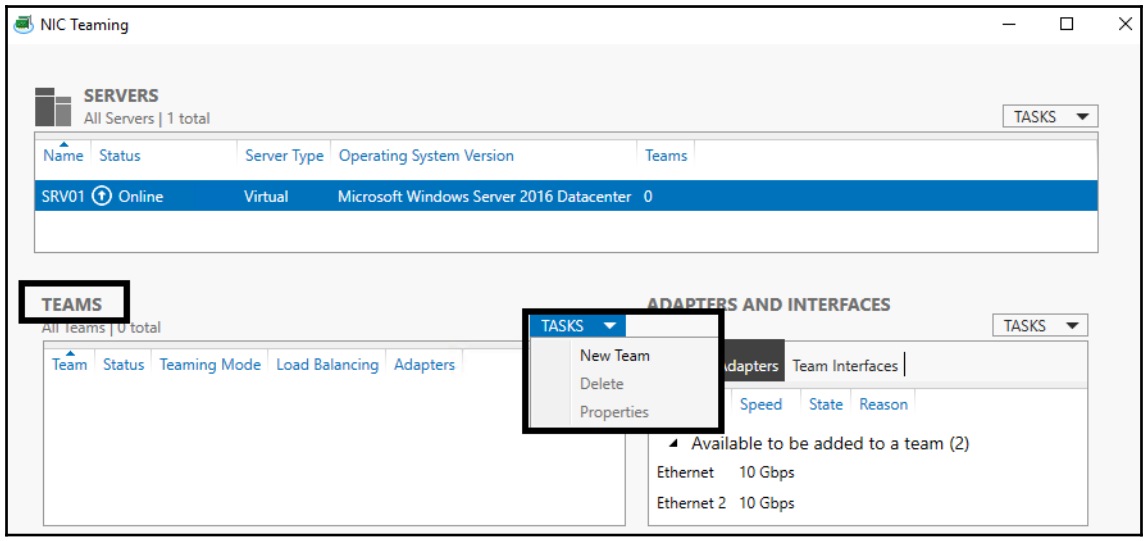

Point-to-Point
Protocol
(PPP)
RADIUS
Protocol
User
database
Dial-up
connection
Network Access Server
(NAS)

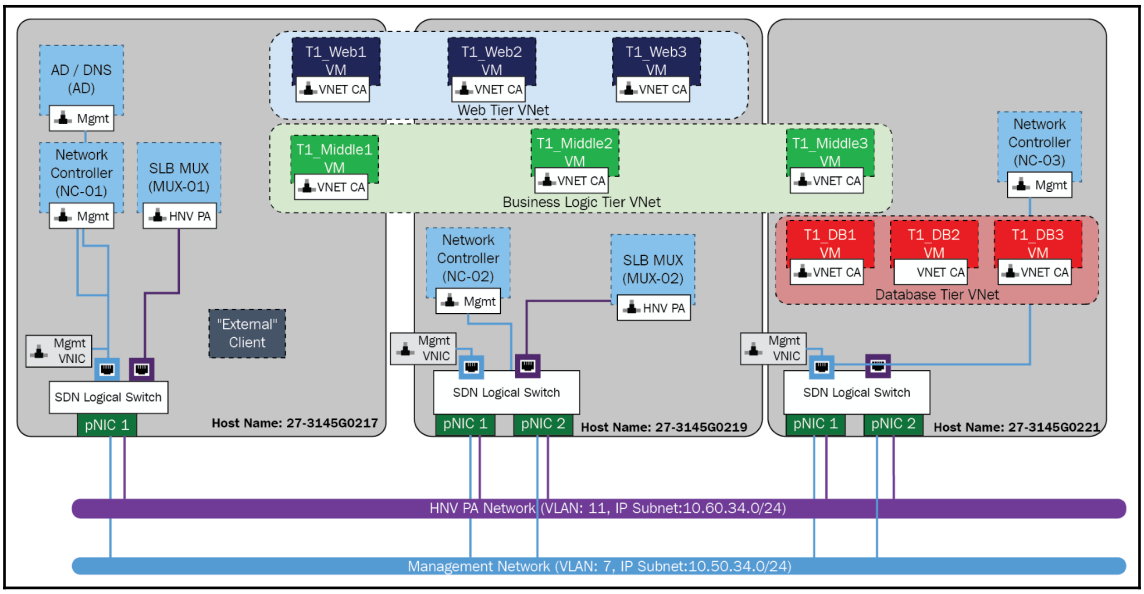
Chapter 6: Understanding Distributed File System

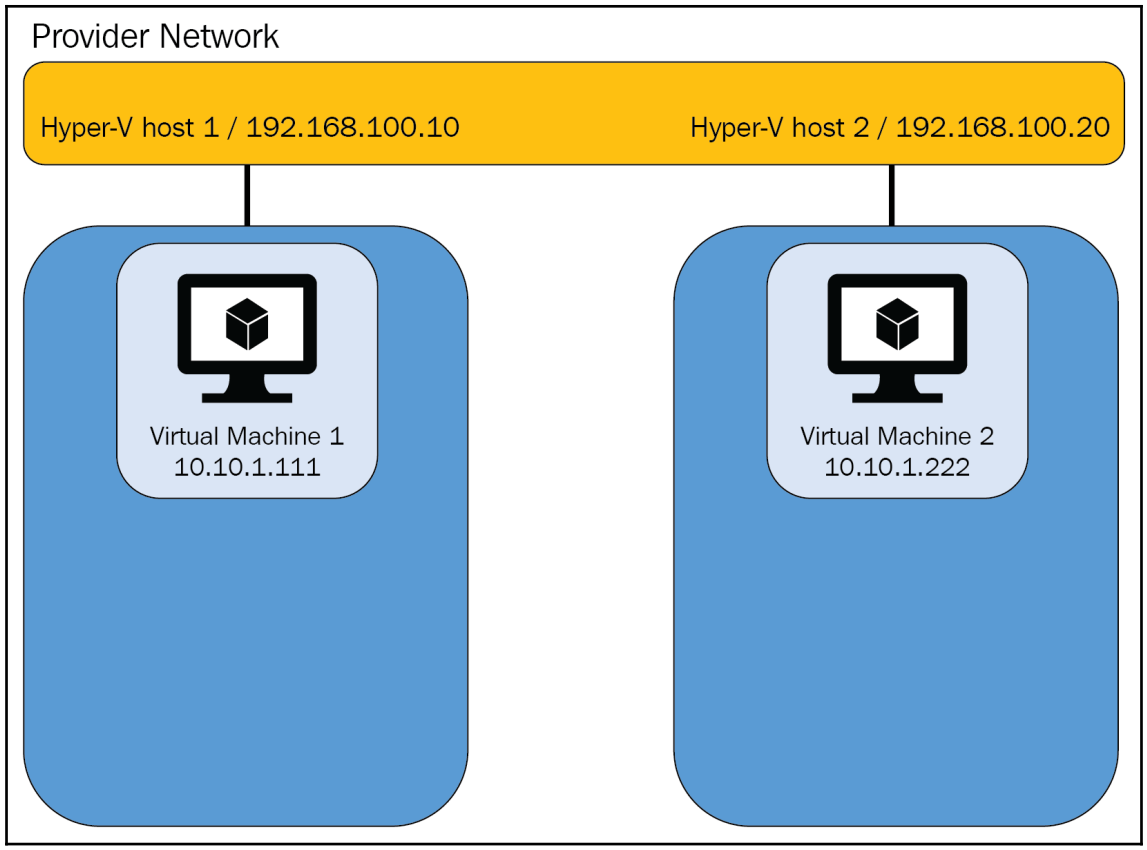


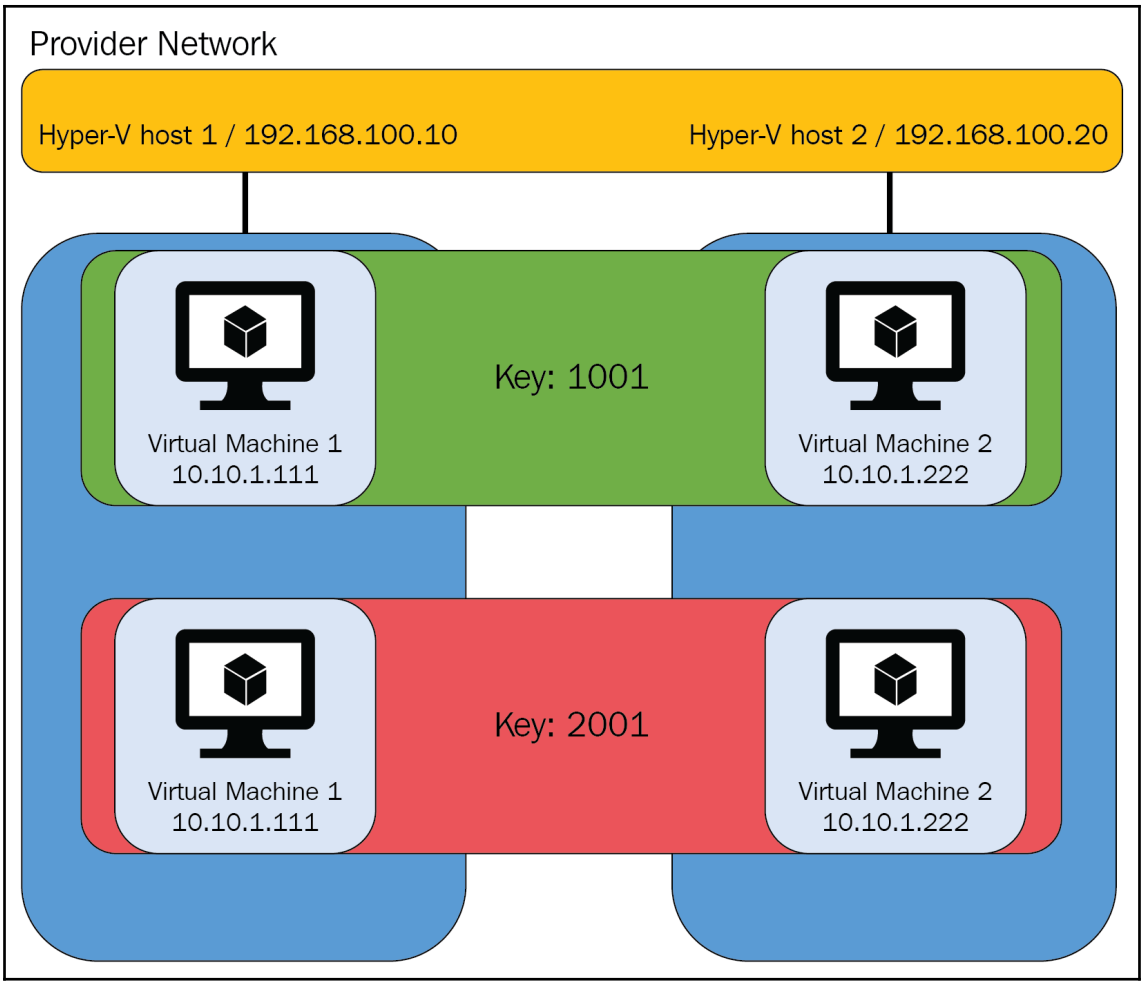
Chapter 7: Advanced Networking Infrastructure






AD / DNS (AD)
Mgmt
Network Controller (NC-01)
Mgmt
SLB MUX (MUX-01)
HNV PA
"External" Client
Mgmt VNIC
SDN Logical Switch
pNIC 1
Host Name: 27-3145G0217
T1_Web1 VM
VNET CA
T1_Web2 VM
VNET CA
T1_Web3 VM
VNET CA
Web Tier VNet
T1_Middle1 VM
VNET CA
T1_Middle2 VM
VNET CA
T1_Middle3 VM
VNET CA
Business Logic Tier VNet
Network Controller (NC-02)
Mgmt
SLB MUX (MUX-02)
HNV PA
Mgmt VNIC
SDN Logical Switch
pNIC 1
pNIC 2
Host Name: 27-3145G0219
Network Controller (NC-03)
Mgmt
T1_DB1 VM
VNET CA
T1_DB2 VM
VNET CA
T1_DB3 VM
VNET CA
Database Tier VNet
Mgmt VNIC
SDN Logical Switch
pNIC 1
pNIC 2
Host Name: 27-3145G0221
HNV PA Network (VLAN: 11, IP Subnet:10.60.34.0/24)
Management Network (VLAN: 7, IP Subnet:10.50.34.0/24)


Provider Network
Hyper-V host 1 / 192.168.100.10
Hyper-V host 2 / 192.168.100.20
Virtual Machine 1
10.10.1.111
Virtual Machine 2
10.10.1.222


Provider Network
Hyper-V host 1 / 192.168.100.10
Hyper-V host 2 / 192.168.100.20
Key: 1001
Virtual Machine 1
10.10.1.111
Virtual Machine 2
10.10.1.222
Key: 2001
Virtual Machine 1
10.10.1.111
Virtual Machine 2
10.10.1.222