Module 1
Implementing Advanced Network Services
Module Overview

• Configuring Advanced DHCP Features
• Configuring Advanced DNS Settings
• Implementing IPAM
• Managing IP Address Spaces with IPAM
Lesson 1: Configuring Advanced DHCP Features

- DHCP Components Overview
- Configuring DHCP Interaction with DNS
- Configuring Advanced DHCP Scope Designs
- DHCP Integration with IPv6
- What Is DHCP Name Protection?
- What Is DHCP Failover?
- Demonstration: Configuring DHCP Failover
DHCP Components Overview

DHCP components consist of:

- The DHCP server service
- DHCP options
- DHCP console
- DHCP scopes
- DHCP database

When you use DHCP:

- Clients request IP configuration through a broadcast
- IP addresses are leased to clients for a configurable period, and are regularly renewed
- DHCP servers must be authorized in AD DS
Configuring DHCP Interaction with DNS

Configuring option 081 allows the DHCP server to register both A and PTR resource records for the client.

Normal option 081 behavior:
1. IP lease request
2. IP lease acknowledgment
3. DNS dynamic update of host (A) name
4. DNS dynamic update of pointer (PTR) name

Modified option 081 behavior:
1. IP lease request
2. IP lease acknowledgment
3. DNS dynamic update of host (A) name
4. DNS dynamic update of pointer (PTR) name
Configuring Advanced DHCP Scope Designs

Superscopes

- Support multiple VLANs on a single physical network
- Can ease transitioning to new IP Scheme
- Require router support between VLANs

Multicast

- Uses the Class D 224.0.0.0/3
- Used for applications that need simultaneous communication with multiple clients
- Use in addition to the Network IP Address
DHCP Integration with IPv6

DHCPv6 supports stateful and stateless configurations

DHCPv6 also supports scopes that you can configure with the following properties:

- Name and description
- Preference
- Valid and Preferred lifetimes
- Prefix
- Exclusions
- DHCP options
What Is DHCP Name Protection?

DHCP Name Protection:

• Prevents Windows operating systems from having their DNS name registrations overwritten by non-Windows operating systems that have the same name

• Uses a DHCID resource record to track the machines that originally requested the DNS names

• Is configurable at the network protocol level and at the scope level
What Is DHCP Failover?

DHCP failover:

• Enables two DHCP servers to provide IP addresses and optional configurations to the same subnets or scopes

• Requires failover relationships to have unique names

• Supports the hot standby mode and the load sharing mode

When you use DHCP failover:

• The MCLT determines when a failover partner assumes control of the subnet or scope

• The auto state switchover interval determines when a failover partner is considered to be down

• Message authentication can validate the failover messages

• Firewall rules are auto-configured during DHCP installation
In this demonstration, you will see how to configure a DHCP failover relationship.
Lesson 2: Configuring Advanced DNS Settings

- Managing DNS Services
- Optimizing DNS Name Resolution
- What Is the GlobalNames Zone?
- Options for Implementing DNS Security
- How DNSSEC Works
- New DNSSEC Features for Windows Server 2012
- Demonstration: Configuring DNSSEC
Managing DNS Services

To manage DNS services:

- Delegate DNS administration through membership in the DNS Admins group
- View DNS logs in Event Viewer
- Enable DNS debug logging in the DNS server properties
- Enable aging and scavenging to remove stale records

Backup methods for the DNS database depend on how the database is deployed:

- Back up Active Directory-integrated zones through system state backups, by using dnscmd, or by using Windows PowerShell
- Non-integrated primary zone are single files that you can copy or back up
## Optimizing DNS Name Resolution

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding</td>
<td>Forwards DNS requests that cannot be resolved locally to other specific DNS servers</td>
</tr>
<tr>
<td>Conditional forwarding</td>
<td>Forwards queries for specific DNS suffixes to specific DNS servers</td>
</tr>
<tr>
<td>Stub zones</td>
<td>A regularly replicated copy of certain resource records that identify authoritative DNS servers for specific DNS domains</td>
</tr>
<tr>
<td>Netmask ordering</td>
<td>Responds with addresses of hosts that are close in proximity based in IP address information of the client to DNS queries</td>
</tr>
</tbody>
</table>
What Is the GlobalNames Zone?

The GlobalNames zone allows single label names to be resolved in multiple DNS domain environments.
# Options for Implementing DNS Security

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS cache locking</td>
<td>Prevents entries in the cache from being overwritten until a percentage of the TTL has expired</td>
</tr>
<tr>
<td>DNS socket pool</td>
<td>Randomizes the source port for issuing DNS queries</td>
</tr>
<tr>
<td></td>
<td>Enabled by default in Windows Server 2012</td>
</tr>
<tr>
<td>DNSSEC</td>
<td>Enables cryptographically signing DNS records so that client computers can validate responses</td>
</tr>
</tbody>
</table>
How DNSSEC Works

DNSSEC functions as follows:

- If a zone has been digitally signed, a query response will contain digital signatures.
- DNSSEC uses trust anchors, which are special zones that store public keys associated with digital signatures.
- Resolvers use trust anchors to retrieve public keys and build trust chains.
- DNSSEC requires trust anchors to be configured on all DNS servers participating in DNSSEC.
- DNSSEC uses the NRPT, which contains rules that control the requesting client computer behavior for sending queries and handling responses.
DNSSEC enhancements for Windows Server 2012 include:

- Simplified DNSSEC implementation
- A DNSSEC Zone Signing Wizard that steps you through the process of signing and configuring signing parameters for zones
- The following new resource records:
  - DNSKEY
  - DS
  - RRSIG
  - NSEC
In this demonstration, you will see how to configure DNSSEC
Lesson 3: Implementing IPAM

• What Is IPAM?
• IPAM Overview
• Requirements for IPAM Implementation
• Demonstration: Implementing IPAM
• Virtual Address Space Management in IPAM
• IPAM RBAC
IPAM facilitates IP management in organizations with complex networks by enabling administration and monitoring of DHCP and DNS.

<table>
<thead>
<tr>
<th>IP administration area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning</td>
<td>Reduces the time and expense of the planning process when changes occur in the network.</td>
</tr>
<tr>
<td>Managing</td>
<td>Provides a single point of management and assists in optimizing utilization and capacity planning for DHCP and DNS.</td>
</tr>
<tr>
<td>Tracking</td>
<td>Enables tracking and forecasting of IP address utilization.</td>
</tr>
<tr>
<td>Auditing</td>
<td>Assists with compliance requirements and provides reporting for forensics and change management.</td>
</tr>
</tbody>
</table>
IPAM Overview

IPAM architecture consists of:

- Four main modules:
  - IPAM discovery
  - IPAM address space management
  - Multiserver management and monitoring
  - Operational auditing and IP address tracking
- A server component and a client component
- You can deploy IPAM in the following topologies:
  - Distributed
  - Centralized
  - Hybrid
- Provisioned either manually or through GPO
## Requirements for IPAM Implementation

<table>
<thead>
<tr>
<th>Prerequisites</th>
<th>Hardware and software requirements</th>
</tr>
</thead>
</table>
| • IPAM server must belong to the domain  
• IPAM server cannot be a domain controller  
• IPv6 must be enabled in order to manage IPv6  
• Log on with a domain account  
• You must be in the correct IPAM local security group  
• Logging account logon events must be enabled for IP address tracking and auditing | • CPU – dual-core 2.0 GHz or higher  
• Windows Server 2012  
• 4 GB of RAM  
• 80 GB free disk space |
Demonstration: Implementing IPAM

- In this demonstration, you will see how to install and configure IPAM management
Virtual Address Space Management in IPAM

- To create a Customer Address Space run the following command:
  ```powershell
  Add-IpamAddressSpace -Name "Security Department" -CustomerAddressSpace -AssociatedProviderAddressSpace "AdatumHQ" -IsolationMethod NVGRE –Description "Security Department Network"
  ```

- To create a Provider Address Space run the following command:
  ```powershell
  Add-IpamAddressSpace -Name "AdatumHQ" -ProviderAddressSpace -Description "Adatum HQ Datacenter"
  ```
### IPAM RBAC

#### Server Manager → IPAM → ACCESS CONTROL → Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Built-in Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Record Administrator Role</td>
<td>Yes</td>
</tr>
<tr>
<td>IP Address Record Administrator Role</td>
<td>Yes</td>
</tr>
<tr>
<td>IPAM Administrator Role</td>
<td>Yes</td>
</tr>
<tr>
<td>IPAM ASM Administrator Role</td>
<td>Yes</td>
</tr>
<tr>
<td>IPAM DHCP Administrator Role</td>
<td>Yes</td>
</tr>
<tr>
<td>IPAM DHCP Reservations Administrator Role</td>
<td>Yes</td>
</tr>
<tr>
<td>IPAM DHCP Scope Administrator Role</td>
<td>Yes</td>
</tr>
<tr>
<td>IPAM MSM Administrator Role</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Tasks:**
- Add User Role...
- Export...

**Filters:**
- Name:
- Built-in Role:

**Side Panel:**
- IP ADDRESS SPACE:
  - IP Address Blocks
  - IP Address Inventory
  - IP Address Range Groups
- VIRTUALIZED IP ADDRESS SPACE
- MONITOR AND MANAGE:
  - DNS and DHCP Servers
  - DHCP Scopes
  - DNS Zone Monitoring
- Server Groups
- EVENT CATALOG
- ACCESS CONTROL:
  - Roles
  - Access Scopes
  - Access Policies
Lesson 4: Managing IP Address Spaces with IPAM

- Using IPAM to Manage IP Addressing
- Adding Address Spaces to IPAM
- Importing and Updating Address Spaces
- Finding, Allocating, and Reclaiming IP Addresses
- Maintaining IP Address Inventory in IPAM
- Demonstration: Using IPAM to Manage IP Addressing
- IPAM Monitoring
- Demonstration: Using IPAM Monitoring
You can view and manage the IP address space using the following views:

- IP address blocks
- IP address ranges
- IP addresses
- IP inventory
- IP address range groups

You can monitor the IP address space using the following views:

- DNS and DHCP servers
- DHCP scopes
- DNS zone monitoring
- Server groups
Adding Address Spaces to IPAM

Modify the values to update the IPv4 address subnet:

- **Name:** Adetum HQ
- **Network ID:** 192.168.20.0
- **Prefix length (22 - 32):** 24
- **VLAN ID:**
  - Add
  - Remove

Owner:

Description:
Importing and Updating Address Spaces

• Use a text file to import individual IP addresses

• The mandatory fields for IP address import are:
  • IP Address
  • Managed by Service
  • Service Instance
  • Device Type
  • IP Address State
  • Assignment Type

• Use a text file to import or update IP address ranges

• The mandatory fields for IP address block import are:
  • Network
  • Start IP address
  • End IP address
  • RIR
Maintaining IP Address Inventory in IPAM

Details View
192.168.30.1

Configuration Details Event Catalog

Duplicate Expiry Status IP Address MAC Address Managed by Service Service Instance Access Scope IP Range Virtualized

No Not expired 192.168.30.1 IPAM Localhost \Global 192.168.30.1-192.168.30.254 No

Edit IP Address... Create DHCP Reservation Create DNS Host Record Create DNS PTR Record Delete DHCP Reservation Delete DNS Host Record Delete DNS PTR Record Delete
Demonstration: Using IPAM to Manage IP Addressing

• In this demonstration, you will see how to use IPAM to manage IP addressing
IPAM Monitoring

With IPAM, you can:

- Monitor IP address space utilization
- Monitor DNS and DHCP health
- Configure many DHCP properties and values from the IPAM console
- Use the event catalog to view a centralized repository for all configuration changes
Demonstration: Using IPAM Monitoring

• In this demonstration, you will see how to use IPAM to monitoring
Lab: Implementing Advanced Network Services

- Exercise 1: Configuring Advanced DHCP Settings
- Exercise 2: Configuring Advanced DNS Settings
- Exercise 3: Configuring IPAM

Logon Information
Virtual machines: 20412D-LON-DC1, 20412D-LON-SVR1, 20412D-LON-SVR2, 20412D-LON-CL1
User Name: Adatum\Administrator
Password: Pa$$w0rd
Estimated Time: 70 minutes
A. Datum Corporation has grown rapidly over the last few years. The company has deployed several new branch offices, and it has increased significantly the number of users in the organization. Additionally, it has expanded the number of partner organizations and customers that access A. Datum websites and applications. Because of this expansion, the network infrastructure complexity has increased, and the organization now needs to be much more aware of network-level security.
Lab Scenario

• As one of the senior network administrators at A. Datum, you are responsible for implementing some of the advanced networking features in Windows Server 2012 R2 to manage the networking infrastructure. You need to implement new features in DHCP and DNS, with the primary goal of providing higher levels of availability while increasing the security of these services. You also need to implement IPAM so that you can simplify and centralize the IP address usage and configuration management in an increasingly complex network.
Lab Review

• Will client computers immediately stop communicating on the network if there is no functioning DHCP server?
• What is the default size of the DNS socket pool?
• What value does the DNS cache lock use to determine when to update an IP address in the DNS cache?
Module Review and Takeaways

• Review Question
• Real-world Issues and Scenarios
• Tools
• Best Practice
• Common Issues and Troubleshooting Tips