Windows Server 2012 R2 Microsoft

Windows Server 2012 R2 – IP Address Management (IPAM)

Windows Server 2012 R2

Hands-on lab

IP Address Management (IPAM) provides a single console to plan, design and administer network services and IP address spaces – physical and virtual. In this lab, you will learn more about how you can use IPAM in your organization to manage physical and virtual address space, delegate permissions in a multi-user environment, perform advanced DHCP configurations, and leverage IPAM PowerShell cmdlets for automating routine operations.

Produced by HynesITe, Inc.
Version 2.2
11/12/2013

holSystems™
Learn. Experience. Collaborate.

This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Introduction

Estimated time to complete this lab

90 minutes

Objectives

After completing this lab, you will be able to:

- Configure role-based access control and delegated administration.
- Manage policy-based DHCP addresses and option assignments by using IPAM.
- Automate IP address lifecycle management.
- Manage DHCP MAC address filters by using IPAM.
- Manager DHCP superscopes by using IPAM.

Prerequisites

Before working on this lab, you must have:

1. Experience working with Windows Server (any version).
2. Experience with network and server administration.
3. An understanding of TCP/IP, in particular DHCP.

Overview of the lab

IP Address Management (IPAM) provides a single console to plan, design and administer network services and IP address spaces – physical and virtual. In this lab, you will learn more about how you can use IPAM in your organization to manage physical and virtual address space, delegate permissions in a multi-user environment, perform advanced DHCP configurations, and leverage IPAM PowerShell cmdlets for automating routine operations.

Virtual machine technology

This lab is completed using virtual machines that run on Windows Server 2012 Hyper-V technology. To log on to the virtual machines, press CTRL+ALT+END and enter your logon credentials.

Computers in this lab

This lab uses computers as described in the following table. Before you begin the lab, you must ensure that the virtual machines are started and then log on to the computers.

Computer	Role	Configuration
DC	Domain controller	Domain controller with Active Directory and DNS

Computer	Role	Configuration
SERVER1	DHCP server used in lab exercises	Server with DHCP
SERVER2	DHCP server used in lab exercises	Server with DHCP
SERVER3	IPAM server	Server with IPAM
Admin	Client computer for the lab	Windows 8.1 client with RSAT

- All user accounts in this lab use the password **Passw0rd!**

Note regarding pre-release software

Portions of this lab may include software that is not yet released, and as such may still contain active or known issues. While every effort has been made to ensure this lab functions as written, unknown or unanticipated results may be encountered as a result of using pre-release software.

Note regarding user account control

Some steps in this lab may be subject to user account control. User account control is a technology which provides additional security to computers by requesting that users confirm actions that require administrative rights. Tasks that generate a user account control confirmation are denoted using a shield icon. If you encounter a shield icon, confirm your action by selecting the appropriate button in the dialog box that is presented.

Note on activation

The virtual machines for these labs may have been built by using software that has not been activated. This is by design in the lab to prevent the redistribution of activated software. The unactivated state of software has been taken into account in the design of the lab. Consequently, the lab is in no way affected by this state. For operating systems other than Windows 8.1, click Cancel or Close if prompted by an activation dialog box. If you are prompted by an Activate screen for Windows 8.1, press the Windows key to display the Start screen.

Exercise 1: Installing and Configuring IPAM

In this exercise, you will install and configure an IPAM server, and then configure it to manage IP services including DHCP, DNS, and Active Directory. IPAM deployment includes many schedule-based activities which run automatically to populate data and configure servers. These tasks include scheduled tasks and group policy refreshes. During this exercise, you will force many of these tasks to run automatically and also perform some manual tasks to speed up the overall deployment.

Install and configure DHCP on Server1 and Server2

In this task, you will use a script to install and configure DHCP on Server2 and Server3. The script will first switch the computers to use static IP addresses, and then install the DHCP role. Finally it will perform DHCP initial configuration which includes adding local groups and performing Active Directory authorization.

✎ Begin this task logged onto **Admin** as **Contoso\Administrator** using the password **Passw0rd!**

1. On the taskbar, right-click the **Windows PowerShell** icon, and then click **Windows PowerShell ISE**.
2. In Windows PowerShell ISE, open the file **C:\LabFiles\IPAM-Setup.ps1**.
3. Press F5, and then press ENTER to run the file.
   - This file will set both servers to use static IP addresses, and then install and configure the DHCP service.
   - After a few minutes, Windows PowerShell will display the running script below the Windows PowerShell window.
   - Windows PowerShell ISE will indicate when the tasks are completed.

Install IPAM on Server3

In this task, you will install the IPAM service on Server3.

✎ Begin this task logged onto **Server3** as **Contoso\Administrator** using the password **Passw0rd!**

1. On **Server3**, in Server Manager, click **Manage**, and then click **Add Roles and Features**.
2. On the Before you Begin page, click **Next**.
3. On the Installation Type page, click **Next**.
4. On the Server Selection page, click **Next**.
5. On the Server Roles page, click **Next**.
6. On the Features page, check **IP Address Management (IPAM) Server**, click **Add Features**, and then click **Next**.
7. Click **Install**, and then when the installation completes, click **Close**.

Configure IPAM on Server3

In this task, you will perform the initial configuration of IPAM on Server3.

Begin this task logged onto **Server3** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Manager, click **IPAM**.
2. In IPAM, click **Provision the IPAM server**.
3. On the Before you begin page, click **Next**.
4. On the Configure database page, click **Next**.
5. On the Select provisioning method page, in GPO name prefix, type **IPAM**, and then click **Next**.
6. Click **Apply**, and then when provisioning completes, click **Close**.
7. Open **Windows PowerShell**.
8. Type the following command, and then press ENTER.

   This command will create the IPAM GPOs.

   ```
   Invoke-IpamGpoProvisioning –Domain contoso.com –GpoPrefixName IPAM –IpamServerFqdn server3.contoso.com –Force
   ```

9. In Server Manager, select **IPAM**, and then click **Configure Server Discovery**.
10. In Configure Server Discovery, click **Add**, and then click **OK**.
11. Click **Start server discovery**.

    IMPORTANT: Server discovery will take a few minutes, possibly longer, to complete. You must wait for this to partially complete before proceeding. You can review the progress of server discovery by clicking the task notification icon next to Manage in the Server Manager Toolbar area.

12. In the navigation tree, click **Server Inventory**. When you see DC listed, it is safe to proceed to the next step.

    Press F5 to refresh this view.

Configure IPAM managed servers

In this task, you will configure DC, Server1, and Server2 to be managed by IPAM. This will involve rebooting the DC, and forcing GPO refresh on all servers. These steps are examples of the steps mentioned in the exercise introduction to speed up the IPAM deployment process in a lab environment. They are not necessary in a production environment where you are able to wait for scheduled tasks to happen.

Begin this task logged onto **Server3** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Inventory, click **Tasks**, and then click **Add Server**.

2. Type **Server1**, and then click **Verify**.
3. Check **DHCP Server**, and then set the Manageability status to **Managed**.
4. Click **OK**.
5. In Server Inventory, click **Tasks**, and then click **Add Server**.
6. Type **Server2**, and then click **Verify**.
7. Check **DHCP Server**, and then set the Manageability status to **Managed**.
8. Click **OK**.
9. Right-click **DC**, and then click **Edit Server**.
10. Set the Manageability status to **Managed**, and then click **OK**.
11. In Windows PowerShell, type the following command, and then press ENTER.

    ```
    ICM DC, Server1, Server2 {GPUpdate /Force}
    ```

12. In Server Manager, in Server Inventory, press the CTRL key, and then click all three servers.
13. Right-click the selected servers, and then click **Refresh Server Access Status**.

    IMPORTANT: Wait for the task to complete before moving to the next step. To check the status of the task, on the Activity bar, click the More link.

14. In Server Inventory, press F5 to refresh the view.

    All three servers will show a status of Managed, an access status of Unblocked, and a green icon if you completed this task correctly.

15. In Server Manager, in Server Inventory, press the CTRL key, and then click all three servers.
16. Right-click the selected servers, and then click **Retrieve All Server Data**.

    IMPORTANT: Wait for the task to complete before moving to the next step. To check the status of the task, on the Activity bar, click the More link.

Exercise 2: Configure Administrative Roles for IPAM Operations

In this exercise, you will configure role-based administration to ensure that an administrator has permission to edit a particular DHCP scope but does not have the ability to modify other IPAM settings.

RBAC Concepts

Role

Role is a collection of IPAM operations. A role can be associated with a Windows user or group through an access policy (see below). The operations that a user can execute are determined by the role. IPAM provides several built-in user roles. Administrators can create new roles as per their business requirements. For example, an administrator can create a Block Admin role that would contain only edit and delete operations for IP address blocks.

Access scope

While a role determines what operations a user can execute, it does not tell what IPAM entities (IP address blocks, IP address range, DHCP server, or DHCP scopes) the user has access to. This is where access scopes come into play. Access scopes define administrative domains in IPAM. IPAM has a built-in access scope called Global. By default, all IPAM entities fall under the Global access scope; however an administrator can create more access scopes as child access scopes of Global based on business requirements. For example, based on geography, an administrator can create Europe and Asia as new access scopes under Global. The administrator can then select any IPAM entity (or group of entities using multi-select) and assign Global\Asia or Global\Europe access scopes to them.

A user or group is associated with an access scope through an access policy (see below).

Access policy

An access policy brings a role and an access scope together and associates these with a Windows user or group. Through an access policy an administrator can pick a Windows user or group and specify a role for the user as well as an access scope in which the role is applicable, effectively specifying what operation a user is allowed to execute and on what IPAM entities these operations can be executed.

For example, an administrator can define an access policy for User1 with a role of Block Admin and an access scope of Global\Asia. User1 will be able to edit and delete IP address blocks that lie under the Global\Asia access scope. User1 will not be able to edit or delete the IP address blocks that lie under the Global\Europe access scope nor will User1 be able to execute any operation other than edit or delete of IP address blocks.

Create a new DHCP scope

In this task, you will create a new DHCP scope name Singapore Lab DHCP Scope.

✎ Begin this task logged on to **Server3** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Manager, in the left navigation pane, click **IPAM**.
2. Under Monitor and Manage, click **DNS and DHCP Servers**.
3. In the contents pane, ensure **DHCP** is selected in the Server Type field.
4. In the View field, select **Server Properties**.

   📌 This will cause a list of the 3 DHCP servers in the lab environment to appear.

5. Right-click **DC.contoso.com**, and then click **Create DHCP Scope**.
6. On the General Properties page, enter the following information in the form:

Property	Value
Scope name	**Singapore Lab Scope**
Start IP address	**40.40.1.0**
End IP address	**40.40.1.100**
Subnet Mask	**255.0.0.0**

7. Scroll to the bottom of the form, and then click **OK**.

Create a new role-based user role for administration of the new scope

In this task, you will create a new role that contains only the Edit DHCP Scope operation user role.

✎ Begin this task logged on to **Server3** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Manager, in the left navigation pane, select IPAM, and then click **Access Control**.

   📌 You may have to scroll down to see this item.

2. Below Access Control, right-click **Role**, and then click **Add User Role**.
3. In the Add or Edit Role dialog box, in Name, type **DHCPScopeEditor**.
4. In the Operations area, expand **DHCP Scope Operations**, and then select **Edit DHCP scope**.
5. Click **OK**.
6. In the left navigation pane, right-click **Access Scopes**, and then click **Add Access Scope**.
7. In the Add Access Scope dialog box, click **New**.
8. In the Add Access Scope dialog box, in Name, type **SingaporeLab**.
9. Click **Add**, and then click **OK**.
10. In the left navigation pane, click **DHCP Scopes**.

11. In the Current view field, select **Scope Properties**.
12. In Filter, type **Singapore lab**.

    📌 The display is filtered to show only the Singapore Lab Scope.

13. Right-click **Singapore Lab Scope**, and then click **Set Access Scope**.
14. In the Set Access Scope dialog box, clear the **Inherit access scope from parent** check box.

    ◈ **CAUTION**: Ensure you clear the check box.

15. Select **Singapore Lab**, and then click **OK**.
16. In the left navigation pane, click **Access Control**.
17. Right-click **Access Policies**, and then click **Add Access Policy**.
18. In the Add Access Policy dialog box, click **Add**.
19. In the Select User, Computer, or Group dialog box, click **Locations**.
20. In the Locations dialog box, click **Entire Directory**, and then click **OK**.
21. In the Enter the object name to select field, type **BenSmith**, and then click **OK**.
22. In the Add Access Policy dialog box, on the left-hand side, click **Access Settings**.
23. Under Access Settings, click **New**.
24. In the New Setting tile that appears below, in Select role, select **DHCPScopeEditor**.
25. In the Select the access scope for the role, click **SingaporeLab**.
26. Click **Add Setting**.

    ◈ **IMPORTANT**: Ensure you add the setting in the above step. You may have to scroll down to see the button.

27. Click **OK**.

Exercise 3: Configure DHCP Policy-Based Assignment using IPAM

DHCP Policy-Based Assignment (PBA) is a powerful feature for IPV4 networks in DHCP server that gives you greater control over your network and the devices accessing it. It allows you to use tools known as DHCP policies or simply policies to identify and group together these devices based on attributes like MAC Address, Vendor Class, and User Class. You can then control the leases (IP addresses) and DHCP options (configuration information) that are assigned to these devices or clients. For example, you can use DHCP policies to match the MAC address of clients and make sure that all virtual machines (VMs) accessing your network are assigned addresses from a specific IP range or are assigned some specific DHCP options.

DHCP policies can be configured at the server level or scope (subnet) level. Until now, policies were accessible only for individual DHCP servers via the management interfaces for the DHCP server role. With the IPAM feature in Windows Server 2012 R2, you can create and manage policies centrally across multiple DHCP servers. You can create a policy for multiple servers or scopes in a single operation. You can also copy policies for one server or scope to another.

In this exercise, you will see how IPAM allows you to centrally manage policies in an easy and simple manner.

Configure new DHCP policies and import existing DHCP policies

You can create new policies on a DHCP server or scope. You can also copy existing policies on a DHCP server or scope by importing them from some other server or scope. These operations are available in the management view of DHCP servers and scopes. In this task, you will create new DHCP policies as well as importing them from another server.

✎ Begin this task logged on to **Server3** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Manager, in the left navigation pane, click **IPAM**.
2. Under Monitor and Manage, click **DNS and DHCP Servers**.
3. In the contents pane, in the Server Type field, ensure **DHCP** is selected.
4. In the View field, select **Server Properties**.

   📌 In the details pane at the bottom, you can view Policies by clicking on the Policies tab.

5. Right-click **Server1.contoso.com**.

   📌 Configure Policy can be used for configuring a new policy on the selected server(s). The Import Policy can be used for copying an existing policy from a different server or scope. The operation Activate Policies can be used to turn ON application of all policies configured the selected server. The operation Deactivate Policies can be used to turn OFF application of all policies configured on the selected server.

6. Click **Configure DHCP Policy**.

7. On the Configure Server policy page, in Name, type **Test Policy**.
8. In the left pane, click **Conditions** if it is not already selected.
9. Under Policy Conditions, click **New**.
10. In the New Condition tile, ensure **Vendor-Class** is selected as the Criteria, **Equals** as the Operator, and **Microsoft Options** as the Value, and then click **Add**.
11. Click **Add Condition**.
12. In the left pane, select **DNS Updates** if it is not already selected.
    - Notice the configuration options that are available for DNS Dynamic Updates. These include the DNS registration settings and DHCP options that you want to apply to the clients that match this policy.
13. Click **OK**.
    - Now that you have configured a policy, you can import this policy to another server.
14. In Server Manager, right-click **Server2.contoso.com**, and then click **Import DHCP Policy**.
    - The Import Policy dialog box provides you with the option to import policies at either the server or the scope level. You can configure or import policies for scopes from the management view for DHCP scopes. For scope policies, you can specify IP address ranges from which the leases will be allocated to the clients.
15. In the Import Policy dialog box, in Select Server, select **Server1.contoso.com**.
16. In Select Policy, select **Test Policy**, and then click **OK**.
17. In the details pane, click the **Policies** tab.
    - Here you can see the various policies that are assigned to each DHCP server. If you do not see the policy you just added, refresh the view.

Exercise 4: Automating IP Address Lifecycle Management

IPAM's new Windows PowerShell interface makes it painless to automate IP address lifecycle management. It provides a rich set of cmdlets that allow you to perform all management functions for your IP addresses, ranges, and blocks. You can leverage these to write scripts to integrate IPAM with various orchestrators to provision network properties for various physical and virtual devices and servers. This saves time, eliminates manual intervention, and reduces operating cost. In this exercise, you will learn how to use some of the IPAM PowerShell cmdlets to introduce more automation into your environment.

> **IMPORTANT**: The IPAM PowerShell cmdlets that are used in this exercise may be found in C:\LabFiles\IPAM-Automation.ps1 on ADMIN. Some of the commands are lengthy and complex. As such, you may prefer to copy this file to Server3 and then copy and paste the commands from the text file to the IPAM PowerShell console, or run them directly from Windows PowerShell ISE.

Managing IP address ranges using IPAM PowerShell cmdlets

In this task, you will learn how to use the Get-IpamRange cmdlet to perform a variety of administrative actions.

Begin this task logged on to **Server3** as **Contoso\Administrator** using the password **Passw0rd!**

1. On the taskbar, click the **Windows PowerShell** icon to open the Windows PowerShell console.
2. In the Windows PowerShell console, type the following command, and then press ENTER.

   ```
   Get-IpamRange –AddressFamily IPv4 –AddressCategory Private
   ```

   This cmdlet lists all IPv4 private address ranges in IPAM. By default, the output shows you the **NetworkId**, **StartIp** address and **EndIp** address of the range, the service which is managing this range, and whether a given IP range is overlapping with another range. You can use the **Format-List** cmdlet to display more details for any given range.

3. In the Windows PowerShell console, type the following two commands, pressing ENTER after each one.

   ```
   $a=Get-IpamRange –AddressFamily IPv4 –AddressCategory Private
   $a[0]|fl *
   ```

   The above cmdlets provide more detail of each IP range.

4. In the Windows PowerShell console, type the following command, and then press ENTER.

   ```
   Get-IpamRange –AddressFamily IPv4 –AddressCategory Private|where-object
   {$_.PercentageUtilized –gt 10}
   ```

- The above cmdlet lists all IPv4 private address ranges with utilization greater than 10%. As shown in the next cmdlet, you can use the **Export-Csv** Windows PowerShell cmdlet to generate a comma-separated file with all the ranges with a utilization greater than 10%.
- In a production environment, you would likely be more interested in utilization percentages that are greater than some value closer to 100% or percentages that are less than some value closer to 0%.

5. In the Windows PowerShell console, type the following two commands, and then press ENTER.

```
↪ Get-IpamRange –AddressFamily IPv4 –AddressCategory Private|where-object
  {$_.PercentageUtilized –gt 10}|Export-Csv –Path
  “C:\Users\Administrator.Contoso\Desktop\OverUtilizedRanges.csv” –NoTypeInformation
  –Force
↪ notepad “C:\Users\Administrator.contoso\Desktop\OverUtilizedRanges.csv”
```

- This will open a Notepad file containing all the over-utilized IPv4 private address ranges. Similarly, you can generate reports about conflicting IP address ranges as shown in next example.

6. In the Windows PowerShell console, type the following command, and then press ENTER.

```
↪ Get-IpamRange –AddressFamily IPv4 –AddressCategory Private|where-object {$_.Overlapping
  –eq “True”}
```

- You may not see any output from this command. This is expected in this environment, as there are no overlapping scopes.
- The next series of commands show how to find a free IP address, and then assign it to a device.

7. In the Windows PowerShell console, type the following two commands, pressing ENTER after each one.

```
↪ $range = Get-IpamRange –StartIPAddress 10.0.0.10 -EndIPAddress 10.0.0.20
↪ Find-IpamFreeAddress –InputObject $range -TestReachability
```

- This cmdlet will output an unutilized IP address from the IP address range with a start IP address of 10.20.1.100 and an end IP address of 10.20.1.200. After you have verified address availability, you can assign the address to a device. To do this, you will first add this IP address to IPAM, and then create a corresponding reservation for this IP.

8. In the Windows PowerShell console, type the following four commands, pressing ENTER after each one.

```
↪ $range = Get-IpamRange –StartIPAddress 10.0.0.10 -EndIPAddress 10.0.0.20

↪ $freeip = Find-IpamFreeAddress –InputObject $range –TestReachability

↪ $ip = Add-IpamAddress –IpAddress $freeIp.Address –ManagedByService
  $range.ManagedByService –ServiceInstance $range.ServiceInstance –DeviceType Printer
```

```
–IpAddressState In-Use –AssignmentType Dynamic –MacAddress ”AA-BB-CC-DD-EE-FF”
–ReservationServer $range.DhcpServerName –ReservationName “B3_F1_Printer_HP”
–ReservationType Both –ReservationDescription “Reservation for printer on first floor of
building 3” –ClientID “B3F1” –PassThru

$ip|fl *
```

This cmdlet will add an IP address to the IPAM system. You can observe in the output of the last cmdlet that the **ReservationScopeName** and **ReservationScopeId** fields have been added automatically. You will still need to create the reservation on DHCP server using the cmdlet in the following step.

9. In the Windows PowerShell console, type the following command, and then press ENTER.

```
Add-DhcpServerv4Reservation –ComputerName $ip.ReservationServer –IPAddress
$ip.IPAddress –ClientId $ip.MacAddress –ScopeId $ip.ReservationScopeID –Name
$ip.ReservationName –Description $ip.ReservationDescription -PassThru
```

Now that you have provisioned a device, you will deprovision it and reclaim the IP address. As a part of this process, you will remove the reservation from the DHCP server, and then delete the IP address from the IPAM server.

10. In the Windows PowerShell console, type the following command, and then press ENTER.

```
Remove-DhcpServerv4Reservation –ComputerName $ip.ReservationServer –IPAddress
$ip.IPAddress -PassThru
```

This command removes the reservation. The command in the following step deletes the IP address from the IPAM system.

11. In the Windows PowerShell console, type the following command, and then press ENTER.

```
Remove-IpamAddress –InputObject $ip -Force
```

Exercise 5: Administering DHCP Failover using IPAM

In this exercise, you will learn how to administer DHCP failover using IPAM. Tasks that you will perform in this exercise include creating, viewing, and editing a failover relationship, replicating scopes, removing scopes, and other related administrative tasks.

Create, view, and edit a failover relationship

In this task, you will create, view, and edit a failover relationship.

✎ Begin this task logged on to **Server3** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Manager, in the left navigation pane, click **IPAM**.
2. Under Monitor and Manage, click **DHCP Scopes**.
3. In the contents pane, in Current view, select **Scope Properties**.

   📌 You may have to clear Singapore Lab from the filter to view all the available scopes.

4. Click the **Scope ID** column to order the list by scope ID.
5. Press the CTRL key, and then select both the Scope IDs **192.168.10.0** and **192.168.11.0**.

   📌 Both of these scopes are configured on **DC.contoso.com**.

6. Right-click the two selected scopes, and then click **Configure DHCP Failover**.
7. On the Configure Failover Relationship page, ensure **Create new relationship** is selected.
8. For Partner server, select **Server1.contoso.com**.
9. In Relationship name, type **Server1-DC**.
10. In Secret, type **secret**.
11. Click **Apply**.

    📌 After clicking Apply, the property sheet will automatically shift to the Summary pane. In this pane, you can see the result of the Configure Failover operation.

12. Click **OK**.

    📌 The IPAM management list (ML) will refresh to display the relationship details for the scopes.

13. In the contents pane, scroll to the right to view the relationship details.
14. In the left navigation pane, click **DNS and DHCP Servers**.
15. Ensure that Server Type is set to **DHCP**, and then in View, select **Failover Relationships**.
16. Right-click **Server1-DC**, and then click **Edit DHCP Failover Relationship**.
17. Under Advanced Properties, change the Percentage of Server to **60**.
18. Click **Apply**, and then click **OK**.

Replicate configuration of failover scopes to partner servers

In this task, you will learn how to replicate DHCP failover server settings.

✎ Begin this task logged on to **Server3** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Manager, in the left navigation pane, click **IPAM**.
2. Under Monitor and Manage, click **DNS and DHCP Servers**.
3. Ensure that Server Type is set to **DHCP**, and then in View, select **Server Properties**.
4. Right-click **DC.contoso.com**, and then click **Replicate DHCP Server**.
5. In the Replicate Server dialog box, click **OK**.

   📌 A dialog box appears showing the status of the replication.

6. When the replication has finished, click **Close**.

Replicate multiple scopes of a server

In this task, you will learn how to replicate multiple server scopes.

✎ Begin this task logged on to **Server3** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Manager, in the left navigation pane, click **IPAM**.
2. Under Monitor and Manage, click **DHCP Scopes**.
3. In the contents pane, in Current view, select **Scope Properties**.
4. Right-click the **Scope ID** column heading, point to **Group by**, and then click **Server Name**.
5. Press the CTRL key, and then under DC.contoso.com, select both of the Scope IDs **192.168.10.0** and **192.168.11.0**.
6. Right-click the selected scopes, and then click **Replicate DHCP Scope**.
7. Click **OK**.
8. In the Replicate Scopes dialog box, click **OK**.

   📌 A dialog box appears showing the status of the replication.

9. When the replication has finished, click **Close**.

Remove scopes from a failover relationship and delete the failover relationship

In this task, you will learn how to remove scopes from a failover relationship and how to delete the failover relationship.

✎ Begin this task logged on to **Server3** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Manager, select **IPAM**, select **Monitor and Manage**, and then click **DHCP Scopes**.
2. In the contents pane, in Current view, select **Scope Properties**.
3. Select the **CorpNet** and **CorpNet2** scopes.
4. Right-click the two selected scopes, and then click **Remove DHCP Failover Configuration**.
5. In the Remove Failover Configuration dialog box, click **OK**.
6. When the task shows as completed, click **Close**.

Exercise 6: Managing DHCP MAC Address Filters using IPAM

MAC address-based filtering or link layer-based filtering for DHCP enables administrators to control network access based on media access control (MAC) address, providing a low-level security method. You can create MAC address-based filters to specify which MAC addresses are allowed on the network and which are denied access.

A DHCP server maintains allow and deny lists of MAC addresses. If you add MAC addresses to the allow list and then enable the list, only these MAC addresses will be granted an IP address by the DHCP server. If you add MAC addresses to the deny list and then enable the list, these MAC addresses will be denied service by the DHCP server. You can enable both allow and deny lists, in which case the deny list takes precedence. This means that the DHCP server provides DHCP services only to clients whose MAC addresses are in the allow list, provided that no corresponding matches are in the deny list.

You can use wildcards to allow or deny network access based on vendor MAC prefixes.

Link layer filtering is currently available for IPv4 address only.

In this exercise, you will see how IPAM allows you to centrally manage MAC address filters in an easy and simple manner.

Add DHCP MAC address filters

In this task, you will add MAC address filters to allow or deny lists on one or more DHCP servers.

✎ Begin this task logged on to **Server3** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Manager, select IPAM, select Monitor and Manage, and then click **DNS and DHCP Servers**.
2. Ensure that Server Type is set to **DHCP**, and then in View, select **Server Properties**.
3. Select one of the DHCP servers, and then review the information in the details pane.

   📌 The Allow MAC Address Filters and the Deny MAC Address Filters are disabled.

4. Right-click **DC.contoso.com**, and then click **Edit DHCP Server Properties**.

   📌 You could also select multiple DHCP servers.

5. In Edit DHCP Server Properties, in the left pane, click **MAC Address Filters**.

   📌 Under MAC Address Filters, you will find the check boxes to enable allow or deny lists.

6. Select the check boxes to enable the **allow** and **deny** lists.
7. Click **OK**.
8. Right-click **DC.contoso.com**, and then click **Add DHCP MAC Address Filter**.

   📌 You could also select multiple DHCP servers.

9. In the Add MAC Address Filter dialog box, click **Deny**.

10. In MAC Address, type **00155D***.
    - Wildcards can be used to filter MAC addresses based on a pattern, such as a vendor ID in the MAC address. Wildcards can only be used if there is an even number of characters.
11. In Description, type **MAC Address Filter for Hyper-V Virtual Machines**.
12. Click **Add MAC Address Filter**.
13. In the Add MAC Address Filter dialog box, click **OK**.
14. In Server Manager, click **View**, and then select **Filters**.
    - Here you can manage filters from DNS and DHCP servers.
15. Right-click the filter created in the previous steps.
    - You can delete the filter, edit the filter, or change it from a deny filter to an allow filter or vice versa depending on its state.
16. Click **Delete**.

Exercise 7: Managing DHCP using IPAM

Consider a situation in which the available address pool for a currently active scope is nearly depleted, and still more computers are expected to be added to the network. In this situation, you can use superscopes that allow a DHCP server to provide leases from more than one scope to clients on a single physical network. The scopes in the same superscope can share IP addresses and give leases to clients on each other's subnet. You can add the depleted scope, along with another scope, to a superscope.

Superscopes can also help you resolve other deployment issues such as migrating clients over time to a new scope, for example, to renumber the current IP network from an address range used in an existing active scope to a new IP network range of addresses used in a new scope.

At present, superscopes are available for IPv4 addresses only.

Add and manage DHCP superscopes

In this task, you will see how you can create and manage DHCP superscopes using IPAM.

✎ Begin this task logged on to **Server3** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Manager, under Monitor and Manage, click **DNS and DHCP Servers**.
2. Ensure that Server Type is set to **DHCP**, and then in View, select **Scope Properties**.
   - You are now in the management view for DHCP scopes. Alternatively, you can select DHCP Scopes in the navigation tab, and then in Current view, select Scope Properties.
3. Scroll to the right to see the Superscope name column.
   - None of the scopes is a member of a superscope. Consequently, the entries in the column are blank.
4. In Filter, type **192.168**.
   - This causes all the scopes starting with 192.168 to be filtered in the display.
5. Right-click the **192.168.10.0** scope, and then click **Add to DHCP Superscope**.
6. In the Add to Superscope dialog box, in Superscope name, type **Dublin Superscope**.
7. Click **OK**.
8. Right-click the **192.168.11.0** scope, and then click **Add to DHCP Superscope**.
9. In the Add to Superscope dialog box, click **Use existing superscope**, and then select **Dublin Superscope**.
10. Click **OK**.
    - You have now created a superscope and added two scopes to it. Each scope can now service each other's clients.
11. In View, select **Superscope Properties**.

12. In the details pane, click the **Superscope Properties** and the **DHCP Scopes** tabs, and then review the information that is presented.
13. In the upper pane, right-click **Dublin Superscope**, note the options presented in the menu, and then click **Delete**.

📌 The operations you can perform on superscopes include:

Rename Superscope: Rename a superscope.

Create DHCP Scope: Create a new DHCP scope to add to this superscope. This is particularly useful when you feel that utilization of the superscope is high and you need another scope to cater to the clients of the member scopes of that superscope.

Configure Failover: Configure a failover relationship for the member scopes of the superscope. See the section on managing a failover relationship.

Remove Failover Configuration: Remove the member scopes of the superscope from failover relationships. See the section on managing a failover relationship.

Set Access Scope: Restrict the permissions on the superscope to only certain users. See the section on restricting user permissions for editing scopes.

Activate DHCP Superscope: Activate all the member scopes of the superscope.

Deactivate DHCP Superscope: Deactivate all the member scopes of the superscope.

Delete: Delete the superscope. The member scopes are not deleted but are simply removed from the superscope.

This is the end of the lab