

**Test Lab Guide: Demonstrate IP Address Management (IPAM) in Windows Server "8" Beta**

Microsoft Corporation

Published: February 2012

**Abstract**

This paper contains an introduction to Windows Server "8" Beta IP Address Management (IPAM), and step-by-step instructions for extending the Windows Server "8" Beta Base Configuration test lab to demonstrate IPAM setup.

**Copyright information**

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious.  No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2012 Microsoft. All rights reserved.

Active Directory, Hyper-V, Microsoft, MS-DOS, Visual Basic, Visual Studio, Windows, Windows NT, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

[Introduction 5](#_Toc309739725)

[In this guide 5](#_Toc309739726)

[Test lab overview 6](#_Toc309739727)

[Hardware and software requirements 7](#_Toc309739728)

[Steps for Configuring the IPAM Test Lab 7](#_Toc309739729)

[Step 1: Set up the Base Configuration Test Lab 8](#_Toc309739730)

[Step 2: Configure APP1 9](#_Toc309739731)

[Install the DHCP Server role on APP1 9](#_Toc309739732)

[Step 3: Add and configure IPAM1 10](#_Toc309739733)

[Install the operating system on IPAM1 10](#_Toc309739734)

[Configure TCP/IP properties on IPAM1 10](#_Toc309739735)

[Join IPAM1 to the CORP domain 11](#_Toc309739736)

[Step 4: Configure DC1 12](#_Toc309739737)

[Create three IPAM GPOs and link them to the corp.contoso.com domain 13](#_Toc309739738)

[Configure settings for the IPAM\_DC\_NPS GPO 14](#_Toc309739739)

[Configure settings for the IPAM\_DHCP GPO 14](#_Toc309739740)

[Configure settings for the IPAM\_DNS GPO 16](#_Toc309739741)

[Step 5: Deploy IP Address Management on IPAM1 18](#_Toc309739742)

[Install the IPAM feature on IPAM1 18](#_Toc309739743)

[Deploy IP Address Management 19](#_Toc309739744)

[Snapshot the Configuration 21](#_Toc309739745)

[Additional Resources 21](#_Toc309739746)

# Introduction

Internet Protocol Address Management (IPAM) is a framework for discovering, monitoring, auditing, and managing the Internet Protocol (IP) address space used in a network. IPAM in Windows Server "8" Beta provides components for IP address space management, audit of configuration changes, monitoring and management of DHCP and DNS services, and IP address usage tracking.

The need for centralized administration of addresses is increasing dramatically over time as mobile computing, virtualization, and IP devices continue to consume more IP addresses. The need for management tools has also increased with deployment and adoption of new Internet Protocol version 6 (IPv6) networks, which have much larger address pools, and a more complex 128-bit hexadecimal notation as compared with 32-bit dotted decimal Internet Protocol version 4 (IPv4) addresses. The length and complexity of IPv6 addresses makes continued tracking of them in a spreadsheet impractical.

The Windows Server vNext IPAM feature provides a framework and tools to meet the following administrative requirements.

* IP address space management
* Server data collection and address discovery
* Server management and monitoring of DNS and DHCP services
* IP address utilization monitoring
* IP address and configuration change auditing

## In this guide

This guide provides step-by-step instructions for setting up a test lab based on the Windows Server "8" Beta Base Configuration and deploying IPAM using three server computers and one client computer. The resulting test lab demonstrates IPAM setup and functionality.

Important

The following instructions are for configuring an IPAM test lab using the minimum number of computers. Individual computers are needed to separate the services provided on the network and to clearly show the desired functionality. This configuration is neither designed to reflect best practices nor does it reflect a desired or recommended configuration for a production network. The configuration, including IP addresses and all other configuration parameters, is designed only to work on a separate test lab network.

Attempting to adapt this IPAM test lab configuration to a pilot or production deployment can result in configuration or functionality issues.

## Test lab overview

In this test lab, IPAM is deployed with:

* One computer running Windows Server "8" Beta named DC1 that is configured as an intranet domain controller, Domain Name System (DNS) server, and Dynamic Host Configuration Protocol (DHCP) server.
* One intranet member server running Windows Server "8" Beta named APP1 that is configured as a general application server and DHCP server.
* One intranet member server running Windows Server "8" Beta name IPAM1 that is configured as an IP Address Management server.
* One member client computer running Windows 8 Consumer Preview named CLIENT1 that is configured as a DHCP client.

The IPAM test lab consists of one subnet that simulates an intranet named Corpnet (10.0.0.0/24).

Computers connect using a hub or switch. See the following figure.



Figure 1 IPAM Test Lab Configuration

The test lab instructions demonstrate the configuration of IPAM using the Group Policy Object creation and the IPAM automated deployment wizard. Steps to view and modify the IPAM configuration are presented, and operation is verified using a test DHCP client.

## Hardware and software requirements

The following are required components of the test lab:

The following are required components of the test lab:

* The product disc or files for Windows Server "8" Beta.
* The product disc or files for Windows 8 Consumer Preview.
* Computers that meet the minimum hardware requirements for Windows Server "8" Beta.

# Steps for Configuring the IPAM Test Lab

There are five steps to follow when setting up the IPAM test lab based on the Test Lab Guide Base Configuration.

1. Set up the Base Configuration test lab.

The IPAM test lab requires the [Test Lab Guide: Windows Server "8" Beta Base Configuration](http://go.microsoft.com/fwlink/p/?LinkId=236358) Corpnet subnet as its starting point.

1. Configure APP1.

APP1 is already a member server computer that is configured with IIS and also acts as a file server. For the IPAM test lab, APP1 must be configured as a DHCP server.

1. Add and Configure IPAM1.

IPAM1 must be installed and configured as a member server running Windows Server "8" Beta.

1. Configure DC1.

DC1 is already configured as a domain controller, DNS and DHCP server for the Corpnet subnet. For the IPAM test lab, DC1 must be configured with Group Policy objects prepopulated with settings to support automated IPAM setup.

1. Deploy IP Address Management.

For the IPAM test lab, IPAM1 will be used to install and demonstrate IP address management features.

Note

You must be logged on as a member of the Domain Admins group or a member of the Administrators group on each computer to complete the tasks described in this guide. If you cannot complete a task while you are logged on with an account that is a member of the Administrators group, try performing the task while you are logged on with an account that is a member of the Domain Admins group.

This guide provides steps for configuring the computers of the Base Configuration test lab, configuring IPAM, and demonstrating IPAM operation. The following sections provide details about how to perform these tasks.

## Step 1: Set up the Base Configuration Test Lab

Set up the Base Configuration test lab for the Corpnet subnet using the procedures in the “Steps for Configuring the Corpnet Subnet” section of the [Test Lab Guide: Windows Server "8" Beta Base Configuration](http://go.microsoft.com/fwlink/p/?LinkId=236358). Connect **DC1**, **APP1**, and **CLIENT1** to the Corpnet subnet.

## Step 2: Configure APP1

APP1 configuration for the IPAM test lab consists of the following procedures:

* Install the DHCP Server role
* Configure APP1 as a split-scope partner to DC1

The following sections explain these procedures in detail.

### Install the DHCP Server role on APP1

Configure APP1 as a second DHCP server in the Corpnet subnet.

**To install the DHCP Server role on APP1**

|  |
| --- |
| 1. In the **Dashboard** console of Server Manager, under **Configure this local server**, click **Add roles and features**.
2. Click **Next** three times to get to the server role selection screen.
3. In the **Select server roles** dialog, select **DHCP Server**, click **Add Features** when prompted, and then click **Next**.
4. In the **Select features** dialog, click **Next**.
5. Click **Next** on the DHCP Server screen, and then click **Install**.
6. Allow the installation to complete, and then in the Results window, click the link for **Complete DHCP configuration**.
7. In the DHCP Post-Install configuration wizard, click **Next**, and then click **Commit**.
8. On the Summary page, click **Close**.
9. In the Add Roles and Features Wizard, click **Close**.
 |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands**  |
| The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. **Install-WindowsFeature DHCP -IncludeManagementTools** |

### Create a scope on APP1

Configure APP1 with a split-scope to service the Corpnet subnet.

**To configure APP1 as a split-scope partner to DC1**

|  |
| --- |
| 1. On **DC1**, from the Start screen, click **DHCP**.
2. In the DHCP console tree, expand **dc1.corp.contoso.com/IPv4/Scope [10.0.0.0] Corpnet**, right-click **Scope [10.0.0.0]**, point to **Advanced**, and then click **Split-Scope**.
3. In the DHCP Split-Scope Configuration Wizard, click **Next**.
4. Under Additional DHCP Server, type **app1.corp.contoso.com**, and then click **Next**.
5. On the Percentage of Split screen, leave the default 80/20 split, and click **Next**.
6. One the Delay in DHCP Offer screen, click **Next**.
7. On the Summary screen, click **Finish**, and then click **Close**.
 |

## Step 3: Add and configure IPAM1

For the IPAM test lab, IPAM1 will be used to install and demonstrate IP address management features. IPAM1 configuration consists of the following:

 Install the operating system.

 Configure TCP/IP.

 Join the computer to the domain.

The following sections explain these procedures in detail.

### Install the operating system on IPAM1

** To install the operating system on IPAM1**

|  |
| --- |
| 1. Start the installation of Windows Server "8" Beta.2. Follow the instructions to complete the installation, specifying a strong password for the local Administrator account. Log on using the local Administrator account.3. Connect IPAM1 to a network that has Internet access and run Windows Update to install the latest updates for Windows Server "8" Beta.4. Connect IPAM1 to the Corpnet subnet. |

### Configure TCP/IP properties on IPAM1

**To configure TCP/IP properties on IPAM1**

|  |
| --- |
| 1. In Server Manager, click **Local Server** in the console tree. Click the link next to **Wired Ethernet Connection** in the Properties tile.2. In **Network Connections**, right-click **Wired Ethernet Connection**, and then click **Properties**.3. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.4. Select **Use the following IP address**. In **IP address**, type **10.0.0.5**. In **Subnet mask**, type **255.255.255.0**.5. Select **Use the following DNS server addresses**. In **Preferred DNS server**, type **10.0.0.1**.6. Click **OK** twice to close the Wired Ethernet Connection Properties window. Close the **Network Connections** window.7. From the Start screen, type **command**, and then click **Command Prompt**.8. To check name resolution and network communication between IPAM1 and DC1, type **ping dc1.corp.contoso.com** in the command prompt windowand hit **ENTER**.9. Verify that there are four replies from 10.0.0.1.10. Close the Command Prompt window. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png**Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. Note that the "Wired Ethernet Connection" interface name may be different on your computer. Use the **ipconfig /all** command to list all the interfaces. **New-NetIPAddress -InterfaceAlias "Wired Ethernet Connection" -IPv4Address 10.0.0.5 -PrefixLength 24****Set-DnsClientServerAddress -InterfaceAlias "Wired Ethernet Connection" -ServerAddresses 10.0.0.1** |

### Join IPAM1 to the CORP domain

**To join IPAM1 to the CORP domain**

|  |
| --- |
| 1. In Server Manager, click **Local Server** in the console tree. Click the link next to **Computer name** in the Properties tile.
2. In the **System Properties** dialog box, click the **Computer Name** tab. On the **Computer Name** tab, click **Change**.
3. In **Computer Name**, type **IPAM1**. Under **Member of**, click **Domain**, and then type **corp.contoso.com**.
4. Click **OK**.
5. When you are prompted for a user name and password, type **User1** and its password, and then click **OK**.
6. When you see a dialog box welcoming you to the corp.contoso.com domain, click **OK**.
7. When you are prompted that you must restart the computer, click **OK**.
8. On the **System Properties** dialog box, click **Close**.
9. When you are prompted to restart the computer, click **Restart Now**.
10. After the computer restarts, click the **Switch User arrow icon**, then click **Other User** and log on to the CORP domain with the **User1** account.
 |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands**  |
| The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. Note that you must supply domain credentials after entering the Add-Computer command below. **Rename-Computer -NewName IPAM1****Restart-Computer****Add-Computer -DomainName corp.contoso.com****Restart-Computer** |

Note

Windows Server "8" Beta build does not correctly support Add-Computer -Newname, requiring an extra step and reboot. This issue is resolved in later builds of Windows Server "8" Beta.

## Step 4: Configure DC1

In this test lab, the Group Policy-based method is used to configure managed server access for IPAM. Group Policy Objects (GPOs) are created that are dynamically applied to managed servers by IPAM when you explicitly define the server as managed by IPAM. These GPOs provide IPAM with the access it requires. Use the following procedures to configure required GPOs on DC1:

* Create three IPAM GPOs and link them to the corp.contoso.com domain
* Configure settings for the IPAM\_DC\_NPS GPO
* Configure settings for the IPAM\_DHCP GPO
* Configure settings for the IPAM\_DNS GPO

The following sections explain these procedures in detail.

### Create three IPAM GPOs and link them to the corp.contoso.com domain

The IPAM automated deployment option relies on Group Policy Objects (GPOs) to apply the necessary settings to managed servers. These GPOs must be created first by the administrator in all domains in the IPAM scope. The deployment wizard then adds managed nodes to the filter list of the relevant GPOs.

Prior to running automated deployment, create target GPOs in each of the domains within the planned IPAM scope. In this step, you will create and configure the following IPAM GPOs:

* IPAMGPO\_DC\_NPS
* IPAMGPO\_DHCP
* IPAMGPO\_DNS

To create the required IPAM GPOs

|  |
| --- |
| 1. On DC1, from the Start screen, click **Group Policy Management**.
2. Expand **Forest: corp.contoso.com**, expand **Domains**, expand **corp.contoso.com**, and then select **Group Policy Objects**.
3. Right-click **Group Policy Objects**, and then click **New**.
4. Under **Name**, type **IPAMGPO\_DC\_NPS**, and then click **OK**.
5. Right-click **Group Policy Objects**, and then click **New**.
6. Under **Name**, type **IPAMGPO\_DHCP**, and then click **OK**.
7. Right-click **Group Policy Objects**, and then click **New**.
8. Under **Name**, type **IPAMGPO\_DNS**, and then click **OK**.
9. Right-click **corp.contoso.com** in the console tree, and click **Link an Existing GPO**.
10. Click **IPAMGPO\_DC \_NPS**. Hold the SHIFT key and click **IPAMGPO\_DNS** to select the three newly created GPOs. Click **OK**.
11. Next, remove **Authenticated Users** from the **Scope** tab for each GPO. To remove this group, click each IPAM GPO under Group Policy Objects, click the **Scope** tab, select **Authenticated Users** under Security Filtering, click **Remove**, and then click **OK** in the confirmation dialog box that appears.
 |

### Configure settings for the IPAMGPO\_DC\_NPS GPO

Configure settings to be applied to Domain Controllers and Network Policy Servers (NPS).

**To configure settings for the IPAMGPO\_DC\_NPS GPO**

|  |
| --- |
| 1. In Group Policy Management console, right-click the **IPAMGPO\_DC\_NPS** GPO and click **Edit**.
2. In Group Policy Management Editor, expand **Computer Configuration>Policies>Windows Settings>Security Settings>Windows Firewall with Advanced Security>Windows Firewall with Advanced Security – LDAP://…>Inbound Rules**.
3. Right-click **Inbound Rules**, and then click **New Rule**.
4. In the New Inbound Rule Wizard, click **Predefined**, and select **Remote Event Log Management** from the drop-down list. Click **Next**.
5. Click **Next** to allow the default predefined rules, and then click **Finish**.
6. In Group Policy Management Editor, expand **Computer Configuration>Policies>Windows Settings>Security Settings>Restricted Groups**.
7. Right-click **Restricted Groups**, and then click **Add Group**.
8. In the Add Group dialog box, under **Group**, type **Event Log Readers** and then click **OK**.
9. In the Event Log Readers Properties dialog box, next to **Members of this group**, click **Add**. Type **corp.contoso.com\IPAM1$**. Click **OK** twice to close the Event Log Readers Properties dialog box.
10. Close the Group Policy Management Editor.
 |

### Configure settings for the IPAMGPO\_DHCP GPO

Configure settings to be applied to Dynamic Host Configuration Protocol (DHCP) Servers.

**To configure settings for the IPAMGPO\_DHCP GPO**

|  |
| --- |
| 1. In Group Policy Management console, right-click the **IPAMGPO\_DHCP** GPO and click **Edit**.
2. In Group Policy Management Editor, expand **Computer Configuration>Policies>Windows Settings>Security Settings>Windows Firewall with Advanced Security>Windows Firewall with Advanced Security – LDAP://…>Inbound Rules**.
3. Right-click **Inbound Rules**, and then click **New Rule**.
4. In the New Inbound Rule Wizard, click **Predefined**, and select **DHCP Server Management** from the drop-down list. Click **Next**.
5. Click **Next** to allow the default predefined rules, and then click **Finish**.
6. Right-click **Inbound Rules**, and then click **New Rule**.
7. In the New Inbound Rule Wizard, click **Predefined**, and select **Remote Service Management** from the drop-down list. Click **Next**.
8. Click **Next** to allow the default predefined rules, and then click **Finish**.
9. Right-click **Inbound Rules**, and then click **New Rule**.
10. In the New Inbound Rule Wizard, click **Predefined**, and select **File and Printer Sharing** from the drop-down list. Click **Next**.
11. Click **Next** to allow the default predefined rules, and then click **Finish**.
12. Right-click **Inbound Rules**, and then click **New Rule**.
13. In the New Inbound Rule Wizard, click **Predefined**, and select **Remote Event Log Management** from the drop-down list. Click **Next**.
14. Click **Next** to allow the default predefined rules, and then click **Finish**.
15. In Group Policy Management Editor, expand **Computer Configuration>Policies>Windows Settings>Security Settings>Restricted Groups**.
16. Right-click **Restricted Groups**, and then click **Add Group**.
17. In the Add Group dialog box, under **Group**, type **Event Log Readers** and then click **OK**.
18. In the Event Log Readers Properties dialog box, next to **Members of this group**, click **Add**. Type **corp.contoso.com\IPAM1$**. Click **OK** twice to close the Event Log Readers Properties dialog box.
19. Right-click **Restricted Groups**, and then click **Add Group**.
20. In the Add Group dialog box, under **Group**, type **DHCP Users** and then click **OK**.
21. In the DHCP Users Properties dialog box, next to **Members of this group**, click **Add**. Type **corp.contoso.com\IPAM1$**. Click **OK** twice to close the DHCP Users Properties dialog box.
22. In Group Policy Management Editor, expand **Computer Configuration>Preferences>Windows Settings>Network Shares**.
23. Right-click **Network Shares**, click **New**, and then click **Network Share**.
24. In the New Network Share Properties dialog box, next to **Share name**, type **DHCPAudit**. Next to **Folder path**, type **%windir%\System32\dhcp**.
25. Click the **Common** tab and select **Remove this item when it is no longer applied**. Click **OK** in the warning that appears.
26. Click **OK** and verify that the **DHCPAudit** share is added.
27. Close the Group Policy Management Editor.
 |

### Configure settings for the IPAMGPO\_DNS GPO

Configure settings to be applied to Domain Name Service (DNS) Servers.

**To configure settings for the IPAMGPO\_DNS GPO**

|  |
| --- |
| 1. In Group Policy Management console, right-click the **IPAMGPO\_DNS** GPO and click **Edit**.
2. In Group Policy Management Editor, expand **Computer Configuration>Policies>Windows Settings>Security Settings>Windows Firewall with Advanced Security>Windows Firewall with Advanced Security – LDAP://…>Inbound Rules**.
3. Right-click **Inbound Rules**, and then click **New Rule**.
4. In the New Inbound Rule Wizard, click **Predefined**, and select **DNS Service** from the drop-down list. Click **Next**.
5. Click **Next** to allow the default predefined rules, and then click **Finish**.
6. Right-click **Inbound Rules**, and then click **New Rule**.
7. In the New Inbound Rule Wizard, click **Predefined**, and select **Remote Service Management** from the drop-down list. Click **Next**.
8. Click **Next** to allow the default predefined rules, and then click **Finish**.
9. Right-click **Inbound Rules**, and then click **New Rule**.
10. In the New Inbound Rule Wizard, click **Predefined**, and select **Remote Event Log Management** from the drop-down list. Click **Next**.
11. Click **Next** to allow the default predefined rules, and then click **Finish**.
12. In Group Policy Management Editor, expand **Computer Configuration>Policies>Windows Settings>Security Settings>Restricted Groups**.
13. Right-click **Restricted Groups**, and then click **Add Group**.
14. In the Add Group dialog box, under **Group**, type **Event Log Readers** and then click **OK**.
15. In the Event Log Readers Properties dialog box, next to **Members of this group**, click **Add**. Type **corp.contoso.com\IPAM1$**. Click **OK** twice to close the Event Log Readers Properties dialog box.
16. Right-click **Restricted Groups**, and then click **Add Group**.
17. In the Add Group dialog box, under **Group**, type **DnsAdmins** and then click **OK**.
18. In the DnsAdmins Properties dialog box, next to **Members of this group**, click **Add**. Type **corp.contoso.com\IPAM1$**. Click **OK** twice to close the DnsAdmins Properties dialog box.
19. In Group Policy Management Editor, expand **Computer Configuration>Policies>Windows Settings>Security Settings>System Services**.
20. In the details pane of System Services, right-click **DNS Server**, and then click **Properties**.
21. In the DNS Server Properties dialog, on the Security Policy Setting tab, check **Define this policy setting**, select **Automatic** startup mode, and then click **Edit Security**.
22. In the Security for DNS Server dialog, click **Add** and then click **Object Types**. Select **Computers**, and then click **OK**. Type **IPAM1**, and then click **OK**.
23. In the Security for DNS Server dialog, select **IPAM1 (CORP\IPAM1$)**. Select the checkbox to allow **Read** permission. Click **OK**, click **Yes** to continue, and then click **OK** to close the DNS Server Properties dialog.
24. In Group Policy Management Editor, expand **Computer Configuration>Preferences>Windows Settings>Registry**.
25. Right-click **Registry**, point to **New**, and then click **Registry Item**.
26. Click the ellipsis next to **Key Path**, and browse to **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\DNS Server**.
27. Click **Custom SD**, and then click **Select**.
28. Click inside the **Value data** text box, and move the cursor to the far right end of the text string that is displayed.
29. Leave the New Registry Properties dialog open, and launch **Windows PowerShell** from the taskbar.
30. In the Windows PowerShell window, type **Get-ADComputer IPAM1** and hit **ENTER**.
31. From the output displayed, highlight the text string next to **SID** and press **ENTER** to copy the text string onto the clipboard.
32. In the New Registry Properties dialog, type **(A;;0x1;;;** and then paste the text string that you copied from the Windows PowerShell prompt. Type a close parenthesis) to complete the value data, and then click **OK**.
33. Verify that the **CustomSD** registry entry was added to the DNS GPO.
34. Close the Group Policy Management Editor.
35. Close the Group Policy Management console.
 |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. **Invoke-IpamGpoProvisioning -Domain corp.contoso.com -GpoPrefixName IPAMGPO -IpamServerFqdn IPAM1.corp.contoso.com -Force** |

## Step 5: Deploy IP Address Management on IPAM1

For the IPAM test lab, IPAM1 will be used to install and demonstrate IP address management features. IPAM1 configuration consists of the following:

 Install the IPAM feature.

 Use the Automated Deployment method to deploy IPAM.

 Demonstrate IPAM functionality.

The following sections explain these procedures in detail.

### Install the IPAM feature on IPAM1

Configure IPAM1 with the IP Address Management feature.

**To install the IPAM feature on IPAM1**

|  |
| --- |
| 1. On IPAM1, in the **Dashboard** console of Server Manager, click **Add roles and features**.
2. Click **Next** four times to get to the **Features** selection screen.
3. In the **Select features** dialog, select **IP Address Management (IPAM) Server**, click **Add Features** when prompted, and then click **Next**.
4. On the Confirmation screen, click **Install**.
5. Allow the installation to complete, and then click **Close**.
 |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. **Install-WindowsFeature IPAM -IncludeManagementTools** |

### Deploy IP Address Management

Use the Automated Deployment method to deploy IP Address Management on IPAM1.

**To deploy IPAM**

|  |
| --- |
| 1. In Server Manager on IPAM1, click **IPAM** in the console tree.
2. Verify that you are connected to **IPAM1.corp.contoso.com**.
3. Click **provision the IPAM server**.
4. In the Provision IPAM wizard, click **Next**.
5. On the Select provisioning method screen, select **Group Policy Based**, and next to GPO name prefix, type **IPAMGPO**. Click **Next**.
6. On the Summary screen, click **Apply**.
7. In the **Completion** dialog box, confirm that IPAM provisioning completed successfully, and then click **Close**.
8. Under IPAM Server Tasks, click **configure server discovery**.
9. In the Configure Discovery Settings wizard, next to **(root domain) corp.contoso.com**, click **Add**.
10. Click **OK** twice to apply the discovery scope.
11. Under IPAM Server Tasks, click **start server discovery**. Click **OK** to acknowledge the discovery triggered dialog.
12. Click **Server Inventory** in the console tree. When the discovery process completes, the console should show DC1 as a discovered server. Note that Manageability Status is displayed as Unspecified, and IPAM access status is Blocked. In order to apply the GPO setting configured in Step 4, you must set manageability status for the server.
13. Right-click the entry for **DC1**, and click **Edit Server**.
14. In the Add or Edit Server dialog, select **DC**, **DNS server**, and **DHCP server** for Server type, and change Manageability status to **Managed**. Click **OK**.
15. Note that the status for DC1 now shows as **Blocked**.
16. From the Start screen, click **Group Policy Management**.
17. In Group Policy Management console, expand **Forest: corp.contoso.com**, expand **Domains**, expand **corp.contoso.com**, and then select **Group Policy Objects**.
18. Expand **Group Policy Objects**, and examine the scope tab for **IPAM\_DC\_NPS**, **IPAM\_DHCP**, and **IPAM\_DNS**. Note that the DC1 computer account has been added to the security filtering for these GPOs.
19. Close the Group Policy Management console. The IPAM settings will be applied the next time group policy is applied to DC1. To speed up this process, you can switch to DC1 and run gpupdate or restart the server.
20. After updating policy on DC1, right-click **DC1** in the IPAM Server Inventory console, and then click **Refresh Server Access Status**. Click **OK** in the resulting prompt.
21. Once IPAM Access Status shows as **Unblocked**, right-click the DC1 entry and click **Retrieve All Server Data**.
22. In the console tree, right-click **IPv4**, and then click **Add Server**.
23. For Server name (FQDN), type **APP1**, and then click **Verify**.
24. Select **DHCP server** for Server type, and then change Manageability status to **Managed**. Click **OK**.
25. Update group policy on APP1 or restart the server, then right-click **APP1** in the IPAM Server Inventory console, and then click **Refresh Server Access Status**.
26. Once IPAM Access Status shows as **Unblocked**, right-click the APP1 entry and click **Retrieve All Server Data**.
 |

### Demonstrate IPAM functionality

Examine IPAM console sections and demonstrate functionality.

**To demonstrate IPAM functionality on IPAM1**

|  |
| --- |
| 1. Click **IP Address Space** in the console tree. Once data retrieval completes, the 10.0.0.0/24 network should appear as an IP Range Block and IP Range Group. In the **Details view**, click the tabs for Utilization Trend, Configuration Details, and Event Catalog to examine the details for 10.0.0./24.
2. Under the Monitor and Manage section of the console tree, click **DNS and DHCP Servers**. Note that DC1 is listed as both a DNS and DHCP server, and APP1 is listed as a DHCP server. Examine the tabs in the Details view to see the monitoring capabilities available.
3. Click **DHCP Scopes** in the console tree. Right-click each of the scopes and click **Edit DHCP Scope** to examine the scope properties on APP1 and DC1. Note that there is no Description value listed for either scope.
4. Next, modify both scopes simultaneously to update the scope description. Click the Corpnet scope on APP1, then hold the SHIFT key and click the scope on DC1 to select both scopes. Right-click and select **Edit DHCP Scope**.
5. For Description, type **Subnet for the Corpnet intranet**. Click **OK**.
6. Right-click each of the scopes again and click **Edit DHCP Scope** to see that the scope description has been updated on both APP1 and DC1.
7. Click **Event Catalog** in the IPAM console tree.
8. Examine the IPAM configuration events and DHCP configuration events that have been captured.
9. Under IP Address Tracking, click **By Host Name**.
10. Type **CLIENT1** in the search box, and then type dates in the two text boxes next to **and DHCP lease events between these dates** in the format of month/day/year. Enter a range of dates that includes today, and then click **Search**.
11. Examine the history of DHCP lease and renewal and DC authentication events for CLIENT1.
 |

# Snapshot the Configuration

This completes the IPAM test lab. To save this configuration so that you can quickly return to a working IPAM configuration from which you can test other modular test lab guides (TLGs), TLG extensions, or for your own experimentation and learning, do the following:

1. On all physical computers or virtual machines in the test lab, close all windows and then perform a graceful shutdown.
2. If your lab is based on virtual machines, save a snapshot of each virtual machine and name the snapshots IPAM TLG. If your lab uses physical computers, create disk images to save the IPAM test lab configuration.

# Additional Resources

For a list of all of the Windows Server “8” Beta TLGs, see [Windows Server “8” Beta Test Lab Guides](http://go.microsoft.com/fwlink/?LinkID=243062) in the TechNet Wiki.

For a list of additional Microsoft TLGs, see [Test Lab Guides](http://go.microsoft.com/fwlink/?LinkID=202817) in the TechNet Wiki.

To provide the authors of this guide with feedback or suggestions for improvement, send an email message to [tlgfb@microsoft.com](file:///C%3A%5CUsers%5Cjosephd%5CDocuments%5CSharePoint%20Drafts%5Ctlgfb%40microsoft.com).