Step-By-Step: Setup Windows Server 2012 IPAM in your environment

Pierre Roman
15 Aug 2013 12:13 PM

- 2

Let me ask you a question. You’re an IT pro, how do you keep track of all the IP addresses on your network?

I don’t mean how you distribute them, but how do you keep track of the static addresses? How do you report on them? Maybe you have them all itemized on an Excel spreadsheet. Does everyone in your shop keep track as diligently as you? Is it up to date?

Now you don’t have to. IPAM to the rescue. It’s part of the new functionalities included in Windows Server 2012 and Windows Server 2012 R2

IPAM in Windows Server 2012 is a new built-in framework for discovering, monitoring, auditing, and managing the IP address space used on your network. IT includes components for:

- Automatic IP address infrastructure discovery: IPAM discovers domain controllers, DHCP servers, and DNS servers in the domains you choose. You can enable or disable management of these servers by IPAM.
- Custom IP address space display, reporting, and management: The display of IP addresses is highly customizable and detailed tracking and utilization data is available. IPv4 and IPv6 address space is organized into IP address blocks, IP address ranges, and individual IP addresses. IP addresses are assigned built-in or user-defined fields that can be used to further organize IP address space into hierarchical, logical groups.
- Audit of server configuration changes and tracking of IP address usage: Operational events are displayed for the IPAM server and managed DHCP servers. IPAM also enables IP address tracking using DHCP lease events and user logon events collected from Network Policy Server (NPS), domain controllers, and DHCP servers. Tracking is available by IP address, client ID, host name, or user name.
- Monitoring and management of DHCP and DNS services: IPAM enables automated service availability monitoring for Microsoft DHCP and DNS servers across the forest. DNS zone health is displayed, and detailed DHCP server and scope management is available using the IPAM console.

It can be a huge help for you to be able to automatically manage your DNS, DHCP and all the monitoring and auditing.Here’s how we do it.

Install IPAM

IPAM is a feature of and it need to be installed using Server Manager or PowerShell.

```
Install-WindowsFeature IPAM –IncludeManagementTools
```

Whichever you're most familiar with.

Choose an IPAM Provisioning Method

Once installed you need to choose your provisioning method. The provisioning method is the process of enabling required permissions, files shares, and access settings on managed servers so that the IPAM server can communicate with them. You can choose either the manual or Group Policy Based method. Pick the one that's best for you and remember, you can't change it later.

1. **Manual**: Typically used when the number of managed servers is small. If you choose the manual provisioning method, access settings must be configured individually on each managed server. Settings must also be removed manually if the server becomes unmanaged. You can use Group Policy to apply settings to managed servers even if the manual provisioning method is chosen, but you must apply and remove GPOs manually. The manual provisioning method is not preferred because it is more complex and less consistent than the Group Policy based method.
2. **Group Policy Based**: The Group Policy based method is preferred because it is simpler and less prone to errors. If you choose the Group Policy based provisioning method, GPOs are applied automatically to servers when they are assigned a status of managed in the IPAM console. GPOs are also removed automatically if the status of a server changes from managed to unmanaged.
   If you chose the Group Policy based method, you must also provide a GPO name prefix in the provisioning wizard. After providing a GPO name prefix, the wizard will display the GPO names that must be created in domains that will be managed by IPAM. The following role-based GPOs are required in each domain that contains managed servers. The wizard does not create these GPOs.
   - **<GPO-prefix>_DHCP**: This GPO is used to apply settings that allow IPAM to monitor, manage, and collect information from managed DHCP servers on the network.
   - **<GPO-prefix>_DNS**: This GPO is used to apply settings that allow IPAM to monitor and collect information from managed DNS servers on the network.
   - **<GPO-prefix>_DC_NPS**: This GPO is used to apply settings that allow IPAM to collect information from managed domain controllers and network policy servers (NPS) on the network for IP address tracking purposes.

In our case we will use the Group Policy method

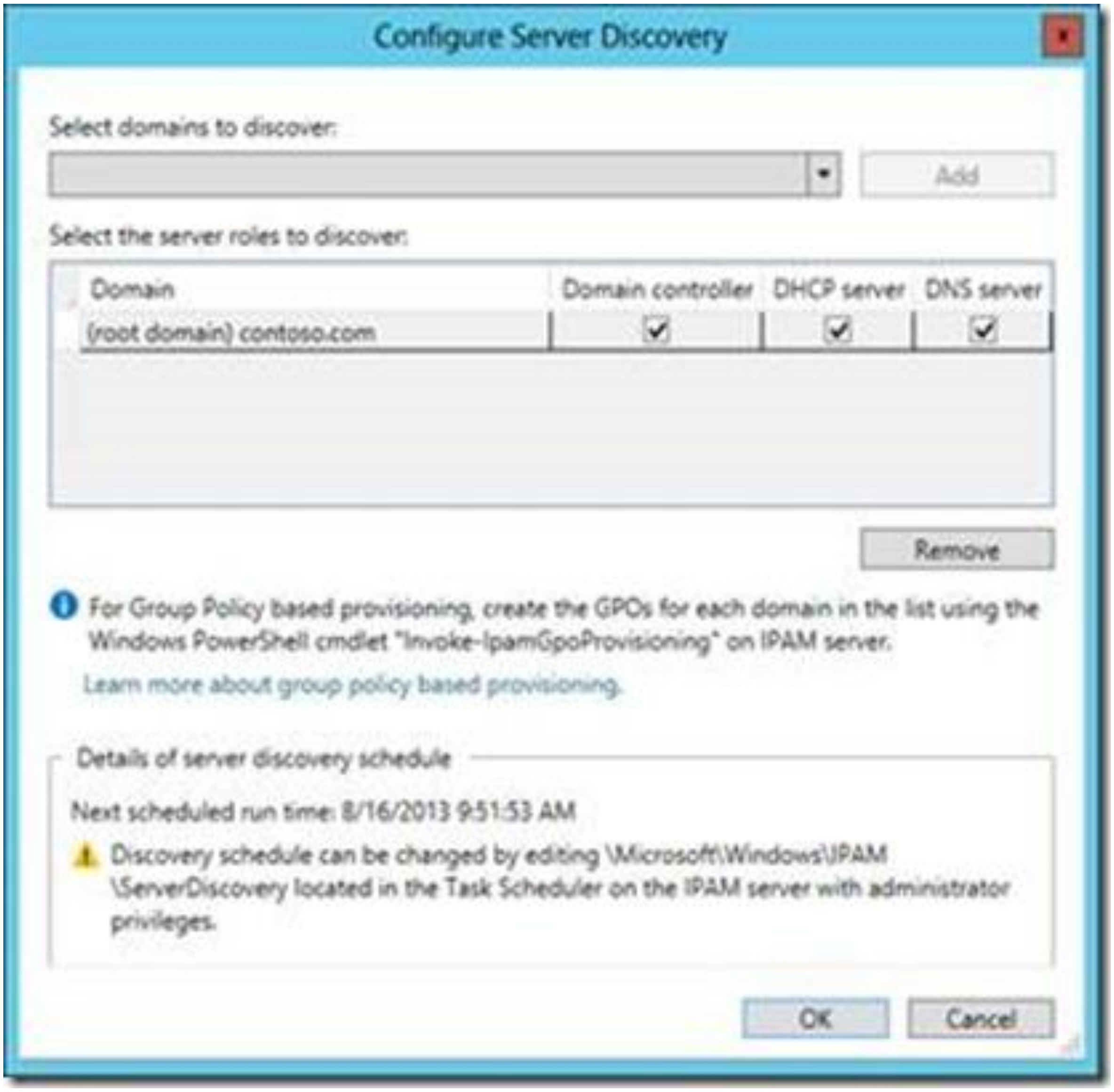
In Server manager, in the IPAM section. Select Provision the IPAM server, and go through the provisioning wizard.

We'll create the GPOs later. Next we need to configure the Server discovery.

Configure Server Discovery

When you configure server discovery, you are defining the domains that the IPAM server can monitor and manage (also called the scope of discovery). An IPAM server can monitor and manage multiple domains as long as they are part of the same Active Directory forest as the IPAM server.

1. On the IPAM Overview page, click **Configure server discovery**.
2. Choose each domain that you will manage with the current IPAM server by selecting it from the drop-down list and then clicking Add.


Configure Server Discovery
Select domains to discover:
Add
Select the server roles to discover:
Remove
Learn more about group policy based provisioning.
OK
Cancel

Domain	Domain controller	DHCP server	DNS server
(root domain) contoso.com	☑	☑	☑

For Group Policy based provisioning, create the GPOs for each domain in the list using the Windows PowerShell cmdlet "Invoke-IpamGpoProvisioning" on IPAM server.

Details of server discovery schedule

Next scheduled run time: 8/16/2013 9:51:53 AM

Discovery schedule can be changed by editing \Microsoft\Windows\IPAM \ServerDiscovery located in the Task Scheduler on the IPAM server with administrator privileges.

3. To remove a domain from the scope of discovery, click the domain and then click **Remove**.

4. By default all server roles are enabled in the domains you select. To remove a server role from the scope of discovery for a specific domain, de-select the checkbox under the appropriate server role.

5. Click **OK** when you are finished.

Discover Servers on the Network

Domain controllers, DHCP servers, and DNS servers can be discovered on the network, provided they are running Windows Server® 2008 or a later operating system. Computers running NPS must be added manually to the server inventory

Since this is the first time we are discovering servers, we will discover servers by running the server discovery task. This task also runs regularly on the IPAM server with a default frequency of once per day, and will discover new servers automatically provided that they meet the conditions for discovery.

Conditions for discovery depend on the type of role services that are installed and running on managed servers. For example, a DHCP server will not be discovered if it is not authorized in Active Directory or does not have any DHCP scopes configured. DHCP scopes do not need to be active to be discovered. A DNS server will not be discovered unless it is authoritative for an Active Directory domain configured in the scope of discovery

1. On the IPAM Overview page, click **Start server discovery**. This will start the IPAM **ServerDiscovery** task. Alternatively, you can click **Manage** on the IPAM console menu, and then click **Start Server Discovery**.
2. Wait for the task to complete. You can click the notification flag to view status of the **ServerDiscovery** task if desired.

1. When the task has completed running, view the **Server inventory** page to display the list of discovered servers.
2. If the list of discovered servers is incomplete, verify that the correct node is selected in the lower navigation pane. By default, IPv4 is selected. You can click **Refresh** to ensure the view is current.

Create IPAM Provisioning GPOs

When we picked the Provisioning method. We picked the GPO method, however the wizard did not actually create the group policies. All it did is configure and assign the names for them.

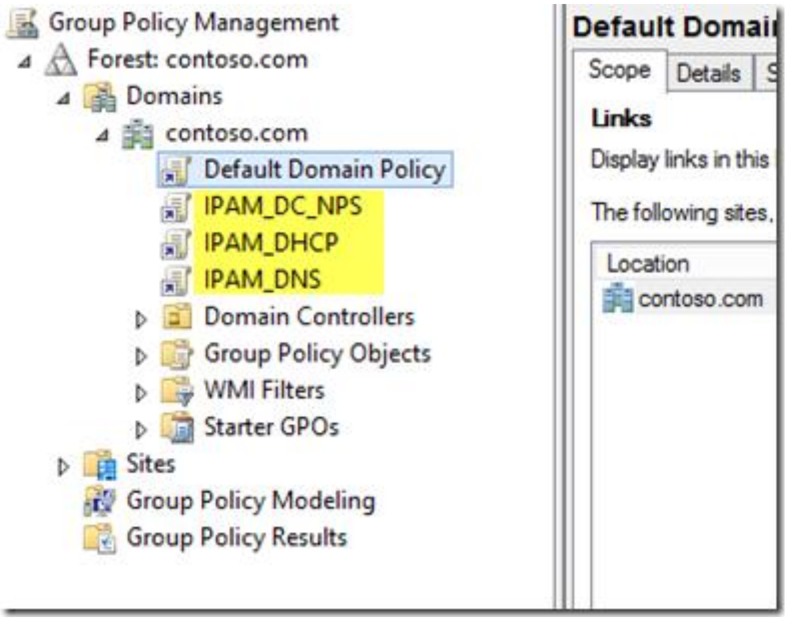
There are 3 policies that need to be created. The GPO Prefix we selected in step 2 is IPAM. So our 3 policies will be:

- **IPAM_DHCP**: For managed DHCP servers.
- **IPAM_DNS**: For managed DNS servers.
- **IPAM_DC_NPS**: For managed domain controllers and NPS servers.

They will created by running the following PowerShell script.

```
Invoke-IpamGpoProvisioning –Domain contoso.com –GpoPrefixName
IPAM –IpamServerFqdn dc1.contoso.com
```

You can find all the info on the available parameters is provided in the following [TechNet article].



Choose Managed Servers

So far we:

- Installed IPAM Server
- Chose an IPAM Provisioning Method
- Configured Server Discovery
- Discovered Servers on the Network
- Created IPAM Provisioning GPOs

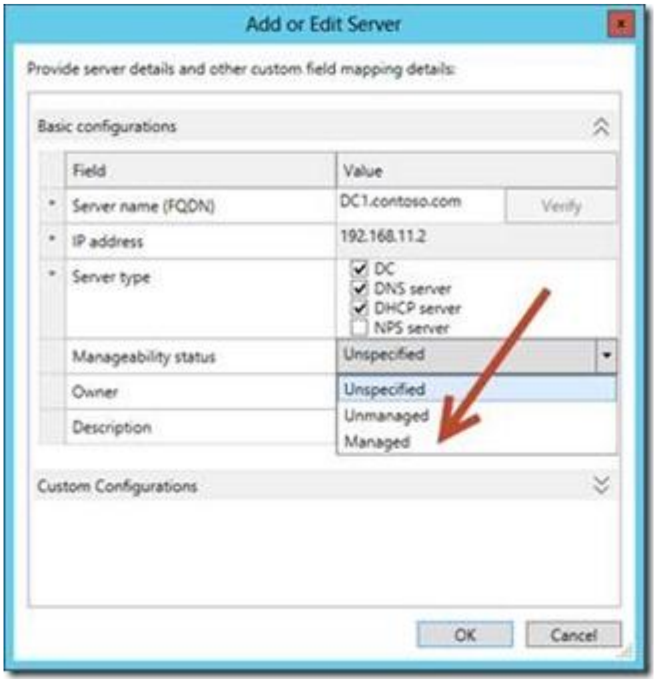
Now we need to choose our managed servers.

Choosing a managed server is done by assigning manageability status. In our case since we chose the GPO method, a manageability status of Managed means that the server will automatically be added to security filtering in the appropriate IPAM GPO.

Membership in the Administrators group, or equivalent, is the minimum required to complete this procedure

1. In the upper IPAM navigation tree, click **SERVER INVENTORY**. The list of servers that have been discovered or manually added is displayed.
2. Right-click the server or servers that you are selecting and then click **Edit Server**.

3. In the **Add or Edit Server** dialog box next to **Manageability status**, select **Managed** from the drop-down list if the server will be managed by the current IPAM server.


Add or Edit Server

Provide server details and other custom field mapping details:

Basic configurations

	Field	Value
*	Server name (FQDN)	DC1.contoso.com
*	IP address	192.168.11.2
*	Server type	☑ DC ☑ DNS server ☑ DHCP server ☐ NPS server
	Manageability status	Unspecified
	Owner	
	Description	

Custom Configurations

Retrieve Data from Managed Servers

After you have verified the IPAM server has access to managed servers, you can retrieve data from managed servers to begin populating the IPAM database. You might also want to retrieve server data after a configuration change or just to obtain updated information. You do not have to manually retrieve data from managed servers because scheduled tasks on the IPAM server will perform this task automatically

1. In the upper IPAM navigation tree, click **SERVER INVENTORY**.
2. Select the managed servers from which you want to collect data. Press and hold CTRL or SHIFT to select multiple servers.
3. Right-click the servers that are selected, and then click **Retrieve All Server Data**.
4. The following data collection tasks will run immediately on the selected servers: **AddressExpiry**, **AddressUtilization**, **Audit**, **ServerAvailability**, **ServiceMonitoring**, **ServerConfiguration**.
5. Wait for the data collection tasks to complete.

You're environment is now set to discover, monitor, auditi, and manage the IP address space used your network.