What's New in IPAM

5 out of 8 rated this helpful - Rate this topic

Published: June 24, 2013

Updated: July 3, 2014

Applies To: Windows Server 2012, Windows Server 2012 R2

This topic describes the IP Address Management (IPAM) functionality that is new or changed in Windows Server 2012 R2 and Windows Server 2012.

IPAM provides highly customizable administrative and monitoring capabilities for the IP address infrastructure on a corporate network. You can monitor, audit, and manage servers running Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS).

In this topic:

What's new in IPAM in Windows Server 2012 R2

In Windows Server 2012 R2, IPAM offers enhanced support in the following areas.

Feature/Functionality	New or improved	Description
Role-based access control	New	Role based access control enables you to customize the types of operations and access permissions for users and groups of users on specific objects.
Virtual address space management	New	IPAM streamlines management of physical and virtual IP address space in System Center Virtual Machine Manager.
Enhanced DHCP server management	Improved	Several new operations are available in IPAM to enhanced the monitoring and management of the DHCP Server service on the network.
External database support	New	In addition to Windows Internal Database (WID), IPAM also optionally supports the use of a Microsoft

		SQL database.
Upgrade and migration support	New	If you installed IPAM on Windows Server 2012, your data is maintained and migrated when you upgrade to Windows Server 2012 R2.
Enhanced Windows PowerShell support	Improved	Windows PowerShell support for IPAM is greatly enhanced to provide extensibility, integration, and automation support.

Role-based access control

Role-based access control provides you with the ability to customize roles, access scopes, and access policies. Thus, you have the ability to define and establish fine-grained control for users and groups, enabling them to perform a specific set of administrative operations on specific objects managed by IPAM.

Roles: A role is a collection of IPAM operations. You can associate a role with a user or group in Windows using an access policy. Eight built-in administrator roles are provided for convenience, but you can also create customized roles to meet your business requirements.

Access scopes: An access scope determines the objects that a user has access to. You can use access scopes to define administrative domains in IPAM. For example, you might create access scopes based on geographical location. By default, IPAM includes an access scope of Global. All other access scopes are subsets of the Global access scope. Users or groups that are assigned to the Global access scope have access to all objects in IPAM that are permitted by their assigned role.

Access Policies: An access policy combines a role with an access scope to assign permission to a user or group. For example, you might define an access policy for a user with a role of IP Block Admin and an access scope of Global\Asia. Therefore, this user will have permission to edit and delete IP address blocks that are associated to the Asia access scope. This user will not have permission to edit or delete any other IP address blocks in IPAM.

The following default access scope and roles are provided:

Type	Name	Description
Role	DNS record administrator	Manages DNS resource records
Role	IP address record administrator	Manages IP addresses but not IP address spaces, ranges, blocks, or subnets.
Role	IPAM administrator	Manages all settings and objects in IPAM
Role	IPAM ASM administrator	Completely manages IP addresses

Role	IPAM DHCP administrator	Completely manages DHCP servers
Role	IPAM DHCP reservations administrator	Manages DHCP reservations
Role	IPAM DHCP scope administrator	Manages DHCP scopes
Role	IPAM MSM administrator	Completely manages DHCP and DNS servers
Access scope	Global	By default, all objects in IPAM are included in the global access scope. All additional scopes that are configured are subsets of the global access scope.

Virtual address space management

IPAM offers a unified, centralized administrative experience for network administrators to manage IP address space on a corporate network and in Microsoft-powered cloud networks. IPAM enables network administrators to completely streamline the IP address space administration of both physical (fabric) and virtual networks. The integration between IPAM and System Center 2012 R2 Virtual Machine Manager provides end-to-end IP address space automation for Microsoft-powered cloud networks. IPAM integration with Virtual Machine Manager enables a single IPAM server to detect and prevent IP address space conflicts, duplicates, and overlaps across multiple instances of Virtual Machine Manager deployed in the large datacenter.

To view virtual address space in IPAM, click the new **VIRTUALIZED ADDRESS SPACE** node in the upper navigation pane of the IPAM console.

Enhanced DHCP server management

DHCP server management with IPAM is greatly enhanced in Windows Server 2012 R2, including multiple new operations for DHCP scope and DHCP servers, and views for the following objects:

- DHCP failover
- DHCP policies
- DHCP superscopes
- DHCP filters
- DHCP reservations

External database support

During the IPAM provisioning process, you have the option of choosing a WID or Microsoft SQL Server for the IPAM database. With Microsoft SQL Server, the IPAM database can be collocated on the IPAM server, or it can be located on a remote computer. Support for SQL enables additional scalability, disaster recovery, and reporting scenarios.

Upgrade and migration support

The IPAM database can be migrated seamlessly when you upgrade from Windows Server 2012 to Windows Server 2012 R2.

Enhanced Windows PowerShell support

55 new Windows PowerShell cmdlets are available for IPAM in Windows Server 2012 R2. For more information, see IPAM Server Cmdlets in Windows PowerShell.