Server Pools

Server Pools

A server pool contains a set of servers. These servers typically share the same characteristics. Those characteristics can be their location in the chassis, or an attribute such as server type, amount of memory, local storage, type of CPU, or local drive configuration. You can manually assign a server to a server pool, or use server pool policies and server pool policy qualifications to automate the assignment.

If your system implements multitenancy through organizations, you can designate one or more server pools to be used by a specific organization. For example, a pool that includes all servers with two CPUs could be assigned to the Marketing organization, while all servers with 64 GB memory could be assigned to the Finance organization.

A server pool can include servers from any chassis in the system. A given server can belong to multiple server pools.

When you select a specific server pool, you can view the individual details for that pool, including the number of servers included in the pool, and the associated qualification policies.

Creating or Editing a Server Pool

To watch a video on creating a server pool, see Video: Creating a Server Pool.

After you create the server pool, you can assign it to a service profile template. See Video: Assigning a Server Pool to a Global Service Profile Template.

Procedure

Step 1 In the Actions bar, type **Create Server Pool** and press **Enter**.

This launches the **Server Pool** dialog box.

Step 2   In **Basic**, click **Organization** and select the location in which you want to create the server pool.

Step 3   Enter a **Name** and optional **Description**.

Step 4   Required: In **Qualification**, click **Add** to add new qualification policies, or **Delete** to remove existing ones.

For more information, see .

Step 5   In **Servers**, add the servers to be included in the pool.

Step 6   Click **Create**.

Server Pool Qualification Policy

The server pool qualification policy qualifies servers based on the server inventory conducted during the discovery process. You can configure these qualifications or individual rules in the policy to determine whether a server meets the selection criteria. For example, you can create a rule that specifies the minimum memory capacity for servers in a data center pool.

Qualifications are used in other policies to place servers, not just by the server pool policies. For example, if a server meets the criteria in a qualification policy, it can be added to one or more server pools or have a service profile automatically associated with it. You can use the server pool policy qualifications to qualify servers according to the following criteria:

- Adapter type

- Chassis location

- Memory type and configuration

- Power group

- CPU cores, type, and configuration

- Storage configuration and capacity

- Server model or server type

- Owner

- Site

- Address

- Domain group

- Domain name

- Product family

Creating or Editing a Server Pool Qualification Policy

Procedure

Step 1	In the **Actions** bar, type **Create Server Pool Qualification Policy** and press Enter.
Step 2	In the **Server Pool Qualification Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.
Step 3	Enter a **Name** and optional **Description** and **Server Model/PID**.
Step 4	(Optional) In **Domain**, click the plus sign to add the **Domain Qualifier**.
	When you click **Domain Qualifier** the system displays available domain qualification options in tabs on the right pane. Click the appropriate tabs and add the qualification.
Step 5	In **Hardware**, select the appropriate qualification if you enable the processor, memory, storage, or adapter options.
Step 6	Click **Create**.

IP Pools

IP pools are a collection of IP IPv4 or IPv6 addresses. You can use IP pools in Cisco UCS Central in one of the following ways:

- For external management of Cisco UCS Managerservers.

- For iSCSI boot initiators.

- For both external management and iSCSI boot initiators in Cisco UCS Manager.

Note The IP pool must not contain any IP addresses that were assigned as static IP addresses for a server or service profile.

A fault is raised if the same IP address is assigned to two different Cisco UCS domains. If you want to use the same IP address, you can use the **scope** property to specify whether the IP addresses in the block are public or private:

- **public**—The IP addresses in the block can be assigned to multiple Cisco UCS domains.

- **private**—You can assign the IP addresses in the block to one and only one registered Cisco UCS domain.

Cisco UCS Central creates public IP pools by default.

Global IP pools should be used for similar geographic locations. If the IP addressing schemes are different, the same IP pool cannot be used for those sites.

Cisco UCS Central supports creating and deleting IPv4 and IPv6 blocks in IP pools. However, iSCSI boot initiators support only IPv4 blocks.

Creating and Editing an IP Pool

After creating an IP pool you can edit it by selecting the **Edit** icon on the overall summary page of the selected IP pool. To select an IP pool, go to **All Pools** page and select the IP pool that you want to edit. The page redirects you to the overall summary page of the selected IP pool.

Procedure

Step 1 In the Task bar, type **Create IP Pool** and press **Enter**.

This launches the **Create IP Pool** dialog box.

Step 2 In **Basic**, complete the following:

a) From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access an IP pool.

b) Enter the name and description of the pool.

Step 3 Click the respective IP blocks to create a block of IP addresses (IPV4 or IPV6) and complete the following:

a) Click the **Plus** sign to create one or more blocks of IP addresses in the selected pool.

b) In the respective IP block start column, enter the first IPv4 or IPv6 addresses in the block.

c) In the **Size** column, enter the total number of IP addresses in the pool.

Step 4 Click the **Apply** icon.

The page displays additional fields.

Step 5 In **Basic**, complete the following fields:

a. Enter the subnet mask associated with the IPv4 or IPv6 address in the block.

b. Enter the default gateway associated with the IPv4 or IPv6 address in the block.

c. Enter the primary DNS server that this block of IPv4 or IPv6 address should access.

d. Enter the secondary DNS server that this block of IPv4 or IPv6 address should access.

e. Select whether the IP addresses in the block can be assigned to one or more Cisco UCS domains registered with Cisco UCS Central. This can be one of the following:

- **Public**—The IP addresses in the block can be assigned to multiple Cisco UCS domains.

- **Private**—The IP addresses in the block can be assigned to one and only one registered Cisco UCS domain.

Note The scope for an IP address within the block cannot be changed after the block has been saved.

Step 6 In **IPv4** or **IPV6** addresses, you can view a graphical representation of the number of IP addresses in the pool, the number of assigned IP addresses and the number of duplicated IP addresses.

Step 7 In **Access Control**, select a policy to associate with this IP address block from the **ID Range Access Control Policy** drop-down list

Step 8 Click **Create**.

Creating and Editing a Management IP Pool

You can create a Management IP Pool and assign it to an Inband policy or use it as KVM Outband Pool from **Domain Configuration Settings** in the **Domains Main View**.

Procedure

Step 1 In the **Actions** bar, type **Create Management IP Pool** and press **Enter**.

Step 2 In the **Create Management IP Pool** dialog box, click **Basic** and choose the **Domain Group** in which you want to create the Management IP pool, and enter the **Name** and optional **Description**.

The name is case sensitive.

Step 3 In **IPv4 Blocks**, select an IPv4 block from the list or click + to enter the IPv4 address and the pool size for the block.

The pool size must range between 1- 1024.

Step 4 In **IPv6 Blocks**, select an IPv6 block from the list or click + to enter the IPv6 address and the pool size for the block. The pool size must range between 1- 1024.

Complete the following details for both the IPv4 and IPv6 blocks:

a. Enter the subnet mask associated with the IPv4 or IPv6 address in the block.

b. Enter the default gateway associated with the IPv4 or IPv6 address in the block.

c. Enter the primary DNS server that this block of IPv4 or IPv6 address should access.

d. Enter the secondary DNS server that this block of IPv4 or IPv6 address should access.

e. Select whether the IP addresses in the block can be assigned to one or more Cisco UCS domains registered with Cisco UCS Central. This can be one of the following:

   • **Public**—The IP addresses in the block can be assigned to one and only one registered Cisco UCS domain.

   • **Private**—The IP addresses in the block can be assigned to multiple Cisco UCS domains.

Note
   1. IPv6 is not supported for Outband KVM.

   2. You cannot change the scope for an IP address within the block after you save the block.

Step 5 Click **Create**.

Step 6 After creating a Management IP pool, you can edit it by selecting the **Edit** icon on the summary page of the selected Management IP Pool. Repeat steps 2-4 and then click **Save**.

Step 7 (Optional) You can favorite this screen and pin it to the Cisco UCS Central dashboard to navigate to it directly.

Configuring Management IPs

You can set Management IPs for KVM in the **Configure Management IPs** window. You can navigate to the **Configure Management IPs** window from the **Tools** menu on the **Server Details** page. To assign the management IPs through an Inband policy, see Creating an Inband Policy. You can set the Management IPs for KVM Outband from **Domains View** > **Domain Configuration Settings** > **Management IP** > **Outband Pool**.

Before you begin

Before you configure management IPs, you must:

- Create a **Management IP Pool** and specify the IPv4 and IPv6 blocks.

- Assign the Inband Policy or Outband Pool to a domain from the **Domain Configurations Settings** window.

- Set the VLAN Group in the Inband Policy assigned to the domain. The VLAN you select for Inband management network for manual assignment must belong to the VLAN Group you set.

Procedure

Step 1	In **Inband Management**, select the VLAN you want to manually assign from the **Inband Management Network** drop-down list. This list displays all VLANs added to the VLAN Group that you assigned in the Inband policy.
Step 2	Select the IPv4 pool that you want to manually assign from the **Inband Management IP Pool (IPv4)** drop-down list.
Step 3	Select the IPv6 pool that you want to manually assign from the **Inband Management IP Pool (IPv6)** drop-down list.
Step 4	Click **Save**.
Step 5	From the **Server Details** page, select **Launch KVM Console** from the **Configuration Settings** menu and select the **Physical IPv4 Inband address** and **Physical IPv6 Inband address** for the KVM.

- The server inherits the configuration settings after you assign the parameters to complete the configuration. You can verify the management IP details from the **CIMC** configuration settings in the **Server Details** page. However, the manually configured servers supersede the configuration settings deployed through the Inband policy. To make them inherit the configuration settings defined in the Inband policy, you must unassign the parameters of the Inband policy and associate them with the Inband policy. To unassign and reassign policy parameters, see Creating an Inband Policy.

- The Inband configurations that are part of a service profile do not impact any of the assignments made through the Inband policy or the manual assignment.

- When you deploy a global Inband policy from Cisco UCS Central to Cisco UCS Manager, it supersedes the local Inband profile in Cisco UCS Manager, and does not allow you to edit the VLAN Group, Network, and IP Pool Name fields under the **Inband Profile** in the **LAN** tab. These fields are grayed out. You can edit them only if you Localize them by clicking the **Use Local for InBand Profile** in the Actions area. For more information about localizing a global policy pushed down from Cisco UCS Central, see Cisco UCS Manager documentation.

- You can verify the status of Management IP pools by clicking **Error Details**.

- When you move a domain across domain groups, the Inband configuration settings are retained. You can click **Reapply Configuration** from the **Domain** tab when you move a domain across domain groups.

IQN Pools

An IQN pool is a collection of iSCSI Qualified Names (IQNs) for use as initiator identifiers by iSCSI vNICs in a Cisco UCS domain. IQN pools created in Cisco UCS Central can be shared between Cisco UCS domains.

IQN pool members are of the form *prefix:suffix:number*, where you can specify the prefix, suffix, and a block (range) of numbers.

An IQN pool can contain more than one IQN block, with different number ranges and different suffixes, but share the same prefix.

Creating and Editing an IQN Pool

Note   In most cases, the maximum iSCSI Qualified Name (IQN) size (prefix + suffix + additional characters) is 223 characters. When using the Cisco UCS NIC M51KR-B adapter, you must limit the IQN size to 128 characters.

After creating an IQN pool you can edit it by selecting the **Edit** icon on the overall summary page of the selected IQN pool. To select an IQN pool, go to **All Pools** page and select the IQN pool that you want to edit. The page redirects you to the overall summary page of the selected IQN pool.

Procedure

Step 1   In the Actions bar, type **Create IQN Pool** and press **Enter**.

This launches the **Create IQN Pool** dialog box.

Step 2   In **Basic**, complete the following:
   a) From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access an IQN pool.
   b) Enter name and description of the IQN pool.
   c) Enter the prefix for any IQN blocks created for this pool.

Step 3   In **Suffix Blocks**, complete the following:
   a) Click the **Plus** icon to create one or more blocks of IQN suffixes in the selected pool.
   b) In the **Suffix Block** column, enter the suffix for this block of IQNs.
   c) In the **Start** column, enter the first IQN suffix in the block.
   d) In the **Size** column, enter the total number of IQN suffixes in the block.

Step 4   Click the **Apply** icon.

Step 5   Click **Create**.

What to do next

Include the IQN suffix pool in a service profile or a service profile template.

UUID Suffix Pools

A UUID suffix pool is a collection of SMBIOS UUIDs that are available to be assigned to servers. The first number of digits that constitute the prefix of the UUID are fixed. The remaining digits, the UUID suffix, are variable values. A UUID suffix pool ensures that these variable values are unique for each server associated with a service profile which uses that particular pool to avoid conflicts.

If you use UUID suffix pools in service profiles, you do not have to manually configure the UUID of the server associated with the service profile. Assigning global UUID suffix pools from Cisco UCS Central to service profiles in Cisco UCS Central or Cisco UCS Manager allows them to be shared across Cisco UCS domains.

Creating and Editing a UUID Suffix Pool

After creating a UUID pool you can edit it by selecting the **Edit** icon on the overall summary page of the selected UUID pool. To select a UUID pool, go to **All Pools** page and select the UUID pool that you want to edit. The page redirects you to the overall summary page of the selected UUID pool.

Procedure

Step 1   In the Actions bar, type **Create UUID Pool** and press **Enter**.

This launches the **Create UUID Pool** dialog box.

Step 2   In **Basic**, complete the following:

a)   From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access an UUID pool.

b)   Enter name and description of the pool.

c)   Enter the sufix for any UUID blocks created for this pool.

Step 3   In **Suffix Blocks**, complete the following:

a)   Click the **Create** icon.

b)   In the **Suffix Block** column, enter the suffix for this block of UUIDs.

c)   In the **Start** column, enter the first UUID suffix in the block.

d)   In the **Size** column, enter the total number of UUIDs in the block.

e)   Click the **Apply** icon.

Additional fields related to UUID pools are displayed.

f)   In **UUIDs**, you can view a graphical representation of the number if UUID addresses in the pool, the number of assigned UUID addresses, duplicate UUID addresses, and UUID summary.

g)   In **Access Control**, select the ID range access control policy to apply to this block. If you do not have a policy, you can create one by typing **Create ID Range Access Control Policy** in the task bar.

Step 4   Click **Create**.

What to do next

Include the UUID suffix pool in a service profile or service profile template.