Understanding Policy Differences in Cisco UCS Manager and Cisco UCS Central

Advanced Policy Resolution

Note Watch a video that demonstrates Advanced Policy Resolution.This video is in English.

You can make a global service profile template reference any policy. Policies with the same name can exist in different levels of the organization structure. However, two policies with the same name cannot exist in the same level of the organization structure.

Service profiles always follow policies in their specific organization level first. Then, if that policy name is not contained at that level, the resolution looks upward, all the way to **/root**.

To demonstrate the advanced policy resolution, in the video that accompanies this topic we discuss replicating a SAN-BOOT policy in different organizations, with different policy settings. Then we use a single global service profile template to instantiate resulting global service profiles into those different suborganizations. This allows for the suborganization to acquire the desired boot policy at that level of the suborganization.

Assume that the SAN-BOOT policy resides in `/root` with generic target initiators. No blade server boots to SAN with this boot policy. It's acting as a placeholder. The global service profile template consumes it.

When you edit the service profile template, click **Policies** and choose the **Boot** policy, you can see the details of the newly created SAN-BOOT policy.

In the SAN-BOOT policy, create generic initiators for the possible boot paths of a UCS or Cisco UCS Central SAN-BOOT policy. It consists of two possible VHBAs, one primary and one secondary. Each VHBA also has its own primary and secondary target initiators.

Create an organizational structure that reflects how the blade servers boot to the SAN. For example, you could have half of the global service profiles booting from one storage array controller, and the other half booting from another. This divides the boot load on the storage array.

In the suborganization created for production, we have SA-controller-A and SA-controller-B. We created boot controller SAN-BOOT policies within each of the SA-controller suborganizations. The SAN-BOOT policies contain the valid, true target initiators for booting the storage array, except that they contain different initiators to separate the boot load when all of the global service profiles boot to the storage array.

The SAN-BOOT policy that lives in the SA-controller-A suborganization, contains the following boot target initiator values. The WWPNs end in 11, 22, 33, 44 for the 4 target initiators. The SAN-BOOT policy that lives in the SA-Controller-B suborganization contains the boot target initiator values. The WWPNs end in 55, 66, 77, 88 for the 4 target initiators.

From the single global service profile template (G-SP-SAN-BOOT), consuming the SAN-BOOT policy, use the feature **Create Service Profile from Template** and instantiate those global service profiles to their respective SA-controller suborganizations.

Once the policy is created and associated to a blade in a UCS domain, you can see the global service profile deployment, SAN-BOOT policy, and the initiators that are copied to the domain. The target initiators precisely match those configured in the SAN-BOOT policy in the SA-controller-A and B suborganizations.

When Cisco UCS Central deploys the policies correctly, there is no object name conflict. The two policies with identical names are contained in different suborganization structures.

VLAN and VSAN ID Aliasing

Note Watch a video that demonstrates setting-up VLAN ID Aliasing. This video is in English.

VLAN ID aliasing may assist you in reducing the overall number of global service profile templates to maintain in Cisco UCS Central. Traditionally, when creating local VLANs or VSANs within Cisco UCS Manager, you create a new VLAN or VSAN for every ID in your network or fabric. For example, if you have different VLAN IDs in different subnets, which coincide with the physical locations of those network subnets, then construct those VLANs separately. They require separate vNIC templates, LAN connectivity policies, and service profile templates. An identical scenario is true for VSANs. With Cisco UCS Central and the use of global objects and policies, this process is much more efficient, and decreases the number of global service profiles templates. Whenever there is less infrastructure, management becomes easier.

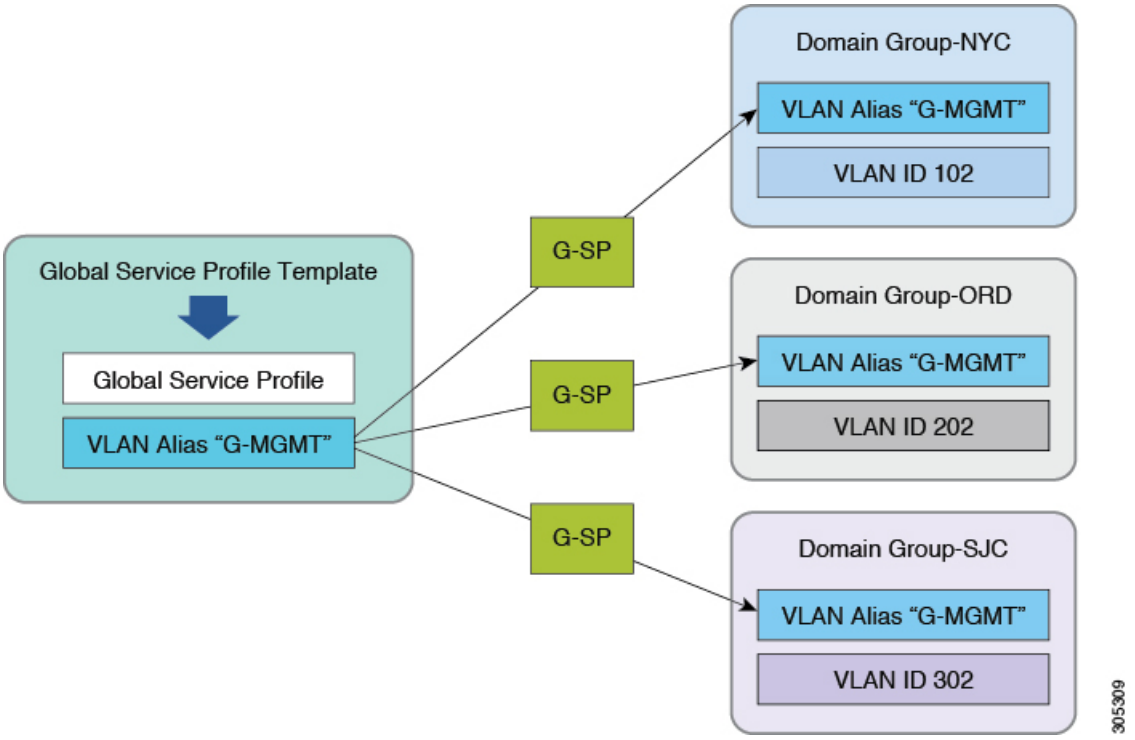
A global service profile is instantiated from its corresponding global service profiles template. When you create a global VLAN in Cisco UCS Central, you must designate its **Domain Group Location**. This designation ties the use of the VLAN or VSAN, and its corresponding ID, to that specific domain group.

You can create VLANS that have identical names but use different VLAN IDs and domain-groups. After creating them, you can see the aliased VLANs in the **All VLANs** tab, and the resulting VLAN IDs associated with the single VLAN.

Once you select the VLAN, you can edit it. You can also go to the **Aliased VLANs** tab and see the corresponding VLAN IDs.

A single global service profile template can provide global service profiles for multiple UCS domains in different domain groups. When you associate the global service profiles with domain groups, then Cisco UCS Central deploys the appropriate VLAN ID with that global service profile.

Figure 1: VLAN and VSAN ID Aliasing: Configuration Example



ID Range Access Control Policy

Note UCS Central ID Access Control Policies. This video is only in English.

You can apply ID-range access control policies to an ID pool. They help manage IP-management-pool IDs in large Cisco UCS Central environments. Management IP addresses for UCS blades and servers, whether in-band, or out-of-band, can be on different IP subnets in UCS domains that are dispersed across the enterprise.

Note ID Range Access Control Policies are designed to direct IDs from certain blocks of IDs within a global ID pool to corresponding UCS Domains in the policy-defined Domain Group. If you choose to use an ID Range Access Control Policy attached to a block of IDs within a given global ID pool, normal ID retention on the Global Service Profile is released. Further, the IDs allocated are not guaranteed to remain unchanged between disassociation and re-association tasks of a Global Service Profile to a blade or server.

Cisco recommends that you refrain from using ID Range Access Control Policies if absolute retention of original ID is required on your Global Service Profiles even after service profile disassociation. However, you can use the policies for Management-KVM IP Addresses, where absolute retention may not always be essential.

ID range access control policies can allow for management IP addresses to adjust when global service profiles are associated with UCS domains. The actual process differs slightly from that for VLAN or VSAN ID aliasing. The policies act as pointers between blocks of management IPs (per subnet) and the domain groups of which the UCS domains are members.

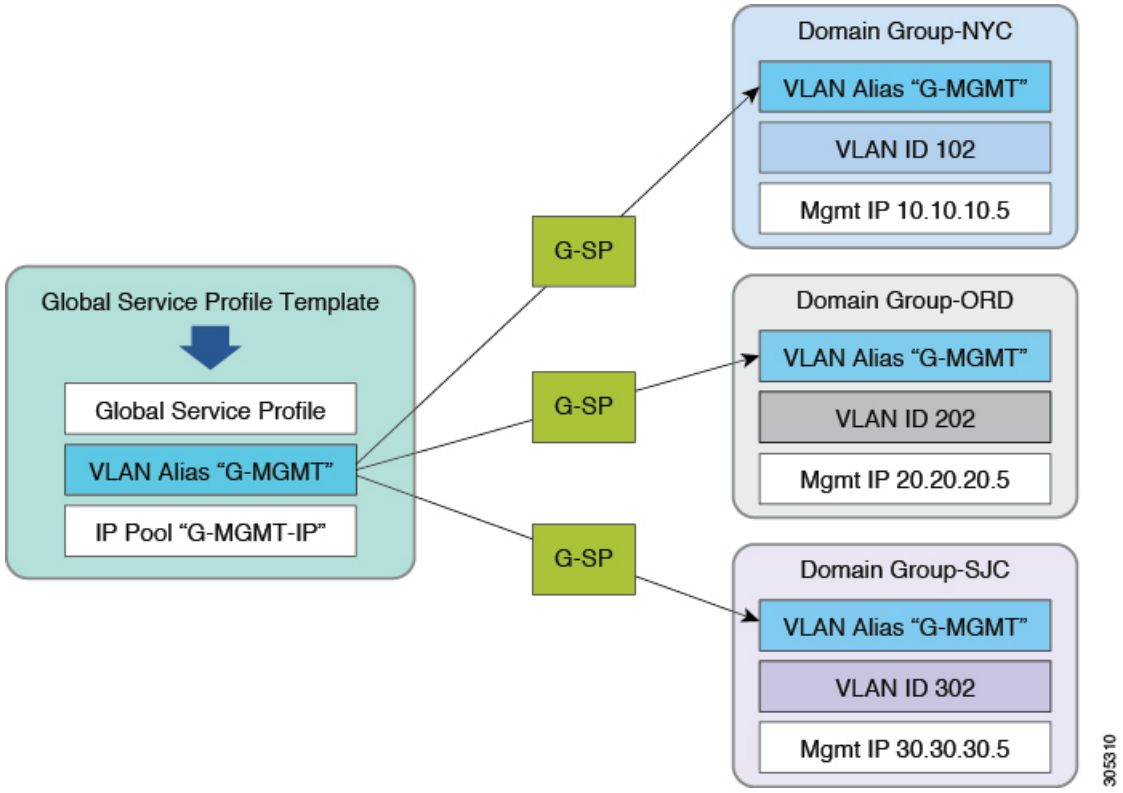
When you create a global IP management pool, use corresponding blocks of management IP addresses that match the management subnets of your different UCS domains. Creating the actual ID-range access control policies is simple, since they coincide with a domain group. Once you create the policies, access them by selecting the correct policy, per the specific block of management addresses in the management IP Pool.

Sequentially, select the appropriate ID-range access control policy for each of the management IP pool subnet blocks. Any global service profile that is using the newly created pool and is associated with a UCS domain, is only issued management IP addresses for that domain group and UCS domain member. If you move that global service profile to another UCS domain, in another domain group, then the policy issues a different management IP for that domain group.

This reduces the number of global service profile templates. Even with multiple UCS sites, UCS domains, VLAN IDs, and management subnets, you can architect all of your global service profiles from a single global service profile template.

Advanced policy resolution, VLAN and VSAN ID aliasing, and ID access control policies can all work collectively to reduce the total number of global service profile templates.

Figure 2: ID Range Access Control Policy: Configuration Example



Brownfield – Accessing Global IDs and Policies with Local Service Profiles

When you register a UCS domain with Cisco UCS Central, you have visibility of all global ID pools and policies from within Cisco UCS Manager. When migrating from a Brownfield to a Greenfield environment, create global policies within Cisco UCS Central. Cisco UCS Manager accesses those policies from Cisco UCS Manager, specifically the local service templates, and local service profiles. You can switch a local service profile from the default host firmware package (local policy) to a global-default (global policy) that exists in Cisco UCS Central.

You can switch any policy and ID from local to global, including local UUID, MAC, IP, WWNN, and WWPN pools. However, sometimes, this is disruptive. If the global policy has the **identical** configuration as the local policy, then there is no disruption to running workloads. If you are switching an ID pool from local to global, then the global pool **must contain** the identical ID format as the local pool. Also, the specific ID must be available to allocate. Anything outside these guidelines causes a disruption (reassociation) of the service profile, or requires a user acknowledgment from a maintenance policy to confirm the disruption.

Note Always test these changes in a lab before deploying them in production. If that is not possible, then choose a single service profile assigned to a blade server that is not running production workloads.

User Acknowledgment Behavior Explained

- Global service profiles with global maintenance policy:
  - Shows pending activities alert in Cisco UCS Manager, **cannot** acknowledge in Cisco UCS Manager.
  - Shows pending activities alert in Cisco UCS Central, can acknowledge in Cisco UCS Central.
- Local service profiles with global maintenance policy:
  - Shows pending activities in Cisco UCS Manager, **cannot** acknowledge in Cisco UCS Manager.
  - Shows in Cisco UCS Central pending activities, must acknowledge in Cisco UCS Central.
- Local service profile with local maintenance policy (UCS domain registered with Cisco UCS Central):
  - Shows pending activities in Cisco UCS Manager, can acknowledge in Cisco UCS Manager.
  - Shows in Cisco UCS Central pending activities, can acknowledge in Cisco UCS Central.

Note If administrators wish to limit the acknowledgment for UCS blade servers to Cisco UCS Central, then all local service profiles must have a global maintenance policy of user-acknowledgment. (Administrators can do this in Brownfield environments with local service profiles that are registered to Cisco UCS Central).

Rule-Based Access Control and UCS Central Custom Views

In Cisco UCS Central, you can create a customized view for what a user can see and manage, as part of Rule Based Access Control (RBAC), unlike in Cisco UCS Manager.

With Cisco UCS Central, use locales to filter what a user can see and manage. The Cisco UCS Central locale is defined not only with organizational permissions, but also with Cisco UCS Central domain group permissions.

For example, create a locale called NYC, with organizational permissions set to `root/Americas/NYC` and domain group permissions of `root/DG-Americas/DG-NYC`.

Once you create the locale, create a user called nyadmin and assign the NYC locale to the account nyadmin.

When you log off and then log in as nyadmin, you see a narrowed view of the organizational structure and the domain group structure.

Unregistering a UCS Domain from UCS Central

In Cisco UCS Manager, you can unregister a UCS domain from Cisco UCS Central at any time. Therefore, you need security for the Cisco UCS Manager administrator account. Cisco strongly advises you to consult with Cisco TAC before unregistering a production UCS domain.

Caution Unregistering a UCS domain, from Cisco UCS Central, immediately transfers ownership to the local Cisco UCS Manager for all of the former global VLANs, VSANs, policies, and service profiles pushed to that domain.

The icons revert from global icons to local icons for the objects. Unregistering a UCS domain does not directly affect any workloads running on UCS blade servers. New localized global objects retain their names as created in Cisco UCS Central.

Cisco's architecture ensures that unregistering will not have operational impact on existing workloads. However, difficulties may arise later if and when you decide to reregister that domain to Cisco UCS Central.

Following are important points to consider:

- If your intent is to never reregister with Cisco UCS Central, then there is no impact to unregistering a UCS domain from Cisco UCS Central. Global objects transform to local objects with absolute object control restored to Cisco UCS Manager.
- If your intent is to reregister, consult Cisco TAC before unregistering a production UCS domain.
- If you unregister, all global objects pushed to the UCS domain transform to local objects. Global default policies, and custom policies, retain their names as local objects. VLANs, VSANs, vHBA templates, vNIC templates, and service profiles also retain their names.
- If you decide to reregister a UCS domain, the local objects with the same name trigger a fault when pushing a global service profile to that domain. The fault is a naming-resource conflict, because a local object and a global object cannot have the same name at the same organizational level. This is a common error for users who have unregistered and then reregistered a UCS domain.

Name Resolution with Pools and Policies

It is important to understand pool and policy name resolution for troubleshooting global service profile association errors. Cisco UCS Manager and Cisco UCS Central place few restrictions on object naming. The lack of naming constraints can lead to ambiguity. When creating managed objects, there is nothing that prevents use of the same object name both locally and globally. When a service profile, VNIC or VHBA reference any policy or pool name, the local Cisco UCS Manager follows a well-defined name resolution process. Cisco UCS Manager gives preference to local names over global names, for both pools and policies. Cisco UCS Manager, when managing local service profiles, gives preference to local objects over global objects in normal policy resolution lookup. Global service profiles can never access or consume a local object within Cisco UCS Manager.

Name Resolution for Locally Managed Objects

Cisco UCS Central follows a hierarchy of rules when resolving names for locally managed objects:

1. Use the object name if found and defined in the local organization.
2. Use the object name if found and defined in higher parent organizations, up through the local organization root.
3. Use the object name if found and defined in the global organization.

4. Use the object name as defined in higher global parent organizations, up through the global organization root.
5. Use the values corresponding to the default object in the local organization, up through the organization root.
6. Use the values corresponding to the global default object in the global organization, up through the organization root.

Name Resolution for Globally Managed Objects

Cisco UCS Central follows a hierarchy of rules when resolving names for globally managed objects:

1. Use the object name if found and defined in the global organization.
2. Use the object name as defined in higher global parent organizations, up through the global organization root.
3. Use the values corresponding to the global default object in the global organization, up through organization root.

Note While local service profiles can reference either local or global pools, policies, or templates, global service profiles can only reference global pools, policies, or templates.

In this case, a reference can be either a direct reference, or an indirect reference through dependency to another policy or template.

Recommended Naming Conventions

Note As a best practice for avoiding ambiguity in Brownfield deployments, do not create or use the same name in both local and global contexts.

To avoid ambiguity, create global policy and pool names with unique prefixes (for example, G-WWPN-A for a global WWPN pool for the A-side fabric WWPN IDs). Another best practice is to always use explicitly defined pools and policies.

Also, do not modify the default and global-default names. If you wish to modify a default policy, create a policy with a new name that best reflects the purpose of the policy. For example, the default maintenance policy is set to require user acknowledgment. An administrator could modify this default policy by creating and using a new custom policy called G-User-Ack.

Class of Object	Local Default object	Global Default object
MAC/WWPN/UUID pools, and most policies	default	global-default
Out-of-band IP addr pool	ext-mgmt	global-ext-mgmt

Class of Object	Local Default object	Global Default object
iSCSI initiator pool	default	global-iscsi-initiator-pool
WWNN IDs	node-default	global-node-default

Greenfield Exceptions

Using the "G-" or "Global-" naming prefix is highly recommended in mixed (local and global) Brownfield environments to avoid naming conflicts. However, for fully globalized Greenfield environments, this convention is not necessary. The primary function of the prefix is to prevent namespace collisions. Assuming that all pools, policies, templates, and objects are initially defined exclusively in Cisco UCS Central, then this prefix practice is unnecessary.

Naming Policies

Cisco UCS Central and Cisco UCS Manager contain many default policies. Some are at the local level within Cisco UCS Manager, while some are at the global level within Cisco UCS Central. It is highly recommended that if you intend to make changes to a default policy, that instead, you make a copy of that policy and change the copy, not the original.

Maintenance Policies

Require user acknowledgment (user-ack) in maintenance policies to avoid unexpected service interruption. Configure it where you need to acknowledge a service disruption using one of the following methods:

- If you want the service interruption locally, then use a local service profile. Point it to either a local or global maintenance policy set for user-acknowledgment. Regardless of whether the maintenance policy is local or global, you can acknowledge at the Cisco UCS Central console.
- If you use a global service profile, then set the user acknowledge within Cisco UCS Central. You can see the pending activity in Cisco UCS Manager, but you can only acknowledge it in Cisco UCS Central.