Medium Cisco UCS Central Environment

Greenfield Environment

In a Greenfield environment, only a Cisco UCS Central administrator can add, modify, or delete objects from UCS Central. Cisco UCS Central maintains read and write ownership of all global objects. When you deploy global service profiles from Cisco UCS Central to a blade server in a UCS domain, a shadow copy of the global service profile deploys to Cisco UCS Manager. In Cisco UCS Manager, objects display with the global icon, indicating that they are global and therefore, controlled by Cisco UCS Central. Global service profile templates do not copy-down to Cisco UCS Manager.

Setting Up Logical Domain Group and Organization Hierarchy in a Greenfield Environment

In a medium-size Greenfield deployment, during the initial setup, you must create and configure the logical domain groups and organization hierarchy correctly. Consider multiple levels of hierarchy to accommodate the different requirements for operational policies among the deployed UCS domains.

In addition to firmware considerations, you may need UCS backups scheduled in different time zones that would most likely have different remote-copy destinations. Also, there may be different user authentication settings based on organization and geographic dispersion.

With the creation of global ID pools for UUID, MAC address, WWNN, WWPN, and management IPs, it is wise to plan for future growth. You can leverage single global pools for each ID type. Then you can add blocks of IDs to their respective pools for scale-out. Typically, it is more efficient for the internal DB to have fewer numbers of overall pools and smaller-size blocks. You can add more blocks of IDs to accomplish the growth and scale.

Configuring MAC Pools

Some clients prefer to segment their MAC pools, rather than using a single pool. If the network administrators must know to which fabric a certain MAC address is assigned, then segmentation is helpful. However, best practices for all UCS deployments recommend FI Ethernet up-linking to a clustered switch technology, either VPC or VSS. The MAC addresses from the two fabrics become meshed as a result.

Configuring WWPNS

Typically, administrators create two separate pools for A fabric and B fabric. They use one of the fields in the WWPN format to define A and B fabrics. This benefits the SAN Administrator by making each ID readily identifiable to the fabric to which the WWPN ID belongs. This is because most SAN fabrics are kept separate within each SAN fabric switch. With the respective fabric identifiers, SAN administrators can quickly tell if they have a crossed-fiber issue with the fabric switches.

Brownfield Environment

In Brownfield environments, if an object is local, that means Cisco UCS Manager owns the object and only a Cisco UCS Manager administrator can add, modify, or delete the object. Effectively, Cisco UCS Manager has read/write control on it.

Converting Brownfield to Greenfield

Medium-sized deployments of UCS managed by Cisco UCS Central are much easier to administer than environments that lack Cisco UCS Central. A medium-sized Brownfield deployment becomes much more manageable when you convert all objects to a global infrastructure.

You can adapt your Brownfield environment to Greenfield as quickly or as slowly as needed. You can initially register your existing UCS domains to Cisco UCS Central, or you can slowly define and build the global infrastructure. You could mirror what exists in the local domains, or make needed changes to policies and pools. There is no urgency to accomplish this conversion. You can also plan and build what makes sense for your organization. Additionally, you can test your setup in a lab with Cisco UCS Central emulator before deploying global infrastructure to UCS domains in production.

You can have duplicate pools, one uniquely defined locally within a UCS domain, and its global counterpart defined within Cisco UCS Central. Cisco UCS Central tracks the status of each ID within all of the local and global pools. While an ID may exist in multiple pool definitions, Cisco UCS Central never issues a duplicate ID to a UCS domain.

Final migration of UCS domains can occur domain by domain. This allows you to gracefully shut down blade servers, remove and delete the local service profiles, and then replace them with the corresponding global service profile. This process is well-defined. You can plan, test and successfully perform conversion with minimal risk.

Domain Group Hierarchy for Medium UCS Central Environments

A medium Cisco UCS Central environment consists of 4-12 registered UCS domains. Scale can be large, with 12 registered domains. The number of global VLANs, VSANs, vNIC, vHBA templates, LAN, SAN connectivity policies, corresponding global service profile templates, and global service profiles is significant. The environment can contain approximately:

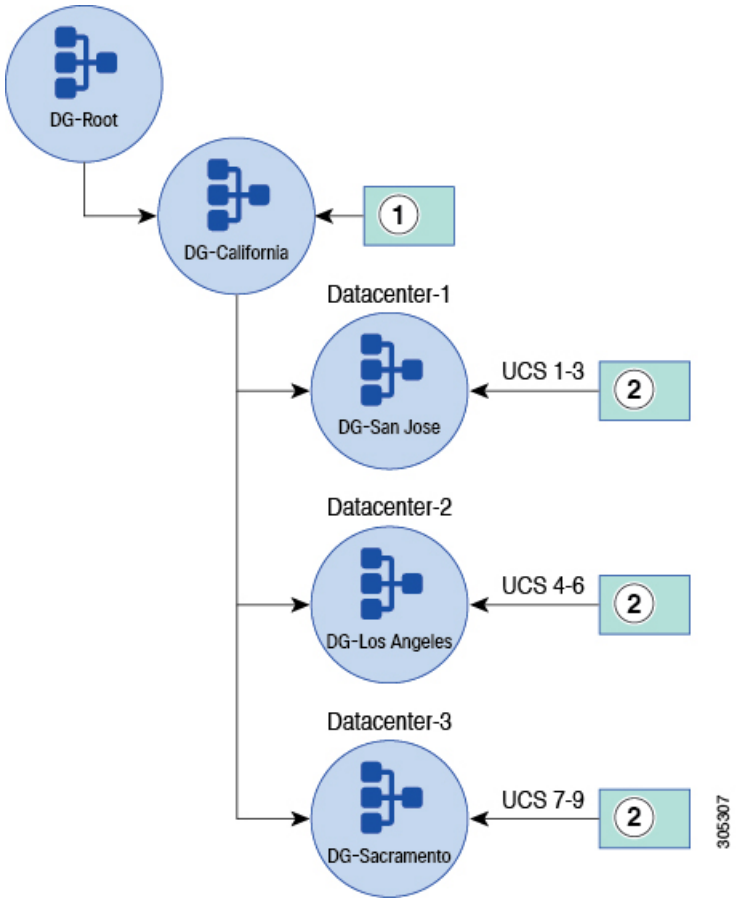
- 768+ servers (12 domains x 8 chassis x 8 blades) with a maximum of (12 domains x 20 chassis x 8 blades)
- 1920 B-series blades
- Multiple manager C-series servers

Consider using a larger domain group hierarchy so as your company grows, you can adapt the environment. With as many as 12 UCS domains, your domains could be in different geographic areas. Therefore, it is best if your domain group structure reflects that. One of the key influences for architecting your Cisco UCS Central domain group structure is the geographic locations of the registered UCS domains. Global operational policies such as time zone, user authentication settings, backups, and firmware work best when you create domain groups based on geography.

For example, if the UCS domains are geographically dispersed, then the remote copy feature should copy those backups to an FTP server located close to the UCS domains. This allows them to potentially leverage those backups, especially in a data recovery (DR) scenario. Therefore, you would not want to perform a DR restoration from an FTP server in New York targeting a pair of FIs in San Jose. With Cisco UCS Central domain group policies, the remote copy FTP server can maintain the proper backups for the UCS domains in close range.

Note Some organizations separate domain groups by business group to support multitenancy.

Figure 1: Medium UCS Central Environment: Configuration Example



1	Global policies could reside here. Cisco UCS Central can push them down to subdomains.
2	Policies such as infrastructure and catalog firmware, backup and export, user management and DNS management could reside here.

VLANs for Medium Environments

When you create Global VLANs in Cisco UCS Central, define the domain group to which a VLAN belongs. The hierarchy can be at the top level (root), or at a lower subdomain group. Attaching a domain group to the global VLAN supports an optional capability called VLAN ID Aliasing. This feature allows you to create multiple global VLANs, which share a common name, with different domain groups and IDs. The global service profile only references the name of the VLAN. The VLAN ID is only set when it is associated with

a UCS Domain, in a specific Domain Group. This process is called sticky-binding. Using VLAN ID Aliasing can potentially decrease the total number of service profile templates required. Consider all aspects and adopt the model and domain group structure that makes the most sense for your operational needs.

The same aliasing concept applies to VSANS. For further details, refer to the section later in this document VLAN/VSAN ID Aliasing.

You can steer certain IDs, from pools, toward certain global service profiles. Use ID Access Control Policies to assign IDs from certain blocks, to a particular UCS domain, within a domain group or subdomain group hierarchy. A use case for this is assigning management IPs to KVMs within global service profiles.

Using VLAN and VSAN ID Aliasing and ID Access Control policies streamlines some of the tasks for managing the infrastructure. These two functions help reduce the overall number of templates you must manage in your infrastructure. However, they provide the uniqueness required to manage different blade servers in different network and fabric segments. Whether your goal is to reduce the number of managed objects, or to achieve better global service profile workload mobility, these functions can be a great asset.

For more information, see ID Range Access Control Policy

Operational Policies for Medium Environments

Domain group hierarchy affects operational policies. In UCS, organizational units affect the multitenancy and access for ID pools, policies, VLANs, VSANs, templates, and service profiles. Organization permissions are optional in locally defined VLANs in Cisco UCS Manager, however, they are mandatory in global VLANs in Cisco UCS Central. You can define root as a single organization permission, effectively giving the entire organization access to a given VLAN. You can also define organization permissions more granularly, for security reasons, such as allowing suborganizations access to only specific VLANs.

Infrastructure and Catalog Firmware for Medium Environments

For infrastructure and catalog firmware updates, typically, you do not construct individual domain groups for UCS domains based on scale.

Note In Cisco UCS Central release 1.5, you update firmware per maintenance group. A maintenance group can contain a group of selected domains, or all of the domains in a domain group.

You can define user-required acknowledgments on a UCS domain that you wish to update. Consider placing this potentially disruptive policy lower in the domain group hierarchy. You can place it in a subdomain group with a few UCS domains registered to minimize the number of user-required acknowledgments on your registered UCS domains.

For each UCS domain, ensure that the operational policy for infrastructure and catalog firmware is set to local within Cisco UCS Manager. When upgrading a maintenance group, join the global policy. This provides for a single user-required acknowledgment on that UCS domain or maintenance group. This is a reasonable and efficient way of addressing global firmware management issues. It leverages the benefits of global management, yet maintains the safety of individual opt-in policies within the registered UCS domains.

Important No global policy applies to a UCS domain unless that UCS domain opts-in to that global policy. The exception is when the UCS domain belongs to a domain group or maintenance group, a configured policy is set, and the policy resolution control is set to **global** within Cisco UCS Manager.

Time Zone Management for Medium Environments

Time zone management is more involved when managing a larger and more geographically dispersed number of registered UCS domains. Place this domain group operational policy as high in the domain group hierarchy as possible. This reduces the amount of time to create and maintain this policy.

An organization that is contained within a single time zone can configure this policy once at the highest levels. An organization that spans several time zones may need to create subdomain group policies that correspond to UCS domains in different time zones.