Small Cisco UCS Central Environment

Small Environments

A small Cisco UCS Central environment consists of 1-3 registered UCS domains. For this environment, consider using a single domain group under the root domain. It can allow for adding domain groups in the future. This can also prevent exposing a single set of operational policies to every registered UCS domain. However, certain policies are best placed at the root level. For example, if your organization has a single LDAP remote authentication configuration, place those LDAP policy configuration settings in the root domain group. This ensures the widest possible adoption.

Note Ensure that you do not unintentionally override the LDAP settings with a subdomain group policy.

Small Greenfield Deployments

If you are implementing Cisco UCS Central for the first time, we strongly recommended leveraging Cisco UCS Central, and creating the entire virtual architecture globally. There are many advantages to administering global objects from a single unified manager:

- Creating and enforcing consistent operational policies
- Achieving maximum global service profile mobility for all registered UCS domains
- Ensuring the best possible implementation with the lowest possible administrative and operational overhead

For example, Cisco UCS Central inventories all global and local pools, and shows if there are any duplicate IDs or conflicts. It also readily identifies the sources of those duplicate IDs.

Small Brownfield Deployments

When you register existing, deployed UCS domains with Cisco UCS Central, Cisco UCS Central presents you with options for architecting and operating. However, you may not have a compelling reason to change the existing local, logical configuration to global objects. You could keep the existing configuration intact, and build anything new as a global configuration. As older localized domains reach end-of-life and are retired, you can replace them with globalized UCS domains.

Conversely, if you need a global configuration, you can build an entire global configuration that mirrors the local configuration. Utilize future maintenance windows to gracefully power-down servers, remove existing local service profiles, and replace them with their global service profile counterparts. Plan for this scenario.

Make sure that you test in a lab before attempting to deploy in production. You can accomplish this by installing Cisco UCS Central in your lab, and then download, install, and register UCS emulators to the lab. This allows you to model the existing production configuration and test the migration process.

Domain Group Structure

For some of the UCS domains registered to UCS, a simple domain group structure is more than sufficient. The best way to analyze this is to look in **Cisco UCS Manager** > **Admin Tab** > **Communication Management** > **UCS Central** > **FSM** > **Policy Resolution Control**. The displayed policies (local or global) are those operational policies that are defined in a Cisco UCS Central domain group, or subdomain group. As you survey the list, you can analyze and determine the best method for constructing your domain groups for your overall architecture. Every operational policy in the list is a policy that is set at the domain group level, or sublevel, within Cisco UCS Central. Therefore, you can control these policies globally, and create a valid hierarchy from root to discreet subdomain groups.

Infrastructure and Catalog Firmware for Small Environments

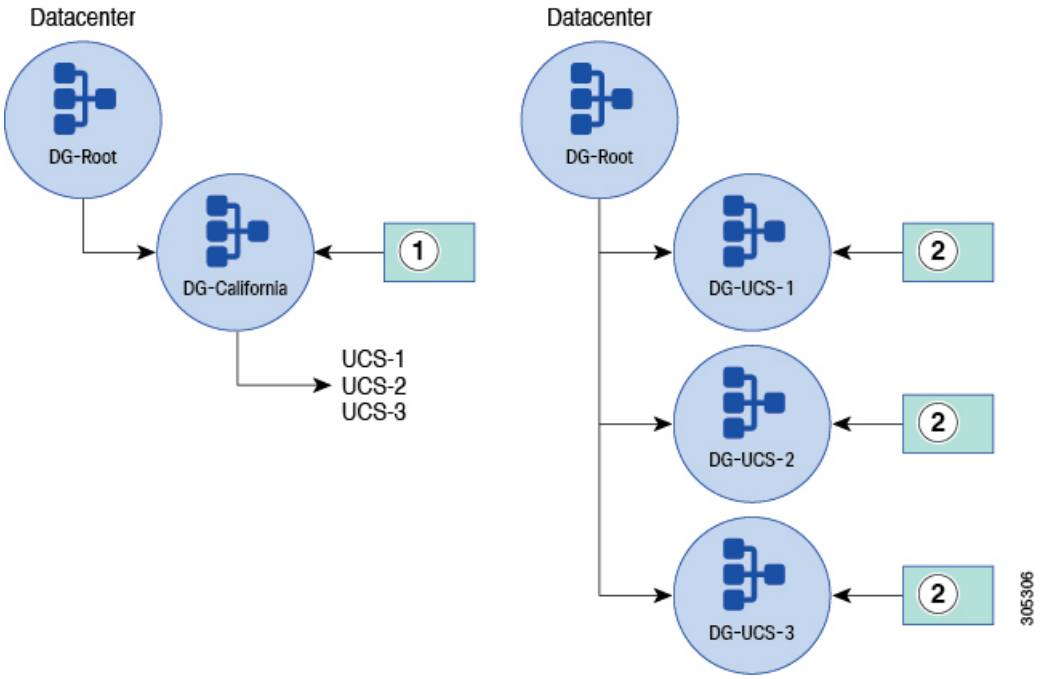
Infrastructure and catalog firmware updates can affect your domain group hierarchy. If you choose global control, and someone modifies it, then it generates a user acknowledgment on all of the UCS domains (Fabric Interconnects) registered to that domain group. This prompts the update of those UCS domains. While this is not disruptive, many users do not wish to acknowledge actions on a UCS domain unless they are immediately ready to update. They also do not want to see it on more than a single UCS domain at a time. Therefore, exercise discretion and consider the following:

- Place each UCS domain into its own maintenance group to segment it.
- Define the domain group policy at the lowest-level, so that only a single UCS domain is pending for acknowledgment or update.

Another option is to define the operational policy as local within Cisco UCS Manager, and then change each domain to global when upgrading. This method leverages the benefits of Cisco UCS Central firmware download

and control, but only affects a single UCS domain at a time. Also, you can configure all remaining operational policies singularly and higher in the hierarchy. This reduces the number of policies that you have to manage.

Figure 1: Infrastructure & Catalog Firmware: Configuration Example



1	Datacenter. Global policies reside here
2	Infrastructure and Catalog Firmware. Global policies could also reside here

Time Zone Management for Small Environments

We recommend that you include this policy in Cisco UCS Central during registration. Place this policy high up in the domain group hierarchy, especially if the UCS domains are in the same time zone. Some clients point to the same NTP server source, but need different time zones configured for the respective UCS domains. In this case, you can use separate domain groups, or subdomain groups, to account for the changes. Regardless, allow Cisco UCS Central to define the proper time zone and NTP server settings to ensure consistency and accuracy for time and time zone in your architecture.

Communication Services for Small Environments

It is ideal to manage the following communication services with global policy management:

- Communication services (for example, SNMP configuration)
- Global fault policy

- User management (for example, LDAP configuration)
- DNS management
- Monitoring (for example, Call Home and Syslog Configuration)
- SEL policy
- Power allocation policy (for example, manual blade or chassis cap)
- Power policy (for example, N+1, or grid)

Global management allows you to set the policy correctly once in Cisco UCS Central. Then all of your registered UCS domains adopt that policy.

Note Cisco UCS Central manages the configuration of policies such as SNMP. The UCS domain sends the SNMP traps directly from the resource manager directly to the configured trap manager or destination.

Backup and Export Policies for Small Environments

Cisco UCS Central helps in scheduling and maintaining proper backups for registered UCS domains. Administrators can create custom schedules so that UCS domain backups occur at a convenient date and time. This affords greater flexibility over what is natively available within Cisco UCS Manager.

Another distinction of backups managed by Cisco UCS Central is that you can use the Remote Copy offline feature. This ensures the safety of backup files by copying them from the local server and storing them on a remote server. The best practice is to create daily backups for each UCS domain.

Configure Cisco UCS Central to back up a UCS domain, and store those backup files in the remote database. You can define the number of backup files to keep (typically 3-5 copies), before subsequent backups overwrite them. This allows a mechanism to limit the amount of space used within the Cisco UCS Central database and disk, and prevents uncontrolled growth.

Global Equipment Policies

Global equipment policy is a new feature that enables Cisco UCS Central to control the following:

- Chassis discovery policy
- Rack management action
- MAC address table aging time
- VLAN port optimization
- Firmware auto sync server state