Cisco UCS Central Operations Guide

First Published: June 10, 2016

Last Modified:

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number:

CONTENTS

Preface

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.

Text Type	Indication
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

Follow Cisco UCS Docs on Twitter to receive document update notifications.

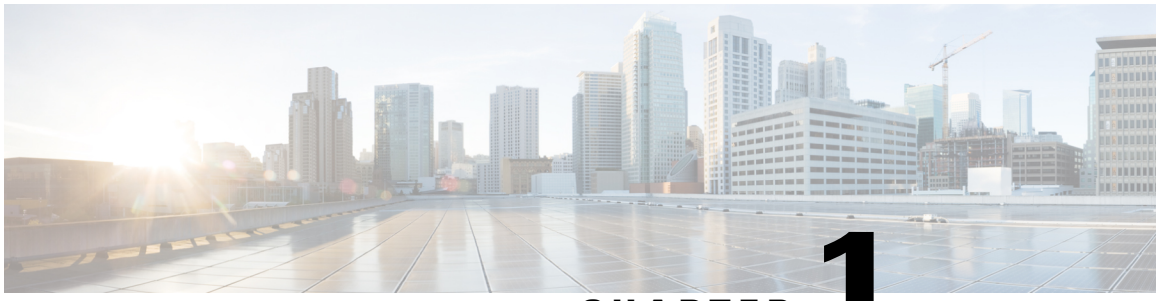
Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@cisco.com. We appreciate your feedback.

Preparing for TAC

For any problems requiring a support case with Cisco TAC, be prepared to supply the output from `show tech-support`.

To generate a tech support file from the GUI, click the **System Tools** icon and choose **Tech Support**. Select the domain and click **Generate Tech Support**. After creates the report, click **Download** to download it to your local system.



CHAPTER 1

Introduction

Introduction

Cisco UCS Central simplifies Cisco UCS management. From a single Cisco UCS domain to multiple Cisco UCS domains, Cisco UCS Central delivers standardization, aggregation, global policy enforcement, and global ID consistency.

While Cisco UCS Manager provides policy-driven management for a single Cisco UCS domain, Cisco UCS Central manages and monitors domain activity globally. These capabilities extend across multiple Cisco UCS Manager domains worldwide, providing an even greater degree of administrative power, operational efficiency, and policy-driven automation.

Cisco UCS Central supports scaling to and managing of 10,000 servers. This represents approximately 70 to125 Cisco UCS Manager domains, depending on domain size. Cisco tested Cisco UCS Central rigorously with more than 200 Cisco UCS domains and more than 6000 service profiles.

The setup architecture of UCS Central is flexible. It allows you to manage your registered UCS domain, and the number and geographic dispersion of those domains. Some principles apply throughout the different architectures, while others are more pertinent for a specific size.

It is important to plan for growth and envision the eventual size and scope of a UCS deployment when implementing Cisco UCS Central. An organization could start with a few UCS domains, but then dramatically scale over a period of 1-3 years. Even if you do not expect significant growth, it is always best to build and plan for future management.

Also, consider whether the environment is Brownfield or Greenfield.

Brownfield

A Brownfield environment is one in which Cisco UCS Central contains UCS domains that were previously built-out and deployed through Cisco UCS Manager. They contain localized objects such as pools, policies, VLANs, VSANs, templates, and service profiles for each UCS domain. In Brownfield environments, if an object is local, that means that the Cisco UCS Manager owns the object, so only a Cisco UCS Manager administrator can add, modify, or delete the object.

Greenfield

A Greenfield environment is one in which Cisco UCS Central only contains objects that were created through Cisco UCS Central. Therefore, these objects are global in scope. Only a Cisco UCS Central Administrator can add, modify, or delete these objects from Cisco UCS Central. A Cisco UCS Manager Administrator cannot change them. 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, in the Server, LAN, and SAN tabs, the global policies, VLANs, VSANs, vNIC/vHBA templates, and global service profiles display with the global icon. This indicates that they are global and therefore, controlled by Cisco UCS Central. Global service profile templates do not copy-down to Cisco UCS Manager.

Cisco UCS Central Use Cases

Cisco UCS Central has many use cases that justify its implementation in all sizes of UCS environments. Before Cisco UCS Central existed, deploying UCS domains was largely repetitive, manual, and time consuming. It required strict attention to the creation and consistency of ID pools, policies, VLANs, VSANs, templates and service profiles.

It is easy to misconfigure an ID pool. For example, you could configure a MAC address pool with the exact scheme of another existing UCS domain in the same environment. This results in MAC address conflicts. Cisco UCS Central inventories the entire registered UCS environment and eliminates such conflicts.

Scope

In this guide, we discuss different architecture considerations for different-size clients.

We categorized environments based on average sizes of the existing UCS Central client base. We also considered some of the largest UCS Central environments, those exceeding 300 registered domains, and more than 6,000 managed servers. The current version of UCS Central has been tested to support environments containing up to 10,000 registered servers.

In this guide, we are defining the following size ranges:

- Small environment: 1-3 registered UCS domains
- Medium environment: 4-12 registered UCS domains
- Large environment: >12 registered UCS domains

Terminology

Term	Description
Cisco UCS Manager	Embedded ASIC software within the Cisco UCS fabric interconnect that manages a Cisco UCS domain .
Cisco UCS domain	A collection of resources that includes a pair of fabric interconnects with connected systems such as: • 1–20 B-Series chassis • C-Series servers • UCS Mini • UCSM domains
Cisco UCS Central	Virtual appliance that aggregates and simplifies the management of one or more Cisco UCS domain (s).
Domain Group	Named grouping of multiple Cisco UCS domains, based on configuration similarities and often based on geography. In a domain group, Cisco UCS Central applies operational and server policies, VLANs and VSANs, for domain group identification. The domain group construct only exists, and is only applied, within Cisco UCS Central. There is no concept of a domain group within a UCS domain.
Subdomain Group	A child of the domain group. Inherits its properties from the parent. Can have unique policies for the domains in the subdomain group. Domain group hierarchy supports up to five nested levels.
Ungrouped domain(s)	Domains that do not belong to any domain group. Upon Cisco UCS domain registration, no operational policies are inherited until a Cisco UCS domain is placed within a domain group.
Local	Reference to an object that is owned and modifiable in a single Cisco UCS Manager domain; for example, local policies or local pools.
Global	A reference to an object that is owned and modifiable in Cisco UCS Central; for example, global service profiles, global policies, and global pools.
Localize	Create a local copy of a global object, which is modifiable from a local domain, and read-only in Cisco UCS Central.
Globalize	Change a pool or policy reference from local to global. For example, use a global action in Cisco UCS Manager to create a reference to a global object. If the global object does not exist, then the reference is not satisfied. Create a global object to satisfy the reference. If no global object exists, the reference remains in a pending global state.

Term	Description
Register	Initial process through which a Cisco UCS Manager domain connects to Cisco UCS Central and sets up management of itself from Cisco UCS Central.
Unregister	Intentional removal of a Cisco UCS domain from Cisco UCS Central management. This is not recommended unless the unregistration is permanent.
Lost Visibility	Unintentional loss of connectivity between Cisco UCS Manager and Cisco UCS Central.
Suspend State	Intentionally halts management communications between Cisco UCS Central and Cisco UCS Manager. Cisco UCS Manager is registered with Cisco UCS Central, but there is no management communication between the two. This is a safety mechanism to prevent unintended changes. Typically initiated by a Cisco UCS domain, due to an unexpected state. For example, if Cisco UCS Central was restored to an older version, and the Cisco UCS domain received an older version of a policy during regular policy resolution.
Acknowledge State	Normal state between Cisco UCS Central and Cisco UCS Manager. Management communications are re-established between Cisco UCS Central and Cisco UCS Manager. Acknowledgement occurs within Cisco UCS Manager in the Admin-Cisco UCS Central registration pane.

Domains, Pods, Clusters, or Blocks

For Cisco UCS fabric interconnects, managing 1 to 20 chassis, avoid using the terms pods, clusters, or blocks, in favor of domains. Past usage of certain terminology in a single Cisco UCS Manager context may need revisiting in the truly global context of Cisco UCS Central. For example, prior to Cisco UCS Manager 2.1, VLANs were referred to as global in scope, within a single UCS domain. This also referred to a VLAN created and used in both fabrics, A and B. Understanding common names, terms, and context is essential.

Ownership

Typically, we use the terms local and global in relation to Cisco UCS managed objects (MOs), such as pool, policies, service profile, adapters, blades, and chassis. Managed objects are owned either locally (by a specific Cisco UCS domain) or globally (by Cisco UCS Central). An object that is owned locally has read-write access in the local domain, but read-only access in Cisco UCS Central.

Correspondingly, an object that is owned globally has read-write access in Cisco UCS Central, but read-only access in any local domain. While Cisco UCS Central does own a global object, it does not directly modify a local copy (at the domain level). Instead, Cisco UCS Central updates the global object in Cisco UCS Central and then issues an update event to the XML-API to update the local shadow copy of that global object.

Best Practice Terminology

The term “Best Practices” is intended more to define guidelines, recommendations and suggestions, rather than specifying the only way to perform desired functions. The only valid Best Practice is whatever works

best for your organization and operating requirements, factoring in the appropriate context and any exceptional conditions.

Flexibility, adaptability, and consistency are all hallmarks of Cisco UCS Manager, and carry forward as architectural goals for Cisco UCS Central. The Cisco UCS Central management model's impact differs significantly from the standalone, local management model. Administrative power is strongly concentrated within Cisco UCS Central, and the scope of change can be broad. Unexpected service interruptions could be a consequence of not following recommended practices. Administrators are strongly advised to:

- Model and test as much as possible, in advance of production deployment. Use a test environment with a Cisco UCS Central instance and registered Cisco UCS emulators.
- Be conservative with global configuration changes that may impact local services.
- Run **Estimate Impact** on actions to ensure that potential impacts are understood. The personalization settings allow you to set the estimate impact to run on most applicable actions.
- Use maintenance polices for service profiles, and service profile templates set to USER-ACK.

Cisco UCS Central is integrated with and leverages Cisco UCS Manager to carry out its actions. Cisco UCS Central is designed to centralize policy definition and to create pools of global identifiers that multiple Cisco UCS domains can consume in a consistent manner.

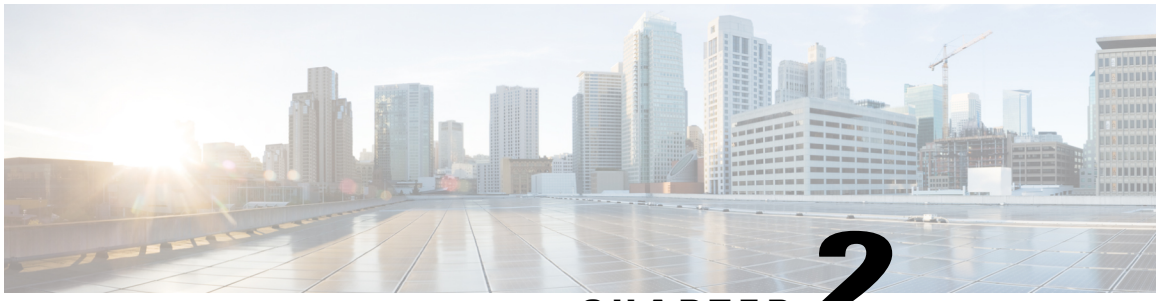
Even as Cisco UCS Central increases its functionality and adds features, Cisco UCS Manager continues to be the interface for direct management of the Cisco UCS domain, as well as the vehicle for enforcing consistency of global policies.

Cisco UCS Central User Documentation Reference

Beginning with release 1.4, the Cisco UCS Central User Guide has been divided into several use case-based documents. You can use the appropriate guide to understand and configure Cisco UCS Central.

Guide	Description
Cisco UCS Central Getting Started Guide	Provides a brief introduction to the Cisco UCS infrastructure, Cisco UCS Manager, and Cisco UCS Central. Includes an overview of the HTML5 UI, how to register Cisco UCS domains in Cisco UCS Central, and how to activate licenses.
Cisco UCS Central Administration Guide	Provides information on administrative tasks, such as user management, communication, firmware management, backup management, and Smart Call Home.
Cisco UCS Central Authentication Guide	Provides information on authentication tasks, such as passwords, users and roles, RBAC, TACACS+, RADIUS, LDAP, and SNMP.
Cisco UCS Central Server Management Guide	Provides information on server management, such as equipment policies, physical inventory, service profiles and templates, server pools, server boot, and server policies.

Guide	Description
Cisco UCS Central Storage Management Guide	Provides information on storage management, such as ports and port channels, VSAN and vHBA management, storage pools, storage policies, storage profiles, disk groups, and disk group configuration.
Cisco UCS Central Network Management Guide	Provides information on network management, such as ports and port channels, VLAN and vNIC management, network pools, and network policies.



CHAPTER 2

UCS Central Implementation: Approaches and Challenges

Implementation Overview

Cisco intends for Cisco UCS Central to be the focal point of Cisco UCS management. For data centers with existing Cisco UCS domains, implementing minimizes challenges to future growth and management.

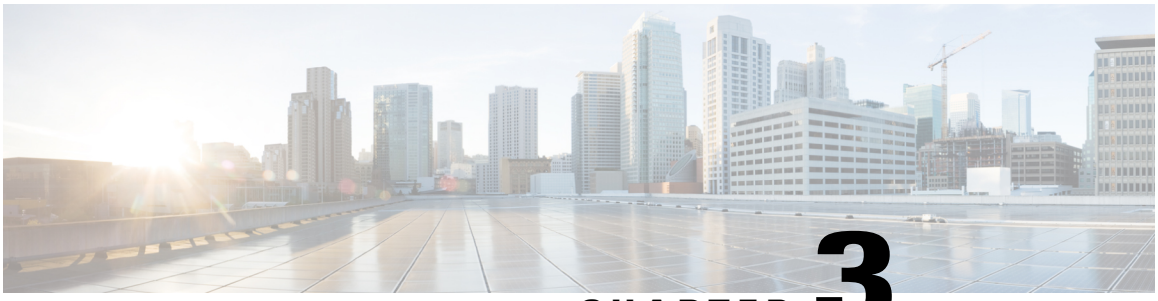
While Cisco UCS Central has a great deal in common with Cisco UCS Manager, you should take the time to become familiar with its unique features.

New Cisco UCS Deployments

For new deployments of Cisco UCS domains, the best practice is to adopt Cisco UCS Central from the start, especially for new workloads, and to reference global pools, policies and templates.

For installations with no previous Cisco UCS footprint, Cisco urges the exclusive use of Cisco UCS Central, avoiding instances of locally managed objects. Global service profiles that refer exclusively to global pools and policies help to ensure global consistency.

Initially using Cisco UCS Central can greatly simplify and enhance the Cisco UCS management experience. Environments that do not initially use Cisco UCS Central are deploying a Brownfield environment. Retrofitting a Brownfield environment to Cisco UCS Central is challenging. However, a well-planned migration to Cisco UCS Central is achievable. Even in a mixed Brownfield-Greenfield environment, there is tremendous value in registering all UCS domains to Cisco UCS Central.



CHAPTER 3

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

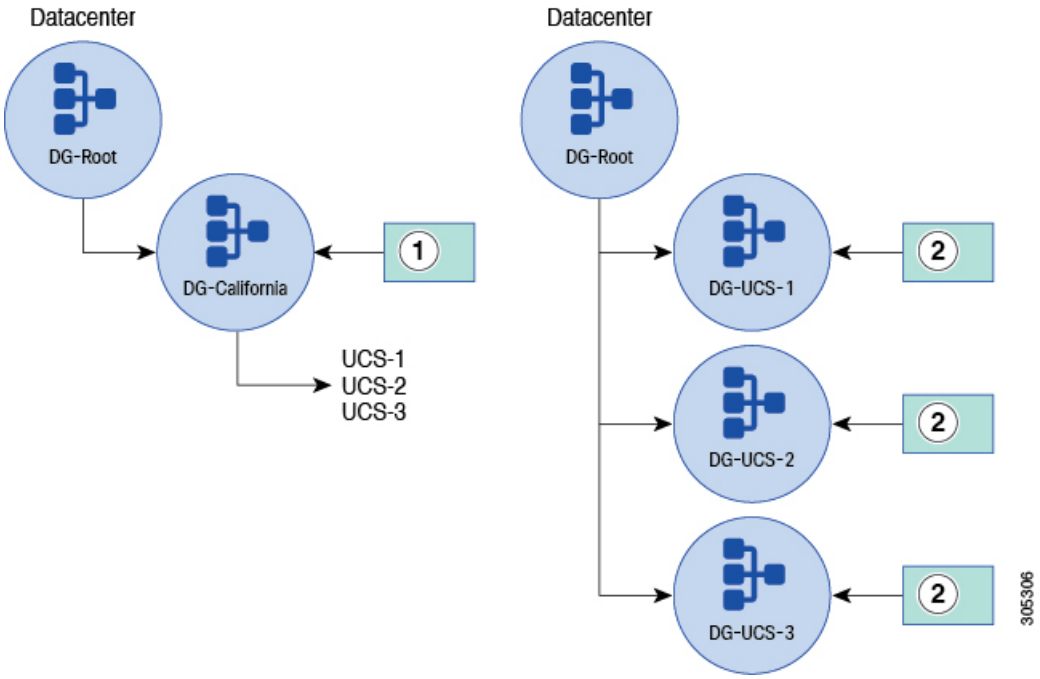
Infrastructure and catalog firmware can affect your domain group hierarchy. If you choose global control, and someone modifies it, then it generates a user acknowledgement on all of the UCS domains (FIs) registered to that domain group. This prompts the upgrade of those UCS domains. While this is not disruptive, many users do not wish to acknowledge actions on a UCS domain unless they are immediately ready to upgrade. 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 subdomain group to segment it.
- Define the domain group policy at the lowest-level subdomain group, so that only a single UCS domain is pending for acknowledgment or upgrade.

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.

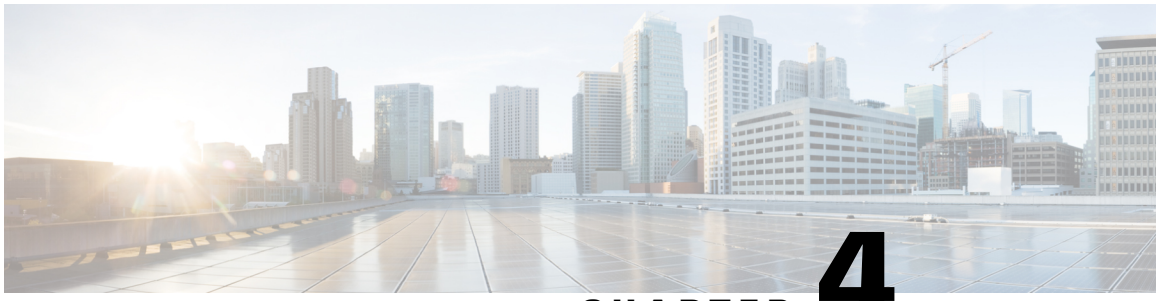
Another distinction of backups managed by Cisco UCS Central is that you can use the Remote Copy offline feature. This ensures the safety of backup files by copying them from the local server and storing them on a remote server. The best practice is to create daily backups for each UCS domain.

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



CHAPTER 4

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:

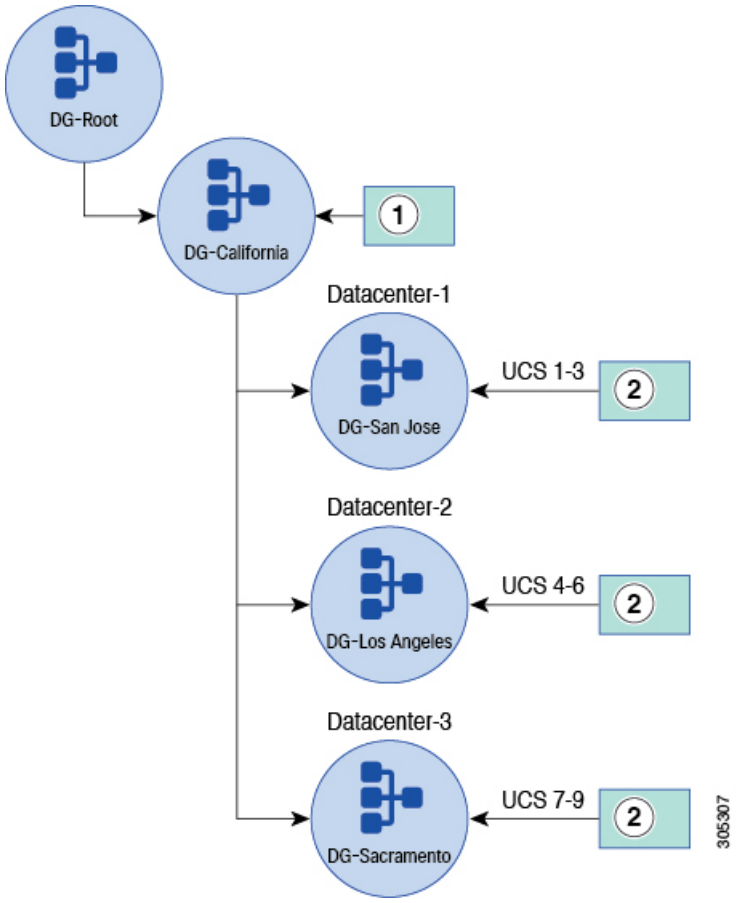
- 768+ servers (12 domains x 8 chassis x 8 blades) with a maximum of (12 domains x 20 chassis x 8 blades)
- 1920 B-series blades
- Multiple manager C-series servers

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 2: 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 and 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, 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, not domain group. A maintenance group contains selected domains.

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.

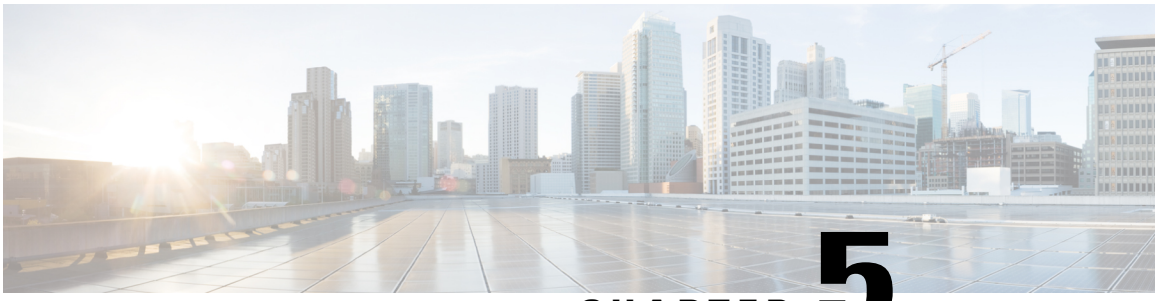
For each UCS domain, ensure that the operational policy for infrastructure and catalog firmware is set to local within Cisco UCS Manager. When upgrading a maintenance group, join the global policy. This provides for a single user-required acknowledgment on that UCS domain or maintenance group. This is 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.



CHAPTER 5

Large Cisco UCS Central Environment

Advantages of UCS Central for a Large Environment

Large deployments of UCS need Cisco UCS Central. Cisco has over 300 registered UCS domains, with 6,000-plus servers. Internal analysis by Cisco IT shows that they save about 1-person/yr in operations equipment workload by leveraging Cisco UCS Central. Cisco manages every UCS domain with Cisco UCS Central.

Cisco tested the latest release of Cisco UCS Central to support up to 10,000 servers in a single instance. This type of scaling drove the complete redesign of the HTML-5 user interface (UI). The HTML-5 UI is much more suited to managing UCS domains and servers when scaling. The older Flash-based UI suffered from performance issues when used in large environments.

With larger deployments, leveraging an efficient domain group hierarchy is critical. A large environment can contain UCS domains dispersed all around a country, or around the world. A domain group might encompass different time zones, DNS servers, user authentications, domain controllers, and remote FTP servers. An efficient domain group hierarchy permits a more granular approach to firmware upgrades and management.

Trying to separately manage the backup-job schedules for dozens of UCS domains is tedious and prone to error. This task is simplified with Cisco UCS Central. You can define custom schedules for backup (`fullstate.bin`), configuration export (`allconfig.xml`), and specific remote-copy FTP servers to ensure proper safeguarding of those backups.

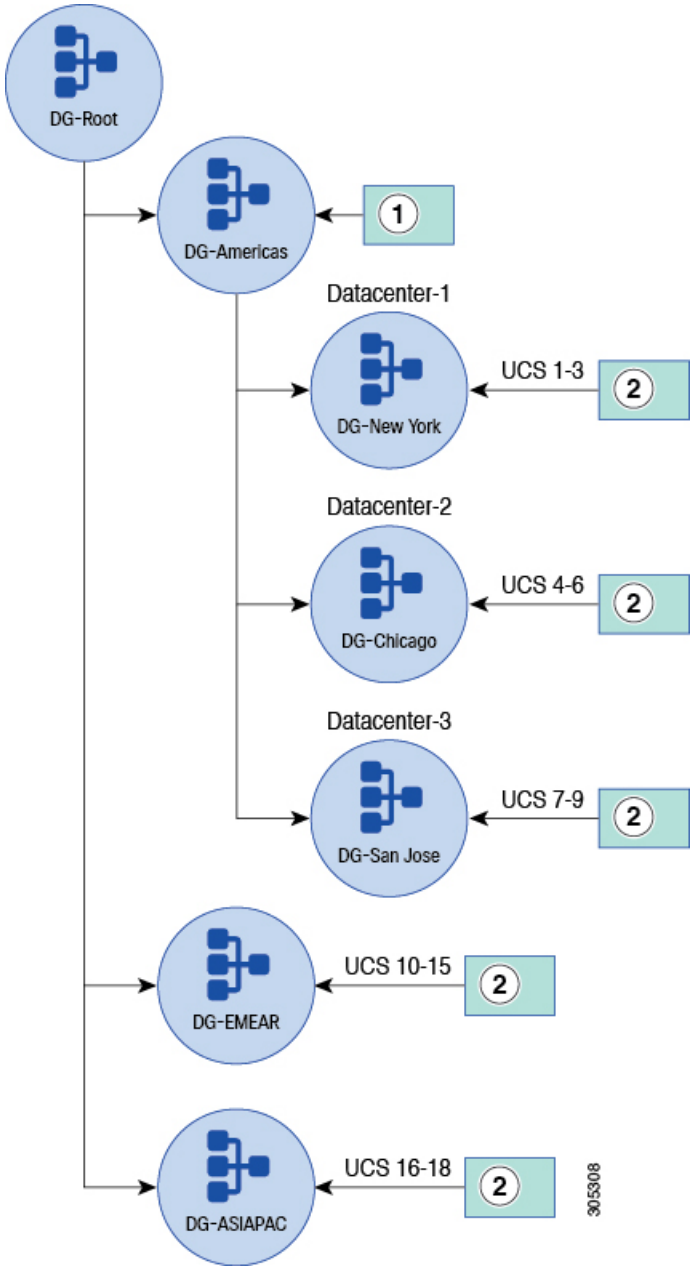
When using LDAP integration for UCS domains with internal LDAP servers, replicating those granular settings is also tedious and prone to error. Cisco UCS Central makes this task much easier. It sets LDAP configurations as part of the domain group hierarchical policy. You can define the policy as broadly, or as granularly, as required.

Note Cisco UCS Central treats the LDAP Policy as a single policy. You cannot break apart different components of the policy, such as defining the group mappings at one level in the hierarchy, and LDAP providers at a lower level.

You can place policies as high up in the domain group hierarchy as applicable for the UCS domain groups registered in your geographic domain group. You can also place infrastructure and catalog firmware more granularly, lower in the subdomain group structure.

Ultimately, what works best for you and your organization will be the best practice. You can always opt for the simple approach and change or expand your subdomain group structure. It is easier to change a domain group structure than to change an organization structure. Changes to organization structure tend to be changes that result in disruption of the environment.

Figure 3: Large 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, DNS management, time zone, and SEL could reside here.

Greenfield Environments in a Large Environment

For large, planned Greenfield deployments, we recommend initially adopting Cisco UCS Central, and designing your global policy and object infrastructure correctly from the beginning. Creating everything globally within Cisco UCS Central saves time and money, and makes scaling much easier. It also saves time when managing daily operations.

Cisco UCS Central closes the gap that has existed between Cisco UCS Central and Cisco UCS Manager in the initial setup of a UCS domain. Cisco UCS Central now includes the ability to define equipment policies, unified port configurations, port roles, and port-channel configurations.

In addition to planning domain group hierarchy, consider the organizational hierarchy before deploying the final architecture. This includes planning for global ID pools, policies, VLANs, VSANs, templates, and service profiles. The ability to intelligently create organizational boundaries benefits multitenancy and potentially decreases the number of global service profile templates needed for the environment.

Other advanced features, such as VLAN and VSAN aliasing, and ID-range access control policies, also support decreasing the number of global service profile templates to manage. You can manage as much, or as little as you wish, but simplifying management always reduces operating costs.

Brownfield Environments in a Large Environment

A large architecture of Cisco UCS Manager and Cisco UCS Central might contain hundreds or thousands of service profiles. Therefore, moving to UCS Central requires careful planning and calculation. Pay attention if moving the object repository to Cisco UCS Central and converting local service profiles to global service profiles. Build the global infrastructure to mirror the local infrastructure in all of your UCS domains.

Remember that converting a local service profile to a global service profile is disruptive. However, the convenience of managing everything globally from a single interface, and gaining workload mobility among multiple UCS domains, outweighs the negatives.

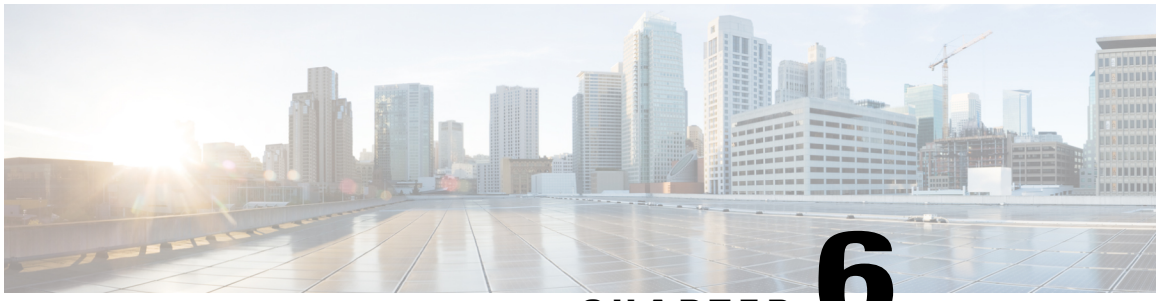
Some large Brownfield clients have opted to move the object repository, and convert the local service profiles slowly, over time. This takes advantage of future maintenance windows to sequentially migrate to Cisco UCS Central. Upgrading host firmware, controller firmware, BIOS, network adapters, CIMC, and storage controllers are all disruptive actions. The hosts require maintenance windows to gracefully shut down and register the service profile to the blade server performing the upgrades. During this time, you can replace the existing local service profile with a new global service profiles.

Other Brownfield clients have adopted a model of operating Brownfield and Greenfield environments in parallel. This means that existing UCS infrastructure remains as Brownfield. It is locally managed within the respective Cisco UCS Manager domains, while anything new in the environment is deployed as global objects from Cisco UCS Central.

As your network evolves, and local infrastructure reaches end-of-life, convert more of the environment to global. Even if you keep local service profiles, use global service profiles by switching from local to global within the service profile or template. This decreases the number of policies and provides management from

one place within Cisco UCS Central. See Brownfield – Accessing Global IDs and Policies with Local Service Profiles

Automation with Powertools and scripts with the XML-API can greatly facilitate the conversion process. See Migrating Brownfield Local Service Profiles to Global Service Profiles in Cisco UCS Central



CHAPTER 6

Sizing and Scaling Considerations

Sizing Considerations

Some Cisco UCS Central customers have scaled their UCS environments from dozens to hundreds of domains and from hundreds to thousands of servers. The scaling metric to determine your needs is not the number of registered UCS domains, but rather the number of blades and servers. Cisco UCS Central has been tested to support up to 10,000 servers. There is no software limit.

If you have a large environment, analyze the performance of the Cisco UCS Central virtual machines (VMs) to determine if you need to increase the CPU and memory resources.

The *Cisco UCS Central Installation Guide* defines the minimum requirements for running Cisco UCS Central. The deployment of the OVA file:

- Creates 2 x 40-GB disks
- Allocates 4 x vCPUs
- Allocates 12-GB RAM

For small to medium-size environments, those settings provides sufficient performance. However, for large environments we recommend increasing those resources by a factor of two. (Cisco IT runs at least 4 vCPUs and 24-GB RAM for their instance of Cisco UCS Central, which exceeds 200 UCS domains and 6,000 servers.)

The best practice is to:

1. Monitor the performance metrics of your Cisco UCS Central VM in your new or growing infrastructure.
2. Adjust CPU and RAM resources accordingly.
3. Verify vCPU and memory usage if performance is noticeably inadequate.
4. Make needed changes with your virtualization administrator.

Scaling Global Service Profiles and Global Service Profile Templates

There is no limit to the number of global service profiles that you can attach to a global service template.

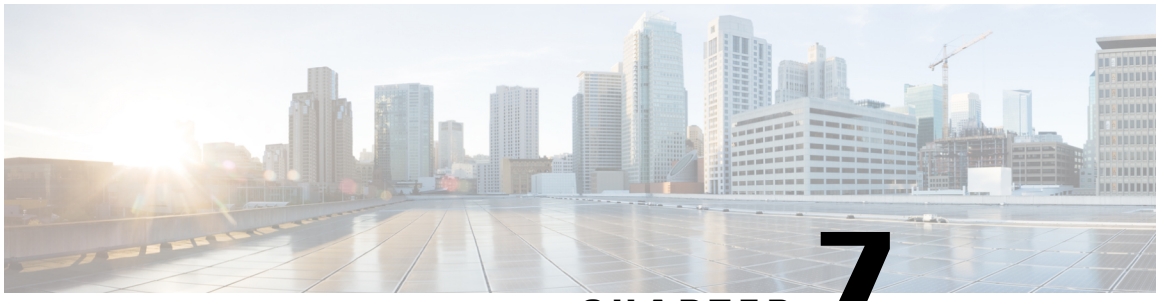
Leveraging templates to make widespread changes is beneficial for simplified management, but it is not best for all environments. Consider the ramifications of a single disruptive change to the environment. Determine how many resources you can safely attach to an updating global service profile template. One mistake could cause a significant outage. Consider reducing the potential for damage. For example, you could decide that a ratio of 100 global service profiles attached to each service profile template is the maximum limit.

Another important consideration is the number of policies. For example, if you have ten global service profile templates, with 100 global service profiles attached, that represents 1,000 blades or servers. If you had all ten templates accessing the same disruptive policies, you could have a single policy that could potentially disrupt 1,000 blades or servers. To reduce the possibilities for failure, it is best to scale across multiple service profile templates, and multiple policies. It is acceptable to have more than one policy that contains the same settings, but is used by different templates.

If you have too many global service profiles attached to too few templates, you can clone the global service profile template. Then unbind some of the profiles from the original template and bind them to the clone. The system is flexible in design and operations. You can balance and scale accordingly.

Note We recommend testing this scenario before deploying it in a production environment.

Although this guide discusses reducing the number of global service profile templates for ease of management, do not attach too many global service profiles to a template. Also, do not use a single policy for too many global service profiletemplates and profiles. This sounds contradictory; however, consider balancing reduction of templates for improved OPEX, with the widespread damage that could be caused by having too many service profiles accessing a template, or policy.



CHAPTER 7

Domain Groups

Domain Group Design

Domain group hierarchy design is one of your more important architectural design decisions. There is no right or wrong method. The goal is to best reflect your specific environment and management design requirements. You must understand the following attributes of domain groups:

- A domain group is an arbitrary grouping of individual Cisco UCS domains. The Cisco UCS Central administrator designs the grouping. A domain group is purely a Cisco UCS Central global construct. A domain is not aware that it is a member of a domain group.
- A Cisco UCS domain can only reside in one domain group at a time, unlike server pools, where one server can reside in multiple server pools.
- Cisco UCS Central places all domains in the **ungrouped** domain group at registration. Domains in the ungrouped domain group **do not** resolve to any global operational policies, even if the local Cisco UCS administrator has opted-in for global policy resolution control.
- Operational policies in effect for all domains in the domain group. They resolve and apply in a domain group.
- You can move Cisco UCS domains between domain groups. However, any domain group-to-domain move can be disruptive, depending on the policies in the destination domain group. Cisco UCS domain groups resolve their own policies from domain groups in which they reside. If a new domain joins a domain group, then it applies the new global operational policies, which may impact service.
- When considering global firmware management, evaluate the impact. Realize that more than one registered Cisco UCS domain might be subject to the policy definitions for that firmware. It might also be subject, simultaneously, to any changes or upgrades to that firmware policy.
- Newly registered domains can automatically join a domain group based on qualification policies at registration time. Domain-group policy qualifications work in a similar manner to server-pool policy qualifications.

- You can place global operational policies anywhere in the domain-group hierarchy, and override policies set at a higher level by setting a policy in a lower domain group.
- When an administrator moves a domain to a new domain group, the policies for the old domain group are not necessarily removed. Instead, the old policies remain in place, until the new policies overwrite the previous ones.

  For example: Let's say that you have a UCS domain backup policy. The old policy defines the backup schedule and the new policy omits this policy. The UCS backups still occur based on the old schedule. They change if you create a new policy for the new domain group.

  Policies which are resolved through references are removed if they are not present in the new domain group.
- Weigh the degree to which you employ the subdomains against the amount of administration and management required for managing the different subdomains.
- You can nest subdomain groups up to five levels deep, hierarchically, for finer granularity of policy control.

Domain Group Partitioning

Some reasons for domain-group partitioning include:

- Geography (continents and time zones)
- Organizations, Business Functions, Business Units (marketing, engineering, finance, HR)
- Production Criticality (production, development, test, QA)
- Network Domains (internal networks, DMZ, external networks)

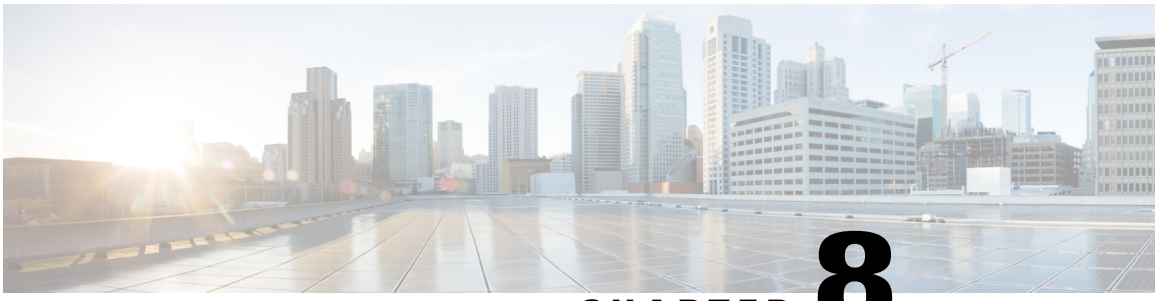
Geography is the most common basis for domain group partitioning. Domains in the same geography most often require the same administrative and operational settings.

Use domain groups to help simplify configuration and deployment of operational policies. Define a hierarchy when it best fits the operational challenge.

Domain Group Reassignment

Changing the domain group policy, after domain registration, no longer automatically reassigns domains to domain groups.

The **Reevaluate Membership** feature affects domain-group reassignment on a domain. This function can move UCS domains to different domain groups, which can result in policy changes.



CHAPTER 8

Registration

Cisco UCS Manager-Cisco UCS Central Registration

Make sure that:

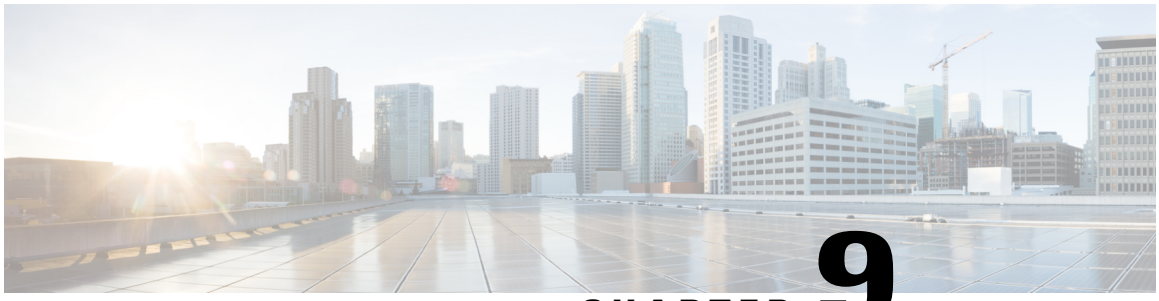
- Existing Cisco UCS Manager domains resolve to the same NTP server
- Register the Cisco UCS domains to the Cisco UCS Central server using the FQDN (Fully Qualified Domain Name)

Name Space Conflicts

Caution Be careful during periods when registered domains are unregistered or are unintentionally deregistered.

Any global objects that are locally cached when unregistered may cause namespace conflicts when reregistered with Cisco UCS Central. A problem occurs if the identical name still exists for an object owned by Cisco UCS Central. To resolve such naming conflicts, and return to global control of the local object, use the **UCSM** > **Use Global** option on the local object.

Note The **Use Global** operation overwrites any changes that were performed on the local policy during the unregistered state.



CHAPTER 9

Migrating Brownfield to Greenfield

Migration of Existing Deployments

When migrating existing local deployments to global deployments, best practices involve using global operational and service profile policies.

Policies in Cisco UCS Central

Cisco UCS Central provides global policies, which automatically enforce consistent global behavior across multiple domains.

In Cisco UCS Central, there are two major types of policies:

- Operational Policies
- Workload Policies (or service profile consumed policies)

Operational Policies

Examples include features in the User Authentication settings, such as call home, user management, time zone, and DNS, NTP, backups, . In Cisco UCS Central, operational policies are applied in the context of a domain group (or subdomain group) and all of its associated domains.

Domain groups and operational policies typically govern site-specific aspects, such as those that would be affected by to physical location, geography, or other factors.

Take advantage of the domain group hierarchy to minimize the number of operational policies that you define. You can segment operational policies into those that are nondisruptive and those that are potentially disruptive.

Best practices dictate that administrators place as many nondisruptive policies as high up in the domain group hierarchy as possible. Similarly, place any potentially disruptive operational policies as low in the domain group hierarchy as possible.

When adopting service profile policies and global service profiles, qualify them based on requirements and constraints. For example, migrating local service profiles to global service profiles is straightforward if there

is no need to maintain the same IDs. It is complicated if IDs must remain the same. Remember that you can view local service profiles from Cisco UCS Central, even if you cannot configure them.

Workload Policies

Workload policies are typically associated with service profile, such as boot policy, VNIC/VHBA templates, network QoS, and BIOS policy. In Cisco UCS Central, apply workload policies in an organization and all of its associated child organizations.

Organizations and workload policies typically govern service profiles and their associated templates, pools, and policies.

When adopting Cisco UCS Central for Cisco UCS domains, take note of current caveats and limitations. The most notable limitation: While local service profiles can refer to global pools and policies, you cannot convert local service profiles to global service profiles. Therefore, leave the existing service profile in a locally managed mode. The only way to re-create the settings is to reconstruct them in a global service profile.

Only adopt service profile policies and global service profiles if they contribute to management simplicity. If their adoption complicates management, avoid adopting them.

There is no dependency between operational policies and service profile policies. There is no requirement in Cisco UCS Central that forces you to adopt global service profile policies as well as global service profiles.

Cisco UCS Manager domains are not aware that they are contained in a domain group. Therefore, they do not share operational structure created within Cisco UCS Central. However, the organizational structure remains consistent and mutually shared between Cisco UCS Manager and Cisco UCS Central with a global scope.

Global Operational Policies

Cisco UCS Central provides global operational policies for one or more Cisco UCS domains. All participation in global policies is on an opt-in basis for Cisco UCS Manager domains. Cisco UCS Central does not take control of global policies unless such control is first delegated from the local Cisco UCS Manager domain administrator. A local Cisco UCS Manager domain administrator can revoke control by opting out of global management for any policy.

All administrative policies are under local domain control, by default, until the following occurs:

1. The local domain is registered to Cisco UCS Central.
2. The local domain is moved from ungrouped domains to a domain group in Cisco UCS Central.
3. The local domain administrator explicitly promotes a given policy from local to global resolution.

There is no dependency between the various policy promotion decisions. For example, you can globalize fault policies while still managing infrastructure and catalog firmware locally. In Cisco UCS Manager **Admin** > **Communication Management** > **Cisco UCS Central**, all of the policies listed within the policy resolution control are independent.

Once a policy is promoted from local to global, you can only change the effective policy definition at the Cisco UCS Central level. This is by design, to enforce the desired consistency across domains. However, administrators can return to locally resolved policies at any time. If an administrator reverts to local management for a policy, that policy setting remains until the local administrator changes it. Then Cisco UCS Central no longer controls that policy.

Best Practices for Global Operational Policies

When contemplating a transition from local operational policy control to global control, maintain local policy resolution prior to a broader adoption of global policies. Adopt global policies on an individual policy basis, phased over time, as you gain familiarity. This is also true for firmware management.

Generally, system health and monitoring are all low-risk candidates for using in global policies. Defining SNMP, syslog, and call home policies as operational policies, as high up in the domain group hierarchy as possible, provides the simplest approach. All domains in the subordinate domain groups inherit these global policy definitions.

Cisco recommends taking advantage of policy consistency and centralized policy enforcement, whenever possible. Global consistency and policy enforcement are among the key architectural goals for Cisco UCS Central. By consolidating policy definition and configuration within Cisco UCS Central, you reduce administrative burdens for local Cisco UCS administrators. Keep in mind that any opportunity to define and manage policy at a higher and more central level promotes greater administrative scalability. Design your policies with an emphasis on simplicity, and centralize policy definitions whenever possible.

Available Global Operational Policies

The following table shows the correspondences between Cisco UCS Central and Cisco UCS Manager. The **UCSM Navigation** column shows where the references are inactive in the GUI once you configure the policies to resolve globally at Cisco UCS Central. It also shows where the references are inactive once the domain becomes part of a domain group.

Policy Type	Cisco UCS Central Reference	Cisco UCS Manager Navigation
Infrastructure & Catalog Firmware	***Domain Group*Firmware Management > Infrastructure Firmware**	**Equipment > Firmware Auto Install**
Time Zone Management	***Domain Group* > Operational Policies > Time Zone**	**Admin > Timezone Management**
Communication Services	***Domain Group* > Operational Policies > Remote Access**	**Admin > Communication Management > Communication Services**
Global Fault Policy	***Domain Group* > Operational Policies > Debug > Global Fault Policy**	**Admin > Faults/Events/Audit > Settings**
User Management	***Domain Group* > Operational Policies > Security**	**Admin > User Management**
DNS Management	***Domain Group* > Operational Policies > DNS**	**Admin > Communications Management > DNS Management**
Backup and Export Policies	***Domain Group* > Backup/Export Policy**	**Admin > All > Backup and Export Policy**

Policy Type	Cisco UCS Central Reference	Cisco UCS Manager Navigation
Monitoring	***Domain Group*** > **Operational Policies** > **Call Home and Debug**	**Admin** > **Faults/Events** > **Syslog Faults/Events** > **Settings** > **TFTP Core Exporter** **Communications Mgmt** > **Call Home**
SEL Policy	***Domain Group*** > **Operational Policies** > **Equipment** > **SEL Policy**	**Equipment** > **Policies** > **SEL Policy**
Power Allocation	***Domain Group*** > **Operational Policies** > **Equipment** > **Global Power Allocation Policy**	**Equipment** > **Policies** > **Global Policies** > **Global Power Allocation Policy**
Power Policy	***Domain Group*** > **Operational Policies** > **Equipment** > **Power Policy**	**Equipment** > **Policies** > **Global Policies** > **Power Policy**

Migrating

In this procedure, we describe how to migrate from a Brownfield environment to a Greenfield environment. We demonstrate with a challenging use case: Boot from SAN with remote storage boot LUNs, which are already zoned to target initiators (WWPNs) within each service profile.

Note IDs must remain the same during migration.

When migrating, you must:

- Register existing UCS domains with Cisco UCS Central.
- Create global pools, policies, VLANS, VSANS, vNIC templates, vHBA templates, LAN connectivity policies, SAN connectivity policies, global service profile templates, and global service profiles.

  Make sure these global ID pools and policies match the exact format, settings and scheme, that are currently built locally in the UCS domains.

  Make sure that all names are unique when creating global counterparts.
- Use the same IDs as those of locally defined VSANs in Cisco UCS Manager, when creating global VSANs.
- Use a “G-“ in front of the VSAN name.
- Make sure that the FCoE VLAN ID, on the newly created global VSAN, exactly matches the FCoE VLAN ID configured on the corresponding local VSAN.

Note If you are creating a global VSAN with the same ID as a global VSAN already defined in a UCS domain, the FCoE ID must match exactly between the local VSAN and global VSAN. If not, the mismatch triggers a fault upon association of a global service profile.

- Create global service profiles that allocate new UUID, MACs, WWNN, and WWPNs from their respective global ID pools.
- Leverage simple Cisco UCS Central Powertools scripts to assign the original (correctly zoned) WWPNs and other IDs.

Migrating Brownfield Local Service Profiles to Global Service Profiles in Cisco UCS Central

Step 1 Document pool IDs, policies, VLANs, VSANs, and templates of the local service profiles.

Step 2 Re-create all IDs, policies, VLANs, VSANs, templates, and global service profiles in Cisco UCS Central.

Step 3 Gracefully shut down the server with the local service profiles.

Step 4 Disassociate the local service profile from the domain.

Step 5 Delete the local service profiles.
This restores and returns allocated IDs to the pool and marks the IDs as unused.

Step 6 Execute a Cisco UCS Central Powertools script to swap IDs for the specific global service profiles.
This makes the global service profiles look identical to their corresponding local service profiles.

Step 7 Verify that the IDs are correct for the specific server in the new global service profile.

Step 8 Associate the global service profiles with the proper server.

Step 9 Boot the server from the SAN LUN.

For the following example, assume that:

```
Global service profile Name: G-Sp-TEST-2 (with global pool derived IDs)
Org: root
Global WWNN pool: G-USA-WWNN
Global UUID pool: G-USA-UUID
Global MAC pool: G-USA-MAC
New (from local service profile) UUID: dc81c8de-3b00-11e5-0000-000000000025
New (from local service profile) MAC for vnic0: 00:25:B5:00:00:25
New (from local service profile) MAC for vnic1: 00:25:B5:00:00:26
New (from local service profile) WWNN ID: 20:00:00:25:B5:00:00:25
New (from local service profile) WWpN for A Fabric: 20:00:00:25:B5:AA:00:25
New (from local service profile) WWPN for B Fabric: 20:00:00:25:B5:BB:00:25
```

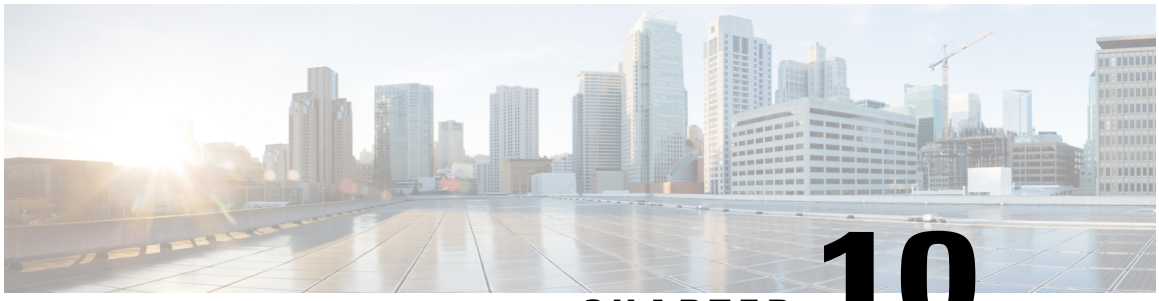
Example of a Cisco UCS Central Powertools Script

Test this script in a lab before using it in production. Edit the script according to your company's needs.

The script is not an officially supported product of Cisco. Use at your own risk.

```
# Start-UcsCentralTransaction
  Get-UcsCentralOrg -Name root | Add-UcsCentralserviceprofile -Name "G-Sp-TEST-2"
```

```
-Modifypresent -IdentpoolName "G-USA-UUID" -Uuid "dc81c8de-3b00-11e5-0000-000000000025"
  $mo = Get-UcsCentralserviceprofile -Name "G-Sp-TEST-2"
  $mo_1 = $mo | Add-UcsCentralVnic -Modifypresent -Name "vnic0" -IdentpoolName "G-USA-MAC"
 -Addr "00:25:B5:00:00:25" -Order "1" -SwitchId "A"
  $mo_2 = $mo | Add-UcsCentralVnic -Modifypresent -Name "vnic1" -IdentpoolName "G-USA-MAC"
 -Addr "00:25:B5:00:00:26" -Order "2" -SwitchId "B"
  $mo_3 = $mo | Add-UcsCentralvhba -Modifypresent -AdaptorprofileName "global-default"-Addr
 "20:00:00:25:B5:AA:00:25"  -AdminVcon "any" -MaxDataFieldSize "2048" -NwTemplName "" -Order
 "3" -pinToGroupName ""-QospolicyName "" -StatspolicyName "global-default" -SwitchId "A"
-Name "vhba0"
  $mo_4= $mo | Add-UcsCentralvhba -Modifypresent -AdaptorprofileName "global-default"-Addr
 "20:00:00:25:B5:BB:00:25"  -AdminVcon "any" -MaxDataFieldSize "2048" -NwTemplName "" -Order
 "4" -pinToGroupName ""-QospolicyName "" -StatspolicyName "global-default" -SwitchId "B"
-Name "vhba1"
  $mo_5 = $mo | Add-UcsCentralVnicFcNode  -Modifypresent -IdentpoolName "G-USA-WWNN" -Addr
 "20:00:00:25:B5:00:00:25"
  Complete-UcsCentralTransaction
```



CHAPTER 10

Organization

Hierarchy

Cisco UCS Manager is hierarchical in nature, as reflected through its structure.

For Cisco UCS Central, the hierarchical structure takes on a global scope.

The structure of the domain group in Cisco UCS Central is also hierarchical. One important distinction is that "domain group" is purely a Cisco UCS Central construct. It is used for the mapping and application of operational policies, VLANS, VSANS, and some special policies such as ID Access Control Policies, to the registered Cisco UCS domains. Local Cisco UCS domains have no visibility of domain groups, but they are impacted by operational policies.

The best practice for organizations and domain groups is to create the hierarchy to best reflect the logical (organization) and physical (domain group) segmentation of the enterprise.

- Ensure that any operational policies created in the `/root` domain group are truly intended to have global applicability for all domains.
- Ensure that any service profile policies placed in the `/root` organization are meant to be exposed to the entire Cisco UCS domain.

Mixed-Workload Environments

For Brownfield environments, consider adopting Cisco UCS Central and global consistency for new workloads that are deployed in existing Cisco UCS domains. Such an environment is called a mixed-workload environment, because it may contain both globally and locally managed objects. Two models exist for mixed-workload environments, where an existing domain may contain managed objects owned by both Cisco UCS Central and Cisco UCS Manager:

- Segregated organizations
- Integrated organizations

Segregated Organizations

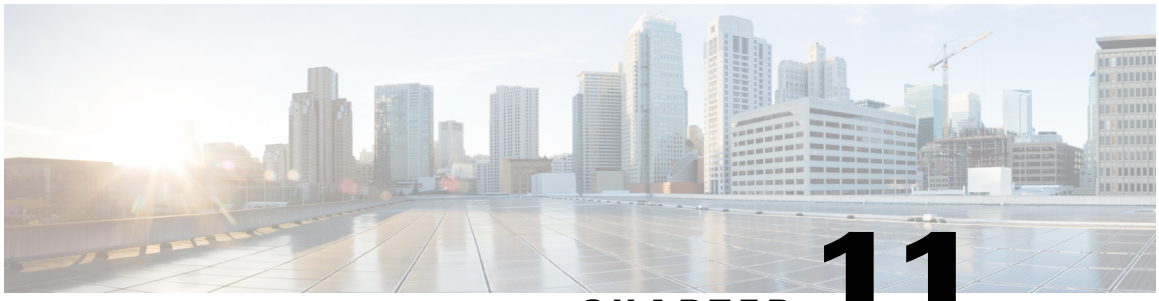
In this model, an organizational hierarchy (starting below `/root`) contains managed objects owned and managed exclusively by either Cisco UCS Central or Cisco UCS Manager.

Using this approach, the best practice would be to create the organization with a distinctly global name where the organization is only populated with globally managed objects. At the same level within the hierarchy, a corresponding organization would only contain locally owned managed objects.

Workload in the local organization would only reference local pools, policies, and templates. Workload in the global organization would only reference global pools, policies, and templatess.

Furthermore, using the **G-** prefix in the organization name would imply global scope for all objects. This reduces the need for a **G-** prefix for each managed object within the organization.

Cisco UCS Central creates this global organization structure and subsequently deploys down during the first association of a global service profile. Best practices dictate that you differentiate the name within this global organization structure. However, we still recommend using the **G-** prefix names for subordinate pools, policies, VLANs, VSANs, templates, and global service profiles.



CHAPTER 11

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.

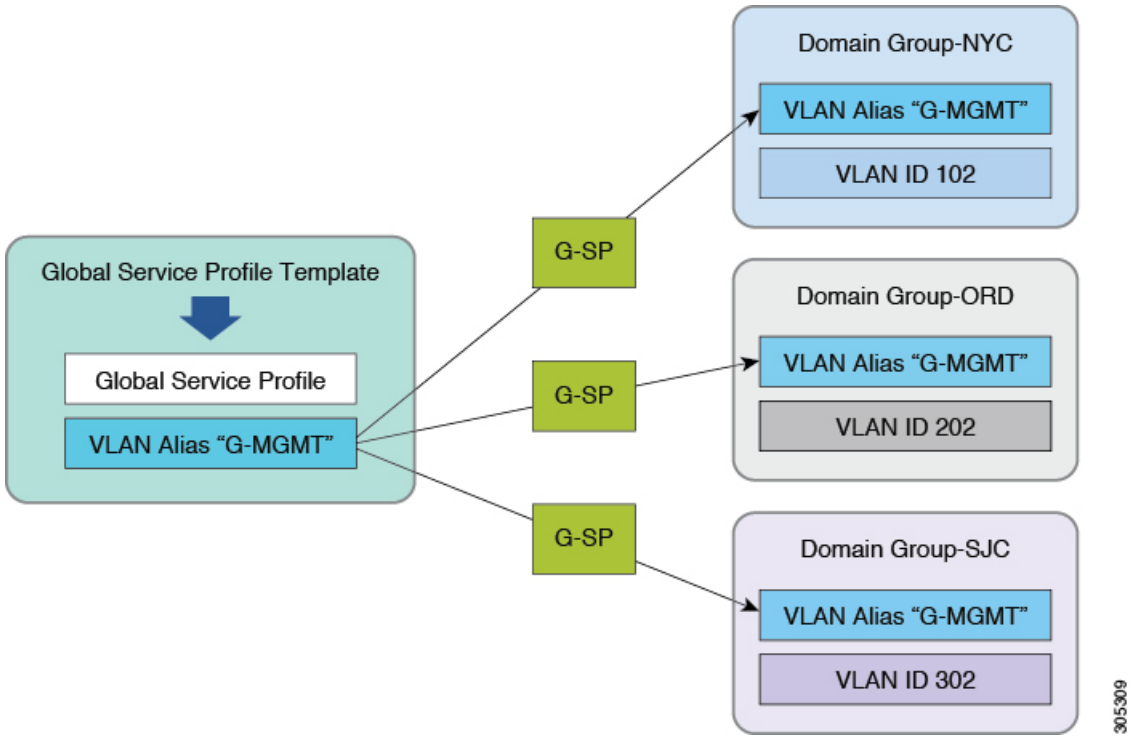
A global service profile is instantiated from its corresponding global service profiles template. When you create a global VLAN in Cisco UCS Central, you must designate its **Domain Group Location**. This designation ties the use of the VLAN or VSAN, and its corresponding ID, to that specific domain 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 4: 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 any ID pool. They help manage IP-management-pool IDs in large Cisco UCS Central environments. Management IPs 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.

ID range access control policies can allow for management IPs 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.

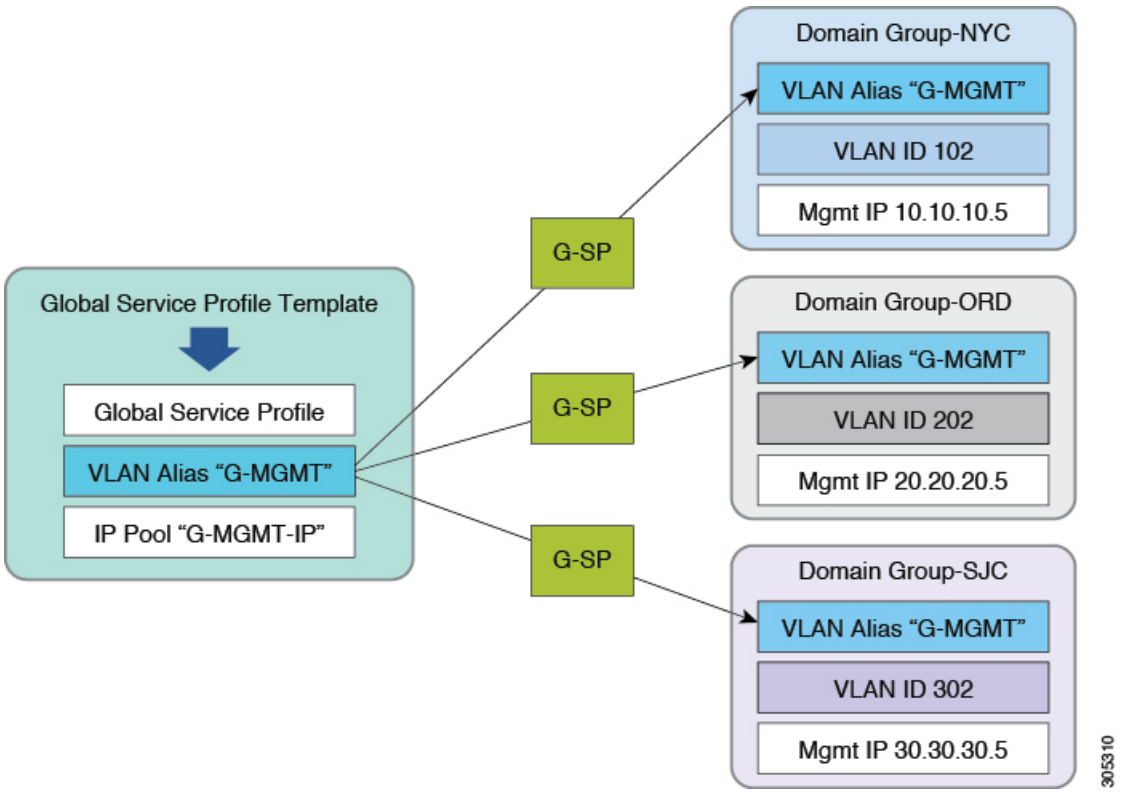
When you create a global IP management pool, use corresponding blocks of management IPs that match the management subnets of your different UCS domains. Creating the actual ID-range access control policies is simple, since they coincide with a domain group. Once you create the policies, access them by 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 5: 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
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.

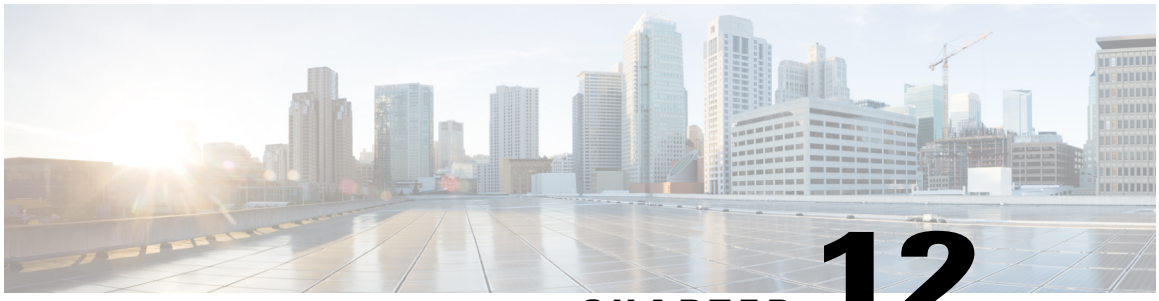
Naming Policies

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.



CHAPTER 12

Configuration

DNS Management

Typically, DNS management is defined at a global or corporate level. Therefore, DNS domain names and DNS servers are good candidates for global policy management. Define them as high in the domain group hierarchy's operational policies as possible.

Power Management

Policies around power management include two different policies:

- **Global power allocation policy—**Determines whether to apply power capping at the chassis level, or manually override the power caps at the individual blade level.
- **Power policy—**Chassis-level configuration for: Nonredundant, N+1, or Grid for the physical AC power.

The power policy is a strong candidate for Cisco UCS Central policy definition.

Global power allocation policy is one of the most sensitive policies for environmental and location dependencies. Best practices depend on your environment.

For example:

- Power budgets, per rack, may vary between different datacenters and locations.
- Some sites may have implemented power groups to create power caps that span multiple racks, specific to a data center layout.

Your global power allocation policy depends on local constraints. Definition schemes, such as creating broadly-scoped policies to restrict power on a per-rack basis, are the simplest. However, a definition scheme is site-specific and hard to generalize.

Fabric Interconnect Port Configuration

Configure physical device configuration for the fabric interconnect ports through Cisco UCS Central. The configuration types now support:

- Server
- Uplink
- Unified Ports

Cisco UCS Central also supports uplink port-channel creation in addition to defining the role of the specific port.

Note You cannot use Cisco UCS Central to manage objects that depend on physical ports, including pin groups and port-channels for both Ethernet and Fibre Channel.

Forced Time Sync in Cisco UCS Manager

After you set the time in the NTP server, Cisco UCS Manager may appear to not sync the time immediately.

Set the NTP server in the **Admin** tab to force Cisco UCS Manager to sync with NTP immediately. Then attempt to set the clock from the CLI with the following sequence:

Note Set the hour using 24-hour military time.

```
scope system
scope services
set clock month day year hour minute second
```

The following example sets the clock to February 22, 2016 at 13:44:00.

```
scope system
scope services
set clock february 22 2016 13 44 00
```

A message follows, indicating, `Clock synchronization successful`, with Cisco UCS Manager time reflecting the change. Your next registration attempt should succeed.

Note A time difference of a few seconds can cause registration to fail. For a successful registration to occur, the Cisco UCS Manager system time cannot be behind the Cisco UCS Central system time.

Service Status in Cisco UCS Central

The following CLI commands show how to check the status of the services running on the Cisco UCS Central server.

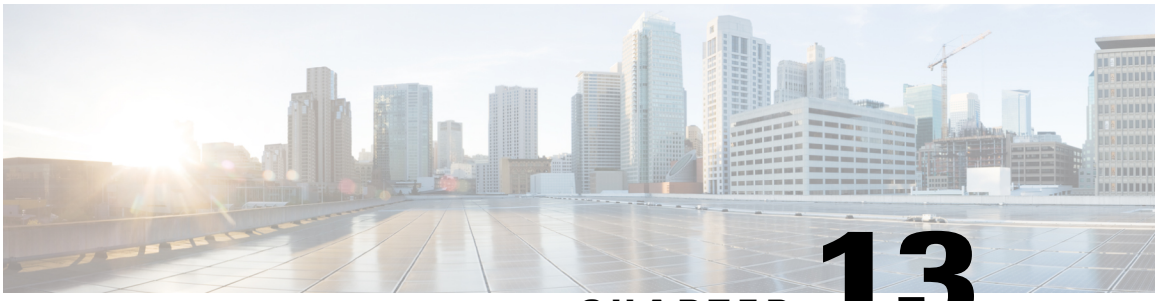
```
UCSC-A# connect local-mgmt
UCSC-A (local-mgmt)# show pmon state
```

Note Do not reset PMON (services) without consulting Cisco TAC.

HTTPS Certificates in Cisco UCS Central

Many features of the Cisco UCS Central management interface rely on available or imported HTTPS certificates (from each Cisco UCS domain managed by Cisco UCS Central) on the client machine.

The browser uses these certificates to manage Cisco UCS Central for invoking features such as KVM launch, Cisco UCS Manager launch, and to query particular faults or alerts in the Cisco UCS fault summary. If you do not import the certificates properly, or if they have expired, or if certain security settings are enabled, you may encounter errors.



CHAPTER 13

Deploying Global VLANs and VSANs

VLAN and VSAN Policy Push

In Cisco UCS Central you can publish, or push, global VLANs, and VSANs down to the Cisco UCS domains. You no longer have to configure and associate a global service profile to deliver a globally defined VLAN or VSAN.

Cisco UCS Central makes all applicable global VLANs and VSANs available for publishing to the registered Cisco UCS domain.

Note This assumes that the global VLANs or VSANs are available to the domain group. You can automate the publishing of the global VLAN or VSAN with either direct API integration or the use of Cisco UCS Central CLI. This functionality is not available through the UI.

Publishing VLANs and VSANs Manually

The following CLI code shows an example of publishing a VLAN and a VSAN manually. It first queries the system for publishable VLANs and VSANs, and then publishes the VLAN.

Note This mechanism is only for publishing. The VLAN or VSAN must have been previously created in Cisco UCS Central.

```
UCSC-A# connect resource-mgr
UCSC-A(resource-mgr)# scope domain-mgmt
UCSC-A(resource-mgr) /domain-mgmt # show ucs-domain
UCSC-A(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC-A(resource-mgr) /domain-mgmt/ucs-domain # publish ?
vlan vlan-name
vsan Vsan
```

Deleting Global VLANs

When you delete VLANs, make sure that the VLAN does not reference any vNIC template or LAN connectivity policy. Also make sure that no service profile uses that global VLAN. If you choose to delete a global VLAN, make sure that you delete its organization permissions first, prior to deleting the global VLAN.

Global VLANs and VSANs Persisting Locally

Once you push global VLANs and VSANs down to a UCS domain, they persist there, even if you disassociate them from the global service profile. This is by design. If you are not going to use the global VLAN or VSAN again, and you wish to delete the deployed VLAN or VSAN in the UCS domain, use the **Make Local** function for the specific VLAN or VSAN. Once it is localized, then you can delete the VLAN or VSAN.

Once a domain is deregistered, Cisco UCS Central converts all global VLANs, VSANs, policies, and service profiles to local objects, as long as you are NOT using the **Deep Remove Global** feature. You can use **Deep Remove Global** during deregistration. It removes all global objects from the Cisco UCS domain.

Note Consult Cisco TAC before deregistering a product UCS Domain from UCS Central.

FCoE VLAN ID Conflicts

When you create new global VSANs from the SAN cloud, the default FCoE VLAN ID value is 1. This is in conflict with the global default VLAN ID value.

Change the FCoE VLAN ID when creating new global VSANs, and specify a VLAN ID that is not currently in use.

Deploying Global VLANS and VSANS from the CLI

You can deploy global VLANs and VSANs to a UCS domain without using a global service profile to deliver them. This feature is only available with the CLI. It can benefit those customers using local service profiles, who want to utilize and access global objects from Cisco UCS Central.

Manually Publishing a Global VLAN from the CLI

Type the following commands, in the CLI, to publish a global VLAN to a UCS domain:

Before You Begin

Create the global VLAN Cisco UCS Central.

Step 1 **# connect resource-mgr**

Step 2 **# scope domain-mgmt**

Step 3 **# show ucs-domain**
Displays the UCS domain IDs for use with the next command.

Step 4 **# scope ucs-domain** *[domain_name]*

Step 5 **# publish vlan** *[vlan_name]*

Manually Publishing a Global VSAN from the CLI

Type the following commands, in the CLI, to publish a global VLAN to a UCS domain:

Before You Begin

Create the global VSAN Cisco UCS Central.

Step 1 # connect resource-mgr

Step 2 # scope domain-mgmt

Step 3 # show ucs-domain
Displays the UCS domain IDs for use with the next command.

Step 4 # scope ucs-domain *[domain_name]*

Step 5 # publish vsan *[vsan_name] [fabric]*
Designate the intended Fabric with either an **a** or **b** at the end of the command.

CLI Troubleshooting Commands

The following CLI commands are the most common and helpful commands used for troubleshooting.

Show Disk Speed

```
# show disk-speed

/dev/mapper/VolGroup00-LogVol00:
Timing cached reads:  12606 MB in 2.00 seconds = 6317.87 MB/sec
Timing buffered disk reads: 106 MB in 3.01 seconds = 35.21 MB/sec

/dev/mapper/VolGroup01-LogVol00:
Timing cached reads:  12600 MB in 2.00 seconds = 6315.33 MB/sec
Timing buffered disk reads: 320 MB in 3.00 seconds = 109.28 MB/sec
```

Show Disk Usage

```
# show disk-usage

Filesystem      Size Used Avail Use%  Mounted on
/dev/mapper/VolGroup00-LogVol00:
                37G   3.2G 32G  10%  /
/dev/sda1       99M   13M  81M  14%  /boot

/dev/mapper/VolGroup01-LogVol00:
                39G   177M 37G  1%  /bootflash
tmpfs           5.9G  728K 5.9G 1%  /dev/shm
```

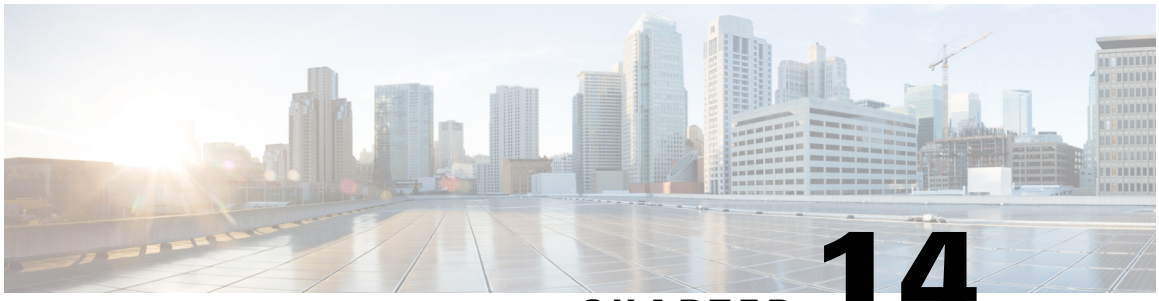
Show Registered Domain IDs

```
# connect service-reg

Cisco UCS Central
TAC support: http://www.cisco.com/tac
.
.
.
# show clients

Registered Clients:
 ID: 1008
 Registered Client IP: 172.22.251.106
 Registered Client IPv6:  ::
 Registered Client Connection Protocol: Ipv4
 Registered Client Name: L14-UCS1
 Registered Client Type: Managed Endpoint

 ID: 1009
 Registered Client IP: 172.22.251.10
 Registered Client IPv6:  ::
 Registered Client Connection Protocol: Ipv4
 Registered Client Name: SJC18-L12-UCS1
 Registered Client Type: Managed Endpoint
```



CHAPTER 14

Pools

Identifier Management

Global identifier management addresses one of the biggest challenges for multidomain management in Cisco UCS: guaranteed unique addressing for system identifiers (MACs, WWxNs, UUIDs). Previously, Cisco UCS Manager best practices suggested embedding a domain ID within the high-order bytes of the ID pool ranges. This is not practical for Cisco UCS Central managed global IDs.

With Cisco UCS Central, you can define all of the ID pools and access them globally across all Cisco UCS domains. This guarantees unique and non-overlapping IDs for service profile assignments across all Cisco UCS domains.

Cisco UCS Central immediately notifies you if you are creating a block of IDs that conflict with another pool or block in the system, at both the local and global levels.

Global ID pools belong to the organization structure. Global pools do not depend on domain groups, as do the Cisco UCS Central operational policies. Instead, the range of global ID pools extends across all Cisco UCS domains in the scope of the organization structure within Cisco UCS Central, regardless of any domain-group partitioning.

When deploying Cisco UCS Central, a best practice is to adopt global IDs along with a global service profile for deployment of new Cisco UCS domains.

Pool Sizing

To minimize the number of managed objects, create a smaller number of pools with a larger number of blocks.

To distinguish A-side versus B-side traffic, create corresponding A-side or B-side pool names. Use an “A” or “B” embedded in the high-order byte of the MAC/WWPN address range. Extending this model toward Cisco

UCS Central involves creating multiple blocks under such a pool structure. The most efficient sizing for each block is 256 addresses (0xFF).

Note Cisco UCS Central imposes a maximum block size of 1,000 addresses (0x3E8) for all pools (UUID, MAC, WWxN).

Duplicate Pool IDs

Cisco UCS Central provides visibility into possible duplicate ID usage.

All pool types (UUID, MAC, WWxN) offer the ability to display duplicate IDs that may exist across Cisco UCS domains. View them in the ID usage summary. Duplicate ID severity is flagged as either "major," for IDs that appear in multiple service profiles, or as "warning," for IDs that appear in multiple local pools.

The only method for viewing local ID pool consumption is to select an individual ID, and view the corresponding local pool and local service profile details.

Transitioning to Global ID Pools

You can reconfigure local service profiles that currently reference local ID pools to instead use global ID pools. Changing any ID for an associated service profile typically causes a service interruption. However, Cisco UCS Central is designed to ease this migration to global ID pools, and not cause a service interruption.

When changing references from a local IS pool to a global ID pool, select the global pool in the vNIC/vHBA reference pull-down in the LAN tab of UCS Manager. First, use **Reset MAC/WWxN/UUID** to change the pool reference from local to global, then perform the reset. Drill down through **ID Usage** to see the definitive way of verifying ID association to a local or global ID pool.

Local service profiles that use global IDs are guaranteed ID uniqueness if the global service profiles that reference the global IDs are exclusive. However, local service profiles that reference global ID pools cannot take advantage of global service profile mobility. They always reside in and are confined to the specific local Cisco UCS domain.

Creating New Global ID Pools

Existing Cisco UCS customers, with multiple domains, may have addressed multiple domain ID challenges by embedding a domain ID within the high-order bytes of ID pool ranges. But some administrators might wish to segregate global IDs in a way that is distinct from the previous local ID consumption method.

Generally, domain IDs are no longer relevant when creating global ID pools for new deployments. The exception to this is if you were using a domain-specific ID qualification policy (or a block within a pool).

The best practice of creating distinct A-side or B-side global pools is useful for troubleshooting.

Challenges When Migrating to Global UUID Pools

Transitioning to global UUID pools from local UUID pools creates some challenges.

Challenge Area	Description
Prefixes	Define UUID prefixes at the domain level. You can use UUID suffixes to create blocks within pools. Adopting global UUIDs that are supersets of all local UUID pools requires creating at least one global UUID pool per Cisco UCS domain. Therefore, the number of global UUID pools must be equal to the number of domains, yielding no consolidation in the number of pools.
Organizations (Orgs)	Global pools are based on organizations, but UUID prefixes are based on domains (internal IDs from the fabric interconnects). There is no mapping between organizations and domains.
Adoption	Existing service profiles cannot adopt the use of global UUIDs in the absence of a reconfiguration cycle and a server reboot. Cisco recommends letting existing local service profiles remain as local service profiles until they reach the end of their life cycle. Create new local service profiles as global service profiles.

Recommendations for Migrating to Global ID Pools

To maintain the same ID for local service profiles, while migrating to global ID pools, construct the global ID pools so that they are supersets of the corresponding local ID pools. This means that the global ID pool contains all identifier blocks that are currently within the local ID pools.

The best practice is to adopt an A/B naming orientation for MAC and WWPN pools for the fabric, such as G-MAC-A or G-WWPN-B. Once you have created the global ID pools, you can change the service profile, VNIC, VHBA, or template to reference the global ID pools. Cisco UCS Central automatically assigns the same identifier that was previously used in the local ID pool, if not already assigned, thus eliminating the need for a service interruption.

When the ID space is already partitioned and not overlapping, adopt as follows:

1 Create a new global ID pool in Cisco UCS Central with a unique name. Use **Global-** or **G-** for the pool-name prefix. For MAC and WWPN pools, add an **-A** or **-B** suffix to the pool name, if desired.

Note For MAC pools, the Network Administrator always sees A and B MACs intermeshed on the network upstream. This is because Cisco UCS Central clusters the upstream connectivity from the FIs to the aggregation layer-2, TOR (top of rack), EOR (end of row) switch.

2 For each local ID block in the local pool, recreate a corresponding ID block in the global pool.

3 Change any existing templates (service profiles, VNICs, and VHBAs) to refer to the corresponding global ID pool name.

4 Change the Pool reference from local to global. Perform a **Reset MAC/WWxN/UUID Address** on the specific instantiated managed object to effect the global ownership change.

5 Verify that the corresponding local ID block has no assignments.

6 Verify, through ID usage, that the address now references a global pool.

7 Delete the corresponding local ID block for each local ID block in the local pool.

For VNICs, or VHBAs, created from initial templates, once the IDs reference the global ID pools, then all subsequently created managed objects reference the new global ID pools.

For VNICs, or VHBAs, that are bound to updating templates, once the IDs reference the global ID pools, then all existing managed objects bound to the template reference the new global ID pools. If the existing managed object's ID is present and unassigned in the global pool, then this transition does not cause a reconfiguration, reboot, or service impact.

For VNICs, or VHBAs, that are not bound to a template, if the service profile pool name is modified to point to a global pool, and the existing ID is already used in the global pool, then the service profile receives a new ID, causing a reconfiguration, reboot, and service impact. If the ID is not already used, then the ID is retained and points to the global pool, without incurring a reconfiguration or service impact.

You can also manage IP addresses for ext-mgmt and iSCSI initiators through global pools.

ID Range Qualifications

In Cisco UCS Central, you can use ID range qualification policies to assign ID blocks within a global pool, to a specific domain or domain group, for any local and global service profiles that reference the global pool. In this way, one or more Cisco UCS domains, from a particular domain group, are assured of using a discrete range of identifiers.

In Cisco UCS Central, global service profiles can reference global pools that utilize ID range qualification policy definitions on one or more ID blocks. Cisco UCS Central created the concept of lazy-binding for ID allocation. Cisco UCS Central waits until you have selected a Cisco UCS server for association. Then it allocates an ID from a pool that contains at least one qualified block.

Global ID Usage by Global Service Profiles

The following describes what happens during the global service profile creation, association, and disassociation process.

Global Service Profiles Without a Binding Server

If the global service profile does not use IDs from any qualified pool, then Cisco UCS Central obtains the ID values from the appropriate ID pool.

If the global service profile does use IDs from a qualified pool, the global service profile moves into a config-failure state which triggers the warning message: `Using ID pool which contains block with Qualifier (Lazy-Binding)`

ID Usage During the Association Process

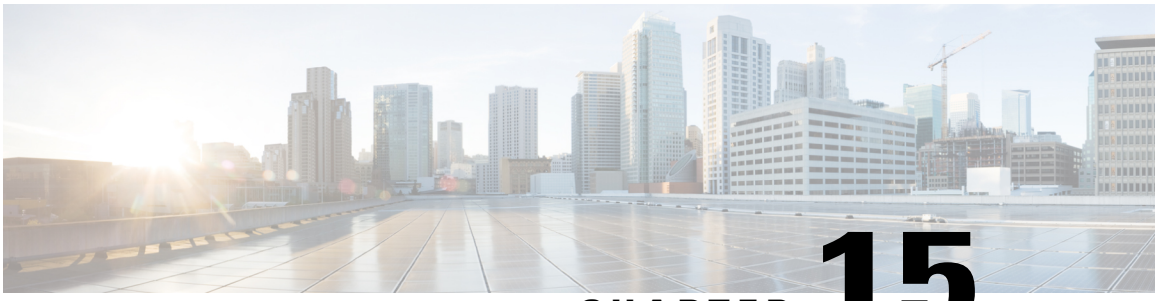
During the global service-profile association process, the target server and the domain access the global service profile.

Cisco UCS Central performs normal ID resolution to consume the IDs from the appropriate ID block for the domain, or domain group, within the global pool.

ID Usage During the Migration or Disassociation Process

During the global service-profile migration, or disassociation, process, the ID consumption performs as follows:

- **Non-Qualified ID pool—**Cisco UCS Central does not release IDs, that are already in use, from the global service profile.
- **Qualified ID pool—**During the global service profile migration process, Cisco UCS Central attempts to reacquire the IDs used in the global pools. This assumes that those IDs are still qualified for the newly targeted domain or domain group. If the newly targeted server is in the same domain, Cisco UCS Central reacquires the same IDs. If the newly targeted server resides in a different domain or domain group, Cisco UCS Central re-evaluates the domain qualification policy. If the previously acquired ID does not meet the qualification policy, the ID is released and a new ID is assigned.



CHAPTER 15

Authentication

Cisco UCS Central Authentication

Cisco UCS Central supports either local or LDAP-based authentication. Other authentication types, such as TACACs+ or RADIUS, are supported in v1.4 and higher. They are not supported for earlier versions. You can use Cisco UCS Central to configure these authentication types for Cisco UCS Manager through operational administrative policies.

Note Do not use '$' as a password character when using local authentication.

In Cisco UCS Central, you can only activate one defined form of native authentication exclusively (either local or LDAP). Cisco UCS Central allows selecting from multiple authentication domains. Unlike Cisco UCS Manager, it does not currently support configuring multiple authentication realms.

Cisco UCS Central includes third-party and self-signed certificate support for LDAP integration and user authentication.

Authentication

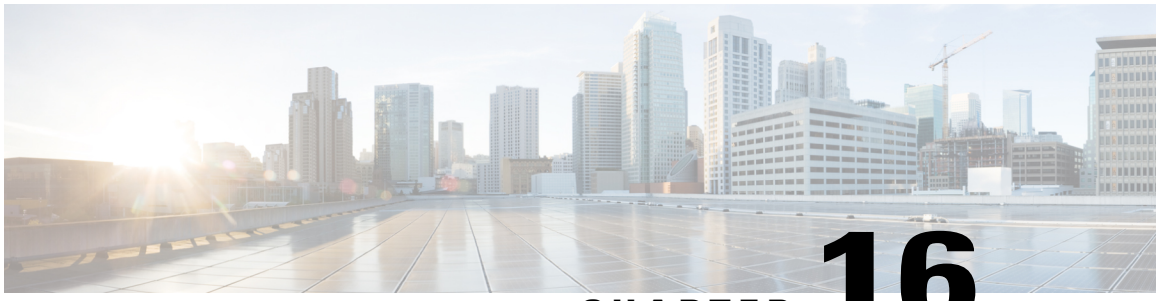
Cisco UCS Central can globalize the configuration of the Cisco UCS Manager GUI authentication model across all registered Cisco UCS domains.

In v1.4, and higher, of Cisco UCS Central you can use RADIUS or TACACS+ as authentication realms. You cannot use them in earlier versions. Aim for simplicity and to minimize and centralize the number of authentication schemes and definitions. Similarly, if you require access to multiple authentication schemes and definitions, then aim for simplicity when constructing authentication scheme maps and definitions in Cisco UCS Central domain groups.

RBAC

RBAC (Role-Based Access Control) is typically linked to global or corporate-level authentication, such as LDAP or AD. For Cisco UCS Central, it is preferable to enforce central control for access.

If you do not currently have central authentication and role management, then the best practice dictates that administrators define role-based access within Cisco UCS Central. Define it as high up in the domain group hierarchy's operational policies as possible.



CHAPTER 16

Firmware Management

Firmware Management

Configuring global firmware management enforces a policy in which all domains within a domain group (v1.4 and below) or maintenance group (v1.5 and above) run a consistent version of the firmware and hardware capability catalog. Enable a global policy resolution when you want to enforce consistent versions of infrastructure firmware among all domains in a domain group or maintenance group.

When a domain group or maintenance group consists of multiple Cisco UCS domains, and you have switched to a global firmware management control policy, be careful of any operational (global) firmware policy changes to that group. Cisco UCS Central tries to upgrade all domains that are members of that domain group or maintenance group, along with any subdomain groups, as defined in the maintenance policy. The default maintenance policy behavior requires user acknowledgment before any updates occur. You can override this behavior by scheduling an acknowledgment or performing an immediate acknowledgment.

Firmware Management for Cisco UCS Domains

Upgrading Cisco UCS domains used to be a manual process, unless you used a Cisco UCS Firmware Upgrade script.

The current release of Cisco UCS Manager includes a firmware automatic-install feature to help automate tasks that were previously manual. Cisco UCS Central builds upon this new feature to help in automating firmware upgrades across multiple Cisco UCS domains.

There are several types of firmware:

- **Infrastructure firmware (A package)**: Refers to the images that run in the I/O modules, the fabric interconnects, and Cisco UCS Manager.

- **Server Blade firmware (B Package)**: Refers to the images that run on a physical Cisco UCS blade server BIOS, CIMC, adaptors, and controllers.

Note Currently, Cisco UCS Central does not support direct endpoint upgrades of blades servers. Use a Host Firmware policy and global service profile association to upgrade the blade or server firmware.

- **Rack-Mounted Server firmware (C Package)**: Refers to the images that run on a physical Cisco UCS-managed rack-mounted server BIOS, CIMC, adaptors, and controllers.
- **Cisco UCS Mini firmware (E Package)**: Refers to the images that run on a physical blade server BIOS, CIMC, adaptors, and controllers that are a part of Cisco UCS Mini.

The best practice for server firmware is to leverage host firmware packages as part of the service profile definition, to guarantee configuration consistency at the application level.

Recommendations for Firmware Management

There are no implicit maintenance policies for server firmware updates. Therefore, a best practice is to explicitly define a maintenance policy that governs server firmware bundle updates.

Infrastructure firmware updates are disruptive to the server. Therefore, when you create your global service profiles, always enable the user-acknowledgment settings. Using user-acknowledgments in your maintenance policy prevents untimely service disruptions.

You must understand the following firmware management issues.

Service Degradation and Disruption

Any Cisco UCS infrastructure firmware update causes service degradation, because each fabric interconnect must sequentially go through a reboot cycle. To avoid service disruption, ensure that appropriate application-level availability schemes are in place, such as Cisco UCS fabric failover, high-availability (HA), NIC bonding, and host-based storage multipathing.

Pending Acknowledgment

Rebooting fabric interconnects requires explicit acknowledgment from the Cisco UCS Central administrator. For domain/maintenance groups of more than one UCS domain, you can switch the Policy Resolution Control to local for each domain you do not wish to upgrade. This prevents simultaneous requests to upgrade UCS domains. Thereafter, changing the Policy Resolution Control to global would cause the upgrade process to proceed.

The default behavior is that you must acknowledge all firmware upgrades (infra-fw) and reboots (fi-reboot) before they proceed. View progress in Cisco UCS Central in the infrastructure firmware upgrade page.

For an individual Cisco UCS domain within Cisco UCS Manager, follow **Operations** > **Firmware** > **FW Operations**.

Firmware Upgrade Process

The upgrade process requires several acknowledgments.

In Cisco UCS Central, multiple upgrades can proceed in parallel. If you are connected to Cisco UCS Manager, those connections to Cisco UCS Manager are reset during an upgrade. As with standalone Cisco UCS Manager upgrades, the infrastructure firmware upgrade takes roughly one hour to complete, but can run in parallel across multiple domains. Blade server upgrades can take longer, depending on the scope of servers involved and whether virtual workloads require migration (vMotion/Life Migration) prior to upgrading the host.

Firmware management can complement host firmware policies. When loading a new Cisco UCS domain for the first time, use both infrastructure and host firmware automatic installation processes. Ensure that a new domain is current with all low-level host firmware, before releasing it to production.

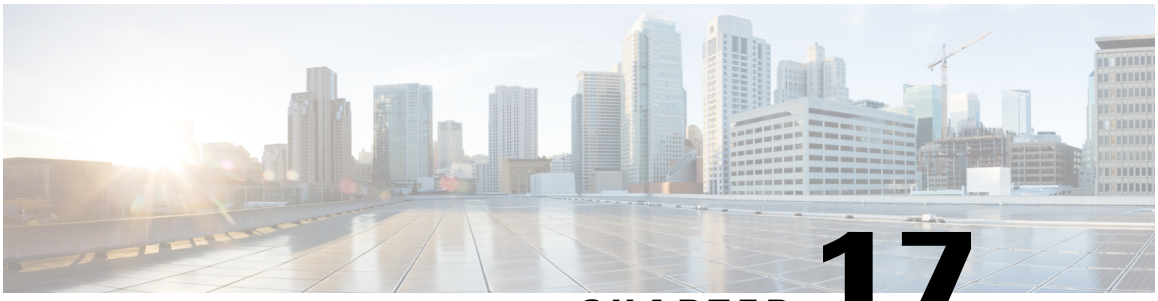
Host Firmware Packages and Maintenance Policies

Host firmware packages and maintenance policies are both visible and configurable from domain groups and organizations.

The expected behavior for Cisco UCS Central is:

- Global service profiles refer to the host firmware policy that is defined under organization and not the domain group.
- After you acknowledge the maintenance policy, Cisco UCS Central pulls the host firmware package, maintenance policy, and any other referenced policies, from Cisco UCS Manager to Cisco UCS Central.
- A local service profile can either reference a local host firmware policy and a local maintenance policy, a global host firmware policy, or global maintenance policy.

The best practice is to configure and use host firmware packages, maintenance policies, and schedules exclusively from the organization.



CHAPTER 17

Backup and Import

Backing Up Cisco UCS Central

Backing up the Cisco UCS Central configuration regularly is essential. Without regular backups, there is no automatic way to reconstruct the mapping of operational policies to domain groups and to subordinate, individual Cisco UCS domains.

Given the small size of a Cisco UCS Central backup (much less than 1 MB), perform a Backup and Configuration Export for UCS Central once a day. Use a **Config-All** (logical) backup and also the **Full-State** (db) backup.

Always use remote copy to store your backups off-line from the Cisco UCS Central virtual appliance. You can also schedule Cisco UCS Central backups on a custom-defined schedule.

Backing Up Cisco UCS Domains

Management through Cisco UCS Central does not change the need for creating frequent Cisco UCS backups. It does, however, help simplify and automate individual backup operations.

Define backup and export policies per domain group. Although backup files vary in size, typical backups for individual Cisco UCS domains are ~100 KB, which is small enough to justify frequent backups. (Full-state binary backups are ~ 2-MB.)

Cisco UCS Central maintains original copies of all backups within the Cisco UCS Central appliance. In addition, you can store copies of backups in remote locations.

Consider backing up Cisco UCS daily, using a **Config-All** (logical) backup. Perform a **Full-State** backup and **Config-All** for each UCS domain. You can also schedule Cisco UCS Central backups on a custom-defined schedule.

Domain Backup Limitations

You can configure two kinds of backups for Cisco UCS Central and for domains:

- Full-state backup—Used for data recovery
- Configuration Export—XML backup of the logical configuration

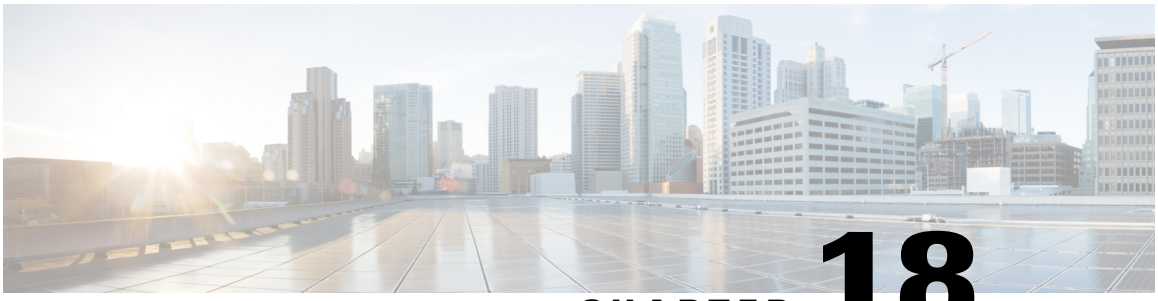
Both backups afford the option of performing a remote copy to an FTP server. Remote Copy is highly recommended, on all scheduled backup jobs, to protect backups from loss in a disaster scenario.

You can only import UCS Central backups from a remote file system. Import any remotely stored domain backups through the local Cisco UCS Manager.

Global References in Local Backups

If you back up at the local Cisco UCS Manager level, then these backups do not contain any references to global objects that are managed by Cisco UCS Central.

Within Cisco UCS Central, use backup and export policies with backup operations managed exclusively by Cisco UCS Central. A UCS domain backup, scheduled and driven by Cisco UCS Central, still backs up all local objects in the UCS domain.



CHAPTER 18

High Availability

High-Availability Cluster-Mode

Cisco UCS Central provides native high-availability (H/A) features primarily for deployments that do not contain a native hypervisor. In general, use a native hypervisor, if available. In cases where native hypervisor H/A is not available or active, you can safely run Cisco UCS Central in standalone mode without using Cisco UCS Central's native H/A clustering.

If your host hypervisor does not provide H/A support, then it is generally a best practice to take advantage of Cisco UCS Central's H/A capabilities.

Note In general, we do not recommend running both Cisco UCS Central H/A and a native hypervisor concurrently.

Keep in mind that Cisco UCS Central can incur a temporary outage without disrupting service. This is because Cisco UCS Central only operates on the control-management plane, not the data plane. If Cisco UCS domains, registered to Cisco UCS Central, lose visibility to the Cisco UCS Central server, services within each Cisco UCS domain continue to operate normally. However, configuration changes to the environment require you to restore Cisco UCS Central server.

Note For situations where Cisco UCS Central is down, and you have to make an administrative edit to a global service profile, you can localize the global service profile such that Cisco UCS Manager can then edit it. This is only recommended for the scenario when you have to edit a service profile when Cisco UCS Central is down.

H/A with Cisco UCS Central in cluster-mode refers to a single logical instance of Cisco UCS Central, using a primary and a subordinate Cisco UCS Central VM with a shared clustered third disk.

You can also achieve H/A by taking advantage of native hypervisor H/A capabilities. In this case, do not use Cisco UCS Central's H/A capabilities. They are not required.

Administrators looking for true DR capabilities are required to leverage any back-end VM DR capabilities that they may have in place.

Achieve H/A with Cisco UCS Central using one of two methods:

- Method 1:
  - Install a new Cisco UCS Central instance as an H/A cluster
  - Convert standalone Cisco UCS Central to an H/A cluster
- Method 2:
  - Take advantage of native hypervisor capabilities
  - Leverage RDM clustering or NFS clustering

Refer to the Installation and Upgrade Guide, before attempting to use either of these methods.

Recommendations for NFS Cluster-Mode

When deploying in NFS cluster-mode, make sure that:

- Both VMs are on separate physical hosts with access to shared storage NFS server
- Both VMs are running the same version of ESX or Hyper-V
- Both VMs are running the same version of Cisco UCS Central
- Both VMs are on the same subnet

Cluster H/A mode requires the configuration of an NFS server and 40GB+ volume:

1. Export the NFS directory per the Cisco UCS Central Installation and Upgrade Guide.
2. Restart the NFS service.
3. Delete or modify any firewall rules on the NFS server that could block the NFS server directories from mounting on the Cisco UCS Central VMs.
4. Specify the IP address of the NFS server during Cisco UCS Central installation.
5. Specify the directory of the NFS server.
6. Use configuration scripts to migrate the database and images from the primary VM to NFS.
7. Mount the NFS server directories on the primary node after election completes.

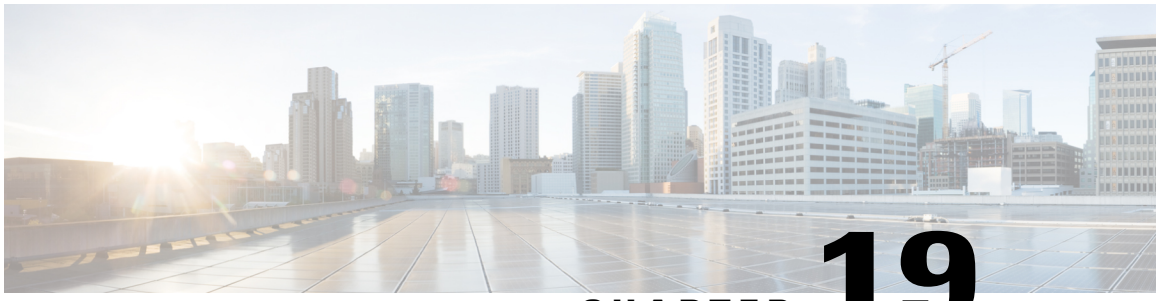
Transitioning from Standalone HA

You can switch from an existing standalone Cisco UCS Central implementation to an H/A configuration. You can also switch from an RDM implementation to an NFS-based implementation. Consult the Installation and Upgrade Guide for further information about the necessary steps.

Recommendations

- If considering Cisco UCS Central H/A options, we recommended using NFS-based H/A.
- If using features such as suspend, resume or restoring VM snapshots, be careful to not create a shared storage conflict of ownership. Always mount shared storage on the primary VM. If the secondary VM claims ownership while the primary is still active, it may result in a crash or the cluster failing.
- If your system has native hypervisor H/A capabilities, then take advantage of those, and only deploy Cisco UCS Central in standalone mode.
- Register all domains to your HA-capable Cisco UCS Central instance at the primary site.
- Perform scheduled backups of Cisco UCS Central and all registered Cisco UCS Manager instances through the Cisco UCS Central interface.
- If a disaster occurs, you can restore Cisco UCS Central to the new site through the backups.

Note Cisco UCS Central is not required for Cisco UCS domain availability, since Cisco UCS Central is not in the primary data path. Cisco UCS Central is the mechanism to configure, manage, and view the domain, from the control plane.



CHAPTER 19

General Best Practices

Platform Emulators

The best way to get oriented and familiar with Cisco UCS Manager and Cisco UCS Central, while minimizing risk, is to take advantage of the Platform Emulators.

The Platform Emulators (PE) run as virtual machines, yet are complete instances of Cisco UCS Manager and Cisco UCS Central. They maintain the Cisco UCS management information tree, and data management engine. They support the use of the Cisco UCS XML API. In addition, you can import both the physical hardware configuration and the logical configuration of an actual Cisco UCS domain.

With the PE, Cisco UCS administrators can effectively model their entire Cisco UCS environment. You can use a sandbox to configure all changes, testing, and everything else, without any impact to the actual production domain. You can also use modeling to facilitate a formal change management sign-off for Cisco UCS Central training.

For testing any integration with Cisco UCS Central, ensure that you use the latest version of the PE.

General Best Practices

Your Cisco UCS Central adoption approach depends primarily on whether you are using a Brownfield environment or a Greenfield environment.

- Use global operational policies, global fault and inventory reporting, and global statistics universally, regardless of workload profile and existing Cisco UCS deployments.
- Understand that new deployments that are 100% globally managed generally do not risk any namespace collision, or conflicts. Therefore, they do not require such attention (“G-“ prefix for managed objects).
- Try to restrict new workloads to new domains that are exclusively globally managed.
- Try not to mix global pools, policies, templates, local service profiles in domains that are also locally managed. This helps avoid name collisions and conflicts in local service profile creation and deployment. If a domain does mix local and global objects, use a segregated organization structure to reduce the potential for naming collisions and conflicts.
- Do not import default objects.
- Use named polices that communicate what the policy does, rather than a default named policy. Someone can accidentally change or hide the value-property behind the name. For example, you might make the mistake of changing a default scrub policy, one that is normally set to **no** for disk scrub or BIOS setting scrub, to **yes**. This would have catastrophic effects on local service profiles disassociated from blades containing local disk-installed operating systems.
- Use the Cisco UCS Platform Emulator to model and test an adoption procedure.

The https://communities.cisco.com/ucs community site hosts valuable content related to Cisco UCS Central and adoption. It includes Brad TerEick’s helpful blog Cisco UCS Central and My Existing Environment - How do I get there?

UCS Central Best Practices

- Ensure that the Cisco UCS Central installation disk (local or remote) read-speed is greater than 125 Mbps. Disk read-speed is critical for UCS Central HA-mode architectures.
- Ensure that your network has less than 500-ms network latency between Cisco UCS Central and any managed UCS domain.
- Ensure that there is 1.5-Mbps bandwidth between the Cisco UCS Central server and any remote UCS domain that it is managing.
- Perform daily backups and configuration exports of Cisco UCS Central and all registered UCS domains. Use the remote-copy feature and copy files to an external file directory.
- Leverage Hypervisor snapshots to protect Cisco UCS Central, especially prior to any upgrades.
- Always register UCS domains to Cisco UCS Central using the FQDN (Fully Qualified Domain Name). Do not use the IP address.
- Always make sure UCS domains and Cisco UCS Central have a valid time source configured before attempting any registration of the UCS domain to Cisco UCS Central.

- Never unregister a UCS domain from Cisco UCS Central that contains global objects pushed down to the UCS domain. Only unregister if there is no intention of ever registering the specific UCS domain back to Cisco UCS Central. Also, perform this with the guidance of Cisco TAC, backed with Cisco UCS Central Engineering approval.
- In mixed Greenfield and Brownfield environments, consider naming all Global ID pools, policies, templates, and service profiles with a prefix such as "G-" to differentiate global objects from local UCS domain objects.

Local Affinity Issues

As you centralize policy and control in Cisco UCS Central, certain challenges may surface that highlight issues best managed with local resources and control points. These are called Local Affinity issues when referencing local domains. The common affinity points are:

- External IP pool (global-ext-mgmt)
- Boot policies
- VLANS and VSANS

External IP Pools Affinity Issues

External IP pools (global-ext-mgmt) contain the addresses for out-of-band management of physical blade servers. However, Cisco UCS Central does not automatically associate these addresses with blade servers and with the CIMC, unlike Cisco UCS Manager.

With UCS Central, there is no hardware-assigned management IP address. Therefore, Cisco UCS Central assigns management IP pool addresses to the global service profile. For greater flexibility and global service profile migration to UCS domains with different management subnets, consider leveraging ID Access Control policies.

Workaround

Use management IP addresses associated with service profiles, or templates, so that Cisco UCS Central can reference global external IP pools.

Note The behavior of external management IP pools is different in Cisco UCS Central than in Cisco UCS Manager. New global service profile support for ID range-qualification policies provides greater ability to maintain flexibility and efficiency in assigning global management IP addresses.

VLAN and VSAN Affinity Issues

To mitigate local affinity issues for VLANs, use the VLAN ID alias feature. This translates the VLAN IDs for a domain, based on their domain group and organization permissions. VSAN aliasing does not exist, requiring you to map both the domain group and organization contexts.

Note When using a VLAN alias, do not include the actual VLAN ID in the name.

When creating VSAN names, append their respective domain group name. For example, use the "VSAN-DG" name pair when creating references such as VHBA templates.

Local Visibility of Global Objects

When you create global objects, they are not automatically presented or pushed to Cisco UCS Manager. Global objects do not appear automatically in the Cisco UCS Manager navigation pane. However, global IDs and global policies may be visible from the Cisco UCS Manager drop-down menus when you are creating or modifying local objects.

Global objects display in the Cisco UCS Manager once you deploy global service profiles to a server. This means that a local service profile, running on the Cisco UCS Manager, references the global objects. At deployment time, the local Cisco UCS Manager receives a read-only copy of the global object and its dependent objects, and then displays them in the GUI.

Hypervisor Contention

Because Cisco UCS Central runs as a virtual appliance, it is subject to resource sharing, governed by the host OS hypervisor.

One method for promoting reasonable performance characteristics is to use resource pools in either the VMware or Hyper-V environments. Resource pools ensure that you avoid or minimize CPU and memory contention for Cisco UCS Central.

To ensure that Cisco UCS Central is favored, place it in its own dedicated resource pool, with both CPU and memory share settings set to High. Refer to the Installation and Upgrade Guide for more information.

ID Range Qualification Polices for Domain Management

Use ID range qualification policies to ensure that Cisco UCS uses the correct blocks of management IPs when a global service profile is migrated from one Cisco UCS domain to another.

You can assign blocks of IPs for a domain or domain group with the ID range qualification policy. As you migrate the local service profile, a new management IP accompanies the association to the respective Cisco UCS domain.

Reducing the Number of Global Service Profile Templates

Some organizations are always looking for ways to reduce the number of global service profile templates they create and maintain in their Cisco UCS Central architecture.

One method is to leverage the hierarchy policy resolution capabilities of Cisco UCS and Cisco UCS Central. Some organizations put their ID pools at a high level, because they cannot justify the need to segregate IDs

based on the downstream organizations. Similarly, they also place the most common configuration policies high in the organizational structure.

They then rely on policy resolution for Cisco UCS and Cisco UCS Central. This allows for a policy with the same name to exist at different organizational levels, but to have different values embedded within those policies. Therefore, when they create or import a global service profile within that organization, the global service profile accesses that particular named policy with the proper values for that particular organization.

In general, define unique LAN connectivity policies and storage connectivity policies at a lower, more granular level. As long as they have the same names in the different organizations, the global service profile uses the correct policy with the correct values.

Before Upgrading Cisco UCS Central

Prior to attempting an upgrade of Cisco UCS Central:

1. Upgrade all registered Cisco UCS domains to a minimum of Cisco UCS Manager release 2.1(2a). Use the most recent maintenance and patch release in the Cisco UCS Manager release 2.1 tree if using Cisco UCS Manager release 2.1.
2. Use Snapshot Manager and take a snapshot of the VM to preserve the state of the original VM.
3. Take both a full-state backup and a config-all backup of Cisco UCS Central. Ensure that the backup state is enabled for both, and make sure that these backups are available offline.

Note During the backup, the local Cisco UCS domains lose visibility to Cisco UCS Central, but the state changes back to registered once the upgrade completes.

4. Complete all infrastructure firmware updates prior to upgrading to Cisco UCS Central release 1.5. The schedule information for infrastructure firmware update jobs does not transfer to the new release. In release 1.5, you create infrastructure firmware update jobs for maintenance groups, not for domain groups.

Do Not perform an unregister/reregister cycle for your Cisco UCS domain as part of the Cisco UCS Central upgrade.

Best Practices for Upgrading Cisco UCS Central

1. Verify upgrade compatibility. Consult release notes for Cisco UCS Manager and Cisco UCS Central.
2. Verify that Cisco UCS Central is not performing any operations. Ensure that no administrators are performing actions.
3. Verify that Cisco UCS Central does not have any pending acknowledgments.
4. Back up Cisco UCS Central. Perform both full-state and configuration backups. Store them remotely and offline.
5. From the CLI, gracefully shut down Cisco UCS Central using the shutdown command.

6 After shutdown, take a hypervisor snapshot of the existing Cisco UCS Central state.

7 Download the new version of UCS Central.

8 In the Hypervisor Manager, mount the new Cisco UCS Central ISO to the existing Cisco UCS Central VM.

9 In the BIOS, edit the Boot Order sequence so that Cisco UCS Central boots from the ISO.

10 Boot Cisco UCS Central from the ISO.

11 Select the upgrade option.

12 Complete the upgrade and automatic reboot.

13 Verify that the Cisco UCS Central upgrade was successful.

14 Back up Cisco UCS Central. Perform both full state and configuration backups. Store them remotely and offline.

For more information on performing these tasks, see the UCSC Getting Started Guide.

Upgrading Cisco UCS Central

Review all available release notes at the time of upgrade: Product Installation Upgrade Guides.

Note the version compatibility requirements:

- Cisco UCS Central 1.2(1a) and forward supports communication only with Cisco UCS Manager 2.1.2 and higher.
- Some new features of Cisco UCS Central may only be available in higher versions of Cisco UCS Manager. For example, Policy Search works with Cisco UCS Manager 2.1(2a) and higher, but Policy Import only works with 2.2(1b) and higher.

The current ISO upgrade method is documented in the Product Installation Upgrade Guides.

Cisco UCS Central Frequently Asked Questions

Q. Can you compare imports from two domains to see if they are different? If you have two domains that you think are configured the same, can you import both and find out?

A. No, Cisco UCS Central does not have a native Diff function today. It may be considered for a future release. You can create tech-support logs from Cisco UCS Central, extract the log files, and import them into an XML editor or repository that performs a Diff function, to compare two configurations.

Q. Can we export Cisco UCS Central reports in CSV or PDF format?

A. Yes.

Q. How large can the embedded database be? The documentation shows up to five domains with the embedded database, but is vague on how large the database is.

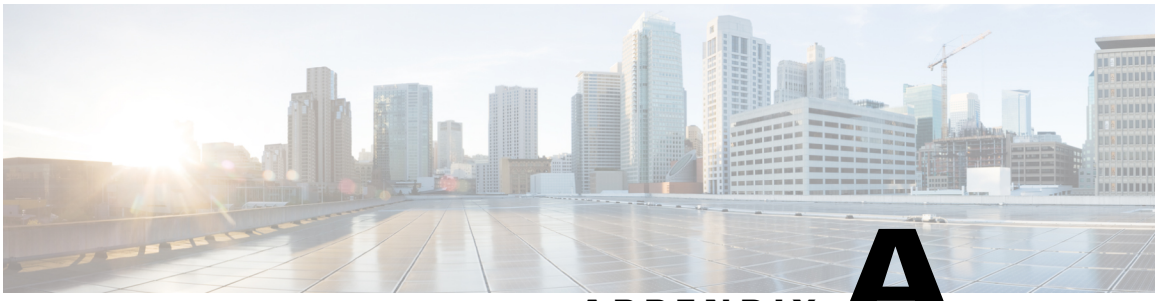
A. For five domains, it's about 240-GB. There is no limit. Cisco UCS Central can support up to 10,000 servers.

Q. Does Cisco UCS Central support alternate Disaster Recovery architectures such as VMware Site Recovery Manager (SRM)?

A. No. Use hypervisor HA tools, like VMware HA, snapshots of VMs, clones, daily backups, and targets. Backup is a Disaster Recovery functionality. Set up a remote copy. Store the remote copies on a different server, like an FTP server. If the Cisco UCS Central fails, you can deploy a new Cisco UCS Central with your backup. Also do not use clustering, use a single VM.

Q. Do I have to still use a global service profile and server association as a delivery mechanism to deliver a VLAN or VSAN down to the Cisco UCS domain?

A. No. Use local service profiles for something that has to be local. If you want to push a target, use a global VLAN service profile. Global VLANS and VSANS stay on the domains, even if you remove the global service profile. Now we have an API that you can use in the CLI to push global VLANS or VSANS down from Cisco UCS Central to a domain. Use an SSH application to access Cisco UCS Central to perform these tasks.



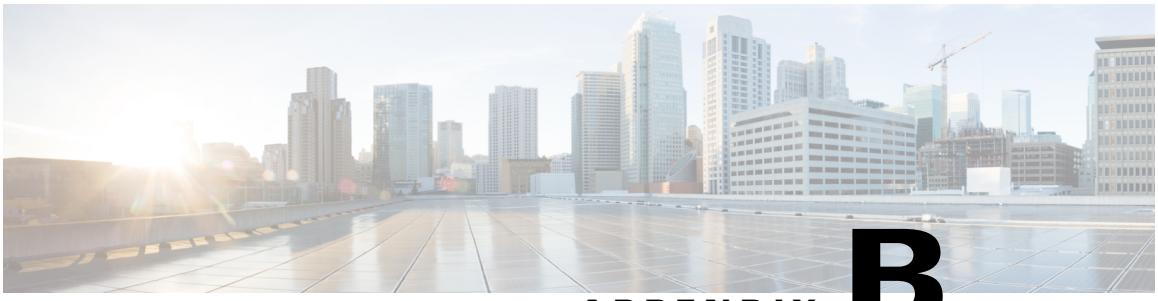
APPENDIX A

UCS Central Internal Processes Defined

UCS Central Internal Processes Defined

Service Name	Description
core-svc_cor_secAG	Implement authentication-related feature, such as local auth and remote authorization
identifier-mgr-svc_idm_dme	Manage ID pool and allocate IDs uniquely in the system
core-solr.sh	SOLR process
resource-mgr-svc_sam_snmpTrapAG	Send SNMP traps from resource manager
central-mgr-svc_centralMgr_dme	Cisco UCS Central NBAPI provider, forwards the NBAPI to a specific DME
policy-mgr-svc_pol_dme	Manage Cisco UCS Central policies
identifier-mgr-svc_sam_snmpTrapAG	Send SNMP traps from identifier manager
core-svc_cor_snmpTrapAG	Send SNMP traps from management controller
operation-mgr-svc_ops_dme	Operation manager DME
policy-mgr-svc_sam_pkiAG	Provide PKI-related service for policy manager DME
core-httpd.sh	Start httpd process
gch-call_home	Cisco GCH call home process; forwards the callhome/smartlicense message to Cisco Cloud Smartlicense Manager
service-reg-svc_sam_snmpTrapAG	Send SNMP trap from service-reg

Service Name	Description
core-svc_cor_sessionmgrAG	Session auditing for Cisco UCS Central HA implementation
core-svc_cor_dme	DME for management control, manage the configuration for Cisco UCS Central VM
resource-mgr-svc_sam_cloudAG	GCH call home/smart license application gateway
stats-mgr-svc_sam_snmpTrapAG	Send SNMP trap from stats manager
service-reg-svc_reg_dme	Implement registration service for different DME and UCSM
operation-mgr-svc_ops_imgMgmtAG	Image management application gateway for operation manager
resource-mgr-svc_rsrcMgr_dme	Resource manager DME where Cisco UCS Manager inventory is kept and manages global service profile
core-tomcat.sh	Controlling script for tomcat process
service-reg-svc_sam_controller	AG to implement Cisco UCS Central HA service
operation-mgr-svc_sam_snmpTrapAG	Send SNMP trap from operation manager
sam_cores_mon.sh	Script to monitor and manage Cisco UCS Central coredump file
core-svc_cor_controllerAG	AG to configure Cisco UCS Central VM policies
service-reg-svc_sam_licenseAG	License AG for domain base license
core-sam_nfs_mon.sh	Script to monitor NFS
gch-xosdsd	Infrastructure process for implementing GCH/smartlicense feature
policy-mgr-svc_sam_snmpTrapAG	Send SNMP trap from policy manager
stats-mgr-svc_statsMgr_dme	Stats manager that collects statistics from different Cisco UCS Manager domains and generates the statistics report



APPENDIX B

UCS Central Communications - Required Ports

Required Ports

Typically, the IP addresses for all existing Cisco UCS Manager domains exist on a common administrative network. If not, Cisco UCS Central requires that you assure routing access to all subordinate management domains. Ensure that you configure any firewalls, proxies, and anything else required to permit read/write access for the following ports, for continuous communications between Cisco UCS Central and all registered UCS domains.

Required Ports for UCSM Domains v2.2(1b) and Earlier

Open the following ports if using UCSM domains v2.2(1b) and below.

Port	Value
LOCKD_TCPPORT	32803 – Linux NFS lock.
MOUNTD_PORT	892 – Linux NFS mount.
RQUOTAD_PORT	875 – Linux remote quota server port (NFS).
STATD_PORT	32805 – Linux – Used by NFS file locking service – lock recovery.
NFS_PORT	"nfs"(2049) – Linux NFS listening port.
RPC_PORT	"sunrpc"(111) – Linux RPCBIND listening port (NFS).

Port	Value
HTTPS_PORT	”https”(443) – Communications from Cisco UCS Central to UCS domain(s) and Cisco UCS Central GUI (always required).
HTTP_PORT	”http”(80) – Communications from Cisco UCS Central to UCS domain(s). This port is configurable, and is only required for the Flash-based Cisco UCS Central GUI.
The PRIVATE_PORT (843)	Required for communication between the Cisco UCS Central Flash-based UI and the Cisco UCS Central VM. Not required for communication between Cisco UCS Central VM and remote UCSM domains. Port 843 is Not Required if using the new HTML-5 UI.

Port 80 is required for the older Flash-based UI communications. As of Cisco UCS Central release 1.4.1a, it is not possible to turn off port 80 within Cisco UCS Central. However, you can deny port 80 traffic to and from Cisco UCS Central by applying Firewall rules.

Required Ports for UCSM Domains v2.2 (2c) and Subsequent Versions

Open the following ports if using UCSM domains v2.2 (2c) and above.

Port	Value
HTTPS_PORT	”https”(443) – Communications from Cisco UCS Central to UCS domain(s) and Cisco UCS Manager (always required).
HTTP_PORT	”http”(80) – Communications from Cisco UCS Central to UCS domain(s). This port is configurable, and is only required for the Flash-based Cisco UCS Manager.
The PRIVATE_PORT (843)	Required for communication between the Cisco UCS Central Flash-based UI and the Cisco UCS Central VM. Not required for communication between Cisco UCS Central VM and remote UCSM domains. Port 843 is Not Required if using the new HTML-5 UI.

Note Port 80 is required for the older flash-based UI communications. As of Cisco UCS Central release 1.4.1a, it is not possible to turn off port 80 within Cisco UCS Central. However, you can deny port 80 traffic to and from Cisco UCS Central by applying firewall rules.

Required Ports for UCSM

Open the following ports so that UCSM works with Cisco UCS Central. Cisco UCS Central accesses the following ports.

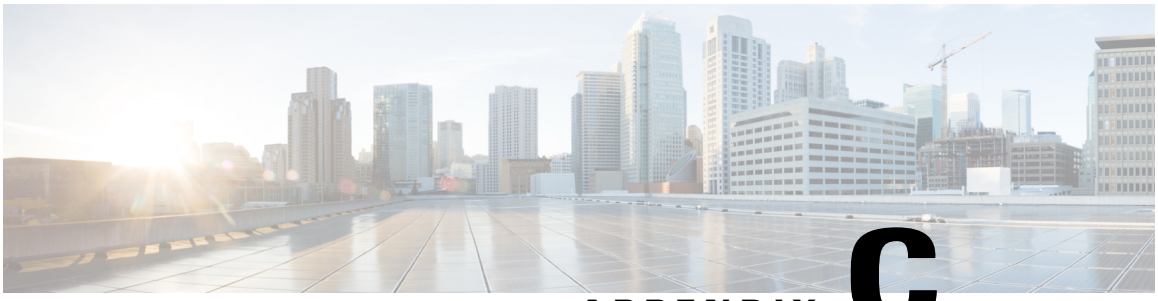
Port	Value
HTTPS_PORT	”https”(443) – Communications from Cisco UCS Central to UCS domain(s) and Cisco UCS Central GUI (always required).
HTTP_PORT	”http”(80) – Communications from Cisco UCS Central to UCS domain(s). This port is configurable, and is only required for the Flash-based Cisco UCS Central GUI.

Port 80 is required for the older Flash-based UI communications. As of Cisco UCS Central release 1.4.1a, it is not possible to turn off port 80 within Cisco UCS Central. However, you can deny port 80 traffic to and from Cisco UCS Central by applying Firewall rules.

Required Ports for Active Directory Server

Open the following ports on the Active Directory server. Cisco UCS Central uses these ports for LDAP Integration with the AD Server.

Port	Value
LDAP Port 389	Cisco UCS Central uses for integration and communication with Microsoft Active Directory LDAP
STARTTLS	Cisco UCS Central uses for supporting LDAP over SSL/TLS, also uses port 389



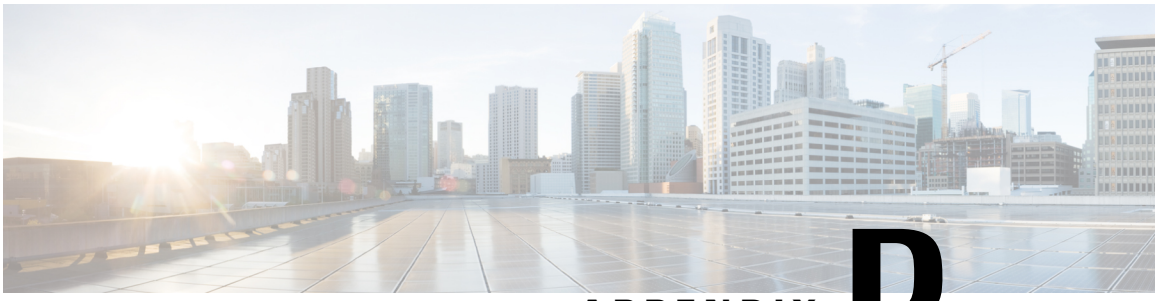
APPENDIX C

Creating a Testing & Development Environment

Creating a Testing and Development Environment

You can create your own testing and development environment. We recommend setting this up offline, thereby creating your own safe environment.

1. Download UCS Emulators and install in your test lab.
2. Download UCS Central and install in your test lab.
3. Register test emulators to test Cisco UCS Central.
4. Import operational configuration export, from Cisco UCS Manager, or build Cisco UCS Central to match production.
5. Import operational configuration export, from Cisco UCS Manager, or build UCS domains to match production.
6. Test scenarios and operations, such as migrating local service profiles to global service profiles.
7. Test automation and the PowerTools Scripts against the API.



APPENDIX D

Online Resources

Online Resources

- UCS Communities - Tech Talks
- UCS Emulator
- DEVnet Learning Labs
- UCS Central PowerTools
- UCS PowerTools
- Cisco dCloud
- UCS Central Documentation
- UCS Tech Talk - UCS Manager Documentation Videos

Online Resources