Cisco UCS Central Best Practices

Updated for Release 1.3(1a)

Revision 2.4.0 2 July 2015

Table of Contents

Forward for the UCS Central 1.3 Release – Release Summary

It is imperative to know that the contents of this document refer to the legacy "Flash Based" UI exclusively, and that the new 1.3 HTML-5 UI, is beyond the scope of this particular document. Please know there will be a follow-on document very soon that addresses working with the new HTML-5 UI.

The UCS Central 1.0 release[1] introduced:

- Global Inventory, Faults, Logs
- Global ID Pools (UUID, MAC, WWNN, WWPN)
- Global Firmware Updates, Global Backups
- Global Administrative and Operational Admin Policies

The key features for the 1.1(1a)[2] release included:

- Global Policies
- Global Service Profiles and Global Templates
- Statistics on External Database for historical reporting
- High-Availability for UCS Central Virtual Machine in Cluster-mode

The UCS Central 1.1(1b)[3] release introduced:

- Enhanced LDAP Support, including:
  - LDAP Group Maps
  - Nested LDAP Groups

1.1(2a)[4] was a major feature release, whose features included:

- Search and Import Policies and other Resources from UCS Manager
- Remote Equipment Actions – Power On/Off, LED, Acknowledgement, etc.
- Nested LDAP Groups
- Sequential IDs
- VLAN/VSAN localization/globalization
- Scheduled Backups to Remote File Share
- Separate UCS Central Operational Policies
- Backup to Remote File Location
- Microsoft SQL Database Support for Stats database
- 3rd Party Certificates Support

[1] UCS Central 1.0 Release Notes: http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/UCS_28314.html
[2] UCS Central 1.1(1a) Release Notes: http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/RN-CiscoUCSCentral_1-1.html
[3] Introduced in UCS Central 1.1(1b): http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/RN-CiscoUCSCentral_1-1.html#pgfId-119367
[4] UCS Central 1.1(2a) Release Notes: http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/RN-CiscoUCSCentral_1-2.html

- Multi-Version UCSM Support
- Authentication Domain Selection
- Improved Reports (Power Consumption, Temperature, Fan Speed, etc.)

The 1.2(1a)[5] release has the following features:

- Support for "UCS-Mini" (aka Cisco UCS 6324 FI-IOM), as well as Classic UCS
- Support for the Virtual Management Information Tree (VMIT) for the XML/API
- Ability to Configure FI ports
- Estimate Impact on Reconnect
- Unified KVM Launch Manager
- Fault Summary and Pending Activity Panel
- Precision Boot Order Control
- WAN Optimizations (1.5 Mbps min bandwidth, 500ms max network latency)

The 1.3.1a[6] release has the following features:

- NFS Shared-Storage Clustering for UCS Central HA
- UI Polling Enhancements for Fault Roll-up
- Added a New HTML5 GUI with New Search-Based, and Task-Based Contexts
- M-Series Support
- Global SPs can leverage ID Pool Qualifiers
- Ability to Schedule Backups
- KVM Hypervisor Support
- Ability to push Global VLANs/VSANs to UCS Domains without using a Global SP association.
- Domain Specific ID Pools that can be used in Global Service Profiles

In terms of scale, UCS Central is designed to manage 10,000 servers, corresponding to roughly 70 – 125 UCS Management domains, depending on domain size. UCS Central 1.3 has been rigorously tested with more than 200 UCS Domains and more than 6000 Service Profiles.

Introduction/Goals/Audience/Scope

Cisco UCS Central simplifies UCS Management --- From a single UCS domain to multiple Cisco UCS domains, including Cisco UCS-Mini[7], UCS Central delivers standardization, aggregation, global policy enforcement and global ID consistency. While UCS Manager provides policy-driven management for a single UCS domain, UCS Central is aimed at the management and monitoring activities of UCS on a global basis. These capabilities extend across multiple UCS Management domains worldwide; providing an even greater degree of administrative power, operational efficiency and policy-driven automation.

This document is intended for UCS administrators (of single or multiple UCS management domains). It will assist in understanding the procedures and impacts to adopting UCS Central. An experienced level of UCS Administration is assumed. This document is intended as an accompaniment, and not a replacement, for the UCS Central product reference guides and documentation[8].

[5] http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/RN-CiscoUCSCentral_1-2.html
[6] http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/ucs_3_0_rn.html
[7] http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-central-software/tsd-products-support-series-home.html
[8] http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-mini/tsd-products-support-series-home.html

Standard Abbreviations

The following standard abbreviations are used throughout this document

Abbreviation	Stands for
UCSM	UCS Manager
SP	Service Profile
LSP	Local Service Profile
GSP	Global Service Profile
DG	Domain Group

UCS Central Version, OS and Feature Compatibility

There are version compatibility requirements between UCS Central, the underlying host OS, and the managed UCS Domain's specific UCS Manager release, as follows:

UCS Central Version	Supported Host OS versions	Min Supported UCSM versions[9][10]	Support different versions of UCSM
1.0(1a)	VMware : ESX4.0u2, 4.1u1, 5.0 Windows : W2K8R2 SP1	2.1(1a)	No
1.1(1a/b)	VMware : ESX4.1u2, 5.0, 5.1 Windows : W2K8R2 SP1, W2012	2.1(2a)	Yes: 2.1(2a), 2.1(3a), 2.1(3b), 2.2(1b),2.2(1c)
1.1(2a)	VMware : ESX4.1u2, 5.0, 5.1, 5.5 Windows : W2K8R2 SP1, W2012	2.1(2a)	Yes : 2.1(2a)/2.1(3x), 2.2(1x), 2.2(2x)
1.2(1a)	VMware: ESXi 5.0u3, ESXi 5.1, ESXi 5.5, ESXi 6.0 Windows: W2K8R2 SP1, W2012,	2.1(2a)	Yes: 2.1(2a)/2.1(3x), 2.2(1x), 2.2(2x), 2.2(3x), 3.0(1x)
1.2(1f)	VMware: ESXi 5.0u3, ESXi 5.1, ESXi 5.5, ESXi 6.0 Windows: W2K8R2 SP1, W2012, MS Hyper-V Server 2012 R2	2.1(2a)	Yes: 2.1(2a)/2.1(3x), 2.2(1x), 2.2(2x), 2.2(3x), 3.0(1x)
1.3.1a	VMware: ESXi 5.0u3, ESXi 5.1, ESXi 5.5, ESXi 6.0 Windows: W2K8R2 SP1, W2012, MS Hyper-V Server 2012 R2, RHEL KVM Support	2.1(2a)	Yes: 2.1(2a)/2.1(3x), 2.2(1x), 2.2(2x), 2.2(3x), 2.2(4x), 2.5(1a), 3.0(1x), 3.0(2x)

[9] Using the latest patch releases is always recommended

[10] While 2.1(2a) is supported, the 2.1(3b) release is strongly urged for the 2.1 release train

Some new features of UCS Central may only be usable in newer versions of UCS Manager. For example, Policy Search works with UCSM 2.1(2a) and newer, but Policy Import only works with 2.2(1b) and newer. Please see the following table for details on features that are available for only specific combinations of UCS Central and UCS Manager:

Cisco UCS Central Features	Support Cisco UCS Central Versions	Supported Cisco UCS Manager Versions						
		2.1(2a) 2.1(3x)*	2.2(1x)	2.2(2x),	2.2(3x)	2.2(4x) GA Soon	2.5(1a)	3.0(1x) 3.0(2x)
Multi-version management support and viewing supported UCS Manager features	1.1(2a)	No	Yes	Yes	No	Yes	Yes	Yes
Importing policy/policy components and resources		No	Yes	Yes	No	Yes	Yes	Yes
Specifying remote location for backup image files		No	No	Yes	No	Yes	Yes	Yes
3rd Party Certificate		No	No	Yes	No	Yes	Yes	Yes
IPv6 in-band management support		No	No	Yes	No	Yes	Yes	Yes
Estimate Impact on Reconnect	1.2(1a)	No	No	Yes	Yes	Yes	Yes	Yes
Precision Boot Control		No	Yes	Yes	Yes	Yes	Yes	Yes
HTML 5 GUI	1.3(1a)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NFS HA Support		Yes	Yes	Yes	Yes	Yes	Yes	Yes

Note:
Searching for policy/policy components or resources is supported in Cisco UCS Manager, releases 2.1(2x) and 2.1(3x). To import policies, you must have Cisco UCS Manager, release 2.2(1b) or higher.

UCS Central 1.3(1a) is expected to work with one or more new releases of UCS Manager when they are released.

Cisco UCS Manager Release 2.5(1a) can only be registered with Cisco UCS Central, Release 1.3(1a) or higher.

Prior to attempting an upgrade of UCS Central to 1.2(1a) and beyond, all registered UCS domains must first be upgraded to a minimum of UCSM 2.1(2a)

In order to be in compliance with the OS Support Matrix, be sure to upgrade the hypervisor Host OS first, if needed, before upgrading UCS Central.

Starting with UCS Central version 1.1(2a), and going forward, there is a “features exchange” during the registration process. This features exchange allows UCS Central to be aware of the features/capabilities of a given UCSM version, thus eliminating future version interlock dependencies.

UCS Central Virtual Machine (VM) system requirements

UCS Central concentrates monitoring, configuration and management across multiple UCS domains and across potentially thousands of servers. There are desirable minimum performance requirements for the UCS Central VM (primarily around disk access) to ensure problem-free operations.

Administrators also need to make sure that the underlying VM storage is sized appropriately for the 80GB VM. If cluster mode is enabled, the shared storage disk needs to be at least 40GB.

UCS Central serves as an image repository for all firmware bundles. If leveraging UCS Central for firmware management, plan for approximately 2.0 GB for each UCS Firmware Release Bundle (Infrastructure, B-Series Blade, C-Series Rack and M-Series) that are fully downloaded and stored in the local Database.

Free space monitoring within the UCS Central VM can only be shown through the CLI. Login from the VM CLI (not the GUI), and type "***scope monitoring; show storage***" to view the percentage of used disk space in the VM.

UCS Central should be deployed on a high-speed datastore, preferably provisioned from high speed SAN. It is **HIGHLY** recommended that the Read speed of the remote storage should be greater than 125 Mbps from a performance perspective.

The underlying VM structure of UCS Central requires:

- 4 vCPU (cores)
- 12 GB Memory
- VM virtual hardware version format change from version 7 to 8 (relevant for VMware only)

Management Access for UCS Central to UCS domains (ports, firewalls etc.)

Typically, the IP addresses for all existing UCS Management domains exist on a common administrative network. If this is not the case, UCS Central will work, provided that routing access is assured from UCS Central to all subordinate management domains. For this reason, care must be taken to ensure that any firewalls/proxies/etc. are configured to permit read/write access on the following ports for continuous communications between UCS Central and all registered UCS domains:

LOCKD_TCPPORT=32803 – Linux NFS Lock
MOUNTD_PORT=892 – Linux NFS Mount
RQUOTAD_PORT=875 – Linux Remote Quota Server Port
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
HTTPS_PORT=”https”(443) – Communications from UCS Central to UCS Domain(s).
PRIVATE_PORT=(843) – UCS Central communications from Flash UI to UCS Central VM.

For sites running Cisco UCS Mini with UCS Manager 3.0(1) and UCS Central 1.2(1a), the only required open firewall port between UCS Central and UCS Mini is HTTPS (port 443).

The PRIVATE_PORT (843) is still required for communication between the UCS Central GUI and the UCS Central VM, but not between remote UCSM domains. Port 843 is required in order to use the legacy Flash-based UI, but Port 843 is Not Required if using the new HTML-5 UI.

Also, any firewall session timeout limits for these ports should be reviewed with respect to sessions being dropped due to inactivity. For the full list of installation pre-requisites, please refer to the UCS Central Installation and Upgrade:
http://www.cisco.com/en/US/products/ps12502/prod_installation_guides_list.html

UCS Central licensing

With UCS Central, the first 5 domains (Cisco Part Number: L-UCS-CTR-INI=) are currently licensed at no charge and additional domains (Cisco Part Number: L-UCS-CTR-LIC=) beyond the 5th domain, at a charge. Support for the initial or additional domains is available as a paid option with the licenses. There is a 120-day “grace period” after the registration of the first domain. Any number of domains can be registered during the “grace period”. After the expiration of the grace period, a license will be required to prevent licensing Fault Alarms within UCS Central.

At any time during the 120-day trial period, an initial license (“L-UCS-CTR-INI=”) can be obtained through the standard Cisco Sales ordering process. At this time, the INI= license price is $0 and does not include support. Additional licenses – beyond the first 5 domains – can be purchased using “L-UCS-CTR-LIC=”.

Additional charges for support/maintenance may also be required. Failure to activate licenses may result in faults being generated in UCSM, indicating that the domain has ended its 120-day grace period. Licenses may be purchased through the same channels as other Cisco products.

Terminology

The Definitions table below applies to naming conventions and terminology:

Term	Description
UCS Manager	Embedded ASIC software within the UCS Fabric Interconnect that manages a UCS Domain
UCS Domain	A collection of resources managed by a UCS Manager – also the client for UCS Central
UCS Central	Virtual Appliance that aggregates and simplifies the management of one or more UCS Domain(s)
Domain Group	Named grouping of multiple UCS domains, based on configuration similarities and often based on geography. Operational Policies are applied with respect to domains in a Domain Group
Sub Domain Group	A child of the Domain Group. Inherits its properties from the parent. Can have specific local policies for the domains in the sub Domain Group
Ungrouped Domains	Domains that do not belong to any Domain Group. Upon UCS Domain Registration, No Operational Policies are inherited until a UCS Domain is placed within a Domain Group
Local	Reference to an object that is owned and modifiable in a single UCS Manager domain, e.g. Local policies or Local pools.
Global	A reference to an object that is owned and modifiable in UCS Central, e.g. 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 from UCS Central. (e.g. “Use Local” action in UCS Manager GUI)
Globalize	Change a Pool or Policy reference from Local to Global. (e.g. “Use Global” action in UCS Manager GUI) Creates a “reference” to a global object. If the global does not exist, then the reference is not satisfied. User must create the global object to satisfy the reference. If no global object exists, the reference will remain in a “Pending Global” state.
Register	Initial process through which a UCS Manager connects to UCS Central and sets up “management” of itself from UCS Central.
Unregister	Intentional removal of UCS Domain from UCS Central management[11]
Lost Visibility	Unintentional loss of connectivity between UCS Manager and UCS Central
Suspend State	Management communications between UCS Central and UCS Manager is intentionally halted. Not an “Unregister” operation. UCS Manager is

[11] This is not recommended unless the desired un-registration is permanent

	registered with UCS Central but there is no management communication between the two[12]
Acknowledge State	Normal state between UCS Central and UCS Manager Management communications is re-established between UCS Central and UCS Manager

For UCS Fabric Interconnects, managing 1 to 20 Chassis, the use of the terms "Pods", "Clusters" or "Blocks" should be avoided, in favor of "Domain". Past usage of certain terminology in a single UCS Manager context may need revisiting in the truly global and multi-UCS context of UCS Central. For example, prior to UCSM 2.1, VLANs were referred to as "global" for scope, but only within the context of a single domain. Going forward, a common understanding of names/terms/contexts is essential.

Ownership

The terms "Local" and "Global" are typically used in relation to UCS Managed Objects (MO's), such as pools, policies, service profiles, adapters, blades, chassis, etc. Managed objects are "owned" either locally (by a given UCS domain) or globally (by UCS Central). An object that is owned locally has "read-write" access by the local domain, but "read-only" access by UCS Central. Correspondingly, an object that is owned globally has "read-write" access by UCS Central, but "read-only" access by any local domain. While UCS Central does own a global object, it does not ever directly modify a local "copy" (at the domain level); instead, UCS Central will update the global object in UCS Central and then issue an "update event" to the XML-API to then update the local copy of that global object.

UCS Central: "Greenfield" and "Brownfield"

There are two distinct contexts, under which UCS Central deployments are considered: Existing UCS deployments ("Brownfield") and brand new UCS deployments ("Greenfield"). Understanding this distinction early on may help in the naming conventions, as discussed in Section 4 Global Operational Policies, and also in the adoption process discussed in Section 8 UCS Central Adoption: Approaches and Challenges.

Customers with existing UCS deployments need to be aware of certain restrictions and limitations related to UCS Central deployment. From UCS Central 1.2(1a) release forward, Pools, Policies and Templates can be "imported" from a local domain to UCS Central. However, this does not apply to individual Local Service Profiles. Service Profile Templates can be imported and "globalized", but individual Local Service Profiles cannot. Therefore, any considerations for globalizing workloads from an existing UCS deployment should focus on Policies and Service Profile Templates, but not individual Local Service Profiles.

[12] Typically initiated by a UCS Domain, due to an unexpected state. For example if UCS Central was restored to an older version, and the UCS Domain receives and older version of a policy during regular policy resolution.

"Best Practices"

The term "Best Practices" is intended more as a set of guidelines, recommendations and suggestions --- not the only way to perform desired functions. The only real "Best Practice" is whatever works best for your specific organization and operating requirements, factoring the appropriate context and any exceptional conditions.

Flexibility, adaptability, and consistency are all hallmarks of UCS Manager, and carry forward as architectural goals for UCS Central. The UCS Central management model's impact differs significantly from the standalone, local management model. Administrative power is *highly* concentrated within 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 (A Test environment with a UCS Central Instance and registered UCS Emulators can quickly be installed and used)
- 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 Estimate Impact to be set to run on most applicable actions.
- Use Maintenance polices for Service Profiles, and Service Profile Templates set to USER-ACK.

UCS Central is not a replacement for UCS Manager. In fact, UCS Central is integrated with and leverages UCS Manager to perform or carry out its actions. UCS Central is designed as the way to centralize policy definition and to create pools of global identifiers that can be consumed across multiple UCS domains in a consistent manner. Over time, even as more functionality becomes available through UCS Central, UCS Manager will continue to be the interface for direct management of the UCS domain, as well as the vehicle for enforcing consistency of global policies.

1. Domain Group (DG) Design

Domain Group (DG) hierarchy design is one of the more important architectural design decisions. There is no right/wrong way. The goal for this feature is to best reflect your specific environment and management design choices. Regardless of DG partitioning schemes, the following attributes of DG's should be understood:

- A Domain Group (DG) is arbitrary grouping of individual UCS domains. Grouping design is left to the UCS Central Administrator. There is nothing within the context of an individual UCS domain that creates affinity for a particular Domain Group. In fact (and very important) --- within the context of an individual UCS domain, there is absolutely no concept/notion whatsoever regarding a "Domain Group". A DG is purely a UCS Central global construct.
- UCS domains can be a part of only one DG at a time. Unlike Server Pools, where one server can be in multiple Server Pools, a given UCS domain can only be in one DG at a time.

- All UCS domains by default are placed in the "Ungrouped Domain Group" at registration. Domains in the Ungrouped DG WILL NOT resolve any global operational policies, even if the local UCS administrator has opted-in for "global policy resolution control".
- Operational policies are defined on a per DG basis, and are in effect for all domains in the DG. A DG is where all Operational Global Policies are resolved or applied.
- UCS domains can be moved between DGs. However, any DG-to-DG move for a domain can be disruptive depending on the policies in the target/destination DG. UCS Domains resolve their own policies from DG's in which they reside. If a new domain joins a DG, then the new Global Operational Policies will be applied --- which may impact service. This is particularly important when considering Global Firmware Management. Realize that more than one registered UCS Domain in a given DG with a Global Firmware Policy would all be subject to the policy definitions for that Firmware, and would all be subject "simultaneously" for any changes or upgrades to that Firmware Policy.
- Newly registered domains can "auto-join" a DG based on qualification policies at registration time. Domain Group Policy Qualifications work in a similar manner to Server Pool Policy qualifiers. ("Equipment -> UCS Domains -> Policies")
- Global Operational Policies can be defined anywhere in the DG hierarchy, and can then be overridden by policies defined at a lower, subordinate DG policy.
- When moving a Domain to a new DG, the policies that are currently binding for the old DG are not necessarily removed (or reset). Instead, the previous operational policies remain in place, unless the new operational policies overwrite the previous ones. If the old policies are not over-written by new binding policies, then the current operational policies remain in place as 'non-binding' policies[13].
- Sub-domain Groups can be created and nested hierarchically for finer granularity of policy control. The degree with which sub-domains are employed should be weighed against the amount of additional administration/management required for managing the different sub-domains.
- Sub-domain Groups can be nested up to 5 levels deep.

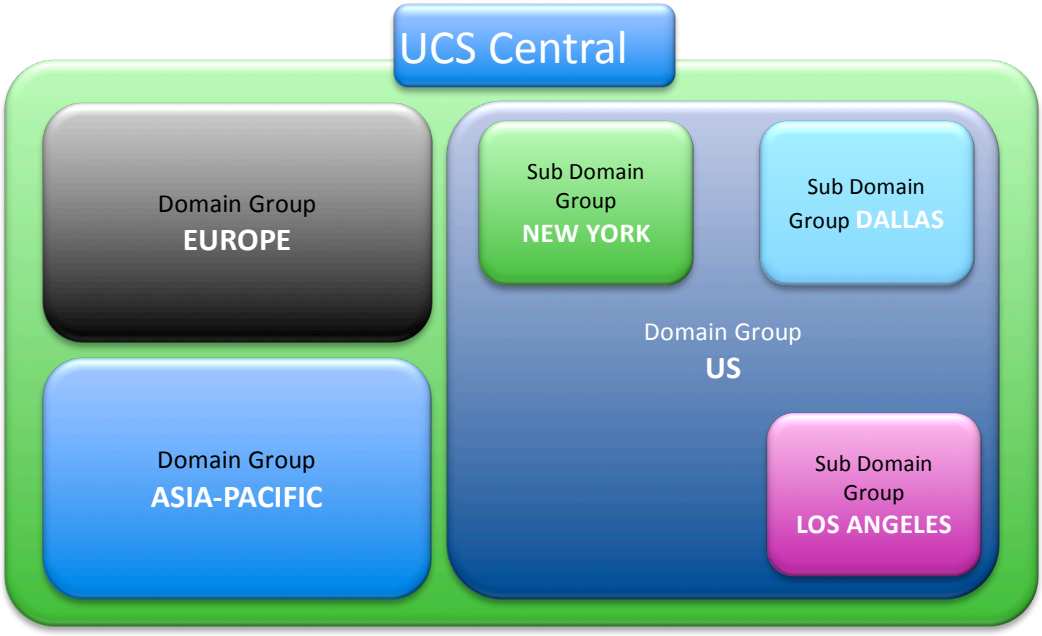
Some examples that might serve as the basis for DG partitioning include:

- Geography (e.g. Europe, Asia, USA, etc.), which includes Timezone considerations.
- Organizations, Business Functions, Business Units (e.g. Mktg, Engr, Finance, HR, etc.)
- Production Criticality (e.g. Prod, Dev, Test/QA, etc.)
- Network Domains (e.g. Internal Networks, DMZ, External Network, etc.)

[13] Policies, which are resolved, based on reference, like host packs, maintenance policy, schedules, firmware distribution bundles (Infra, B, C) will be removed if they are not present in the new domain group. Among the operational policies that are resolved based on operational policy controls (local-global radio buttons within UCSM), named policies like roles, locales, trust points will be removed if they are not present under new domain groups.

Best Practice

Geography has emerged as the most common basis for DG partitioning. Domains in the same geography most often require the same administrative and operational settings.



Domain Group hierarchy example, based on Geography

Domain Groups should be used to help simplify configuration and deployment of operational policy. Use of Domain Group hierarchy should only be used when it best fits the operational challenge.

2. UCS Central Authentication

UCS Central version 1.2(1a) forward supports either local[14] or LDAP based authentication. Other authentication types such as TACACs+ or RADIUS are currently not supported for UCS Central itself, but UCS Central can be used to configure these authentication types for UCSM through operational admin policies. UCS Central supports one defined form of Native Authentication to be active at once (either local or LDAP). UCS Central does allow selecting from multiple authentication domains and does not currently support the ability to configure multiple authentication realms like UCS Manager does.

UCS Central version 1.2(1a) introduced 3rd-party certificate support for LDAP Integration and User Authentication.

UCS Central version 1.3 now additionally supports self-signed certificates for use LDAP Integration and User Authentication.

[14] The '$' should not be used as a password character when using local authentication.

3. Policies, Orgs and Domain Groups

UCS Central provides global policies, which automatically enforce behavior that is configured to be consistent on a global basis across multiple domains.

In UCS Central, there are two major types of policies, which can be referred to as “Operational Policies” and “Workload Policies” (or Service Profile consumed policies).

a) Operational Policies

Operational Policies are the policies that are typically associated with the “Admin” tab in the UCSM GUI, such as “Call Home”, “User Management”, “Timezone”, “DNS”, etc. In UCS Central, Operational Policies are applied in the context of a Domain Group (or sub domain group) and all its associated domains. Note that since version 1.2(1a), UCS Central has its own Operational Policies under the “Administration” tab.

b) Workload Policies

Workload Policies are those that are typically associated with Service Profiles, such as “Boot Policy”, “VNIC/VHBA Templates”, “Network QoS”, “BIOS Policy”, etc. In UCS Central, Workload Policies are applied in the context of an “Organization” and all its associated “Sub-Organizations”.

Domain Groups and Operational Policies typically govern the site-specific aspects, such as those that would be sensitive in some way to physical location, geography, etc.

Orgs and Workload Policies typically govern the “logical” aspects, such as Service Profiles and their associated templates, pools, policies, etc.

There is no inherent relationship whatsoever between Domain Groups and Organizations. While UCSM has no concept of the DG “Operational” structure created within UCSC, the Organizational (Org) structure remains consistent and mutually shared between UCSM and UCS Central with a Global Scope.

c) Hierarchies

The UCS Manager is hierarchical in nature, as reflected through the “Organization” structure. For UCS Central, the hierarchical “Organization” structure takes on a global scope.

The DG structure in UCS Central is also hierarchical. One important distinction is that DG is purely a UCS Central construct and used for the mapping and application of Operational Policies to the registered UCS Domains. Local UCS domains have no visibility to DGs, but they do reflect the impact of a Domain Group specific operational policy.

Best Practice

The best practice for both Organizations and DG's is to take advantage of the hierarchy to best reflect the logical (Org) and physical (DG) 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 Workload Policies placed in the "root" Organization are meant to be exposed to the entire UCS Domain. Be aware that creating an Operational Policy in the "root" DG can have unexpectedly broad consequences[15].[16]

4. Global Operational Policies

This section refers to Global Operational Policies and not Service-Profile or workload-oriented policies. Configuring Operation Policies for UCS Central itself is done through the "Administration" tab[17].

UCS Central provides Global Operational Policies for one or more UCS domains --- but all participation of global policies is on an "opt-in" basis, with respect to the local UCS manager. UCS Central does not "take-control" of global policies, unless such control is first delegated from the local UCSM Domain Administrator. Note that a local UCSM Domain Administrator can subsequently "pull back" control by "opting out" of global management for a given policy.

All administrative policies are under local domain control by default and remain that way until all of the following occur:

1. The local domain is registered to UCS Central
2. The local domain is made part of a DG in UCS Central (Moved from Ungrouped Domains)
3. The local domain administrator explicitly promotes a given policy from "Local" to "Global" resolution within the UCSM Admin Tab.

There is no dependency between the various policy promotion decisions. For example, Infrastructure/Catalogue Firmware management can be globalized, while Fault Policies can still be managed locally. Within UCSM "Admin -> Communication Management -> UCS Central" all the Policies listed within the Policy Resolution Control are all independent from each other.

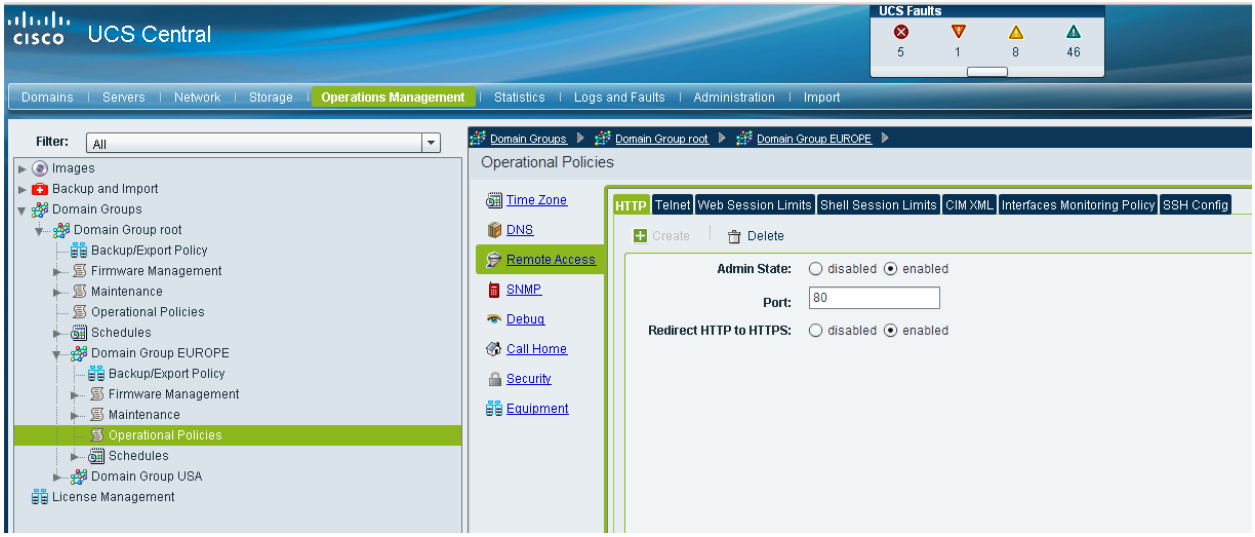
Once policy is promoted from local to global, then the effective policy definition can only be changed at the UCS Central level. This is by design, to enforce the desired consistency across domains. However, administrators may at any time decide to return to locally resolved policies. If an administrator reverts back to local management for a given policy, that policy setting remains until the local administrator changes it. UCS Central will no longer control that policy.

[15] Prior to release 1.1(2a), the Operational Policies applying to UCS Central itself were grouped in the "root" DG. Any Operational Policies under the "root" DG that were intended for UCS Central will need to be moved to the new "Administration" Tab.
[16] Operational Policies in the "root" DG will apply to all UCS domains that have chosen to opt-in on the specific operational policy.,
[17] Prior to release 1.1(2a), the Operational Policies applying to UCS Central itself were grouped in the "root" DG. As of 1.1(2a), the Operational Policies for UCS Central itself fall under the "Administration" tab.

Best Practice

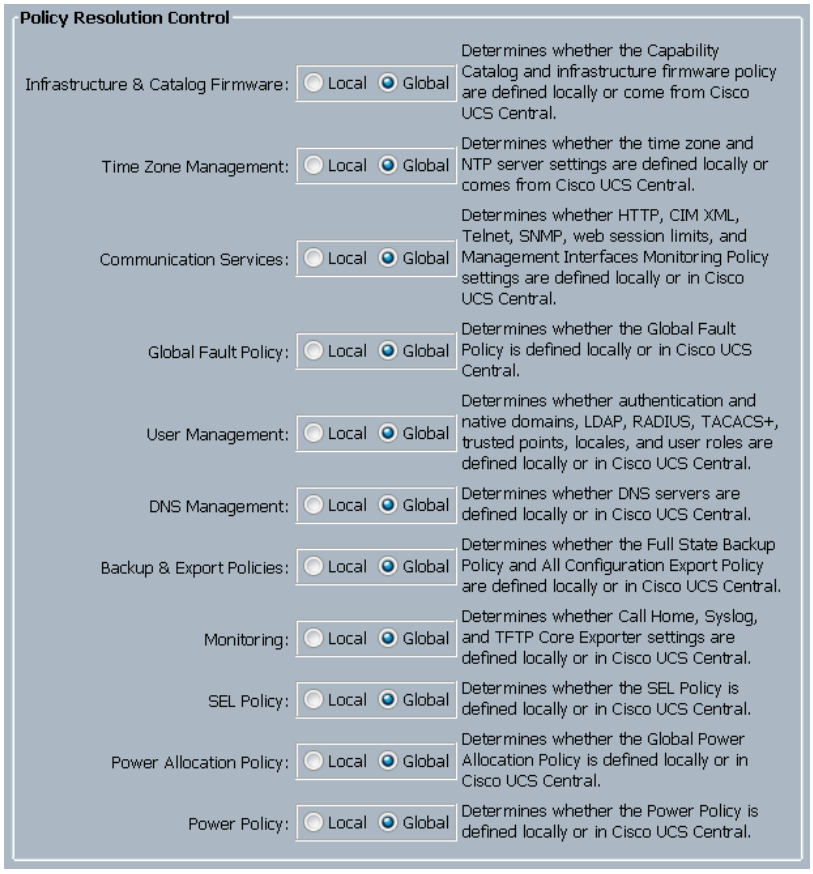
When contemplating transitioning from Local Operational Policy control to Global Operational Policy control, a general best practice would be to maintain local policy resolution and to gain comfort and understanding, prior to a broader adoption of global policies. Global policy adoption should be done on an individual policy basis, phased over time, as familiarity and comfort are gained. This is particularly true of Firmware Management. Also, try to minimize the number of transitions between local and global policy control.

UCS administrators are encouraged to take increasing advantage of policy consistency and centralized policy enforcement, whenever possible. Global consistency and policy enforcements are among the key architectural goals for UCS Central. By consolidating policy definition and configuration within UCS Central, the administrative burdens of local UCS administrators will be reduced. Keep in mind that any opportunity to define and manage policy at a higher and more central-level will promote greater administrative scalability. Administrators are encouraged to design policy towards simplicity, and to centralize policy definition, whenever possible, as a general best practice.



UCS Central Screenshot above shows Global Operational Policies for the DG "root/Europe"

UCS Manager Screenshot below shows the breakdown of each type of Global Operational Policy available for Policy Resolution Control. Each Policy is completely independent of the other as far as Local verses Global control.



UCS Manager Reference	UCS Central Reference	UCSM GUI Navigation
Infrastructure & Catalog Firmware	Operations Management -> [DG] -> Firmware Management -> Infrastructure Firmware	Equipment -> Firmware Auto Install
Time Zone Management	Operations Management -> [DG] -> Operational Policies -> Time Zone	Admin -> Timezone Management
Communication Services	Operational Management -> [DG] -> Operational Policies -> Remote Access	Admin -> Communication Management -> Communication Services
Global Fault Policy	Operational Management -> [DG] -> Operational Policies -> Debug -> Global Fault Policy	Admin -> Faults/Events/Audit -> Settings
User Management	Operational Management -> [DG] -> Operational Policies -> Security	Admin -> User Management

DNS Management	Operational Management -> [DG] -> Operational Policies -> DNS	Admin -> Communications Management -> DNS Management
Backup and Export Policies	Operational Management -> [DG] -> Backup/Export Policy	Admin -> All -> Backup and Export Policy
Monitoring	Operational Management -> [DG] -> Operational Policies -> Call Home **and** Debug	Admin -> Faults/Events -> Syslog Faults/Events -> Settings -> TFTP Core Exporter Communications Mgmt -> Call Home
SEL Policy	Operational Management -> [DG] -> Operational Policies -> Equipment -> SEL Policy	Equipment -> Policies -> SEL Policy
Power Allocation	Operational Management -> [DG] -> Operational Policies -> Equipment -> Global Power Allocation Policy	Equipment -> Policies -> Global Policies -> Global Power Allocation Policy
Power Policy	Operational Management -> [DG] -> Operational Policies -> Equipment -> Power Policy	Equipment -> Policies -> Global Policies -> Power Policy

Table above shows the correspondence of references between UCS Central and UCS Manager. The "UCSM GUI Navigation" column shows where the references will be "greyed-out" in the GUI, once the policies are configured to resolve globally at UCS Central and once the domain becomes part of a Domain Group.

a) General Best Practice

Best Practice

Take advantage of the Domain Group hierarchy to minimize the number of Operational Policies defined. Operational Policies could be segmented in to non-disruptive (e.g. “DNS”, “Time Zone”, “Call Home”, etc.), and potentially disruptive (e.g. “Firmware Management”). Administrators are encouraged to put as much non-disruptive common policy configuration as high up in the DG hierarchy as possible. Similarly, any potentially disruptive Operational Policies should be put as low in the DG hierarchy as possible.

b) UCSM-UCSC Registration

Make sure your existing UCSM Domain(s) are resolving to a reliable time-source by the NTP Server setting, and also make sure you UCS Central is resolved to the same NTP to alleviate any registration failures. **Also make sure you register the UCS Domain to the UCS Central Server using the Fully Qualified Domain Name of the UCS Central Server, verses the IP Address**. This will afford flexibility if the subnet location of the UCS Central Server changes in the future, and alleviate an unwanted Unregister/Reregister cycle.

c) Authentication

UCS Central provides the ability to globalize the configuration of the UCSM Authentication model across all registered UCS domains.

Currently, UCS Central does not provide the ability to use RADIUS or TACACS+ as authentication realms for UCS Central itself. General best practices are to aim for simplicity and to minimize/centralize the number of authentication schemes/definitions, whenever possible. Similarly, if access to multiple authentication schemes/definitions is required, then aim for simplicity when constructing the mapping of authentication schemes/definitions on to UCS Central DGs.

d) Monitoring (SNMP, Syslog, Call Home)

Generally, system health and monitoring (SNMP, Syslog, Call Home, etc) are all low-risk candidates for common Global Policy. Defining SNMP, syslog, and Call Home policies as Operational Policies as high up in the DG hierarchy as possible provides the simplest approach. All domains in the subordinate DG’s would then inherit these global policy definitions.

e) DNS management

Typically, DNS management is defined at a global/corporate level. Therefore, DNS "domain" names and DNS servers are easy candidates for Global Policy management, typically defined as high up in the DG hierarchy's Operational Policies as possible.

f) Firmware Management

Configuring Global Firmware Management ("Infrastructure and Catalog Firmware") enforces that all domains within a Domain Group (and Sub Domain Groups) are running a consistent version of the UCS Manager Firmware and Hardware Capability Catalog. Enable global policy resolution when you want to enforce consistent versions of Infrastructure firmware amongst all domains in a Domain Group.

When multiple UCS Domains are members of a DG, and the Firmware Management Control Policy within UCS Manager has been switched from UCS Manager-Local to UCS Central-Global, be careful of any Operational UCS Central (Global) firmware policy changes to that DG, or Sub-DG's. UCS Central will try to upgrade all UCS Domains that are members of that specific Domain Group and any Sub-DGs based upon the defined Maintenance Policy. Please know that the default Maintenance Policy behavior is still "USER-ACK" before any FI, or UCS Domain is updated. Also note that this behavior can be over-written with a "Scheduled" Acknowledgement or an "Immediate" Acknowledgement.

g) RBAC

RBAC (Role-Based Access Control) is typically linked in to global/corporate level authentication, such as LDAP/AD. For UCS Central, continuing to enforce central control on access would be a preferred best practice, whenever possible.

If central authentication and role management is not currently in place, then administrators would be encouraged to define role-based access within UCS Central, as high up in the DG hierarchy's Operational Policies as possible, as a best practice.

h) Power Management

Policies around Power Management include two different policies:

- "Global Power Allocation Policy". Determines whether caps are applied at the chassis level, or manually overridden at the individual blade level
- "Power Policy". Chassis-level configuration of "Non-redundant", "N+1", or "Grid" for the physical AC power.
-

The "Power Policy" is a strong candidate for central policy definition.

"Global Power Allocation Policy" is possibly the most sensitive to environmental/location dependencies, with no obvious best practice to offer.
For example:

- Power budgets per rack could vary amongst different datacenters and locations.
- Some sites may have taken advantage of Power Groups to create power caps that span multiple racks, specific to a given datacenter layout.

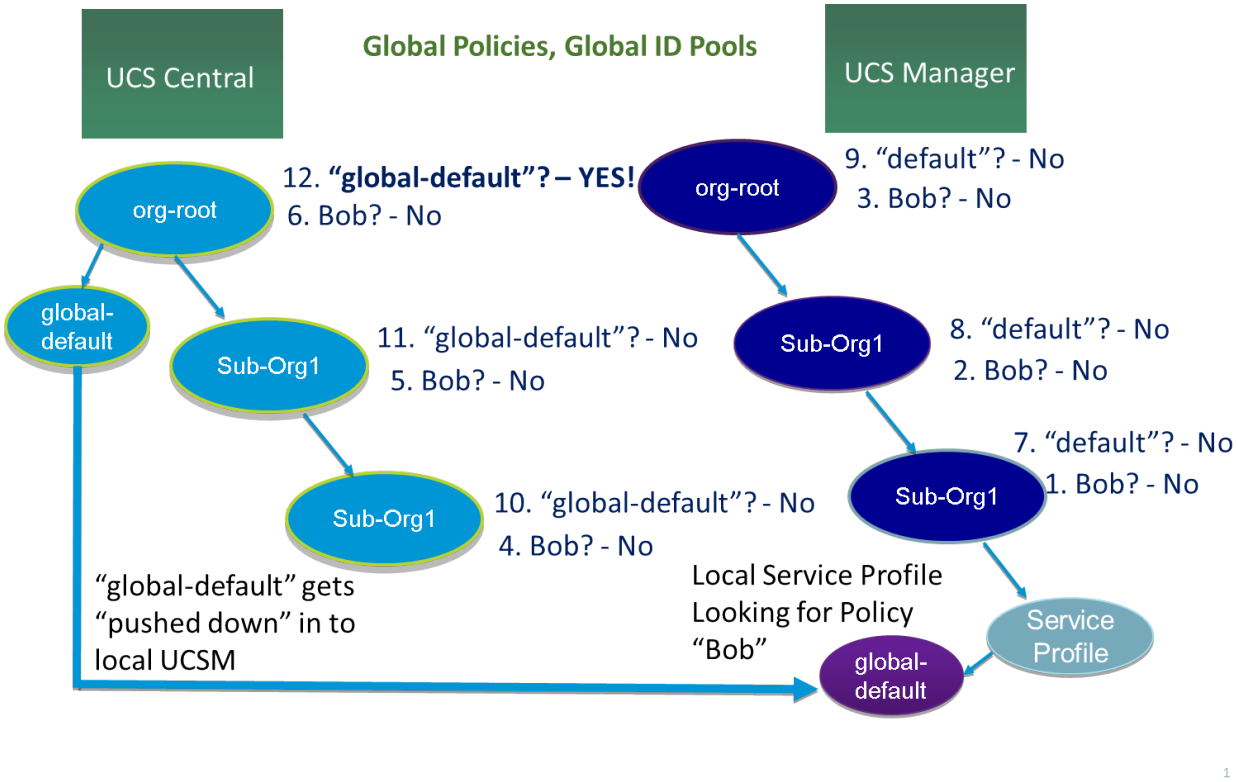
The "Global Power Allocation Policy" is very dependent on local constraints. Definition schemes, such as creating broadly scoped policy to restrict power on a per-rack basis would be the most simple. However, its practicality is going to be site specific and hard to generalize.

5. Pool/Policy Name Ambiguity and Resolution

Understanding of Pool/Policy name resolution is important to troubleshooting GSP association errors. Few restrictions are placed on object naming within both UCSM and UCS Central. The lack of naming constraints could in some cases lead to ambiguity. When creating managed objects, there is nothing (except best practices) that prevents the same object "name" from being defined both a locally and globally. When any policy or pool name is referenced in a Service Profile, VNIC or VHBA, a well defined "name-resolution-process" is followed by the local UCS Manager. Preference is given to local names over global names, for both pools and policies.

Resolution for locally managed objects (objects referenced by a **Local Service Profile**) happens in the following order for a given "name":

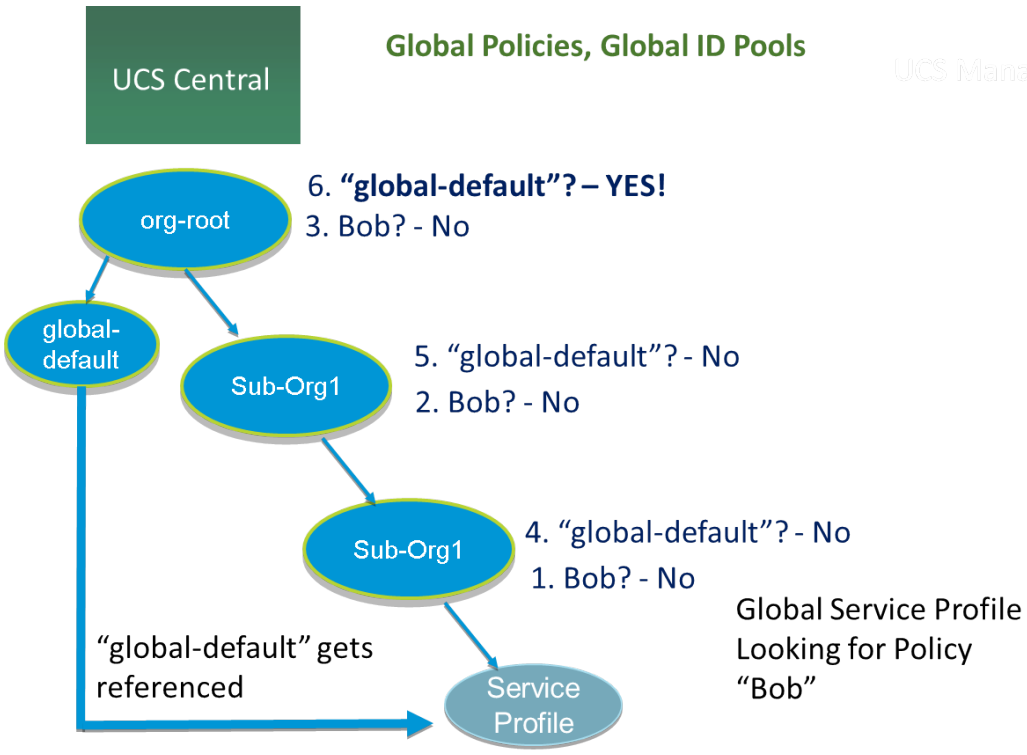
1. Use the object name if found and defined in the local org --- else…
2. Use the object name if found and defined in subsequently higher parent orgs, up through the local "org-root" --- else …
3. Use the object name if found and defined in the global org --- else …
4. Use the object name as defined in subsequently higher global parent orgs up through the global "org-root".
5. Use the values corresponding to the "default" object in the local org, and up through "org-root"
6. Use the values corresponding to the "global-default" object in the global org, and up through "org-root".



Example of Hierarchical Name Resolution Order for Policy "Bob" by a Local Service Profile

Resolution for globally managed objects (objects referenced by a **Global Service Profile** – Everything Global) happens in the following order for a given "name":

1. Use the object name if found and defined in the global org --- else …
2. Use the object name as defined in subsequently higher global parent orgs up through the global "org-root".
3. Use the values corresponding to the "global-default" object in the global org, and up through "org-root".



Example of Hierarchical Name Resolution Order for Policy "Bob" by a Global Service Profile

Note that while Local Service Profiles could reference either Local or Global pools/policies/templates, Global Service Profiles can only ever reference Global Pools/Policies/Templates[18].

Best Practice

As a best practice for avoiding ambiguity in Brownfield Deployments, administrators should not create nor use the same "name" in both local and global contexts. To avoid ambiguity, Global Policy and Pool names should have unique prefixes (Ex: "G-MAC-A" for all VNICs bound to the A-side fabric). Another best practice is to always make use of explicitly defined pools and policies, and to avoid reliance/use of the

[18] A "reference" can be either direct reference, or an indirect reference via dependency to another policy/template.

"default" and "global-default" names altogether. If you wish to modify a default policy, create and use a new named policy instead.

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 ID's	node-default	global-node-default

a) 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 for the "G-/Global-" prefix is to prevent namespace collisions. Assuming that all pools/policies/templates/etc. are all defined exclusively in UCS Central from Day One, then this prefix practice can be safely avoided.

b) Naming Policies

Throughout the UCS and UCS Central System, there are many "default" policies, whether at the Local Level within UCSM or the Global Level within UCS Central. It is highly recommended that if you intend to make changes to a default policy, to create a "New" policy that reflects those changes from the system defaults that load with the system. Then simply use the new, named policy reflecting those changes.

6. Registration and Certificates

Registration is the process by which UCS domains and UCS Central establish a trusted communication path for the first time using a shared secret. Once the initial communication is done, and security certificates have been exchanged, all subsequent communication between UCSM and UCS Central uses HTTPS and the signed certificates. Therefore, the system time must be the same between UCSM and UCS Central for registration to complete successfully.

Best Practice

Also, as mentioned previously in this document, always consider registering your UCS Domains to UCS Central using the Fully Qualified Domain Name of UCS Central, rather than the IP Address. If UCS Central in the future requires being relocated within your network, and the IP Address Changes…. the UCS Domains will still find the newly changed-IP of UCS Central registered in DNS. Otherwise, a much more disruptive Un-Register, Re-Register process will be necessary.

UCS Central supports 3rd Party Certificates. With UCS Central 1.3, UCS Central now fully supports self-signed Certificates.

Best Practice

3rd party certificates are more secure, compared to default certificates, providing users the ability to configure secure communication in the form of certificates that can be issued and/or authenticated from a valid trustpoint. A trustpoint could be from either an internal site, or an external site (e.g. Verisign, Thawte, etc.). Once 3rd party certificates are adopted, UCS Central and open UCSM GUI sessions will close; UCS Central registration will remain intact. [3rd party certificate support requires UCSM support, provided in the 2.2(2x) release and above].

7. Identifier Management

Global identifier management addresses one of the biggest challenges around UCS, multi-domain management: guaranteed unique addressing for system identifiers (MAC's, WWxN's, UUID's). Previously, UCSM best practices suggested embedding a "domain ID" within the high-order bytes of the ID pool ranges. This practice is not practical for UCS Central managed global IDs.

With UCS Central, all the ID pools can be defined and accessed globally across all UCS domains. Service Profile assignment can be guaranteed unique and non-overlapping with respect to ID's across all UCS domains.

Global ID Pools belong to the "Organization" or "org" structure. Global Pools do not depend on DGs, as the UCS Central "Operational Policies" do. Instead, the range of Global ID Pools extends across all UCS domains in the scope of the org structure within UCS Central, regardless of any DG partitioning.

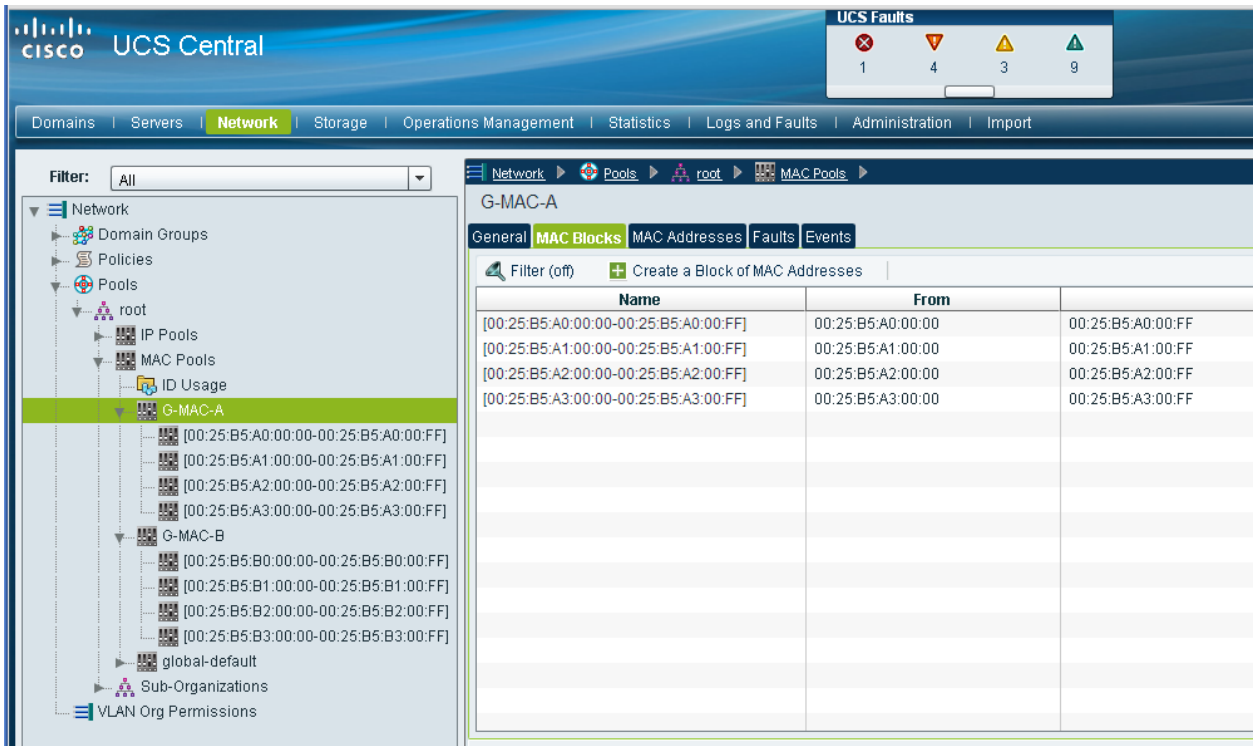
Best Practice

When deploying UCS Central, a Best Practice is to adopt Global IDs along with Global Service Profiles for deployment of new UCS domains.

a) **Pool sizing**

As a way of minimizing the number of managed objects, consider creating a smaller number of pools with a larger number of blocks, as opposed to creating a larger number of individual pools themselves.

A common existing UCS best practice involves creating corresponding A-side/B-side pool names, with an "A" or "B" embedded in the high-order byte of the MAC/WWPN address range, as a way of distinguishing A-side versus B-side traffic. Extending this model towards UCS Central would involve creating multiple blocks under such a pool structure. The most efficient sizing for each block is with 256 addresses (0xFF)[19].



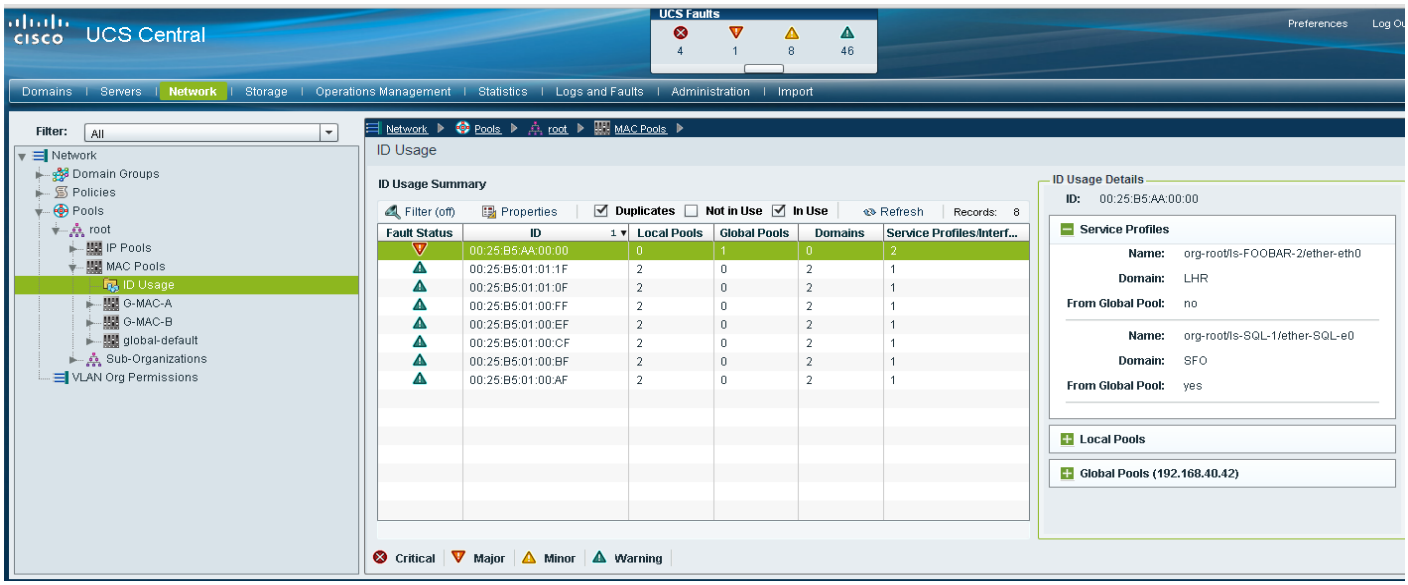
Example of Global Mac Pools (A-side, B-side) with multiple blocks

[19] UCS Central imposes a maximum block size of 1000 addresses (0x3E8) for all pools (UUID, MAC, WWxN)

b) **Checking for Duplicates**

UCS Central provides visibility into possible duplicate ID usage.
All of the pool types (UUID, MAC, WWxN) offer the ability to display duplicate IDs that may exist across UCS domains, through the “ID Usage Summary”. Duplicate ID severity will be flagged as either “Major”, for IDs that appear in multiple Service Profiles, or flagged as “Warning” for IDs that appear in multiple local pools.

Note that the only way to view Local ID Pool consumption is to select an individual ID, and view the corresponding drill-down details to the right (Local Pool and Local Service Profile)



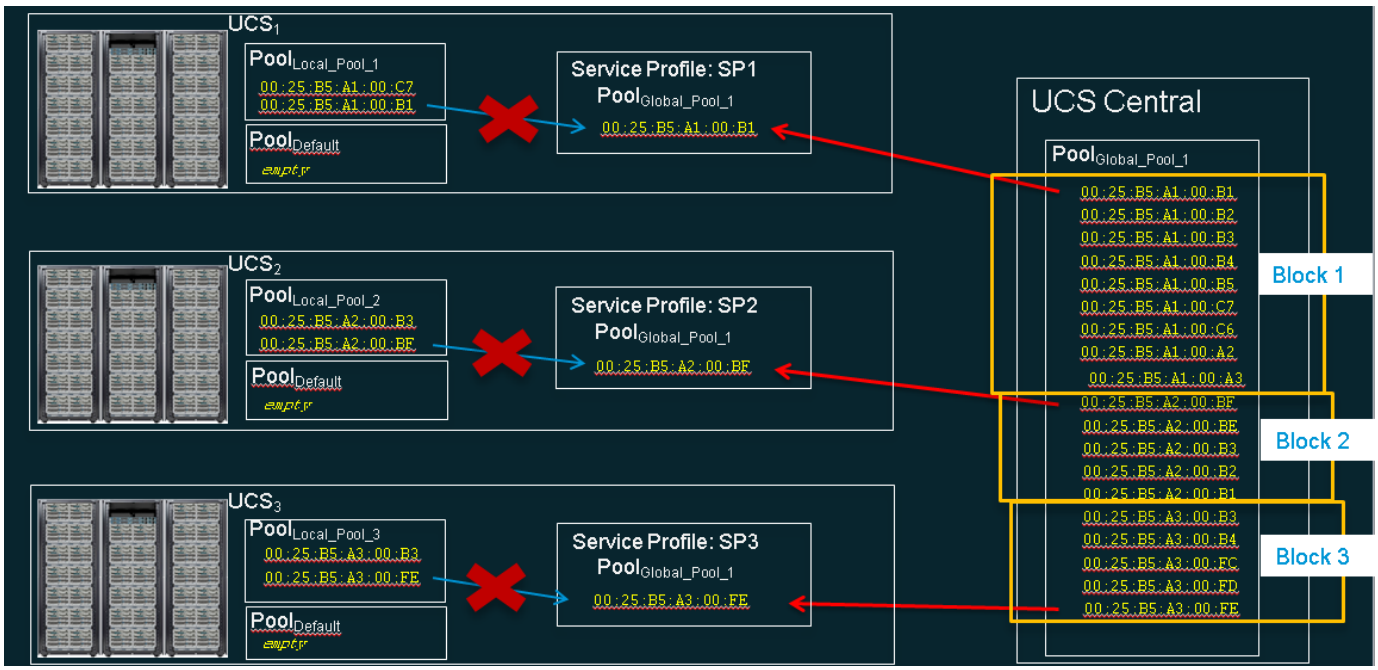
Example of detecting presence of duplicate ID’s

c) Transitioning to Global ID Pools

Local Service Profiles (LSPs) that currently reference local ID pools can be reconfigured to use Global ID pools. Changing any ID for an associated Service Profile would typically cause a service interruption. However, UCS Central was designed to ease this migration to Global ID pools and not cause a service interruption if the transition results in assignment of the SAME identifiers.[20]

Any reference change from a local to global ID pool must be accompanied by a "Reset MAC/WWxN/UUID", for the ownership to change from local to global. Drill down through "ID Usage" to see the definitive way of verifying ID association to a Local or Global ID Pool (See Example Screenshot above).

LSPs that use Global ID's will be guaranteed ID uniqueness across all LSPs (where all LSPs use Global IDs) and GSPs that reference Global ID's exclusively (GSPs can only reference Global IDs). However, LSPs that reference Global ID Pools will not be able to take advantage of Global Service Profile (GSP) mobility. LSPs that use Global ID's will always continue to reside and be confined to the specific local UCS domain.



Example : Local to Global ID Pool Migration

[20] You must run UCSM version 2.1(3a) or above when migrating from local to global pools.

d) **Creating New Global ID Pools**

Existing UCS customers with multiple domains may likely have addressed multi-domain ID challenges through best practices, such as embedding a "domain ID" within the high-order bytes of ID pool ranges. Transitioning to Global Pools was highlighted in the previous section. But some admins might wish to segregate Global ID's in a way that is completely distinct from previous local ID consumption method.

Generally, the notion of "domain ID" would no longer be relevant when creating Global ID pools for new deployments. The exception to this would be if you were using Domain Specific ID Qualification Policies (or a Block within a Pool).

The best practice of creating distinct "A-side"/"B-side" global pools may still provide utility from a troubleshooting standpoint.

e) **Migrating from Existing ID Pools**

To maintain the same ID for LSPs while migrating to Global ID Pools, construct the Global ID pools so that they are "supersets" of the corresponding Local ID pools (i.e., the Global ID pool should contain all of the identifier blocks that are currently within the Local ID pools). A possible best practice may be to adopt an "A/B" naming orientation for MAC and WWPN pools with respect to the fabric, such as "G-MAC-A" or "G-WWPN-B". Once the Global ID pools have been created, the Administrator can change the Service Profile/VNIC/VHBA/Template to reference the Global ID pools. If not already assigned, UCS Central will automatically assign the same identifier that was previously used in the local ID pool, thus eliminating the need for a service interruption[21].

When the ID space is already partitioned and completely non-overlapping, the adoption sequence could be as follows:

1. Create new Global ID Pool in UCS Central with unambiguous name and a "Global-" or "G-" in the pool name prefix. For MAC and WWPN pools, add a "-A" or "-B" suffix to the pool name, if desired.
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, VHBAs) to refer to the corresponding global ID pool name.
4. Perform a "Reset MAC/WWxN/UUID Address" on the specific instantiated managed object to effect the global ownership change
5. Verify the corresponding local ID block has no assignments

[21] The 1.0(1a) and 1.1(1a) releases unfortunately cause service interruptions when migrating to Global Pools in this manner. This was identified as bug CSCud44377 and has been fixed in UCSM release 2.1(3a) and above

6. Verify through “ID Usage” that the address now comes a Global Pool
7. Delete the corresponding local ID block for each local ID block in the local pool

For VNICs/VHBAs based on “initial templates”, once the ID’s reference Global ID Pools, then all subsequently created managed objects should reference the new Global ID pools. This is by nature of “initial templates”.

For VNICs/VHBAs that are bound to “updating templates”, once the ID’s reference Global ID Pools, then all existing managed objects bound to the template will reference the new Global ID pools. If the existing managed object’s ID is present and unassigned in the Global Pool, then this transition will not cause a reconfiguration, reboot or service impact.

For VNICs/VHBAs that are not bound to a template, if service-profile’s pool name is modified to point to Global Pool, and the existing ID is already consumed in the Global Pool, then the service-profile will get a new ID, causing a reconfiguration, reboot and service impact. If the ID is not already consumed, then the ID will be retained and will point to the Global Pool, without incurring a reconfiguration or service impact.

Note that IP addresses for “ext-mgmt” and “iscsi-initiators” can also be managed through Global Pools. Similarly, the current allocations for existing domains can be viewed from Network->Pools->[Org]->IP Pools->ID Usage

f) ID Range Qualifications

UCS Central provides the ability to use ID Range Qualification Policies to assign ID blocks within a Global Pool to a specific domain(s) or domain group(s) for any Local and Global Service Profiles that reference the Global Pool. In this way, one or more UCS domains from a particular DG can be assured of consuming a discrete range of identifiers, as illustrated below.

UCSC Central version 1.3 introduces the ability for Global Service Profiles to reference Global Pools that utilize ID Range Qualification Policy definitions on one or more ID Blocks. UCS Central 1.3 introduces the concept of “Lazy-Binding” for ID allocation, where UCS Central waits until a UCS Server has been selected for association, prior to allocating an ID from a Pool that has a at least one Qualified Block within a Pool.

Prior to UCS Central release 1.3, only Local Service Profiles could consume IDs from a Qualified ID Pool.

What happens during the GSP creation, association, and disassociation process?

i. GSP without Binding Server (Disassociated GSP)

If the GSP does not consume IDs from any Qualified Pool (a Pool with one or more ID Range Qualification Policies), then UCS Central will immediately obtain the ID values from the appropriate ID pool.

If the GSP does consume IDs from a Qualified Pool, the GSP will move into a ***Config-Failure*** State where you will observe the warning message: '***Using ID pool which contains block with Qualifier***' (Lazy-Binding)

ii. GSP Association - Process

During the GSP Association Process, the target server and the domain is known for the GSP.

UCS Central will now perform normal ID resolution to consume the IDs from the appropriate ID Block for the Domain and/or Domain Group within the Global Pool.

iii. GSP Disassociation - Process

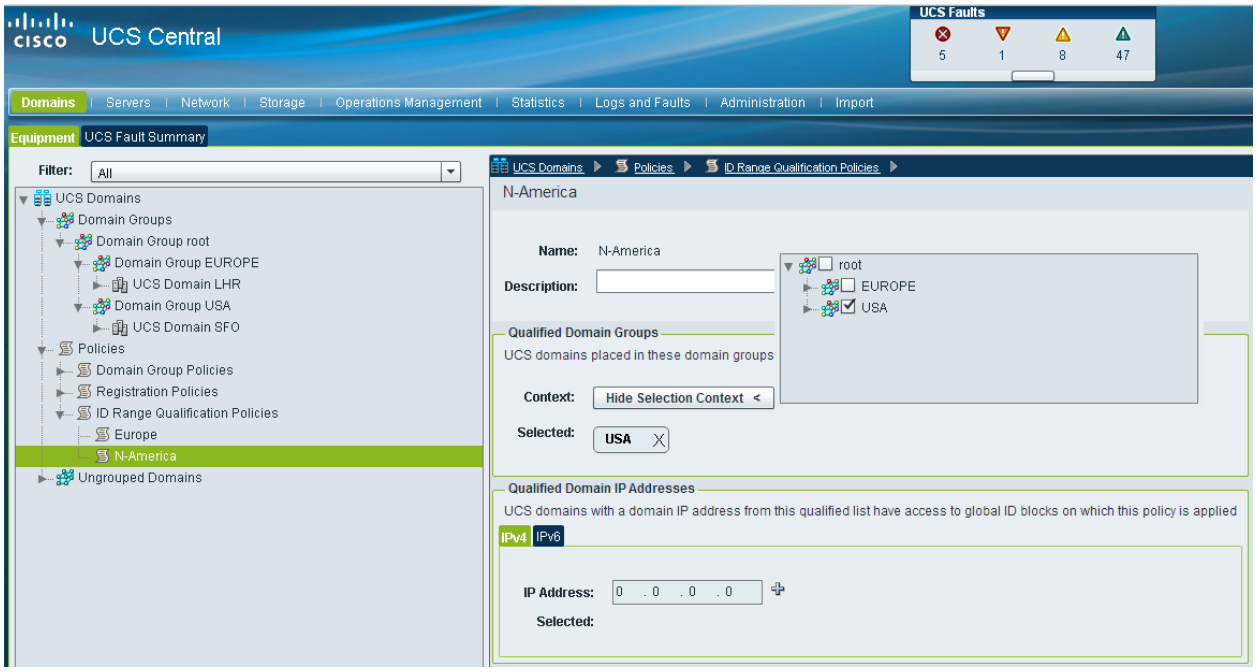
During the GSP Disassociation Process, the ID consumption will perform as follows:

- **Non-Qualified-ID pool:** UCS Central will not release the IDs in use from the GSP.
- **Qualified-ID pool:** Since the server Domain and Domain Group could change, UCS Central will release the IDs in use from the GSP because the Qualified ID Block could be different with either the new UCS Domain or Domain Group that is targeted.

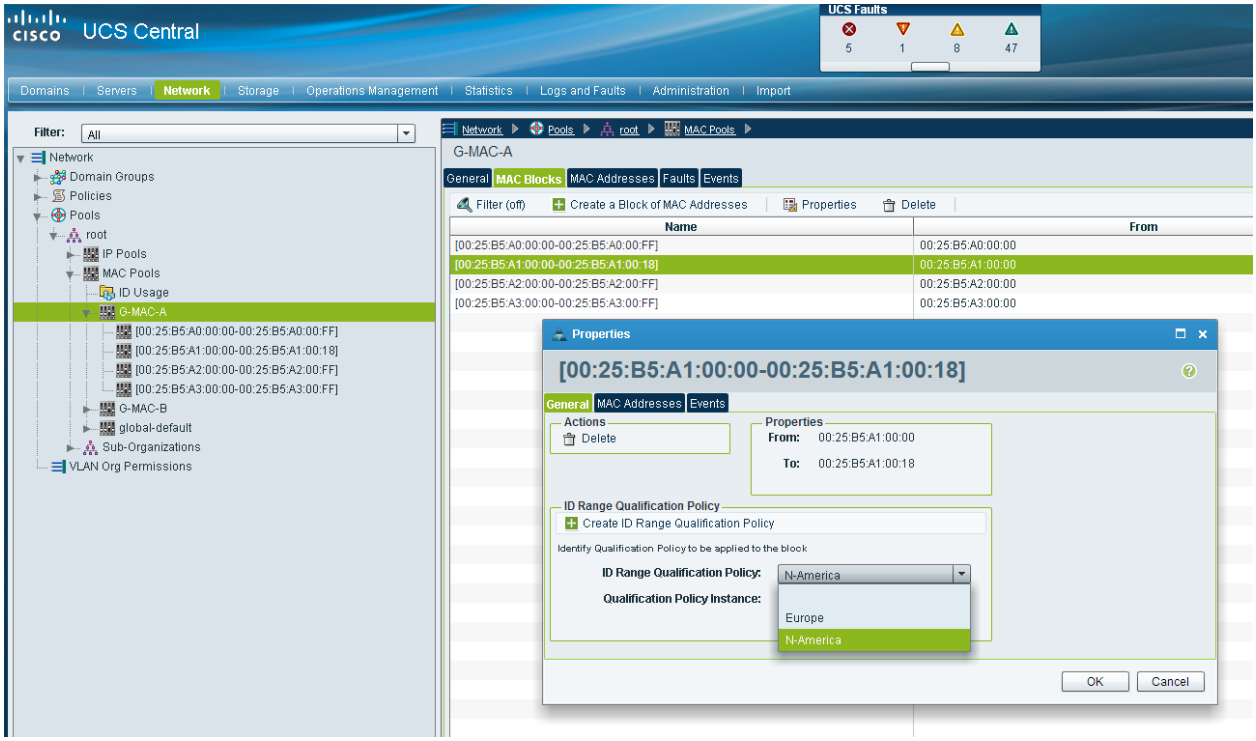
iv. GSP Migration – Process

During the GSP Migration Process, the ID consumption will perform as follows:

- **Non-Qualified-ID pool:** UCS Central will not release the IDs in use from the GSP.
- **Qualified-ID pool:** During the GSP Migration Process, UCS Central will attempt to re-acquire the same IDs from the Global Pools, if those IDs are still Qualified for the new targeted Domain or Domain Group. If the new targeted server is in the same domain, UCS Central will reacquire the same IDs. If the new targeted server resides in a different Domain or Domain Group, UCS Central will re-evaluate the Domain Qualification Policy. If the previously acquired ID does not meet the Qualification Policy, the ID will be released and a new ID will be assigned.



Creating ID Range Qualification Policies for Domain Groups



Referring to ID Range Qualifications within an ID Block

8. UCS Central Adoption: Approaches and Challenges

UCS Central is intended to be the focal point of UCS Management going forward. For datacenters with existing UCS domains, adoption of UCS Central should be strongly considered for simplifying future growth and management challenges. Successful adoption of UCS Central requires a sense of comfort that comes with familiarity and a sense of orientation. While UCS Central has a great deal in common with UCSM, there are also some differences and challenges, outlined in this section.

a) New UCS Domain Deployments ("Greenfield")

Best Practice

For new deployments of UCS domains, the best practice is to adopt UCS Central from Day One, especially for new workload, and to reference Global Pools, Policies and Templates. Environments with no previous UCS footprint are strongly urged to use UCS Central with Global Service Profiles/Pools/Policies during the adoption and deployment of Cisco UCS and to avoid any use of locally managed objects. Global Service Profiles that refer exclusively to Global Pools and Policies help to ensure global consistency. Environments that refrain from not using UCS Central from Day One are deploying a "brownfield" framework that will need to be retrofitted to UCS Central down the road. The use of UCS Central from Day One can greatly simplify and enhance the UCS management experience.

b) Migration of Existing Deployments ("Brownfield")

v. Operational Policies

Existing deployments of UCS should take full advantage of Global Operational Policies, as described in **Section 4 Global Operational Policies**. Administrators can "opt-in" to the UCS Central global operational management model gradually over time, as comfort increases.

In addition to Global Operational Policies, existing UCS domains can take advantage of the centralized/Global view of UCSM Faults, Inventory, and Statistics.

vi. Workload Policies (e.g. Service Profiles)

When adopting UCS Central for UCS domains with existing workloads, please take note of current caveats and limitations[22]. The most notable limitation: while Local Service Profiles can refer to Global Pools and Policies, individual Local Service Profiles cannot be converted into Global Service Profiles. Therefore, existing workload must be left in a locally managed mode. The only way to recreate the settings defined by a Local Service Profile in a Global Service Profile is to reconstruct these settings in a Global Service Profile.

[22] See Sections 15 and 16 ("Take Note" and "Known Caveats")

In general, the Best Practice would be to adopt Operational Policies. However, questions should be asked when considering a migration of existing UCS deployments in to UCS Central, and the adoption of Workload Policies and GSP's should be qualified, based on requirements and constraints. For example, migrating LSPs to GSPs might be straightforward if there is no need to maintain the same ID's --- or it may be quite complicated if ID's do need to stay the same. Keep in mind that LSP's can still be visible and monitored from UCS Central, even if they can't be configured.

Best Practice

Workload Policies and GSP's should only be adopted if they contribute to management simplicity, if their adoption complicates management, then they should be avoided. There is absolutely no dependency between Operational and Workload Policies. There is no requirement in UCS Central that forces Global Workload Policies and GSP's to be adopted.

c) Policy Browser and Policy Import

UCS Central allows for existing local policies (both operational and workload policies) to be imported in to UCS Central as Global Policies. This is an easy way to operationalize any "gold" or "standard" policies on a global basis across domains.

"Policy Import" refers to individual policies (workload and operational), templates (VNIC, VHBA and Service Profile), VLANs, VSANs and ID pools.

"Policy Import" implies importing source policies from existing domains. The destination for an imported policy can only be a Global Org, owned by UCS Central.

"Policy Import" optionally allows any "dependent" policies to be included as part of an import operation, as well as dependent resources, such as VLANs and VSANs.

Note/Caveat: "Import dependencies"

"Policy Import" allows renaming of the object from the source to the import destination. In keeping with best practices, a VNIC template "vnic-A" and all its dependencies could be imported and renamed as "G-vnic-A", to distinguish it as a global object. However, the renaming capability only applies to the top-most imported object and not the dependencies. If "vnic-A" referenced a QoS Policy called "Bronze", then "Bronze" would be imported as a global object, but cannot be renamed in a globally distinguished manner.

Note/Caveat: "Import dependencies"

If the source object for a Policy Import refers to other managed objects that are higher up the Org hierarchy than the source object, then using "import dependencies" will copy those objects in to the same Org hierarchy as the target. No existing hierarchical relationships will be preserved.[23]

[23] If maintaining the hierarchical relationship is desired, then import the dependent polices to higher Org levels first, then import the remaining policies in the desired Org. Be sure to run Estimate Impact for all such operations.

Use of Policy Import should focus on the "Golden"/"Standard" model, to import and globalize the most commonly used workload policies/templates.

Best Practice

Import all individual policy dependencies first, so that they can be renamed with a "G-" prefix, if appropriate. Then if/when the top-most policy is imported, modify its attributes to refer to the newly renamed Global Policies.

One challenge in using "Policy Import" is to understand the relationship and potential conflicts between the local and global namespaces --- especially for workload policies; less-so for operational policies, which have far fewer dependencies on the Organization hierarchy. Common adoption obstacles may include UCS Central "config-failure" when instantiating GSP's from imported templates, or when associating GSP's on to a local domain.

For "brownfield" environments, administrators may want to consider adopting UCS Central and global consistency for new workloads that get deployed in existing UCS domains. Such an environment would be called a "mixed-workload", since it may contain both globally and locally managed objects. Two models exist for "mixed-workload" environments, where an existing domain may contain managed objects that are owned by both UCS Central and UCS Manager:

Best Practice

i. Segregated Organizations

In this model, a given Organizational hierarchy (starting below "root") will have managed objects that are all owned and managed exclusively by **either** UCS Central **or** UCS Manager.

Using this approach within an existing domain, domain owners would create an Organization with a distinctly global name (e.g. "G-PROD"), which would only be populated with globally managed objects. At the same/peer level within the hierarchy, a corresponding Organization (e.g. "PROD") would contain locally owned managed objects exclusively.

Workload in the local Org would only reference local pools/policies/templates. Workload in the global Org would only reference global pools/policies/templates.

Using this approach makes it easier to take advantage of the "Import Dependencies" feature, without causing naming conflicts. If objects are imported from a strictly locally managed Org (e.g. "PROD"), and the imported objects and dependencies are then placed under a globally distinct Org (e.g. "G-PROD"), then the risk naming conflicts is greatly reduced.

Furthermore, the "G-" prefix in the Organization name implies Global scope for all objects, and therefore reduces the need for a "G-" prefix for each managed object contained within the Organization.

ii. Integrated Organizations

In this model, the administrator creates a Global Organization with the exact same name as a given Local Organization in a domain that has been registered with UCS Central, resulting in an Organization merge. The workloads within the Organization may include a mix of both locally and globally owned managed-objects. During Policy Import operations for "integrated organizations", additional care must be taken, in order to avoid potential naming conflicts:

- Do not import dependencies when importing policies. If dependencies exist, note the dependent policies and import them individually.
- Be sure to add "G-" to the destination name for each imported object, to keep the namespace "unique" for all policies/templates.
- Do not import resources (VLANs/VSANs). Make sure to configure Global VLANs[24] that are aligned with the Org Permissions and DG mapping. The Org Permissions ensure proper masking of VLAN visibility to appropriate SP's; the DG mapping ensures proper correspondence of VLAN ID, based on physical location (typical DG partition attribute).

Best Practice

Regardless of whether Segregated or Integrated Organizations are used, the following guidelines should always apply when using the "import dependencies" feature:

- Never include any "default" pool, policy nor any object name that ends with "default" (e.g. "thr-policy-default")
- Never include the "default" VLAN or VSAN
- Ensure that any imported VLANs/VSANs have been defined globally and mapped accordingly in to the global Org structure with respect to their ID's and the Org permissions.
- After importing any VNICs/VHBAs/ServiceProfiles/Templates, make sure to change any local pool references to Global Pool References.

Operational Policies also get imported through the "Policy Browser"[25]. Again, this is an easy and convenient way of "promoting" a locally defined "gold" or "standard" policy in to UCS Central, and then ensuring consistency by applying the new global policy across multiple domains.

d) Local Affinity Issues

As policy and control becomes centralized in UCS Central, certain challenges may surface that highlight affinity for local resources and control points. These are referred to as "Local Affinity" issues, with respect to local/individual domains. Here is a list of common affinity points, along with possible workarounds[26]:

[24] VSAN aliases do not exist yet, as of release 1.2(1a)
[25] Previous versions of UCS Central allowed these to be imported through the Operational Policies. However, this is no longer supported.
[26] External IP Pools and Boot Policies are targeted for "alias" capability in an upcoming release, similar to the existing "ID Range Qualification" policies for Domain Groups.

i. External IP Pools (global-ext-mgmt)

These are the addresses for out-of-band management of physical blades (KVM, Power, etc.). However, UCS Central does not automatically associate these addresses to blades, to the CIMC, as UCS Manager does. Workaround: Use Management IP Addresses associated with Service Profiles (or Templates), so that Global External IP Pools can be referenced. The point here is the behavior of "ext-mgmt" Ip Pools is completely different in UCS Central verses UCSM. New Global SP Support for ID Range Qualification Policies provides greater ability to maintain flexibility and efficiency in assigning Global Mgmt IPs.

ii. Boot Policies

These have hard association to the WWPNs of a specific Storage Array, making it hard to configure Global Service Profiles with the same boot policies on a worldwide basis, potentially across different Storage Arrays. Workaround: Use the same workaround as today with UCSM: create SP Templates that are named as "SP-StorageArray" pairs, where the WWPNs of the Storage Array are effectively hardcoded in to the SP Template definition.

iii. VLANS and VSANS

To mitigate local affinity issues for VLANs, take advantage of the VLAN ID alias capability, which translates the VLAN IDs for a domain, based on its Domain Group and Org Permissions. VSAN aliasing does not exist, requiring mapping to be done individually for both the DG and Org contexts[27]. Note: When using VLAN alias, do not include the actual VLAN ID in the name.

iv. Fabric Interconnect Port Configuration

With UCS Central 1.2(1a), physical device configuration of the Fabric Interconnect ports can now be configured through UCS Central. However, the configuration types are currently limited to "Server" and "Uplink" ports. Managed objects that depend on physical ports cannot be managed through UCS Central, including Pin Groups and Port-Channels for both Ethernet and FC.

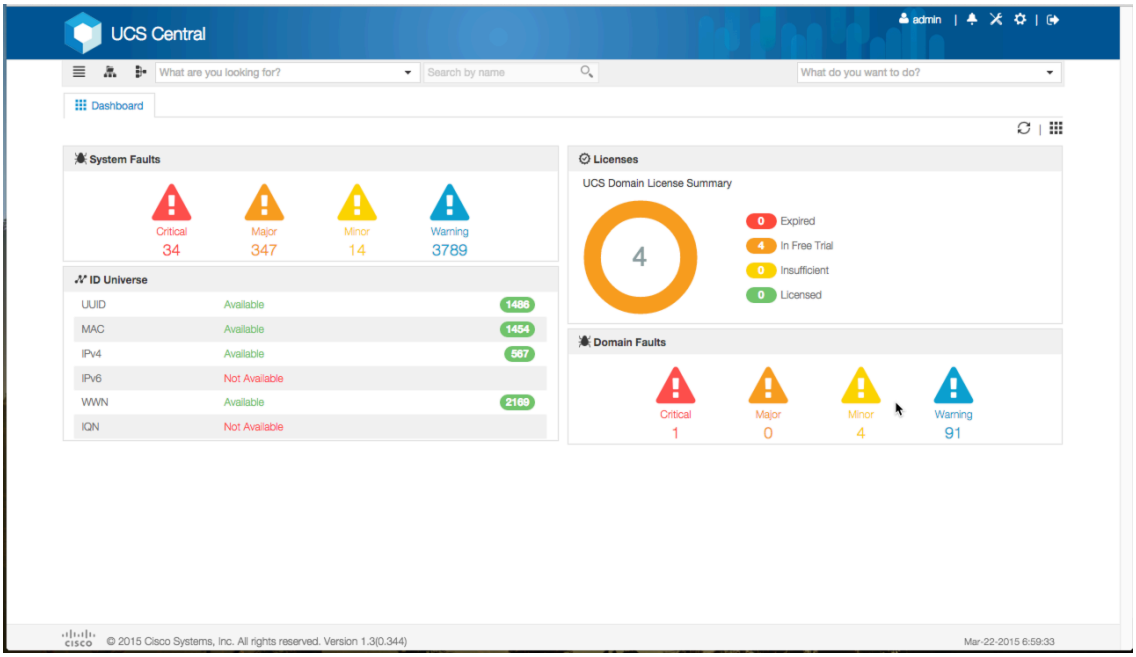
[27] Create VSAN names that append their respective DG name. Use the "VSAN-DG" name pair when creating references such as VHBA templates.

e) VLAN and VSAN Policy Push

UCS Central 1.3 introduces a new capability to publish Global VLANs and VSANs down to the UCS Domains. In previous releases, the process of delivering Globally Defined VLANs and VSANs down to a UCS Domain required the configuration and association of a Global Service Profile. In purely Global Environments, this was standard order of business, however in Brownfield type of implementations, where Local Service Profiles are still being utilized, requiring the association of a Global SP just to deliver a Globally defined VLAN or VSAN was additional work. With UCS Central 1.3, all applicable Global VLANs and VSANs are available to be published to the registered UCS Domain. This assumes the Global VLAN or VSAN are available to the DG. The publishing of the Global VLAN or VSAN can be automated with either direct API Integration or the use of UCS Central CLI. This functionality is not available through the legacy or HTML-5 UI.

f) New HTML-5 UI introduced with version 1.3

An Exciting New enhancement to UCS Central is the introduction of a new UI based-upon HTML-5. This new UI will be available to use along side the original Flash-based UI allowing existing clients time to adjust and adapt to the new look and feel. All the features and functionality of this new UI is beyond the scope of this Best Practices document, but a follow-on UCS Central 1.3 HTML-5 User's Guide will be available soon. The performance and power of the new UI will provide a better management experience for users going forward.



g) UCSM Platform Emulator

The best way to get oriented and gain familiarity, while averting all risk, is to take advantage of the UCSM Platform Emulator http://communities.cisco.com/ucspe

The UCSM Platform Emulator (PE) runs as a virtual machine, yet is a complete instance of the UCS Manager that maintains the UCS Management Information Tree, Data Management Engine, and exports the UCS XML/API. In addition, the PE has the ability to import both the physical hardware configuration and also the logical configuration of an actual UCS domain.

Best Practice

With the PE, UCS administrators can effectively model their entire UCS environment, along with UCS Central. In this way, all configuration changes, testing, etc. can be done in a "safe sandbox", without any impact to actual production domains. The modeling could even be adopted to facilitate a formal "Change Management" sign-off or for UCS Central training.
For testing any integration with UCS Central, be sure to use the latest version of the UCSPE.

Best Practice

h) Adoption Summary: Best Practices

Much of the UCS Central Adoption approach depends on to what extent UCS Central will be used with existing UCS domains, or exclusively for new UCS deployments.

- Use Global Operational Policies, Global Fault and Inventory reporting, Global Statistics universally, regardless of workload profile and existing UCS deployments.
- New UCS deployments and environments that are 100% Globally managed generally do not risk any namespace collision/conflicts, and do not require such attention (i.e "G-" prefix for managed objects)
- Individual Local Service Profiles cannot easily be converted to Global. Existing SP's should remain in locally managed mode, but may possibly reference Global ID Pools and Policies
- Try to restrict new workload to new domains that are exclusively globally managed.
- Try not to mix Global Pools/Policies/Templates/SPs in domains that are also locally managed, so as to avoid name collisions and conflicts in SP creation and deployment. If a given domain does mix Local and Global objects, use a "Segregated Organization" structure to reduce the potential for naming collisions/conflicts.
- Import most common/well-used "Golden" Policies/Templates from local domain, using Policy Import, to become the new Global standards.
- Do not import "default" objects.
- Rather than using a "default" named policy, which someone can accidently change or hide the value-property behind the name (perhaps not understanding the broader consequences), consider using "named" polices that communicate what exactly the policy is doing. For instance, a default scrub policy that is normally set to "No" for Disk Scrub or BIOS Setting Scrub could be changed inadvertently to "Yes" and have catastrophic effects on SP's disassociated from blades containing Local Disk installed operating systems. As a suggestion, if you intend on creating and using a "Scrub" policy, then perhaps create a policy called "Scrub-Disk".

- Use the UCS Platform Emulator to dry-run and model adoption

The communities.cisco.com/ucs community site hosts some valuable content around UCS Central and adoption, including Brad TerEick's blog "UCS Central and My Existing Environment - How do I get there?" https://communities.cisco.com/community/technology/datacenter/compute-and-storage/ucs_management/blog/2013/10/02/ucs-central--my-existing-environment-how-do-i-get-there

9. Backup of UCS Central

Backup of UCS Central configuration on a regular basis is essential. The UCS Central management model is an extension of the core UCS management model. But there are constructs within UCS Central that are not present within the base UCS model. For example, the construct of "Domain Groups" is only present within UCS Central. Without proper/regular backups, there is no automatic way to reconstruct DG configuration.

Similarly, since Operational Policies terminate on DGs, without proper/regular backups of UCS Central, there is no automatic way to reconstruct the mapping of these Operational Policies on to DGs and the subordinate, individual UCS domains.

Given the small size of a UCS Central backup (usually much less than 1 MB), backups should be scheduled once a day.

Best Practice

Consider Backing-up your UCS Central Configuration Daily, using a Config-All (logical) backup and also the Full-State (db) Backup. ALWAYS use the remote copy ability of UCS Central to store your backups off-line from the UCS Central Virtual Appliance**. New with UCS Central 1.3 is the ability to schedule UCS Central Backups on a custom defined schedule**.

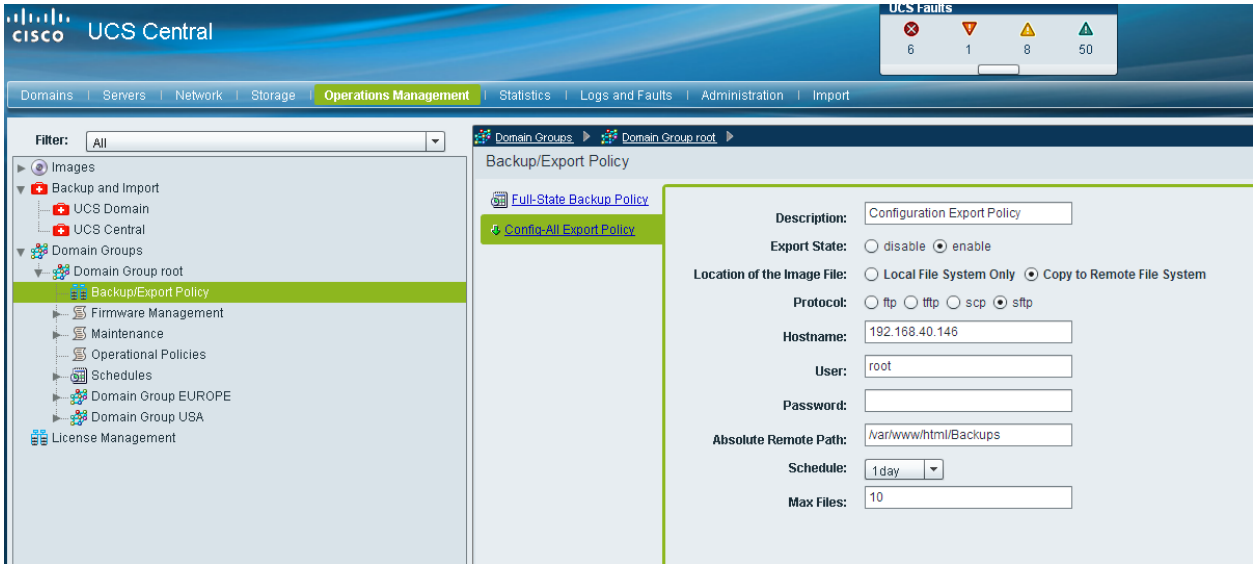
10. Backup of UCS Domains

Management through UCS Central does not change the need for taking regular/frequent UCS backups. But management through UCS Central does help simplify and automate individual backup operations.

Backup and Export Policies are defined per DG. However, a best practice would be to define these policies in the "root" DG, so that backups can be easily and automatically taken for all domains.

Typical backups of individual UCS domains might be ~100 KB, which is easily small enough to justify frequent backups. (Full-state binary backups might be ~2MB).

UCS Central maintains original copies of all backups within the UCS Central appliance itself. In addition, copies of backups can be made to remote locations as well.



Copying domain backups to remote location

Best Practice

Consider Backing-up your UCS Domains Daily, using a Config-All (logical) backup and also the Full-State (db) Backup. New with UCS Central 1.3 is the ability to now schedule UCS Central Backups on a custom defined schedule.

11. Upgrading UCS Central

Please review all available release notes at time of upgrade.
http://www.cisco.com/en/US/products/ps12502/prod_installation_guides_list.html

Please note the version compatibility requirements:

- UCS Central 1.2(1a) and forward supports communication **only** with UCSM 2.1.2 and above[28]

Prior to attempting an upgrade of UCS Central to 1.2(1a) and forward releases, all registered UCS domains must first be upgraded to a minimum of UCSM 2.1(2a)[29]

The in-place ISO upgrade method is documented in the Upgrade/Installation Guide.
http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-central/install-upgrade/1.1/b_UCSC_Installation_and_Upgrade_Guide_11.html

Before Upgrading UCS Central:

- Take a snapshot of the VM using Snapshot Manager to preserve the state of the original VM, in case there is a need to revert to original state.
- Take both a "full-state" backup and a "config-all" backup of UCS Central. Ensure the Backup State is "enabled" for both, and make sure these backups are available "offline".

The local UCS domains will lose visibility to UCS Central, but should change state back to "registered" once upgrade is complete. **Do Not perform an Unregister/Reregister cycle for your UCS Domain as part of the UCS Central Upgrade**.

12. Statistics Database Support

UCS Central provides support for statistics to be maintained for long-term historical trending, using either the internal UCS Central database, or an external database. The external databases supported are Microsoft SQL, Oracle, and Postgres.

Statistics Collection for UCS-UCSC is as Follows:

- Each separate, UCSM can hold about 24-hours worth of statistical data.
- A UCS Domain Registered to UCS Central with Statistics Collection enabled, and using UCSC's internal db can hold about 2 weeks worth of data.
- A UCS Domain Registered to UCS Central with Statistics Collection enabled, and using an external db can hold about year+ worth of data.

[28] Some new features of UCS Central may only be available in newer versions of UCS Manager. For example, Policy Search works with UCSM 2.1(2a) and newer, but Policy Import only works with 2.2(1b) and newer.
[29] Please use the most recent maintenance and patch release in the UCSM 2.1 tree if using UCSM 2.1

Use of an external database can be configured at any time after an installation or upgrade. Furthermore, the database type can be changed after the fact, though must be done out-of-band with respect to UCS Central and will involve a complete database export/import operation. Any database conversion would need to be done at the SQL/database level. Configuration of an external database can only be done through the CLI. Please refer to the CLI Configuration Guide.
http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-central/cli/config-guide/1.1/b_UCSC_CLI_Configuration_Guide_1_1.pdf

Best Practice

It is **HIGHLY** recommended to use an External Database for statistics collections in Production Environments.

The following guidelines should be used to help size an external database[30]:

- Collecting statistics data from 20 UCS Domains each with 5 Chassis (800 servers total) for 1 year requires a minimum of 400GB storage on the database server.
- Collecting statistics data from 100 UCS Domains each with 5 Chassis (4000 servers total) for 1 year requires a minimum of 2TB storage on the database server.

UCS Central does not backup the externally connected Statistics Database. Backup of the Statistics Database must be managed independently from UCS Central.

A preconfigured Postgres database appliance is available on http://communites.cisco.com/ucsm for Demo's and Proof-of-Concept testing --- but is not supported for production environments.

13. Firmware Management for UCS domains

Upgrading UCS domains has typically been a manual process, up until now[31]. The 2.1 release of UCSM included a new "Firmware Auto Install" feature, to help automate tasks that were previously manual[32]. UCS Central builds upon this new feature to help in automating firmware upgrades across potentially multiple UCS domains.

Please keep in mind 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 the UCS Manager. Server Blade firmware (B Package) refers to the images that run on a physical UCS Blade server's BIOS, CIMC, Adaptors and Controllers. Rack-Mount Server firmware (C Package) refers to the images that run on a physical UCS-Managed Rack-Mounted Server's BIOS, CIMC, Adaptors and Controllers. UCS Mini firmware (E Package) refers to the images that run on a physical Blade Server's BIOS, CIMC, Adaptors and Controllers that are a part of UCS Mini. As with UCS Manager in general, the best practices for server firmware are to leverage Host Firmware Packages as part of the Service Profile definition, to guarantee configuration consistency at the application level.

[30] Generally plan on 0.5GB per server per year
[31] Unless you used Eric William's UCS Firmware Upgrade script: http://developer.cisco.com/web/unifiedcomputing/community/-/blogs/cisco-ucs-powertool-examples
[32] The "autoinstall" feature is not recommended for upgrading to UCSM 2.1(2a)

Several important points need to be clear, regarding firmware management:

a) Service degradation and/or disruption

Any UCS infrastructure firmware upgrade will cause service degradation if done during normal production, as each Fabric Interconnect must sequentially go through a reboot cycle. To avoid service disruption, administrators and operators are urged to ensure that appropriate application-level "availability" schemes are in place, such as UCS Fabric Failover or NIC teaming/bonding and also host-based storage multi-pathing.

b) Pending Acknowledgement

Rebooting FI's require explicit acknowledgement from the UCS Central administrator. Administrators should pay attention for "Pending Acknowledgements" under "Schedules"[33] for the DG's that are being upgraded. Default behavior is that all Firmware Upgrades ("infra-fw") and reboots ("fi-reboot") need to be "Acknowledged" before they proceed. The best vantage points for viewing progress on UCS Central is the "Active Tasks"[34] tab from the "Schedules" menu; for an individual UCS domain, within UCSM follow "Equipment -> Firmware Management -> Firmware Auto Install -> FSM".

Best Practice

There are no implicit maintenance policies for **server firmware** bundles. Therefore a best practice would be explicitly defining a maintenance policy that governed server firmware bundle upgrades. Best practice would be to define maintenance policies with "USER-ACK" chosen to avoid unexpected service interruptions.

The upgrade process does not complete in an "unattended" mode and will involve several Acknowledgements to complete.

One benefit of UCS Central is that multiple upgrades can proceed in parallel. If you are connected to the individual UCSM's, those connections will get reset, as you'd expect during an upgrade. As with standalone UCSM upgrades, the infrastructure process takes roughly one hour to complete, but can run in parallel across multiple domains[35]. Blade upgrades can take longer depending upon 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 bringing up a new UCS domain for the first time, using both infra and host firmware auto install triggered from UCS Central can ensure that a new domain is current with all low-level host firmware before being put into production.

[33] Also visible under the InfraPack -> Pending-ack for each DG.
[34] Also visible in the InfraPack -> Status for each DG.
[35] The concurrency setting can be provided in the InfraPack tab(for infra firmware upgrades) and in the maintenance policy schedule(for server firmware upgrades)

14. High-Availability Cluster-mode

UCS Central has native High-availability (H/A) features, which are provided primarily for deployments where hypervisor-based H/A is not available. In general, hypervisor-based H/A should be used, if available. In cases where native hypervisor H/A is available and active, UCS Central can safely run in standalone mode without using UCS Central's native H/A clustering.

If your host hypervisor does not provide H/A support, then it's generally a good idea to take advantage of UCS Central's native H/A capabilities.

In general, it is not recommended to run both UCS Central H/A and hypervisor-based H/A together, concurrently.

Keep in mind that UCS Central can incur a temporary outage without disrupting service because UCS Central only operates on the control-management plan, not the data plane. If UCS Domains registered to UCS Central lose visibility to the UCS Central Server, services (Service Profiles, Operating Systems, Network, Storage) within each UCS Domain continue to operate normally, however, configuration changes to the environment will require UCS Central Server to be restored.

High-availability (H/A) with UCS Central in Cluster-mode refers to a single logical instance of UCS Central, using a Primary and a Subordinate UCS Central VM with a Shared-Clustered 3rd Disk.

H/A can also be achieved by taking advantage of native Hypervisor-based H/A capabilities. In this case, UCS Central's H/A capabilities are not required and should not be used.

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

H/A with UCS Central can be achieved by:

- Installing a new UCS Central instance as an H/A cluster
- Converting standalone UCS Central to an H/A cluster.
- First upgrading to 1.1(1a) or higher and then enabling H/A cluster mode

OR

- Taking advantage of native hypervisor-based H/A capabilities.
- Leverage/Choose RDM-based Clustering or New NFS-Based Clustering.

Be sure to refer to the Installation/Upgrade Guide, before attempting[36].
http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-central/install-upgrade/1.1/b_UCSC_Installation_and_Upgrade_Guide_11.pdf

[36] Upgrading from 1.0(1a) can only be done in Standalone mode.

a) UCS Central H/A with shared-storage RDM LUN

When deploying in RDM Cluster-mode, make sure that:

- Both VMs are on separate physical hosts with access to shared storage.
- Both VMs are running the same version of ESX or Hyper-V.
- Both VMs are running the same version of UCS Central.
- Both VMs are on the same sub-net.

Cluster H/A mode does require the configuration of a Shared LUN[37], presented as a raw device. This will require configuration privileges on the SAN in order to:

- Zone both hypervisor clustered hosts with the Storage Array from the SAN switch
- Provide access to the Shared LUN for the clustered hosts from the Storage Array (LUN masking)

Ensure sure that:

- Thick Provisioning is used for the Shared LUN (not Thin Provisioning)
- Access to the Shared LUN is exclusive for the 2 clustered hosts (not being used by any other hosts)
- LUN is not configured in multi-pathing mode on the hosts (e.g. LUN should be mapped in Fixed I/O mode on ESX hosts)

For best performance of the shared storage:

- Configure high speed SAN connections to enable fastest access
- Select the best performing RAID type for the shared LUN
- Make sure the storage is write-cache enabled and properly configured[38].

b) UCS Central H/A with shared NFS-based Storage Server

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 UCS Central.
- Both VMs are on the same subnet.

Cluster H/A mode does require the configuration of a NFS Server & 40GB+ Volume

- Export the NFS Directory per the UCS Central 1.3 Installation and Upgrade Guide
- Restart the NFS Service
- Delete/Modify any Firewall Rule on the NFS Server that could block the mount of the NFS Server directories from the UCS Central VMs.

[37] Use “raw device mapping”

[38] For example, an EMC storage array should have the following cache configuration: Page Size: 8KB, Low watermark: 60%, High Watermark: 80%

- During UCS Central Installation, specify the IP address of the NFS Server
- Specify the Directory of the NFS Server
- Configuration scripts migrate the database and images from the Primary VM to NFS
- The NFS Server directories are mounted on the Primary Node after election is complete.

c) Switching from Standalone to H/A or from RDM to NFS

The ability to switch an existing Standalone UCS Central Implementation to a H/A configuration exists, as well as switching a RDM Implementation to a NFS-based Implementation. Please consult the UCC Central 1.3 Installation and Upgrade Guide for further information about the necessary steps.

Best Practice

If considering UCS Central H/A options, it is highly recommended to use NFS-based H/A.

Take care if using features such as suspend/resume or restoring VM snapshots, which could create a shared storage "conflict of ownership". Shared storage is always mounted on the Primary VM. Having the Secondary VM claim ownership while the Primary is still active may result in a crash or the cluster going down.

Best Practice

If native hypervisor-based H/A capabilities are available, then take advantage of those, and only deploy UCS Central in “standalone” (not H/A) mode.

Best Practice

Register all domains to your HA-capable UCS Central instance at the primary site and perform scheduled backups of UCS Central and all registered UCSM instances (via the UCS Central interface). In the event of a disaster, UCS Central can easily be restored to the new site via UCS Central backups. If a new IP address is required for UCS Central, the restoration can be completed and then the IP addressed can be “changed” via the console or web-interface.

Note: UCS Central is not required for a UCS domain to be “available”, since UCS Central is not in the primary data path. UCS Central is the mechanism to configure/manage/view the domain, from the perspective of the control plane.

15. Preparing for TAC

For any problems requiring a support case with Cisco TAC, be prepared to supply the output from "show tech-support". This can be done in the UCS Central GUI by navigating to "Administration -> Tech Support Files", and "Create Tech Support File", followed by a "Download".

16. Take Note

This section lists challenges that admins should be aware of, but which don't constitute product "Caveats"

a) Individual LSP cannot be promoted to GSP

Individual local service profiles can refer to Global ID Pools and Global Policies. However, an individual local service profile cannot be promoted to a Global Service Profile. Instead, local SP templates and their dependencies should be imported as Global SP templates. Any new SP's instantiated from the Global SP templates will then be Global SP's. Note that a Local SP can be used to create a Local SP template, which can then be imported as a Global SP.

b) Local Visibility of Global Objects

When Global Objects are created, they are not presented nor pushed in to UCSM automatically. Global IDs and Global Policies may be visible from the UCSM GUI drop-down menus when creating/modifying local objects. But Global Objects, once created, will not appear automatically in the UCSM GUI's left-hand navigation pane. Global Objects become visible in the UCSM GUI once Global Service Profiles are deployed to a server, and hence referenced by a SP running on the UCSM. At deployment-time, a read-only copy of the Global Object and its dependent objects gets "pulled down" by the local UCSM, and are then visible in the GUI.

c) Maintenance Policies (local and global)

The "USER-ACK" Maintenance Policy is generally recommended universally, to avoid unexpected service interruption. "Where" you wish to acknowledge any given Service Disruption can be configured in one of 2 ways:

- If you want the Pending Activity for service interruption to be given LOCALLY within UCSM, then you must leverage a Local Service Profile, pointing to either a Local or Global Maintenance Policy with "USER-ACK". Regardless of whether the Maintenance Policy is Local or Global, the user acknowledgement may still be given at the UCS Central Console.

- If you leverage a Global Service Profile, with a Global "USER-ACK" Maintenance Policy, then the Pending Activity must be acknowledged within UCS Central. The pending activity can be seen in UCSM, but not actually acknowledged.

d) Using Policy "Import" may flatten any hierarchical dependencies

Local policies that are imported may have dependencies on other policies that are higher in the Org hierarchy. During an import, UCS Central will not attempt to preserve any hierarchical dependency. Instead, for any/all policies that refer up the Org tree, those policies will be "flattened" and imported in to the same target Org specified for the policy import destination, if the "Import All Policies and Pools" option is checked.

e) Operational Policy Imports moved to "Import" tab

Earlier versions of UCS Central included the ability to import existing Operational Policies from the Operational Policies tab. The ability to Import Operational Policies is now done exclusively through the "Import" tab.

f) External Statistics Database Backup

UCS Central does not backup the externally connected Statistics Database. Backup of the Statistics Database must be managed independently from UCS Central.

g) UCSM may require a forced Time sync

UCSM may appear to not sync the time, immediately after setting NTP.

UCSM can be forced to sync with NTP immediately, by setting the NTP Server in Admin tab, followed by attempting to set clock from the CLI with the following sequence:

- ***"scope system"***
- ***"scope services"***
- ***"set clock x x x x"*** (Ex: "set clock may 22 2013 13 44 00")

A message should follow, indicating, "Clock synchronization successful", with UCSM time reflecting the change. Next registration attempt should then succeed.

Note: A time difference of just a couple seconds when UCSM is behind UCS Central will cause a Failed Registration. There is more flexibility if the UCSM time is ahead of the UCS Central Time.

h) Avoid Hypervisor Contention

Since UCS Central runs as a virtual appliance, it is subject to resource sharing, governed by the host OS hypervisor. One way to promote reasonable performance characteristics is to make use of "resource pools" in either the VMware or Hyper-V environments. The purpose of using "resource pools" is to make sure that CPU and/or Memory contention is avoided or minimized for UCS Central. To ensure that UCS Central is appropriately favored, it can be placed in its own dedicated resource pool, with both CPU and Memory Shares settings set to "High", instead of the default "Normal". Please refer to the Installation/Upgrade Guide.

http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-central/install-upgrade/1.1/b_UCSC_Installation_and_Upgrade_Guide_11.pdf

i) Global Org merging for Locales

"Orgs" that have service profiles are presented from UCSM to UCS Central as read-only local objects. "Locales" in UCS Central possess true multi-tenancy, in that user visibility to org's and DG's is truly limited to the "locale's" corresponding to those org-DG pairs.

However, global "locales" can only be created on global orgs. Therefore, for sites using "orgs" and desiring true multi-tenancy, the following sequence should be followed:

1) Create Global Orgs in UCS Central for all UCS domains prior to actually registering with UCS Central
2) Register UCS domain with UCS Central. The local/global org namespace will get merged upon registration
3) Create Global Locales in UCS Central that map to the Global Orgs.

Admins not following this procedure will not be able to create global "locales" with true multi-tenancy. Any mistakes here may require unregister/re-register cycling, along with re-creation of the global orgs, in order to correct. As a workaround, creating a Global Org from the Network or Storage tab in UCS Central may allow Global Locales to be created without the re-register/re-create cycle.

j) Global UUID Pools

Transitioning to Global UUID pools from local UUID pools creates particular challenges.

Prefixes. UUID Prefixes are defined at the domain level; UUID Suffixes can be used to create blocks within pools. Adopting Global UUIDs that are supersets of all local UUID pools would require creating at minimum one Global UUID pool per UCS domain. Therefore, the number of Global UUID Pools would be equal to the number of domains, at minimum, yielding no consolidation in the number of pools.

Orgs. Global Pools are based on Orgs. But UUID prefixes are based on Domains (internal IDs from the fabric interconnects). There is no mapping between Orgs and Domains, making it difficult to generalize a best practice.

Adoption. Existing Service Profiles cannot easily and seamlessly adopt to using Global UUIDs without incurring a reconfiguration cycle and a server reboot.

Workaround: Let existing local SP's remain as local SP's, until the reach the end of their lifecycle. Any new SP's should be created as GSP's.

k) Domain Group Re-assignment from Domain Group Policy

Changing the Domain Group Policy (subsequent to domain registration) no longer automatically re-assigns domains to DGs. DG re-assignment of domains will now only be affected by an explicit "Re-evaluate Membership" action on a given domain. This change in behavior was implemented starting in 1.1(1a) to reduce the impact of human errors.

l) VLAN can appear unreferenced

If using "Modify VLAN Org Permissions" from the Network tab to limit VLAN scope across Orgs, and the VLAN is subsequently deleted, then other Global Service Profile VNICs within the referenced Orgs will still see the unreferenced "VLAN alias", presenting itself as a VLAN.

Workaround is to ensure that any VLAN alias gets deleted prior to deleting the respective VLAN itself.

Best Practice

It is recommended to delete the VLAN Org Permissions before deleting the actual VLAN. Ghost" VLAN Objects may still remain in the system until the actual VLAN Org Permissions are finally deleted.

m) Namespace conflicts during Unregister/Re-register cycles

Care should be taken during periods where registered domains are unregistered or unintentionally de-registered. Any Global objects that are locally cached during an unregisters operation may present namespace conflicts when re-registered with UCS Central if the exact same name still happens to exist for an object owned by UCS Central. To resolve such naming conflicts and return to Global control of the local object, use the globalize option on local object ("Use Global" Action from the UCSM GUI)[39]

n) VLANs and VSANs may persist locally

If VLANs/VSANs were created globally and subsequently pushed down through a GSP deployment, then they may persist in the local domain's MIT, even after the domain has de-registered. Upon de-registration when NOT using "Deep Remove Global", all Global VLANs/VSANs, Policies and Service Profiles are converted to local objects. An option would be to utilize "Deep Remove Global" during de-registration which will remove all global objects from the UCS Domain.

[39] The "Use Global" operation will overwrite any local changes that may have been performed on the local policy during the unregistered state.

o) Local UCS backups will not have global references

If backups are taken at the local UCSM level, then these backups will not have any references to Global objects that are managed by UCS Central.

If using UCS Central, then Backup/Export Policies should be used, with Backup operations managed exclusively by UCS Central.

17. Known Caveats as of 1.3(1a)

a) Adopting Global MAC/WWxN Pools

If changing Local Service Profile VNICs/VHBAs from local to global ID pool references, make sure to use UCSM 2.1(3a) at minimum, due to a defect fixed in 2.1(3a).

b) Server Pool members aren't masked by RBAC

Viewing members of a Global Server Pool are not currently masked by RBAC. As a workaround, please use the "Equipment View" for viewing Server inventory. Viewing servers through the Global Server Pool view may allow visibility to pool members, for which any access and configuration may actually be constrained, due to RBAC enforcement.

c) Host FW Package and Maintenance Policies

During the 1.0(1a) release, Host FW Packages and Maintenance Policies were erroneously structured within the Domain Group context. Due to the resulting backward compatibility issues, Host Firmware Packages & Maintenance Policies are now both visible and configurable from a Domain Groups context as well as Orgs context.

The expected behavior for UCS Central going forward is:

- Global Service Profiles will only refer to the Host FW Package that is defined under Organization context and not the Domain Group context.
- Local Service Profile (created in UCSM) can only refer to the Host FW Package from the Domain Group context --- same as release 1.0(1a)
- After a Global Service Profile is associated with a Server, the Host FW Package and Maintenance Policy (and any other referenced policies) are "pulled" from UCSM to UCS Central.
- Subsequently, a Local Service Profile can then refer to either the Host FW Package or Maintenance Policy from either the Org or Domain Group context.

- Global Service Profiles will only reference Host FW Packages and Maintenance Policies from Organization context.

This behavior is due to backward compatibility issues with the 1.0(1a) release, where Maintenance policies, Host FW packages, and Schedulers are defined under the Domain Group context.

Best Practice

The Best Practice would be to configure and use Host FW Packages, Maintenance Policies and Schedules exclusively from the Organization context.

d) Import UCS Central Configuration from Backup

Backups of UCS Central itself that are created on the "Administration" tab must be imported through "Operations Management -> Backup and Import -> UCS Central".

e) Default FCoE VLAN ID is "1" for VSANs

When creating new VSANs from the "SAN Cloud", the default FCoE VLAN ID value is "1", which is in conflict with the "global-default" VLAN ID value.

Be sure to change the FCoE VLAN ID when creating new VSANs, and specify a VLAN that is not currently in use anywhere else.

f) Unable to Import backups from Remote file locations for domains

Backups for UCS Central itself and for Domains can be configured (Full-State Backup or Config-All Export Policies) for "Copy to Remote File System". However, only the UCS Central backups can be subsequently imported from a Remote File System. Any Domain backups that only reside on a Remote File System would have to be imported through the local UCSM.

18. Summary

With great power comes great responsibility.

Please be careful and use your new power wisely.

JEFF Silberman is a Data Center Architect and part of the original UCS Technical Marketing Team, Jeff has authored the original "UCS Best Practice/Quickstart Guide", the "UCS Test Drive" and the "UCS Deep Dive Methodology". At Cisco, Jeff has been responsible for managing hundreds of customer proof of concepts, product reviews/demos, technical "Deep Dives" with UCS, and numerous Cisco Live presentations. Prior to Cisco, Jeff spent four years at NetApp in the Advanced Product Development Group, bringing some of the industry's first Unified Fabric solutions to market for Oracle®/NetApp environments.

19. Appendix I - UCS Central Frequently Asked Questions

Can you compare imports from two domains to see if they are different? If you have two UCS domains where you think things are configured the same, can you import both into UCS Central and see if they are the same or different?

No, it doesn't have a native diff function today. That is something that we may consider for about a year from now. You can export a Config-All backup from UCSC, extract the .tgz file, and import the policy-mgr.xml file into an XML Editor than performs a "Diff" function to compare two configurations.

Can we export UCS Central Reports in CSV or PDF format?

Not from the GUI at this time. I hope to see something in the GUI in 2H CY15, but that isn't committed yet. However, you can use the PowerTool, which now supports UCS Central to generate scripted reports that can be dumped into a file today.

How big 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.

The disk size requirement is a minimum of 80 Gb for the internal disks (2x 40GB Disks required for UCS Central Virtual Appliance). There is a limitation on 5 Domains for the Internal Database Statistics Collection, which only holds data for 2 weeks before rolling-over. Basically, outside of testing or a POC, you would ALWAYS want to leverage the ability to link UCS Central to an External (Postgres, SQL, Oracle) database for Statistics Collection. This integration may be enabled and integrated after installation. Consult the Install/Upgrade CLI Guide for UCSC.

Does UCS Central support alternate Disaster Recovery architectures such as VMware Site Recovery Manager (SRM)? Today, UCS Central does not support VMware Site Recovery Manager, but this is an enhancement that is being considered for a future release.

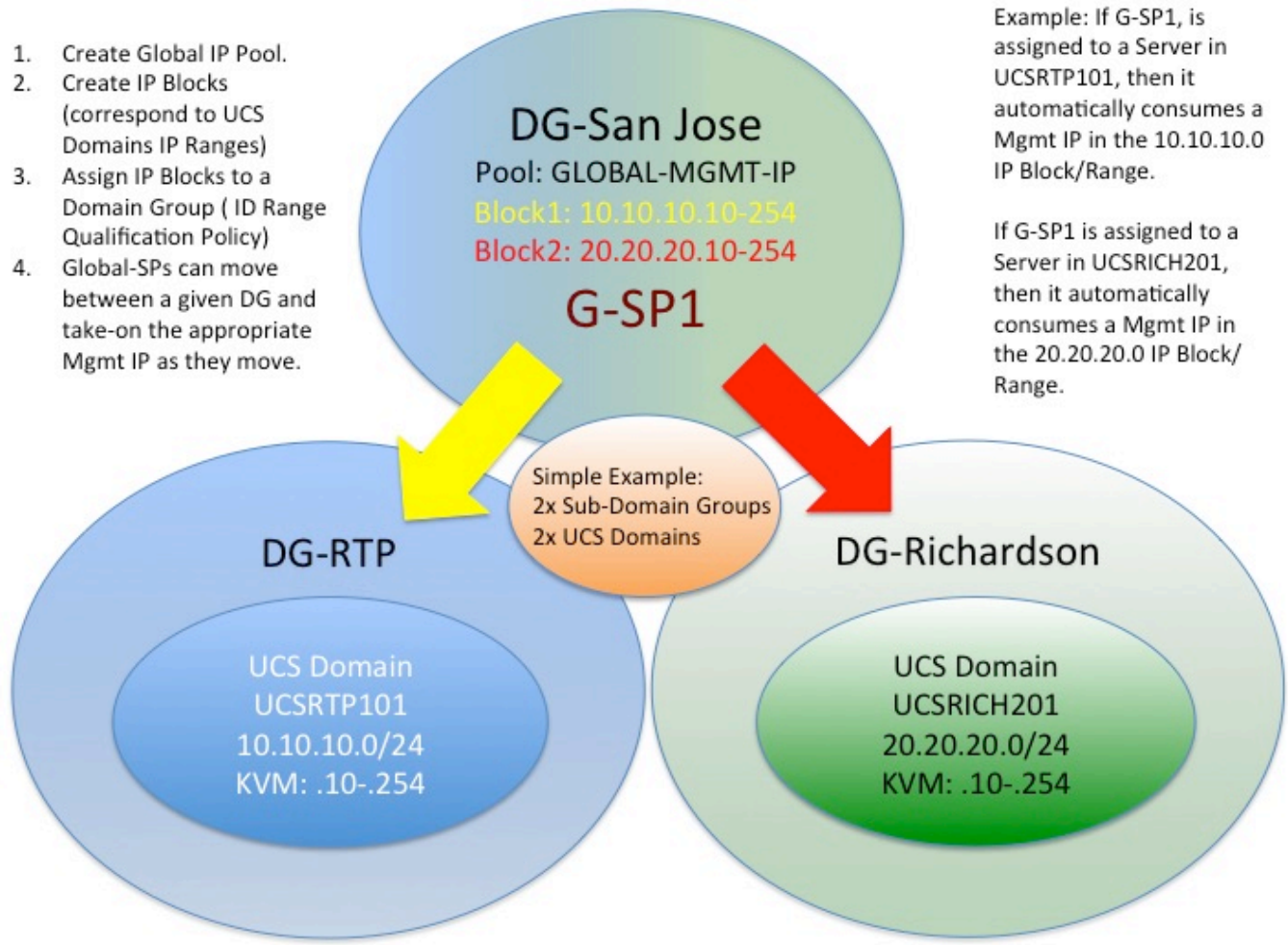
Explain UCS Central Licensing? Cisco UCS Central can be trialed for 120-days. At any time during the 120-day trial period, an initial license ("L-UCS-CTR-INI=") can be obtained through the standard Cisco Sales ordering process. At this time, the INI= license price is $0 and does not include support. Additional licenses – beyond the first 5 domains – can be purchased using "L-UCS-CTR-LIC=". Scenario: If you initially registered 5 UCS Domains to UCSC, then you would need the ("L-UCS-CTR-INI="). If later, you registered 5 additional UCS Domains, you would need ("L-UCS-CTR-INI=") plus ("L-UCS-CTR-LIC=5")

Do I have to still use a Global Service Profile and subsequent Server Association as a delivery mechanism in order to deliver/expose a VLAN or VSAN down to the UCS Domain? With UCS Central 1.3, there are new CLI Commands to push VLANs and VSANs down to the Registered UCS Domains. Consult the UCS Central CLI User's Guide for more information.

20. Appendix II – Example UCS Central Use Cases

a) Using ID Range Qualification Policies for Domain IP Management

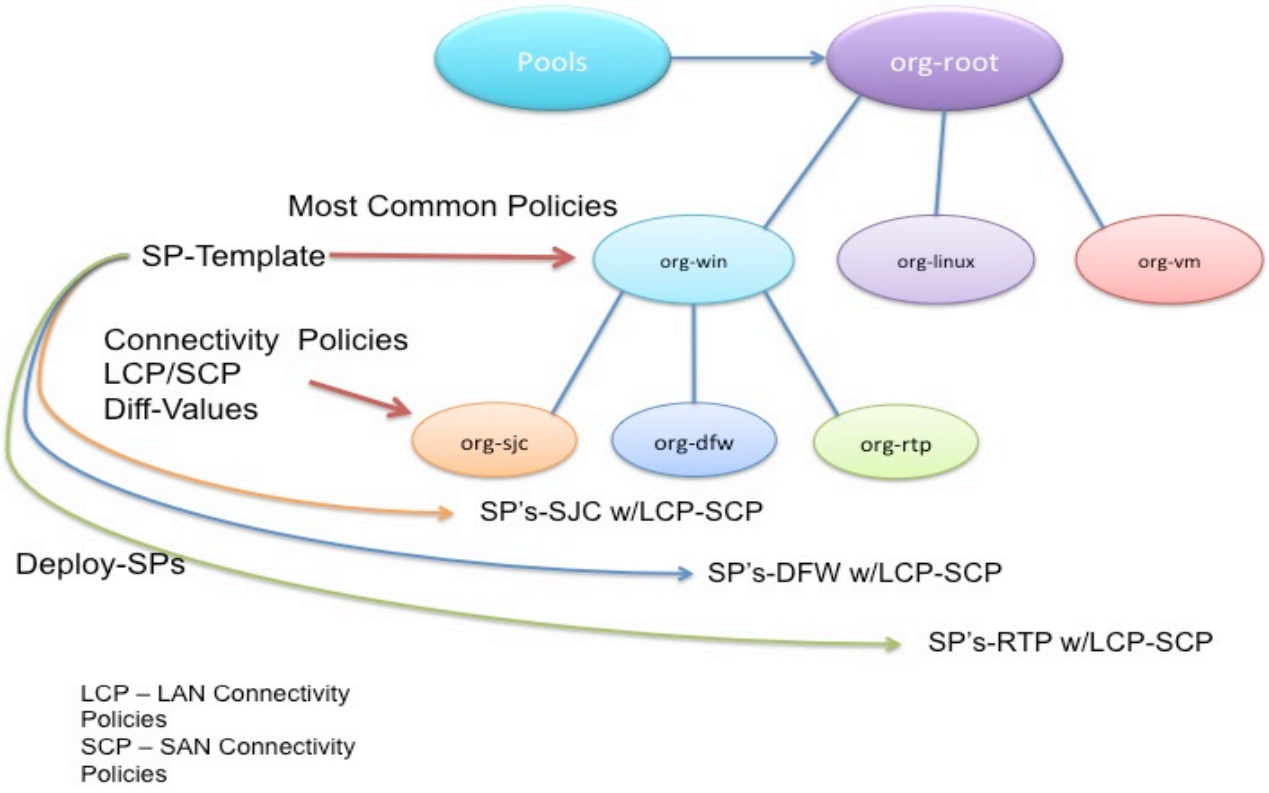
Here is an example of using ID Range Qualification Policies (now supported with Global SP's in UCS Central 1.3) to utilize the correct blocks of Management IPs to the proper UCS Domain as a Global Service Profile is migrated from one UCS Domain to Another. The Block(s) of IPs can be "assigned" to a Domain or Domain Group with the ID Range Qualification Policy. As the Global SP is migrated, a new Mgmt IP will accompany the association to the respective UCS Domain.



b) **Reduction of Global SP Templates**

Some larger organizations are always looking for ways to reduce the number of Global Service Profile Templates they have to create and maintain in their UCS Central Architecture. One way of achieving this goal (doing more with less) is to leverage the hierarchy policy resolution capabilities of UCS and UCS Central. Some organizations are putting their ID Pools at a very high level within the Organizational Structure because they cannot justify the absolute need to "segregate" ID's based upon the downstream organizations. Similarly, they also place the "most common" configuration policies very high in the organizational structure. With this mindset, they then rely on a great Policy Resolution Feature of UCS and UCS Central, by which a given policy with the same "name" can "exist" at different Organizational Levels or Organizations at the same level, but have different "values" embedded within those policies. Consequently, when a Global SP is created within that Organization, or moved to that Organization, the Global SP will "access" that particular named policy with the proper values for that particular organization.

In the example below, ID Pools and "most" polices are identified at a very high level within the overall Organizational Structure, but very "unique" LAN Connectivity Policies and Storage Connectivity Policies are defined at a lower, more granular level. However, they have the "Same Names" in the different Organizations. Thus, the Global SP will consume and use the correct Policy with the Correct Values based upon "where" that Global SP exists.



21. Appendix III UCS Central 1.3 Manual VLAN/VSAN Publishing

EXAMPLE:

UCSC-131S7-TRAIN# ***connect resource-mgr***
UCSC-131S7-TRAIN(resource-mgr)# ***scope domain-mgmt***
UCSC-131S7-TRAIN(resource-mgr) /domain-mgmt # ***show ucs-domain***
UCSC-131S7-TRAIN(resource-mgr) /domain-mgmt # ***scope ucs-domain 1008***
UCSC-131S7-TRAIN(resource-mgr) /domain-mgmt/ucs-domain # ***publish ?***
vlan Vlan
vsan Vsan
UCSC-131S7-TRAIN(resource-mgr) /domain-mgmt/ucs-domain # ***publish vlan vlan-name***

Note: This is only a "Publishing" mechanism; the VLAN or VSAN have to be previously created in UCS Central.

22. Appendix IV Check UCS Central Running-Services Status

UCSC-131S7-TRAIN# ***connect local-mgmt***
UCSC-131S7-TRAIN (local-mgmt)# ***show pmon state***

23. Appendix V UCS Central 1.3 HTML-5 Introduction VOD

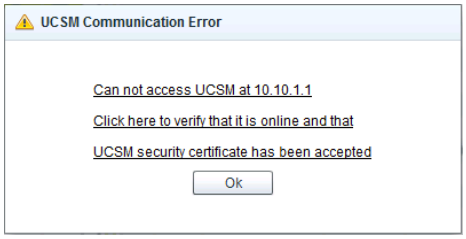
Introducing Cisco UCS Central 1.3(1a) HTML-5 UI

http://www-author.cisco.com/c/dam/assets/TD/video/repository/UCS/UCS_Central/Introducing_UCS_Central_1-3/introducing_cisco_ucs_central_1_3.mp4

24. Appendix VI Certificate Troubleshooting

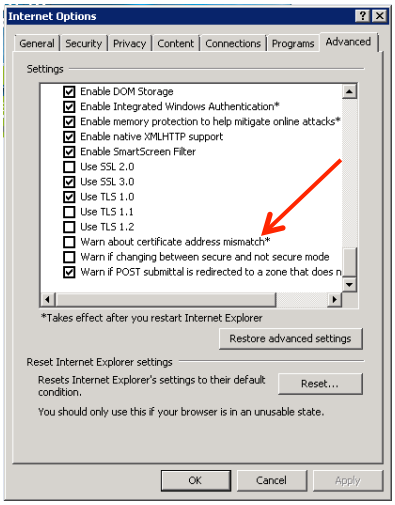
Cisco UCS Central – Troubleshooting Certificate errors

Many features of the UCS Central management interface rely on https certificates (from each UCS Domain being managed by UCS Central) to be available and imported on the client machine.
These certificates are used by the browser managing UCS Central for invoking features such as KVM Launch, UCSM GUI Launch, and query of particular faults/alerts in the UCS Fault Summary. If the certificates are not imported properly, have expired, or if the Web Browser being used has certain security settings enabled, the user may encounter the errors seen below:

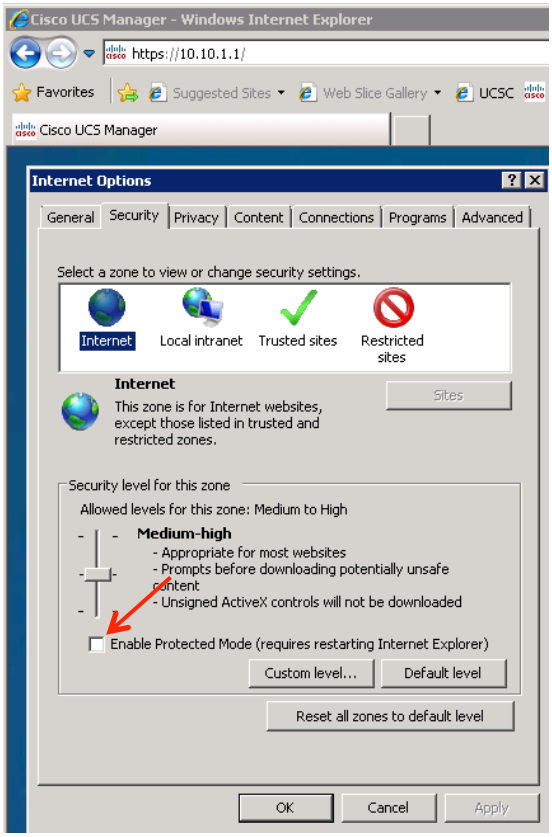


Internet Explorer

1. Be sure that IE is configured to NOT warn about a certificate address mismatch
   a. In IE: Tools → Internet Options → Advanced – at the very bottom in the section "Security", be sure to uncheck "Warn about certificate address mismatch" (Requires restart of IE)

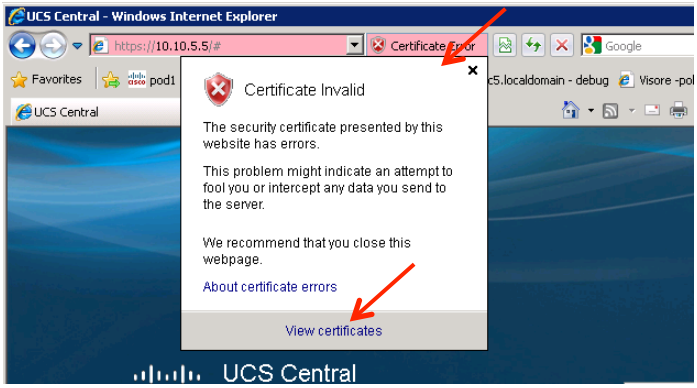


2. You may need to turn off “Protected Mode” so that Certificates can be imported.
    a. Tools → Options → Security Tab → uncheck the Enable Protected Mode checkbox for each zone:

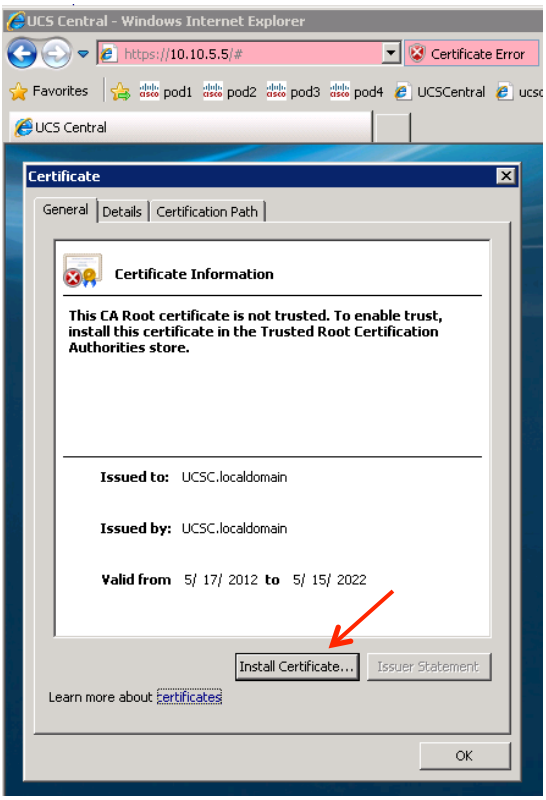


3. Upon initial connection to any UCS Central or UCS Manager, you will receive a Certificate Error. Import the presented certificate using this process:

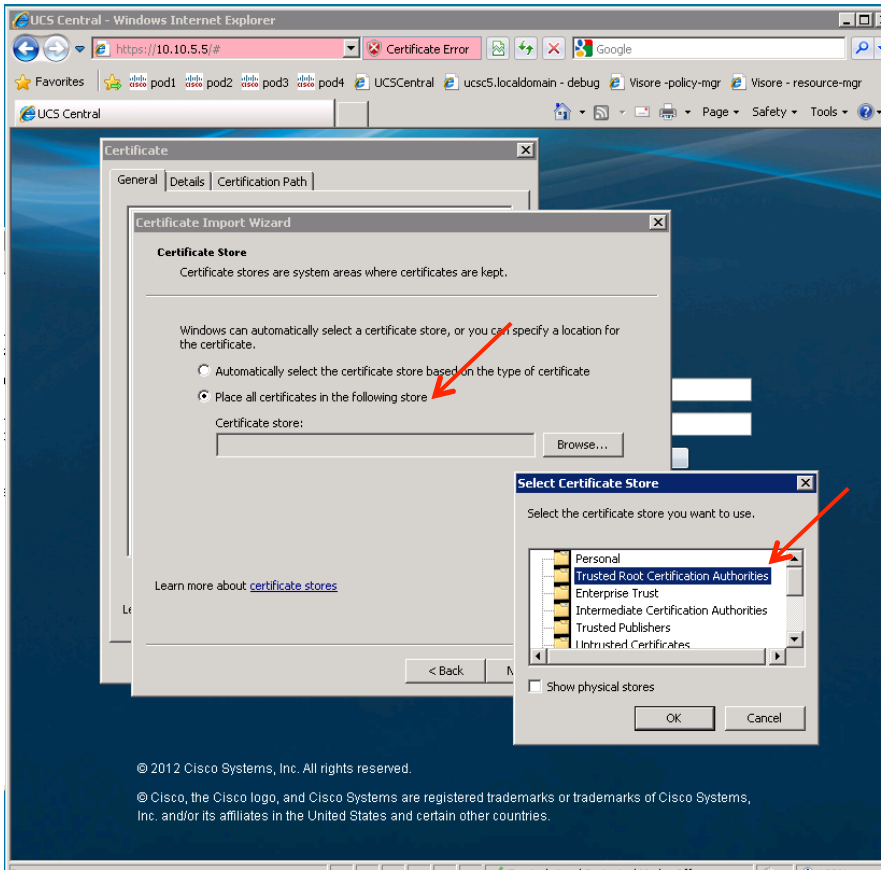
Click the Certificate error, and then click view Certificates, followed by clicking Import



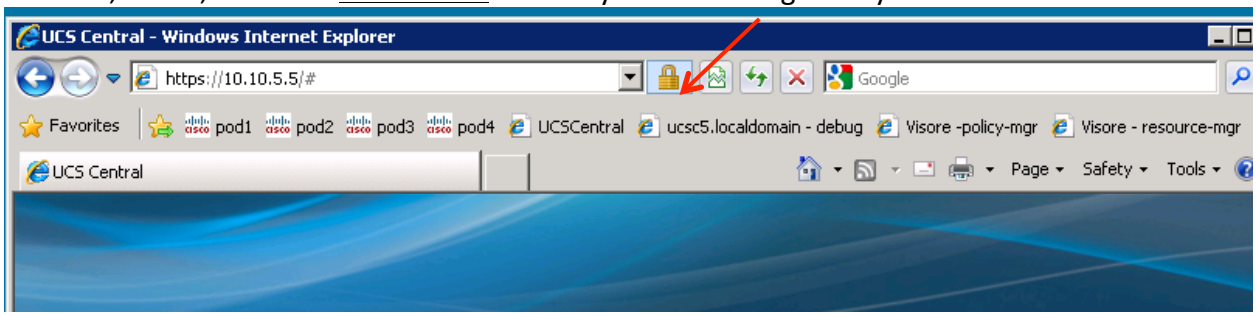
Then click Install Certificate:



Click next and select “Place all Certificates in the following store” radio button



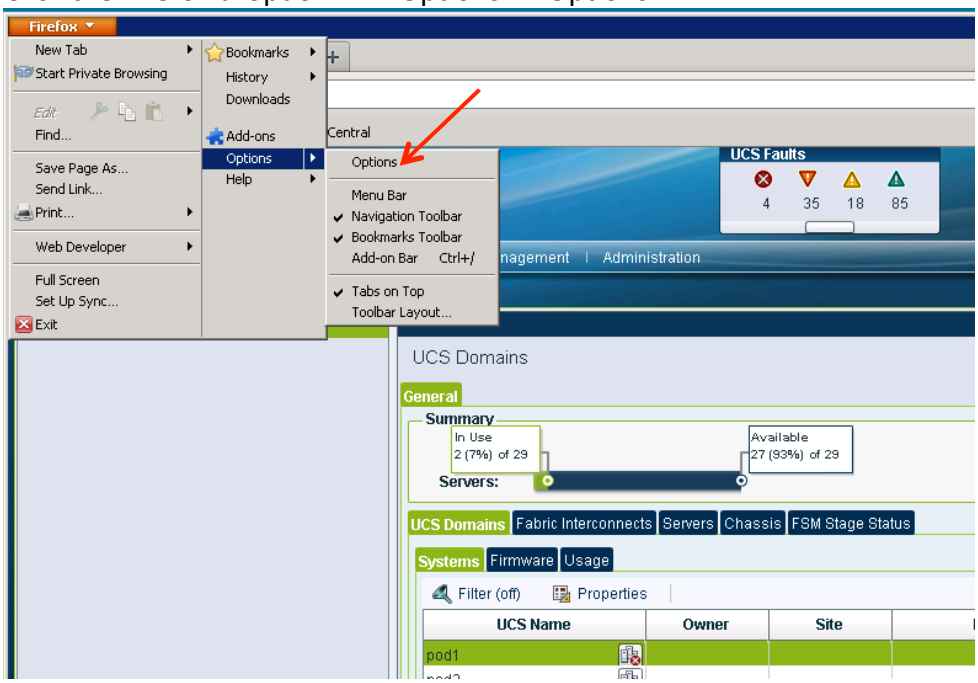
Click OK, Finish, and then **RESTART IE** – when you connect again in you should not see the certificate errors:

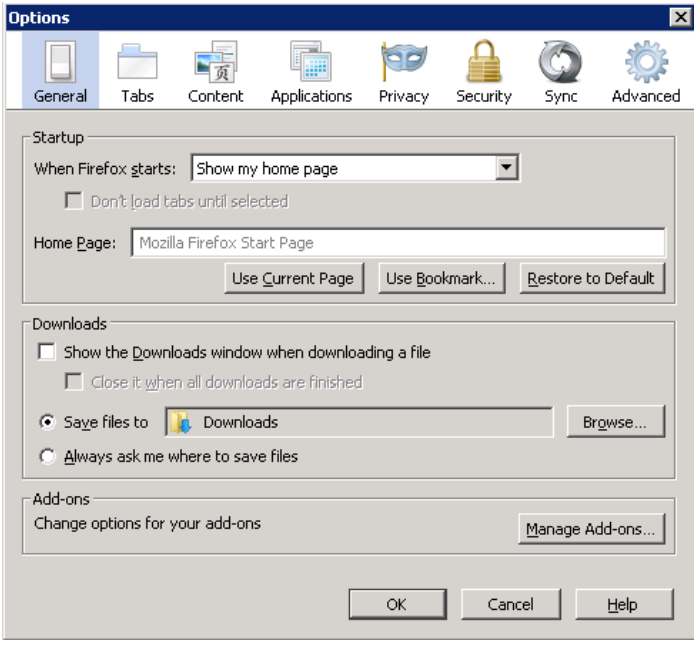


Mozilla Firefox

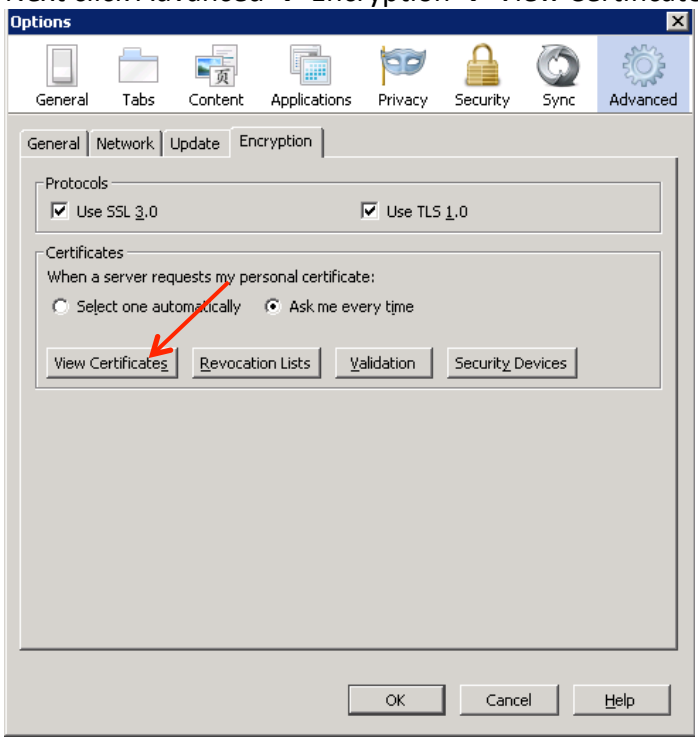
Steps to clear out all Certificates / cache:

Click the Firefox dropdown → Options → Options:

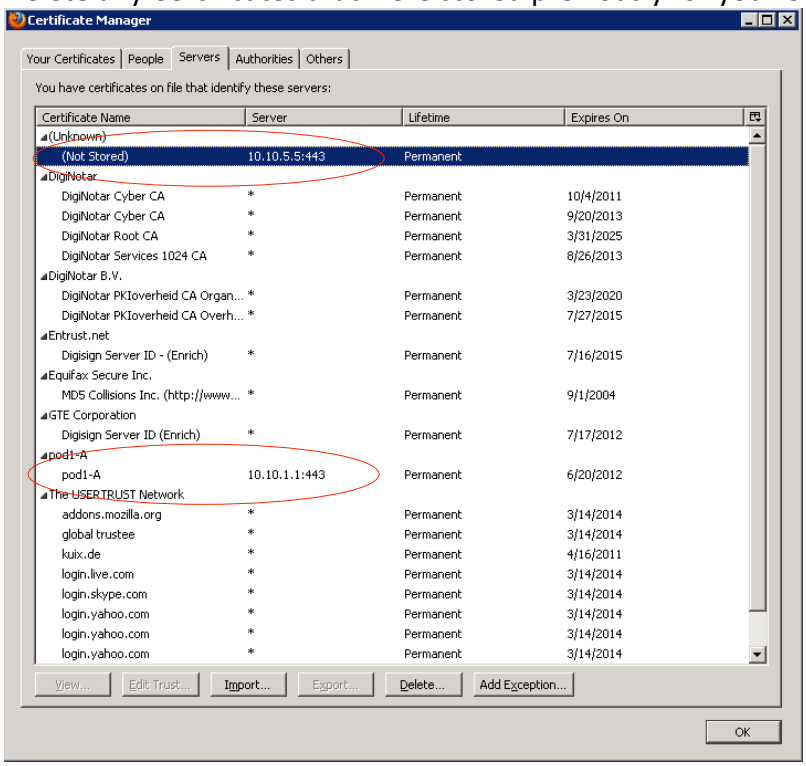




Next click Advanced → Encryption → View Certificates:

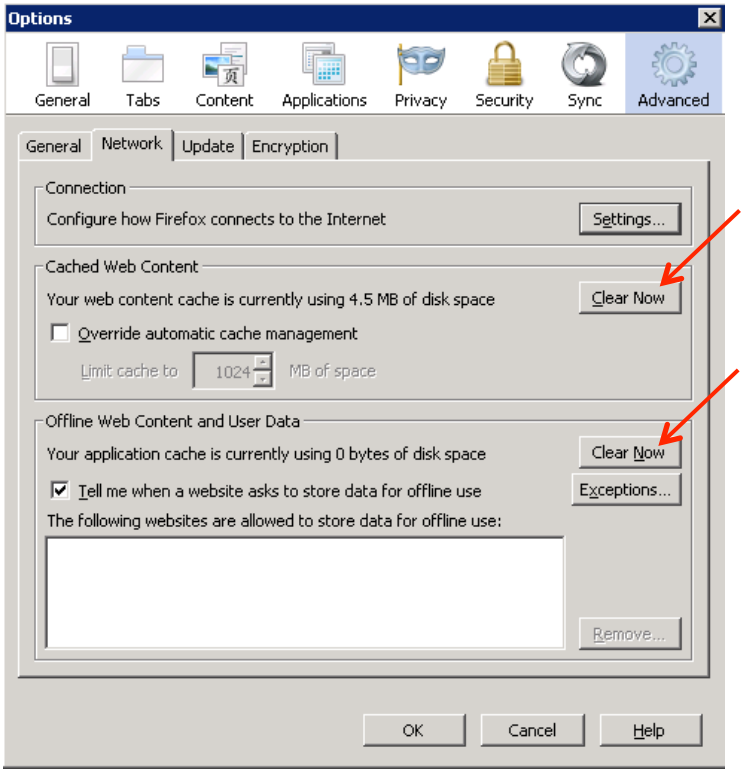


Delete any Certificates that were stored previously for your UCS or UCSCentral systems (only)



Once complete, clear the Web Cache. Click the Firefox dropdown → Options → Options, and then click The Advanced button, then Network tab.

- Click both of the "Clear Now" button s on this page – then click OK to close.

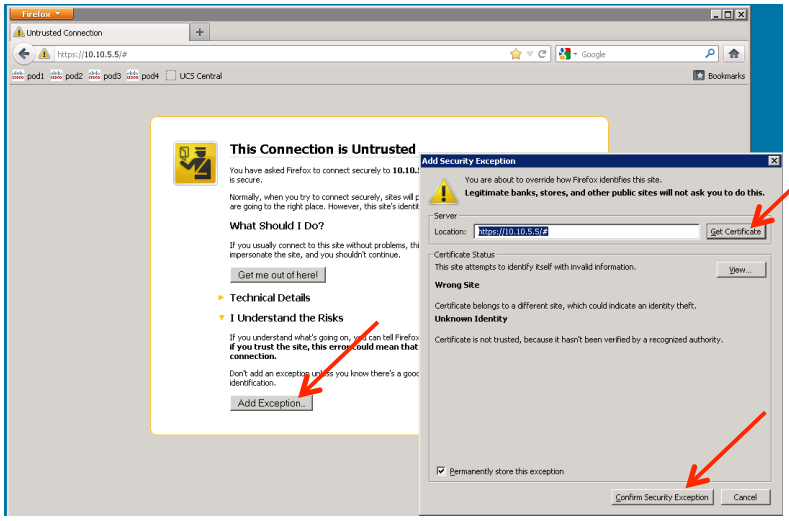


You should now be able to connect to UCS Central (import certificate) and launch UCSM.

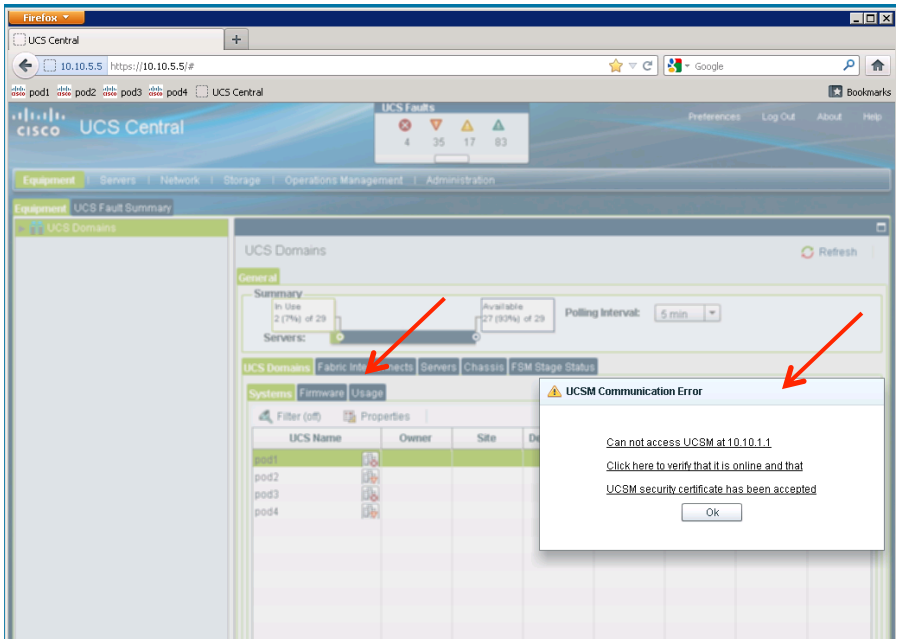
- Note: You will need to connect to each UCSM system (manually, or through UCS Central) at least once to import the certificate, so that subsequent attempts to launch the GUI from within UCS Central will happen without certificate errors.

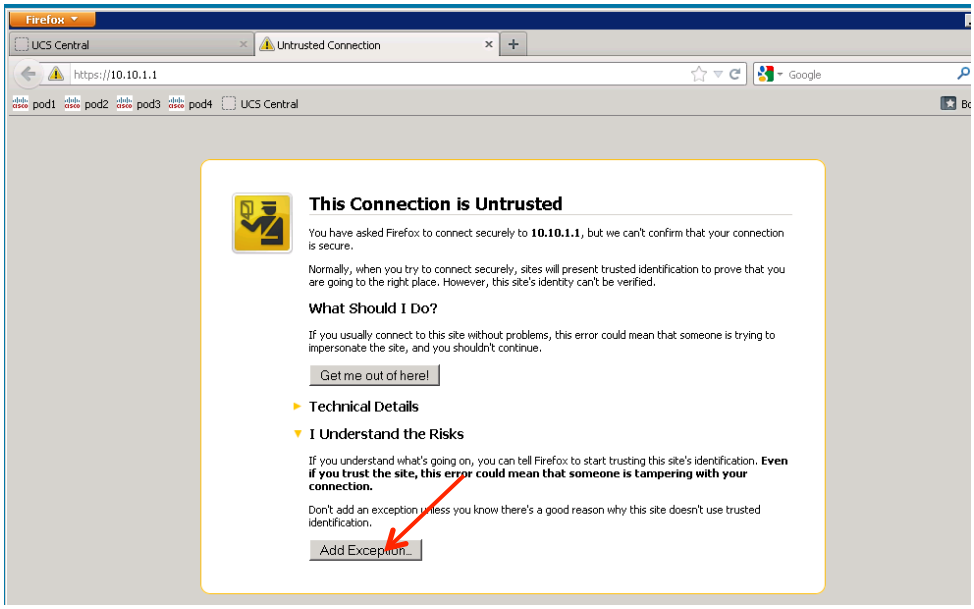
To add the certificate using Firefox:

- Click Add Exception, Get Certificate, and Confirm Security Exception as seen below



If Launching from UCS Central, Clicking the error in the link below will launch UCSM and allow you to import the Certificate





Other

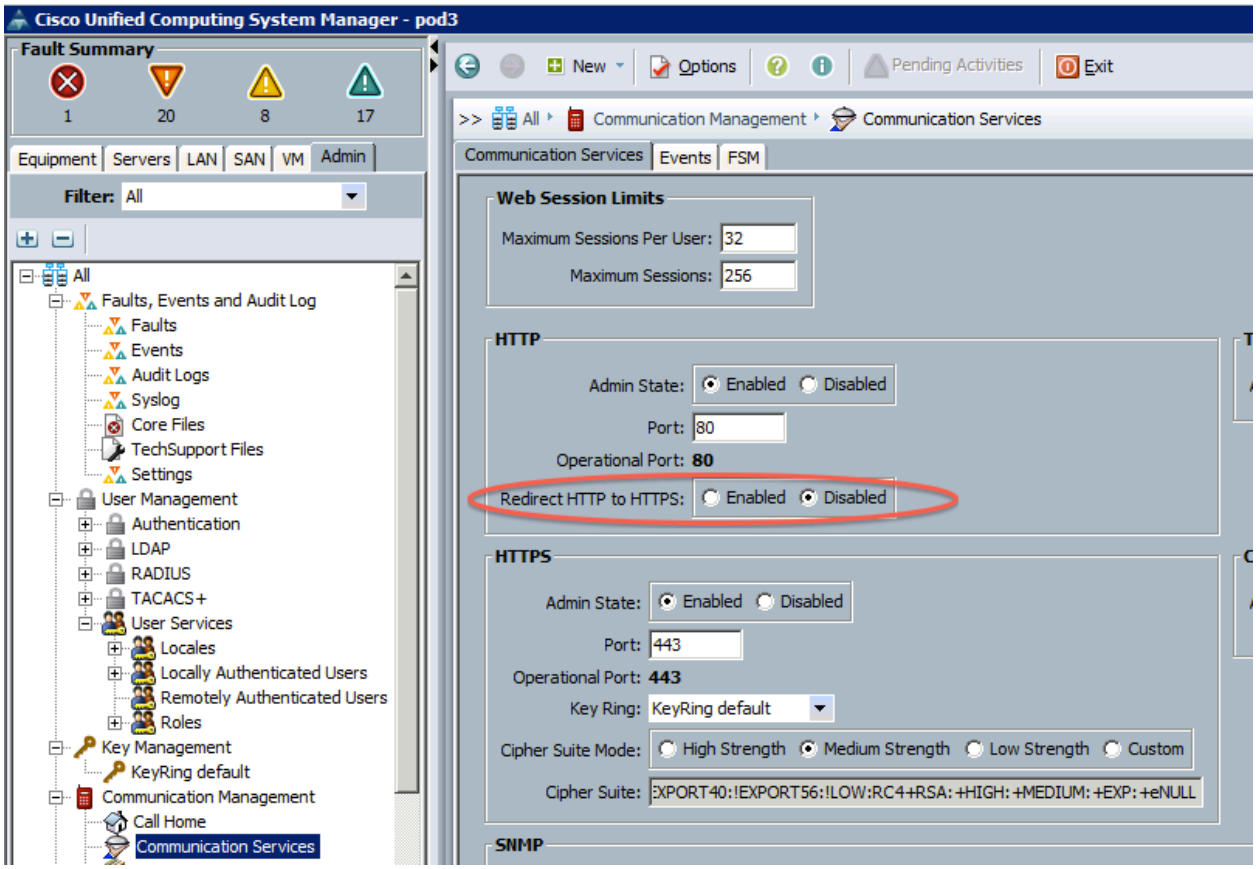
1. Expired Certificates:

Make sure that the HTTPS Certificates being presented by the Fabric Interconnects are not expired.

- If the Certificates are expired, The UCS Documentation details the process to "regenerate" new HTTPS Certificates:
- UCSM CLI commands: scope security; scope keyring <keyring_name>; set regenerate yes; commit-buffer

2. Bug affecting regeneration of new HTTPS Certificates on the Fabric Interconnects:

NOTE: There is a bug in 2.1(1a), where in some cases, after regenerating new HTTPS Certificates, that the old certificate are not published immediately to the web servers on the Fabric Interconnects. To work around this bug (until it is fixed in the next release), toggle the HTTP → HTTPS redirection setting in the Admin Tab / Communication Services:


Cisco Unified Computing System Manager - pod3
Fault Summary
1
20
8
17
Equipment
Servers
LAN
SAN
VM
Admin
Filter: All
All
Faults, Events and Audit Log
Faults
Events
Audit Logs
Syslog
Core Files
TechSupport Files
Settings
User Management
Authentication
LDAP
RADIUS
TACACS+
User Services
Locales
Locally Authenticated Users
Remotely Authenticated Users
Roles
Key Management
KeyRing default
Communication Management
Call Home
Communication Services
New
Options
Pending Activities
Exit
>> All
Communication Management
Communication Services
Communication Services
Events
FSM
Web Session Limits
Maximum Sessions Per User: 32
Maximum Sessions: 256
HTTP
Admin State: Enabled Disabled
Port: 80
Operational Port: 80
Redirect HTTP to HTTPS: Enabled Disabled
HTTPS
Admin State: Enabled Disabled
Port: 443
Operational Port: 443
Key Ring: KeyRing default
Cipher Suite Mode: High Strength Medium Strength Low Strength Custom
Cipher Suite: EXPORT40:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL
SNMP