Managing UCS Central at Scale

Scaling Considerations for different UCS Central Architectures

Updated for UCS Central 1.4.1a

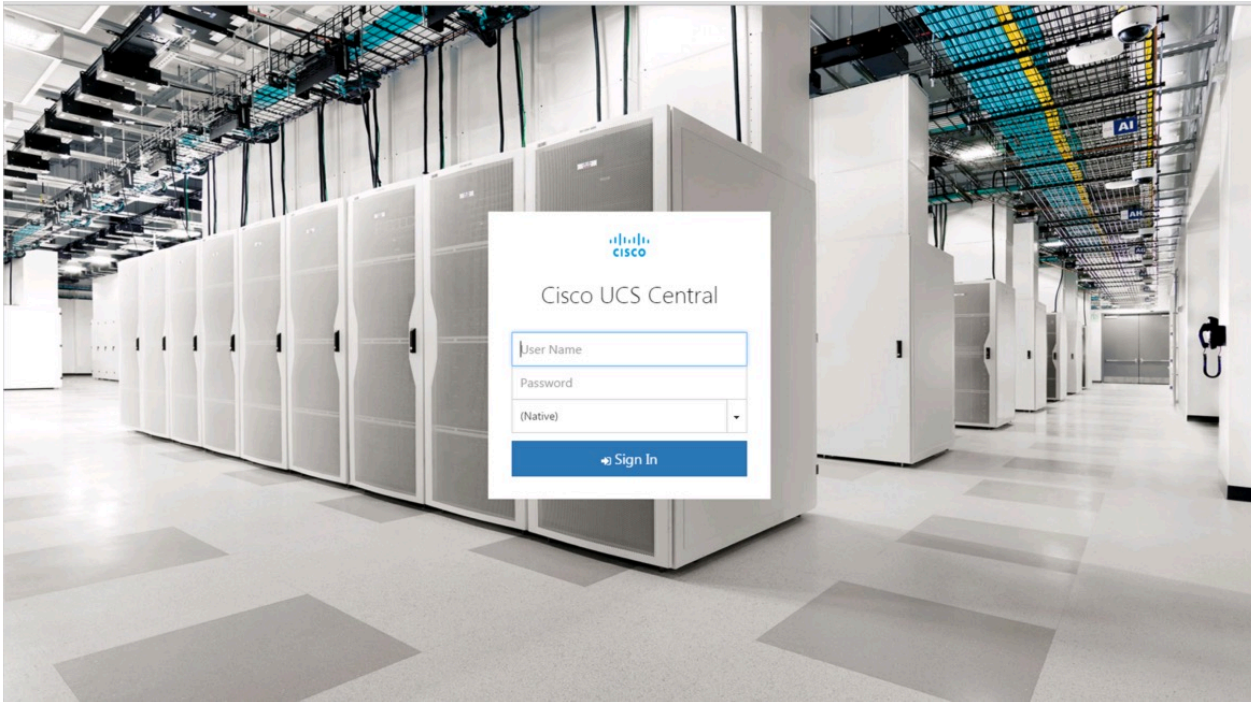


Table of Contents

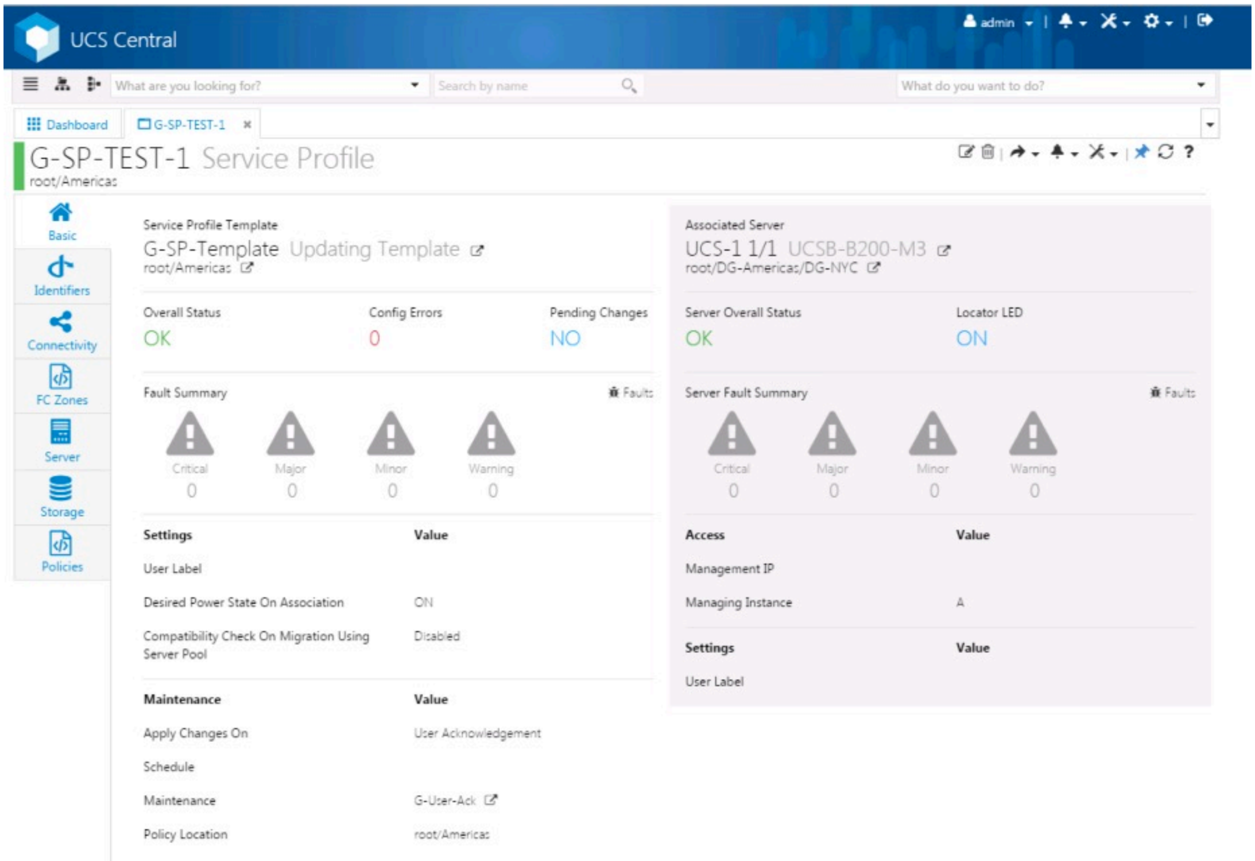
Introduction

The setup architecture of UCS Central can be very flexible in how you manage your registered UCS Domains, especially considering number and geographic dispersion of those domains. Some principles will carry forward throughout the different architectures regardless of size and scope, while others might be more conducive to a specific size.

It's important to envision the "eventual" size and scope of a UCS Deployment when implementing UCS Central. An organization might start with a relatively few number of new UCS Domains, but have the expectation of dramatically scaling the number of those domains, and servers over a period of 1-3 years. Alternatively, they may start with an environment that isn't expected to have significant scale changes. Regardless of the scenario, UCS Central provides a tremendous amount of value to any size organization and it's always best to build and plan for future management.

In addition to size, there is also the considerations of whether the environment is "Brownfield" or "Greenfield". In terms of UCS Central, Brownfield environments would include UCS Central registration of UCS Domains that have been previously built-out and deployed, and contain localized objects such as Pools, Policies, VLANs/VSANs, Templates and Service Profiles for each UCS Domain. If an object is "Local", that means the object is owned by UCS Manager (UCSM), and only a UCS Manager administrator can add/modify/delete the object. Effectively, UCS Manager has read/write control on the object. If an organization deploys UCS and UCS Central in a Greenfield environment, that means all objects (Pools, Policies, VLANs/VSANs, Templates and Service Profiles) are created global in scope. If an object is "Global", that means the object is owned by UCS Central, and only a UCS Central Administrator can add/modify/delete the object from UCS Central, not from UCS Manager in a specific domain. UCS Central maintains read/write ownership of all global objects. When you deploy a Global Service Profiles (G-SPs) from UCS Central to a blade/server in a UCS Domain, a "Shadow Copy" of the Global Service Profile actually deploys down to UCS Manager and is instantiated into the proper Org on the Server Tab. I view of the Server Tab, LAN Tab and SAN Tab will show that Global Policies, VLANs, VSANs, vNIC/vHBA Templates, and ultimately Global SPs will appear, with the special Global Icon. By design, Global Service Profile Templates will not copy-down to UCS Manager, as there is no meaningful reason to copy-down that Global Object.

Global Service Profile: G-SP-TEST-1



G-SP-TEST-1 Service Profile
root/Americas

Service Profile Template
G-SP-Template Updating Template
root/Americas

Associated Server
UCS-1 1/1 UCSB-B200-M3
root/DG-Americas/DG-NYC

Overall Status	Config Errors	Pending Changes
OK	0	NO

Server Overall Status	Locator LED
OK	ON

Fault Summary

Critical	Major	Minor	Warning
0	0	0	0

Server Fault Summary

Critical	Major	Minor	Warning
0	0	0	0

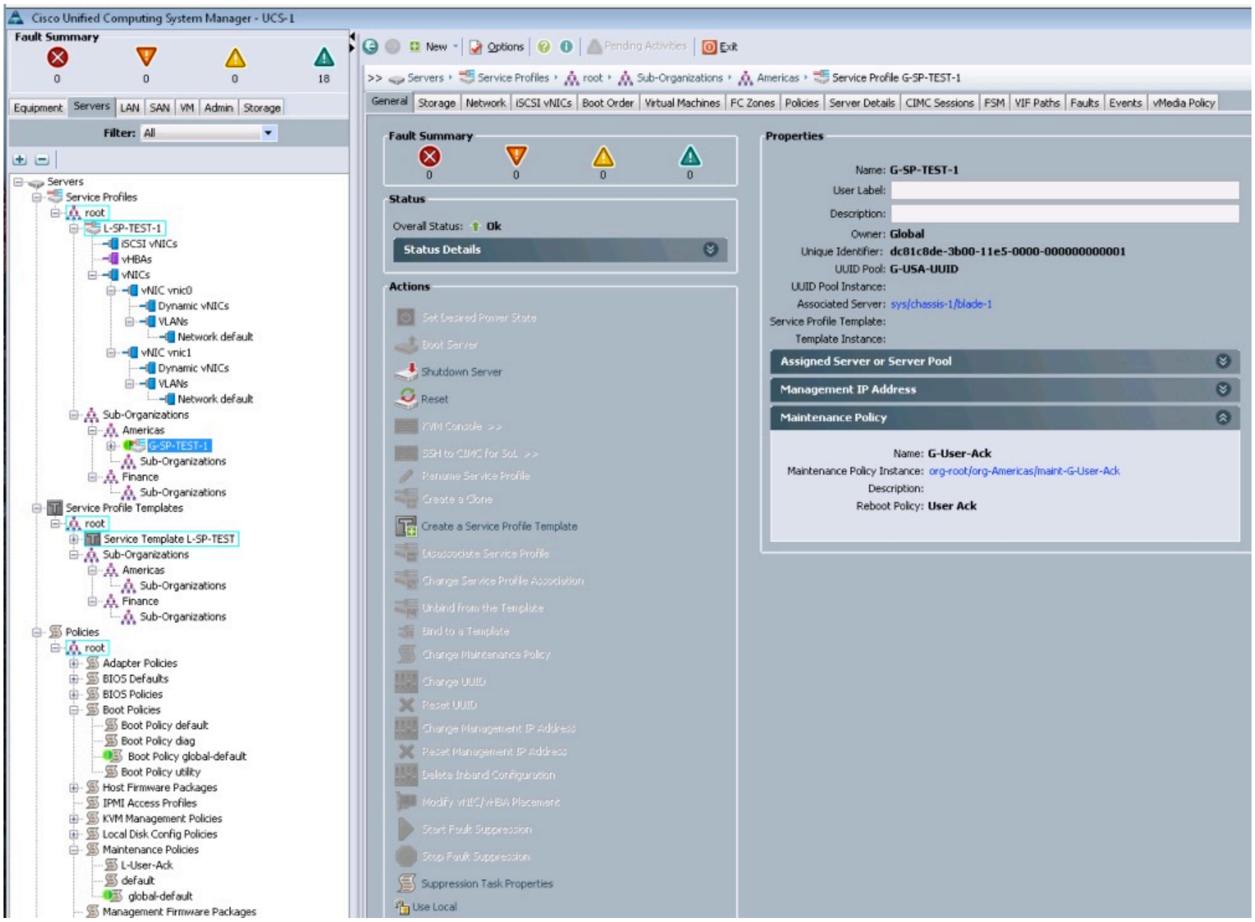
Settings	Value
User Label	
Desired Power State On Association	ON
Compatibility Check On Migration Using Server Pool	Disabled

Maintenance	Value
Apply Changes On	User Acknowledgement
Schedule	
Maintenance	G-User-Ack
Policy Location	root/Americas

Access	Value
Management IP	
Managing Instance	A

Settings	Value
User Label	

UCS Manager showing deployed G-SP-TEST-1



Overall Status: Ok

Name: G-SP-TEST-1
User Label:
Description:
Owner: Global
Unique Identifier: dc81c8de-3b00-11e5-0000-000000000001
UUID Pool: G-USA-UUID
UUID Pool Instance:
Associated Server: sys/chassis-1/blade-1
Service Profile Template:
Template Instance:

Name: G-User-Ack
Maintenance Policy Instance: org-root/org-Americas/maint-G-User-Ack
Description:
Reboot Policy: User Ack

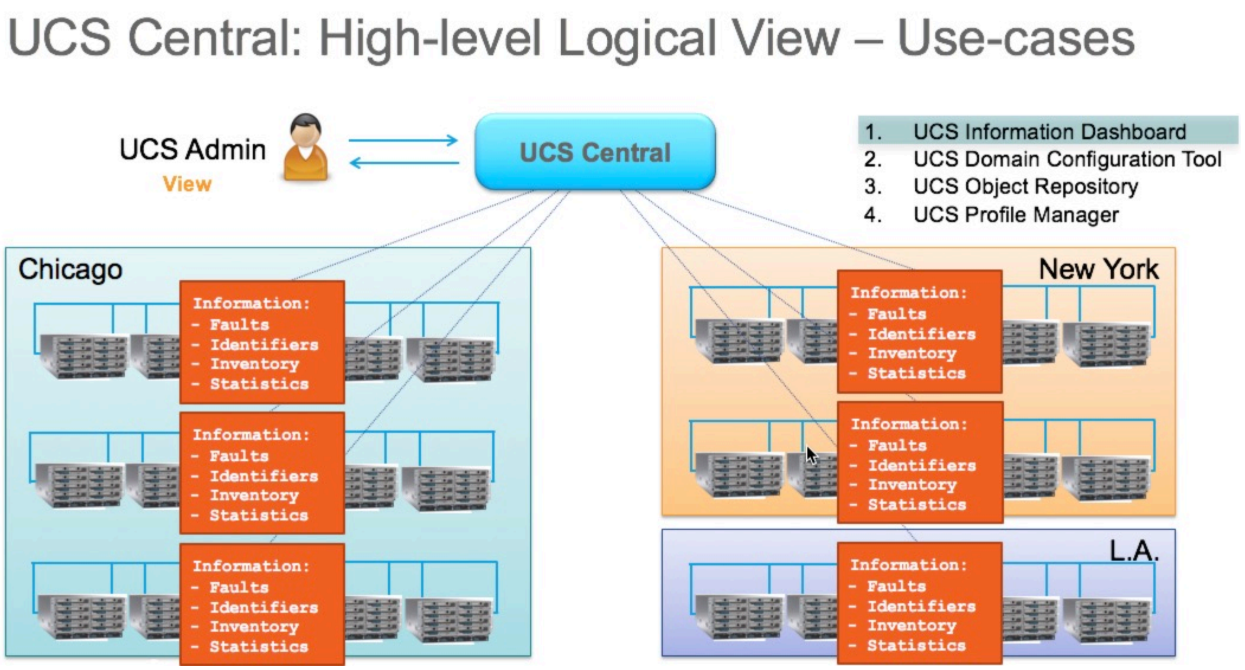
In this document, we'll discuss different architecture considerations for different size clients. While it's hard to label the "size" of an environment, we tried to categorize based upon average sizes of the existing UCS Central client base, as well as considering some of the largest UCS Central Environments, those exceeding 300 registered domains and in excess of 6000 managed servers. The current version of UCS Central, version 1.4 has been tested to support environments up to 10,000 registered servers. While it is impossible to actually label the size and scale of environment, based upon numbers of Domains (for instance a UCS Mini Environment may only have a single chassis), for the purpose of this document, we'll define following size ranges:

- Small Environment: 1-3 Registered UCS Domains.
- Medium Environment: 4-12 Registered UCS Domains
- Large Environment: >12 Registered UCS Domains

UCS Central Use Cases – Revisited

UCS Central has many uses that justify its implementation in all sizes of UCS Environments. Before UCS Central existed, deployments of UCS Domains were largely repetitive, manual, time consuming exercises that requires strict attention to the creation and consistency of ID Pools, Policies, VLANs/VSANs, Templates and Service Profiles. It was especially easy to misconfigure an ID Pool, perhaps a MAC Address Pool with the exact “scheme” of another existing UCS Domain in the environment. For example, “00:25:B5:00:00:00” is the default start-construct of each block of MAC addresses defined in UCS Manager. If an administrator or implementer uses this exact scheme in more than one UCS Domain, within the same Layer-2 Domain, then serious problems arise with MAC Address conflicts. UCS Central inventories the entire registered UCS environment and eliminates the possibility of such conflicts. Let’s review and discuss the major Use Cases for UCS Central in detail.

1. UCS Information Dashboard

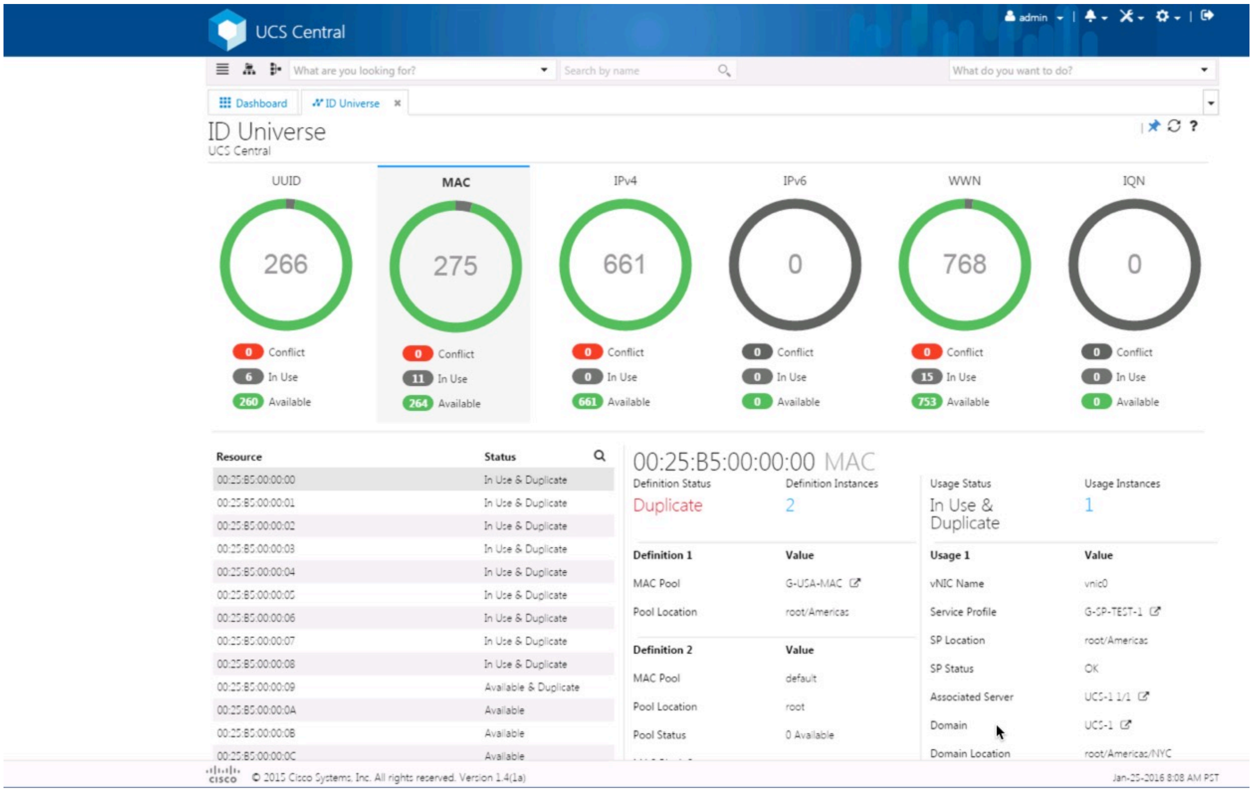


UCS Central: High-level Logical View – Use-cases

1. UCS Information Dashboard
2. UCS Domain Configuration Tool
3. UCS Object Repository
4. UCS Profile Manager

After registering a UCS Domain to UCS Central for the first time, an extensive inventory of the UCS Domain is taken and that information is passed up to the UCS Central database. Critical information from each registered UCS Domain, such as Faults, ID Pools (Used IDs and Available IDs), UCS Hardware Inventory for the entire UCS Domain and Statistics get populated into UCS Central. This process happens quickly upon registration and does not pose any threat to possible existing servers running local workloads with locally defined service profiles. Just to reiterate, it is always safe to register a UCS Domain to UCS Central. There is no chance of the registration causing an outage with running workloads on a UCS Domain. If a current UCS Domain is operating in a brownfield scenario, administrators can still leverage the great utility benefit of this “Dashboard” use case from the first day of registration. For example, by registering all UCS Domains to UCS Central, administrators will have full accountability of all created ID pools and IDs across their entire infrastructure. Administrators can leverage the “ID Universe” in the HTML-5 UI of UCS Central to see, maintain and enforce ID accountability.

ID Universe



ID Universe
UCS Central

	UUID	MAC	IPv4	IPv6	WWN	IQN
Total	266	275	661	0	768	0
Conflict	0	0	0	0	0	0
In Use	6	11	0	0	15	0
Available	260	264	661	0	753	0

Resource	Status
00:25:B5:00:00:00	In Use & Duplicate
00:25:B5:00:00:01	In Use & Duplicate
00:25:B5:00:00:02	In Use & Duplicate
00:25:B5:00:00:03	In Use & Duplicate
00:25:B5:00:00:04	In Use & Duplicate
00:25:B5:00:00:05	In Use & Duplicate
00:25:B5:00:00:06	In Use & Duplicate
00:25:B5:00:00:07	In Use & Duplicate
00:25:B5:00:00:08	In Use & Duplicate
00:25:B5:00:00:09	Available & Duplicate
00:25:B5:00:00:0A	Available
00:25:B5:00:00:0B	Available
00:25:B5:00:00:0C	Available

00:25:B5:00:00:00 MAC

Definition Status	Definition Instances	Usage Status	Usage Instances
Duplicate	2	In Use & Duplicate	1

Definition 1	Value
MAC Pool	G-USA-MAC
Pool Location	root/Americas

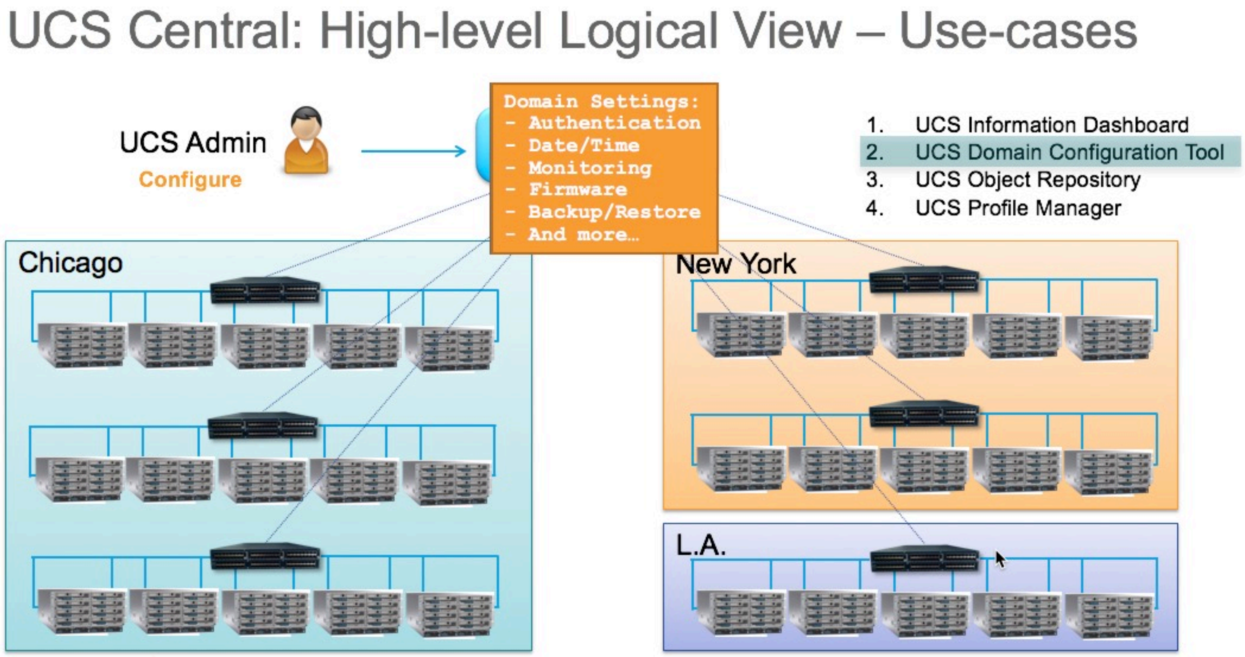
Definition 2	Value
MAC Pool	default
Pool Location	root
Pool Status	0 Available

Usage 1	Value
vNIC Name	vnic0
Service Profile	G-SP-TEST-1
SP Location	root/Americas
SP Status	OK
Associated Server	UCS-1 1/1
Domain	UCS-1
Domain Location	root/Americas/NYC

© 2015 Cisco Systems, Inc. All rights reserved. Version 1.4(1a)   Jan-25-2016 8:08 AM PST

Another interesting fact about UCS Central is its ability to provide a “Custom View” of the environment, based upon a User’s Login ID and “locale” as defined within UCS Central. Whereas UCS Manager will provide a read-only view to the entire infrastructure from an organizational basis, UCS Central can limit the user to a specific “branch” or subset of the Organization by defining and using locales. There will be more detail about using this functionality later in the document in the section Rule-Based Access Control (RBAC) and UCS Central Custom Views.

2. UCS Domain Configuration Tool (Operational Policies)

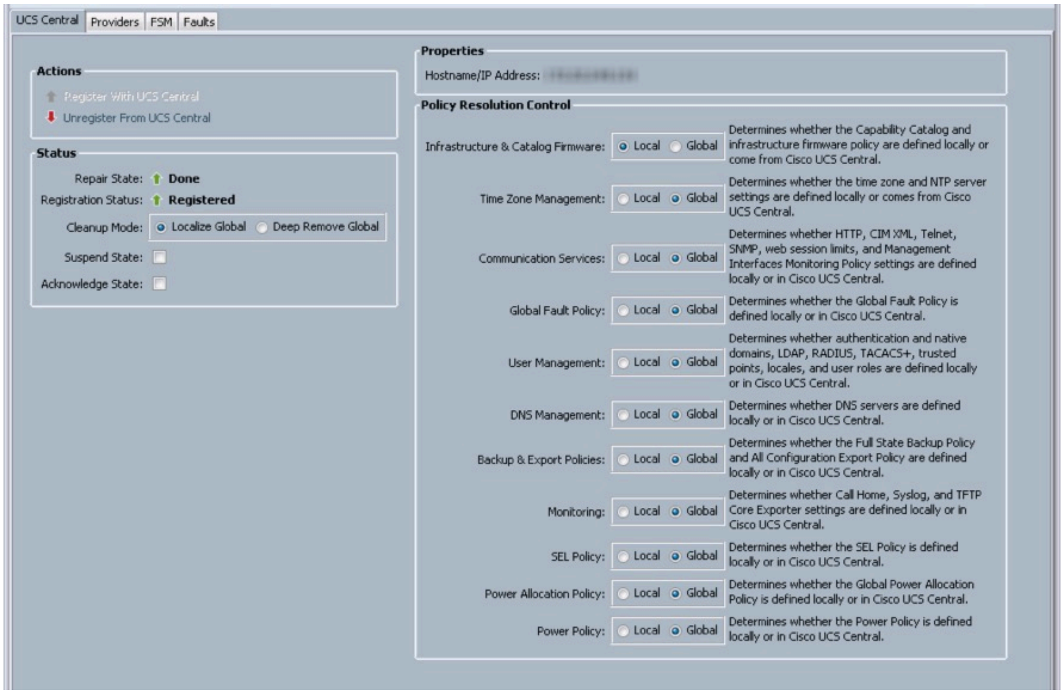


UCS Central: High-level Logical View – Use-cases

1. UCS Information Dashboard
2. UCS Domain Configuration Tool
3. UCS Object Repository
4. UCS Profile Manager

Another great use case and ability of UCS Central is managing “Global” operational policies from a single management point in your infrastructure. These Policies are the operational policies you find on the UCS Central registration tab within UCS Manager, as appears below.

UCS Central Registration in UCS Manager



Actions

Register With UCS Central

Unregister From UCS Central

Status

Repair State: Done

Registration Status: Registered

Cleanup Mode: ● Localize Global ○ Deep Remove Global

Suspend State: □

Acknowledge State: □

Properties

Hostname/IP Address: [redacted]

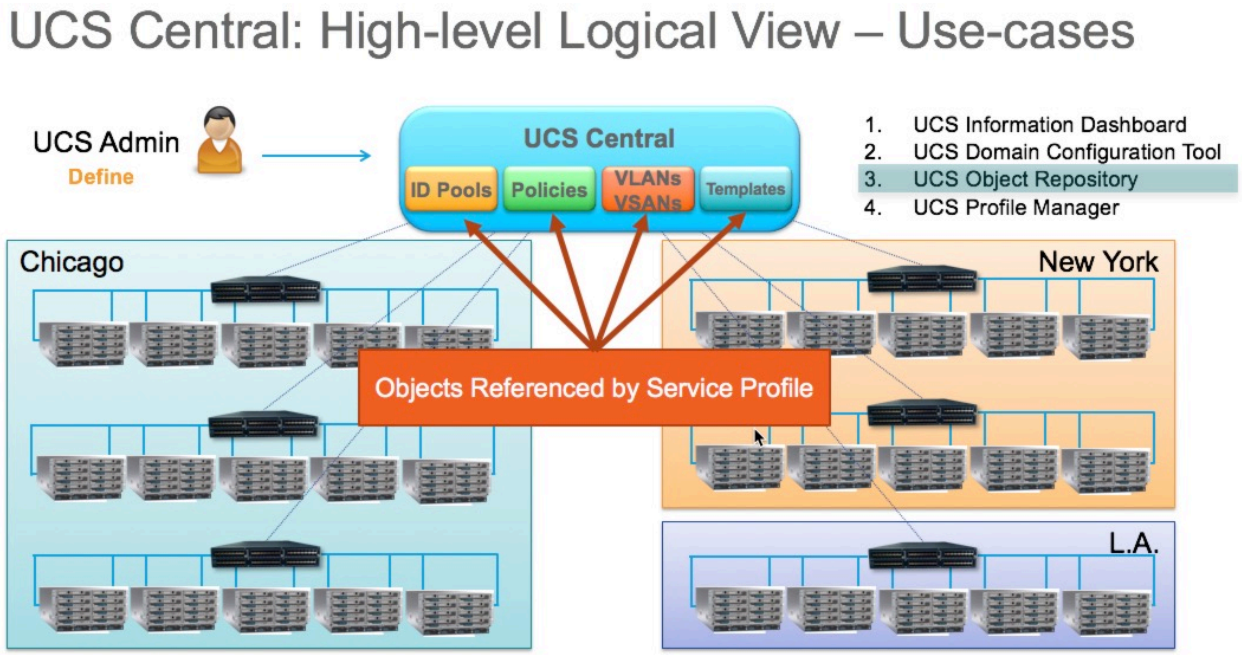
Policy Resolution Control

Infrastructure & Catalog Firmware:	● Local ○ Global	Determines whether the Capability Catalog and infrastructure firmware policy are defined locally or come from Cisco UCS Central.
Time Zone Management:	○ Local ● Global	Determines whether the time zone and NTP server settings are defined locally or comes from Cisco UCS Central.
Communication Services:	○ Local ● Global	Determines whether HTTP, CIM XML, Telnet, SNMP, web session limits, and Management Interfaces Monitoring Policy settings are defined locally or in Cisco UCS Central.
Global Fault Policy:	○ Local ● Global	Determines whether the Global Fault Policy is defined locally or in Cisco UCS Central.
User Management:	○ Local ● Global	Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined locally or in Cisco UCS Central.
DNS Management:	○ Local ● Global	Determines whether DNS servers are defined locally or in Cisco UCS Central.
Backup & Export Policies:	○ Local ● Global	Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally or in Cisco UCS Central.
Monitoring:	○ Local ● Global	Determines whether Call Home, Syslog, and TFTP Core Exporter settings are defined locally or in Cisco UCS Central.
SEL Policy:	○ Local ● Global	Determines whether the SEL Policy is defined locally or in Cisco UCS Central.
Power Allocation Policy:	○ Local ● Global	Determines whether the Global Power Allocation Policy is defined locally or in Cisco UCS Central.
Power Policy:	○ Local ● Global	Determines whether the Power Policy is defined locally or in Cisco UCS Central.

Without UCS Central, one must configure Time Zone, DNS, User Authentication Settings, Backups, etc. within each and every UCS Domain. This practice is repetitious and lends itself to having some setting or configuration wrong somewhere the UCS Domain infrastructure. With registration to UCS Central, the ability to set a Global Policy for each of the above categories in the picture above and also choose to "opt-in" by changing the radio button from Local UCSM Control to Global UCS Central Control, the ability to define the policy in a single place and make sure the accuracy is being enforced lends to easier management of all registered UCS Domains. Additionally, these operations policy settings may be customized as required…. multiple Domain Groups might leverage the same NPT Server source, for example, but yet have a different Time Zone configured. Regardless of whether a UCS infrastructure is brownfield or greenfield, the management of global operational policies can be leveraged from the first day UCS Central is installed and UCS Domains are registered; and, with the possible exception of managing firmware, are not disruptive to any existing running workloads in the UCS Domains.

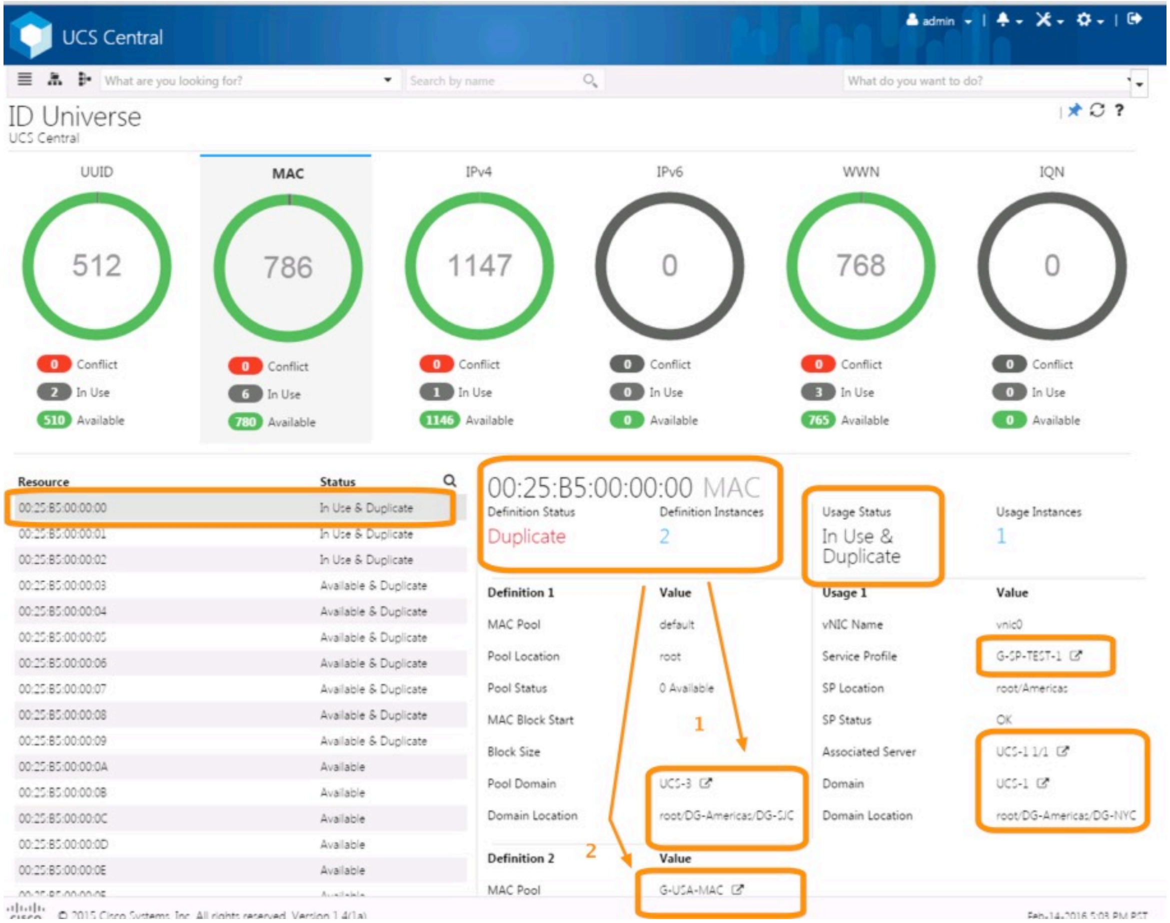
3. UCS Object Repository

Graphic Below:


UCS Central: High-level Logical View – Use-cases
UCS Admin
Define
UCS Central
ID Pools
Policies
VLANs VSANs
Templates
1. UCS Information Dashboard
2. UCS Domain Configuration Tool
3. UCS Object Repository
4. UCS Profile Manager
Chicago
New York
L.A.
Objects Referenced by Service Profile

When UCS Central becomes the object repository for your UCS Domain infrastructure it provides a very powerful and flexible management architecture for UCS deployments. This is a core use case for UCS Central, as crafting Global Objects for ID Pools, Policies, VLANs, VSANs, vNIC/vHBA Templates, Connectivity Policies, Global Service Profile Templates, and Global Service Profiles permit global control and consolidated management for the entire UCS infrastructure. Certainly there's the ease of management from a single unified manager, as evidenced with the ID Universe in the graphic below.

ID Universe – Checking status of a specific MAC Address



ID Universe
UCS Central

	UUID	MAC	IPv4	IPv6	WWN	IQN
	512	786	1147	0	768	0
Conflict	0	0	0	0	0	0
In Use	2	6	1	0	3	0
Available	510	780	1146	0	765	0

Resource	Status
00:25:B5:00:00:00	In Use & Duplicate
00:25:B5:00:00:01	In Use & Duplicate
00:25:B5:00:00:02	In Use & Duplicate
00:25:B5:00:00:03	Available & Duplicate
00:25:B5:00:00:04	Available & Duplicate
00:25:B5:00:00:05	Available & Duplicate
00:25:B5:00:00:06	Available & Duplicate
00:25:B5:00:00:07	Available & Duplicate
00:25:B5:00:00:08	Available & Duplicate
00:25:B5:00:00:09	Available & Duplicate
00:25:B5:00:00:0A	Available
00:25:B5:00:00:0B	Available
00:25:B5:00:00:0C	Available
00:25:B5:00:00:0D	Available
00:25:B5:00:00:0E	Available
00:25:B5:00:00:0F	Available

00:25:B5:00:00:00 MAC

Definition Status: Duplicate
Definition Instances: 2
Usage Status: In Use & Duplicate
Usage Instances: 1

Definition 1	Value
MAC Pool	default
Pool Location	root
Pool Status	0 Available
MAC Block Start	
Block Size	
Pool Domain	UCS-3
Domain Location	root/DG-Americas/DG-SJC

Definition 2	Value
MAC Pool	G-USA-MAC

Usage 1	Value
vNIC Name	vnic0
Service Profile	G-SP-TEST-1
SP Location	root/Americas
SP Status	OK
Associated Server	UCS-1 1/1
Domain	UCS-1
Domain Location	root/DG-Americas/DG-NYC

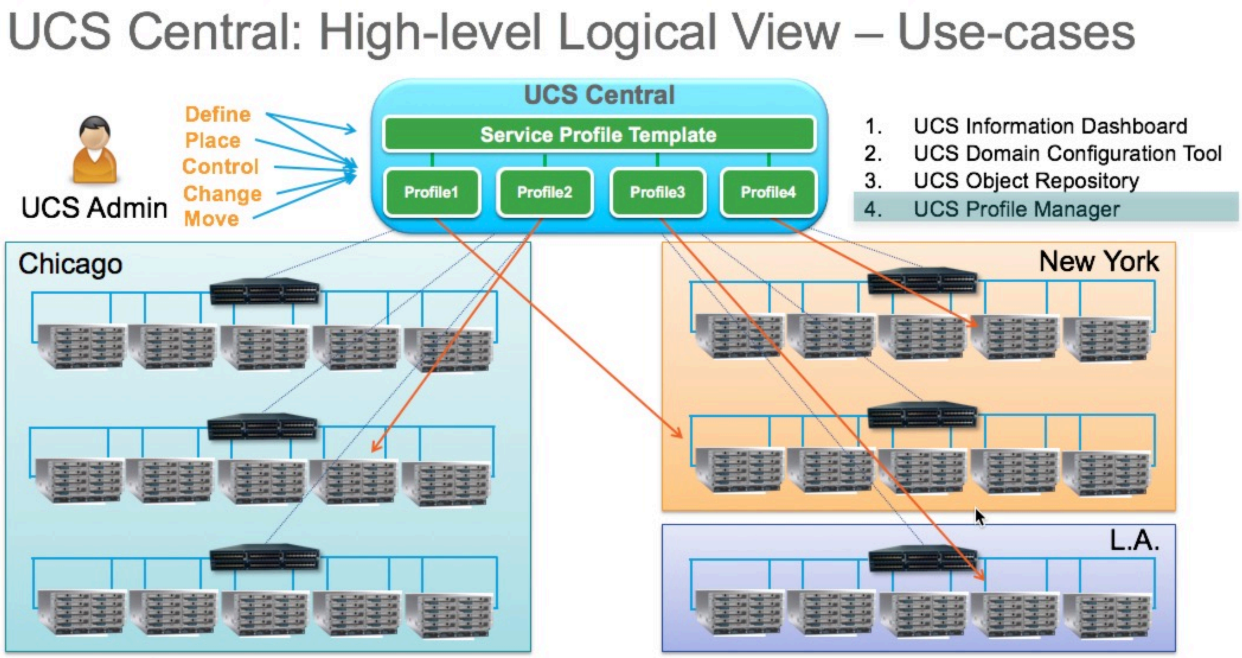
© 2015 Cisco Systems, Inc. All rights reserved. Version 1.4(1a)

Feb-14-2016 5:03 PM PST

There’s a tremendous amount of detail that is automatically inventoried across every UCS Domain and UCS Central, and also the absolute detail of “What, How Many and Where” for each and every single ID. There’s also the ability to have the correct checks and balances for IDs and Policy enforcement without having to log into the UCS Manager on each and every UCS Domain. Whenever an Object is created within UCS Central, only UCS Central has the ability to modify or delete those objects. When leveraging these objects for a registered UCS Domain, “shadow” copies of those objects get created and pushed down to the registered UCS Domain, for instance when a Global Service Profile is associated to a server in a particular UCS Domain. While a UCS Manager administrator can view and see the global objects that get pushed down, the UCSM administrator cannot modify or delete the Global Object from UCS Manager…aside from special troubleshooting use cases when the UCS Domain is “unregistered” from UCS Central or, the UCSM administrator needs to localize the shadow-copied global objects. Both “unregistering” UCS Domains and “localizing objects” global objects from UCS Central is highly regarded as “contingency-steps” in troubleshooting, and should only be performed with the direction of Cisco TAC.

Additionally, considering the UCS brownfield install base, there is nothing wrong with architecting UCS Central to operate both brownfield and greenfield environments simultaneously. Basically some large clients adopt UCS Central with the thought that anything new will become globally managed, and everything that is currently implemented with local IDs, Policies, Templates, and Service Profiles will remain locally managed within each UCS Manager. Later in the document, we'll provide a detailed discussion on how to perform a Local Service Profile to Global Service Profile Migration.

4. UCS Service Profile Manager



Ultimately, for most customers, the idea of having consolidated, single-source management for ID Pools, Policies, VLANs/VSANs, Templates, and Service Profiles is very compelling, and the ability to manage "less" infrastructure by reducing the total number of required Service Profile Templates means less OPEX.

For other customers, there's also the desire of having Service Profile mobility across multiple UCS Domains. As such, if a UCS Central environment is truly global in scope, then the corresponding Global Service Profiles can be associated across any registered UCS Domain, assuming like network and storage connectivity. Additionally, many large clients with various hardware server options (models, cpus, memory, and adapters) leverage dynamic Server Pools with policy to create a specific subset of servers based upon the server hardware specifications and/or location, for association of their Service Profiles. With UCS Central and Global Service Profiles, these server pool policies now take-on a global scope, across all your registered UCS Domains. There are no Domain-based boundaries in a Global infrastructure with UCS Central.

Managing UCS at Scale with UCS Central

Regardless of the size of the UCS Central environment, there are certain Best Practices and Considerations that should be noted and/or followed.

UCS Central Best Practices and Considerations

- Best Practice – Performance – Ensure UCS Central installation disk (local or remote) read speed is greater than 125 Mbps. Disk Read Speed is more critical for UCS Central HA-Mode Architectures (2 UCSC vApps accessing a 3rd RDM/NFS mapped Remote Disk).
- Best Practice - Performance – Ensure less than 500ms network latency between UCS Central and any managed UCS Domain. High Latency most affects inventory collection, and Firmware deployment/upgrades to UCS Domains. UCS Firmware newer than 2.2.2x have better latency handling with UCS Central.
- Best Practice – Performance – Ensure bandwidth is at least 1.5 Mbps in remote WAN Connections of UCS Domains to UCS Central.
- Best Practice – Perform Daily Backups and Configuration Exports of UCS Central and all registered UCS Domains, ensuring Remote Copy to an external file directory. This guidance can be reduced for UCS Domains to several times per week if the environment is rather static with few changes.
- Best Practice – Leverage Hypervisor Snapshots to protect UCS Central, especially prior to any upgrades.
- Best Practice - Always register UCS Domains to UCS Central using the Fully Qualified Domain Name, verses using the IP Address of UCS Central.
- Best Practice - Always make sure UCS Domains and UCS Central have a valid Time Source configured before attempting any registration of the UCS Domain to UCS Central.
- Best Practice - Never “Unregister” a UCS Domain from UCS Central that contains Global Objects copied down to the UCS Domain. Only unregister if there is no intention of registering the specific UCS Domain back to UCS Central in the future, and with the guidance of Cisco TAC, backed with UCS Central Engineering approval.
- Best Practice - In mixed “Greenfield” and “Brownfield” environments, consider naming all Global ID Pools, Policies, Templates, and Service Profiles with a “G-” or similar naming convention to distinctly differentiate Global Objects from Local UCS Domain Objects.
- Do Consider, in mixed environments, placing newly deployed “Greenfield” infrastructure in a separate organizational structure than the existing Local “Brownfield” infrastructure. This is an easy way to maintain segmentation and simplicity in operating in both environments.
- Do consider placing widely adopted, and less disruptive Global Operational Policies (Backups for instance) higher in the Domain Group hierarchy. Keep in mind, that the “Remote-Copy” functionality of the Backup Job should utilize a FTP/SFTP/SCP/ remote directory that is somewhat geographically close to the UCS Domain.

- Do consider placing potentially more disruptive Global Operation Policies (Infrastructure Firmware for instance) lower in the Domain Group hierarchy.
- Do consider HA – Use Hypervisor HA to protect single UCS Central vApp, Snapshots and ensure Daily Backups.
- Do consider creating fewer Global ID Pools, and simply add ID Range Blocks to a Global Pool to scale. Fewer Pools, with greater blocks of IDs result in a more efficient use of the internal db and proves to be easier to manage for customers requiring large quantities of IDs.
- Do consider using VLAN/VSAN Aliasing to potentially minimize the number of required Global SP Templates and Global SPs.
- Do consider using Advanced Policy Resolution to minimize overall number of policies and corresponding Global SP Templates. Another way to state this is that more than one given policy can have the same name, as long as it's not in the same Org Hierarchy. Consider placing Global Service Profile Templates "High" in the Hierarchy referencing the given policy "names", then use "Create Global SP from Template" functionality to instantiate the G-SP down at the correct Sub-Org, , where the common policy name exists (but different values) to adopt the settings of that specific Policy. This is a mechanism that can significantly reduce the amount of required Global Service Profile Templates.
- Do consider and discuss attaching too many Global Service Profiles to a single Global Service Profile Template. Consider Fault Domains. See section on Sizing and Scaling Considerations for UCS Central.

Sizing and Scaling Considerations for UCS Central

Sizing the UCS Central VM Resources

Some UCS Central Customers have scaled their UCS Environments from literally Dozens to Hundreds of Domains and from Hundreds to Thousands of servers. As previously mentioned in this document, the scaling metric to focus-upon is not so much the number of registered UCS Domains, but rather number of Blades and Servers. Currently, UCS Central 1.4.1a has been QA Tested to support up to 10,000 Servers…. however, there's no real software limit.

Very Large customers should take a look at the performance of their UCS Central VMs and gauge whether or not to increase cpu and memory resources to the UCS Central Server VM. In the UCS Central Install Guide, you can easily see the minimum requirements for running UCS Central. You'll notice that the deployment of the OVA File, will actually carve-out 2 x 40 GB Disks, allocate 4 x vCPUs and 16 GB RAM. It's important to realize that these parameters are the absolute minimum requirements….and for small to medium size environments, they should provide sufficient performance, however…. for large environments, it's wise to increase those resources by a factor of two. Cisco IT internally runs at least 4 vCPUs and 24 GB Ram for their instance of UCS Central, which exceeds 200 UCS Domains and close to 6,000 Servers. Bottom line, it's recommended to monitor the performance metrics of the UCS Central VM in new or growing infrastructures, and adjust CPU and RAM resources accordingly. If performance is noticeably lacking, please verify vCPU and Memory usage and make needed changes with your virtualization administrator.

Scaling Global Service Profiles and Global Service Profile Templates

I'd like to express that there's no software hard-limit to the number of Global Service Profile's that can be attached-to a Global Service Template. While the OPEX benefits of leveraging Templates to make wide-spread changes is beneficial to many customers and many architectures, I want to also express and bring attention to the fact that too much of anything is likely not a good.

One has to consider the "Fault Domain" of a single disruptive change to the environment. This is something that's difficult to place an exact number upon, or claim an absolute "Best Practice", however in architecting your environment, how many resources (Global Service Profiles & Servers) are you willing to attach to an updating Global Service Profile Template, whereby a single wrong/disastrous change can cause a wide-spread outage? Sure, there are "User-Ack" Maintenance Policies…and Cisco absolutely recommends using Maintenance Policies as a Best Practice, but regardless one should consider leveling the playing field and reducing the potential Fault Domain…. aside, does anyone want to see the majority of their environment (servers) have User-Acks pending? Perhaps a scale of 100 Global Service Profiles to a single Global Profile Template should be considered the very max. Again, there's no hard fast limits. I've heard of architectures that have 1000's of Global Service Profiles attached to a single Global Service Profile Template, but that is beyond extreme and certainly would not be considered a Best Practice.

In addition to the scaling of GSPs to GSP Templates, another important aspect to consider is the quantity of a given policy. For instance, if you have 10 Global Service Profile Templates…with 100 Global Service Profiles attached…that's 1000 Blades or Servers. As such, perhaps you have ALL 10 Templates accessing the same Disruptive Policy (Boot/FW/BIOS/LAN-SAN Connectivity Policy) in your environment. Now, irrespective of Global Maintenance Policies (User-Ack), you have a single policy that can potentially disrupt 1000 Blades/Servers (same policy is being used by all your Global Service Profile Templates) if something is done incorrectly, administratively in editing that policy. As with spreading or balancing some of the scale across multiple Service Profile Templates, you can also create multiple Policies…perhaps with the same exact settings, but different names, so those policies can be consumed by their respective Global Service Profile Templates. Again, all in the spirit of reducing the Fault Domain.

Perhaps the given numbers are somewhat extreme….and certainly User-Ack Maintenance Policies will be your friend…. however, it's still unnerving to receive wide-spread User-Acks on all your Blades/Servers just because an Admin incorrectly edited a disruptive policy…perhaps a Boot Policy, or a LAN/SAN Connectivity Policy.

If you are in a situation of having too many Global Service Profiles attached to Too-Few Templates, you can easily Clone the Global Service Profile Template and Unbind-Bind a percentage of the Global Service Profiles to the Cloned Templates (Test First!) The entire system is so flexible in design and operations, that It's easy to balance and scale according to refined designs. But remember, it really does no good to increase the spread of your GSPs-Templates, if they are all accessing the same policy on the backend.

You might we thinking, in some sections of this document, I showed you ways of reducing the number of Global Service Profile Templates…. certainly, VLAN/VSAN ID Aliasing, Advanced Policy Resolution and ID Access Control Policies can all be used to reduce the numbers of required Global Service Profile Templates…but then, I warn or guard you against putting "all your eggs in one basket" so-to-speak by attaching too many Global Service Profiles to a given Template, or using a single policy for too many Global Service Profile Templates/Global Service Profiles. This sounds contradictory….and in a sense, it is…however, what I am trying to communicate to you are the techniques to reduce-down the number of Global Service Profile Templates to make them manageable…. but also keep in mind your desired size of your "Fault Domain" as discussed above. There's no magic or easy concrete answer…. I cannot provide a spreadsheet with numbers…but taking all that's been discussed in consideration, I am sure you are armed with enough detailed information to make the right design decisions, and changes, for your business and environment. Frankly, you could ask 5 different architects about how to do this, and probably get 5 different answers. I think the important thing is you realize the capabilities of the system, and the consequences for doing things a certain way, and you work towards mitigating the overall risk just like everywhere else in your IT environment.

Small UCS Central Environment: 1-3 Registered UCS Domains (example)

Small UCS Central Environments:

In regards to Domain Group setup, consider using a Single Domain Group under root. While there is nothing inherently wrong with placing UCS Domains under the root Domain Group, creating at least a single sub Domain Group and placing UCS Domains there, with corresponding operational policies, can allow for future horizontal growth (addition of future Domain Groups) and flexibility. This can possibly prevent the situation of a single set of operational policies being exposed to every registered UCS Domain. However, in contrast, certain policies might be best placed at the root level. For instance, if your organization has a single LDAP Remote Authentication configuration for the entire corporation, placing those LDAP policy configuration settings in the root Domain Group will ensure the widest possible adoption for any registered UCS Domain in any sub Domain Group, assuming you don't override those LDAP settings with a sub Domain Group policy.

Small Size Greenfield Deployments of UCS Central:

If you are implementing UCS for the first time, it's strongly recommended leveraging UCS Central, and creating the entire virtual architecture globally from the beginning within UCS Central. The advantages of being able to administer all global objects (pools, policies, VLANs, VSANs, templates and service profiles) from a single unified manager, creating and enforcing consistent operational policies, and achieving maximum global service profile mobility to all registered UCS Domains will ensure the best possible implementation, with the lowest possible administrative and operational overhead. From an ID Pool perspective alone, UCS Central will inventory all Global and Local Pools, and show at a glance in the ID Universe if there is any duplicate IDs or conflicts, and readily identify the sources of those IDs.

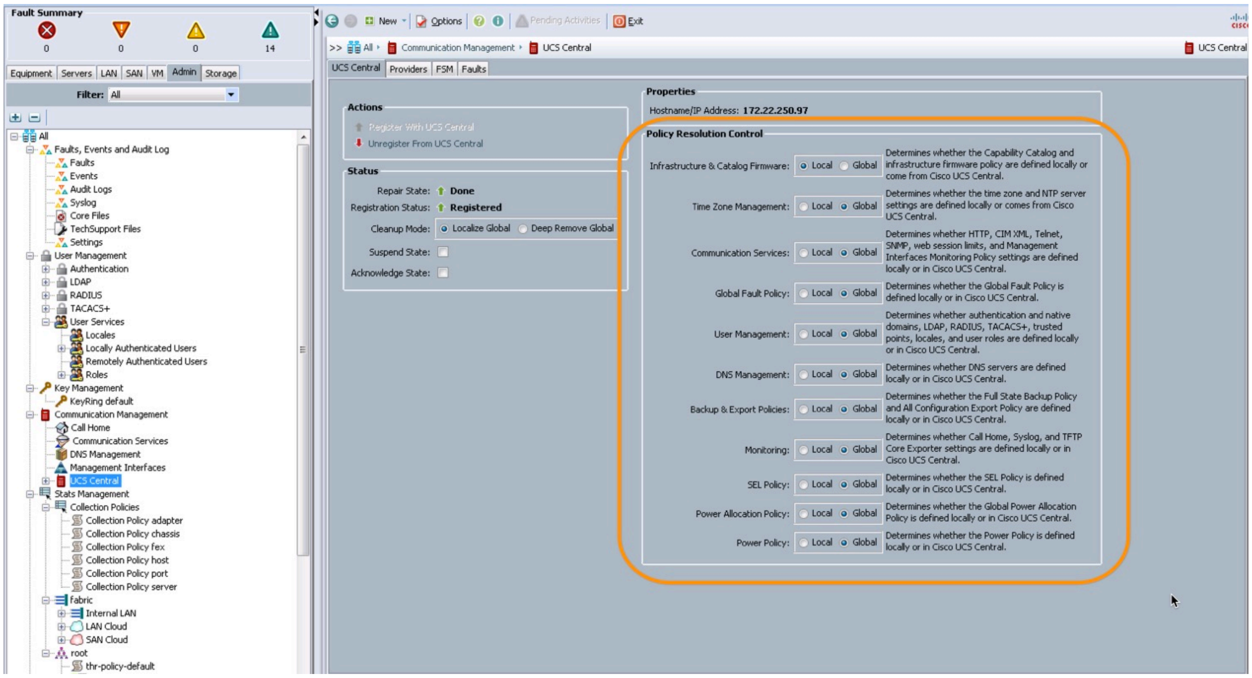
Small Size Brownfield Deployments of UCS Central:

By registering existing, deployed UCS Domains with UCS Central, one is presented with options in how to architect and operate going forward. With previously deployed Local Service Profiles and operational servers, and without the specific requirement, or desire, to move Service Profiles from one UCS Domain to another (UCS Domain workload mobility), there very well may be no absolute, compelling reason to change the existing local, logical configuration to global objects. One could keep the existing configuration intact, and simply build-out anything "New" as a global configuration. As older localized domains reach end of life and are retired, they can be replaced by globalized UCS Domains.

Conversely, if there is the desire or need for the configuration to be global, one can build-out the entire global configuration that mirrors the local configuration, and utilize future maintenance windows to gracefully power-down servers, remove existing local service profiles, and replace them with their global service profiles counterparts. This scenario can be somewhat “involved”, but it can be easily planned and it absolutely should be tested in a lab before attempting in production. A great way to accomplish this is to install UCS Central in your lab, and download-install-register UCS Emulators to the lab UCS Central in order to model the existing production configuration and test the migration process.

For a small number of UCS Domains being registered to UCS, a simple Domain Group (DG) structure is more than sufficient. You might ask, what influences the Domain Group Structure? The best way to analyze this is to look at the UCS Central Registration Tab in UCS Manager, specifically the Admin Tab/Policy Resolution Control. The displayed policies (Local vs. Global) are those operational policies that are defined in a UCS Central Domain Group, or sub Domain Group. As you survey down the list, you can better rationalize how best to construct your Domain Groups for your overall architecture. Every operational policy you see in the list, is a policy that is set at the Domain Group level, or sub-level within UCS Central. As such, these policies can be controlled Globally as hierarchically as you need from root to discreet Sub-Domain Groups.

UCS Central Registration in UCS Manager – Policy Resolution Control



Actions

Register With UCS Central

Unregister From UCS Central

Status

Repair State: Done

Registration Status: Registered

Cleanup Mode: ● Localize Global ○ Deep Remove Global

Suspend State: □

Acknowledge State: □

Properties

Hostname/IP Address: **172.22.250.97**

Policy Resolution Control

Infrastructure & Catalog Firmware: ● Local ○ Global — Determines whether the Capability Catalog and infrastructure firmware policy are defined locally or come from Cisco UCS Central.

Time Zone Management: ○ Local ● Global — Determines whether the time zone and NTP server settings are defined locally or comes from Cisco UCS Central.

Communication Services: ○ Local ● Global — Determines whether HTTP, CIM XML, Telnet, SNMP, web session limits, and Management Interfaces Monitoring Policy settings are defined locally or in Cisco UCS Central.

Global Fault Policy: ○ Local ● Global — Determines whether the Global Fault Policy is defined locally or in Cisco UCS Central.

User Management: ○ Local ● Global — Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined locally or in Cisco UCS Central.

DNS Management: ○ Local ● Global — Determines whether DNS servers are defined locally or in Cisco UCS Central.

Backup & Export Policies: ○ Local ● Global — Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally or in Cisco UCS Central.

Monitoring: ○ Local ● Global — Determines whether Call Home, Syslog, and TFTP Core Exporter settings are defined locally or in Cisco UCS Central.

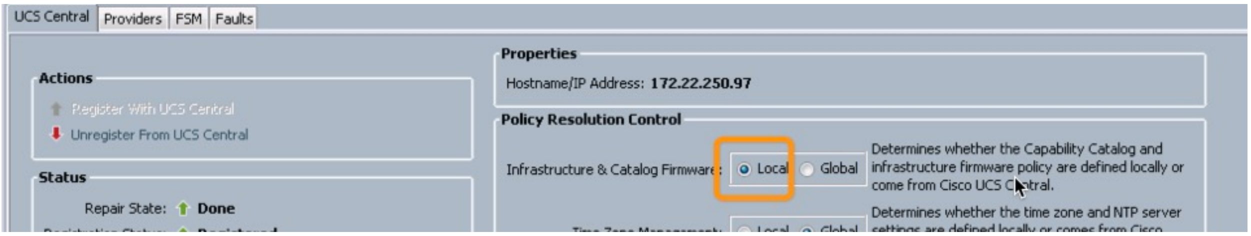
SEL Policy: ○ Local ● Global — Determines whether the SEL Policy is defined locally or in Cisco UCS Central.

Power Allocation Policy: ○ Local ● Global — Determines whether the Global Power Allocation Policy is defined locally or in Cisco UCS Central.

Power Policy: ○ Local ● Global — Determines whether the Power Policy is defined locally or in Cisco UCS Central.

Infrastructure & Catalog Firmware can certainly effect your Domain Group hierarchy. Remember, if one chooses to opt-in to Global Control for this policy, and one modifies the Domain Group Policy in UCS Central and sets it to a higher level of Infrastructure Firmware, then you will get User-Acknowledgement (User-Ack) on all the UCS Domains (FIs) registered to that specific Domain Group, prompting the upgrade of those UCS Domains. While this is not disruptive in of itself, there are many users that do not wish to see a User-Ack on a UCS Domain unless they are immediately ready to upgrade, and also not on more than a single UCS Domain at a time…therefore exercise discretion and consider the following. One way of achieving segmentation of the UCS Domains with regards to Infrastructure Firmware Policy is to place each UCS Domain into it’s own Sub-Domain Group. As such, you then can define the Domain Group policy for Infrastructure Firmware at the lowest level sub Domain Group hierarchically, and only a single UCS Domain will ever be “pending” for User-Ack, or upgrade. Another great way to manage this scenario is to simply keep the operational policy defined as ***Local*** within UCS Manager, and then Opt-In each Domain to global at time of Upgrade. In this way, one can leverage the benefits of UCS Central Firmware download and control, but only affect a single UCS Domain at a time. Additionally, all remaining operational policies can be configured singularly, higher in the hierarchy, as to reduce the number of policies being managed.

UCS Central Registration in UCS Manager – Infrastructure FW Resolution Control



Status

Repair State: Done

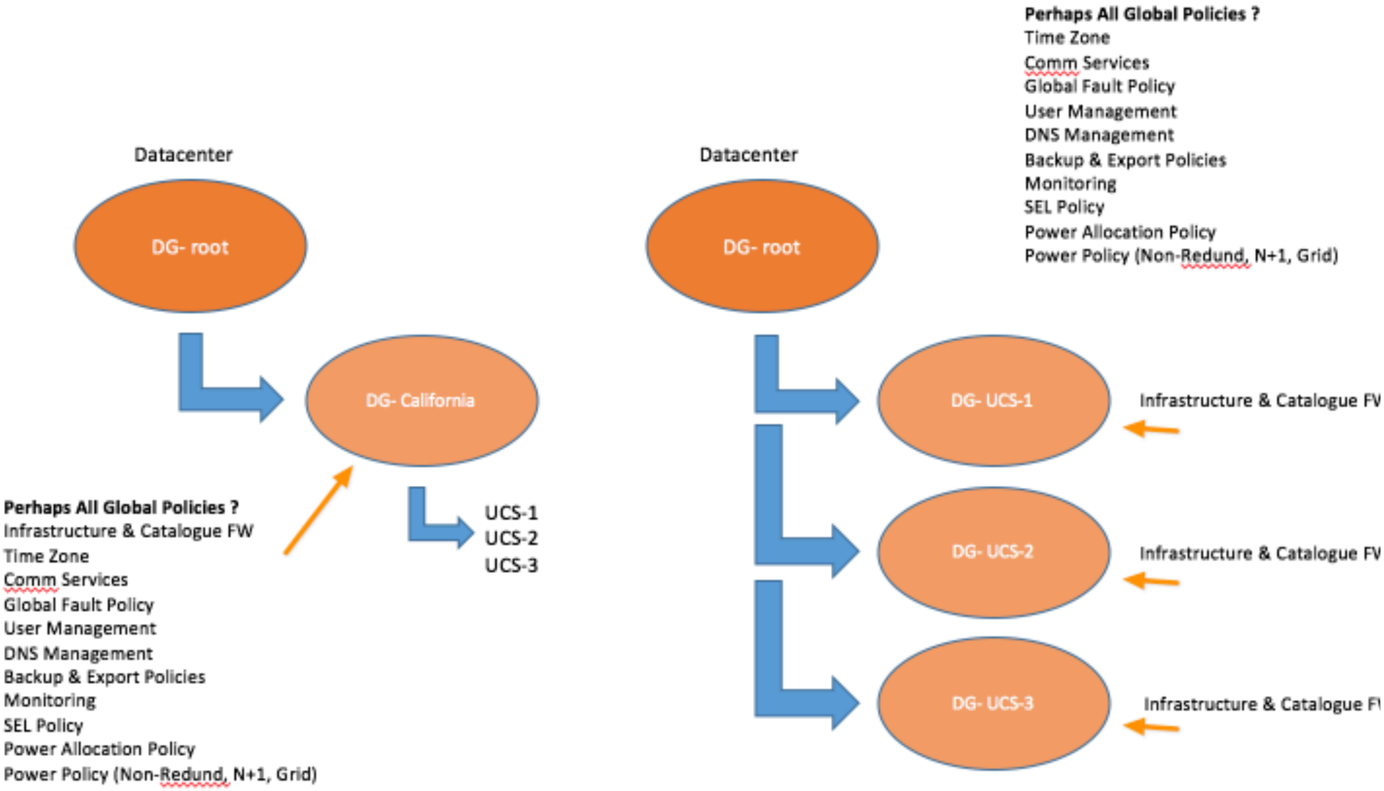
Properties

Hostname/IP Address: 172.22.250.97

Policy Resolution Control

Infrastructure & Catalog Firmware: ● Local ○ Global — Determines whether the Capability Catalog and infrastructure firmware policy are defined locally or come from Cisco UCS Central.

Time Zone Management: ○ Local ○ Global — Determines whether the time zone and NTP server settings are defined locally or comes from Cisco

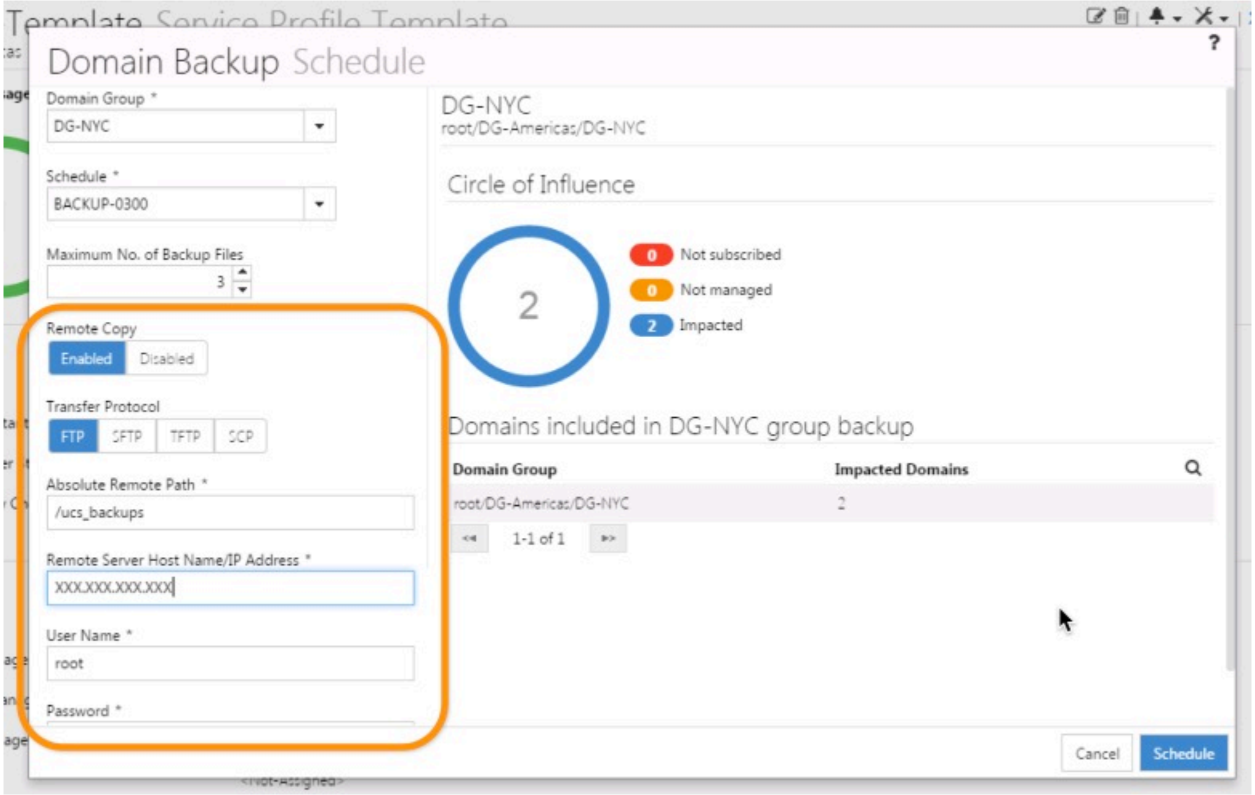


Time Zone Management – This is a great policy to opt-in to UCS Central at time of registration. This policy can be placed-up high in the Domain Group hierarchy, especially in small deployments, as there is a good chance the UCS Domain's will be in the same time-zone. Also to note, some clients will point to the same NTP server source, but wish to have different Time Zones configured for the respective UCS Domains. In this case, separate Domain Groups, or Sub-Domain Groups can be used to account for the changes. Regardless, allow UCS Central to define the proper Time Zone and NTP Server Settings to ensure consistency and accuracy of Time and Time-Zone in your architecture.

Communication Services (for example SNMP Configuration), Global Fault Policy, User Management (for example LDAP Configuration), DNS Management, Monitoring (for Example Call Home and Syslog Configuration), SEL Policy, Power Allocation Policy (for example Manual Blade vs Chassis Cap) and Power Policy (for example N+1, or Grid) all make great candidates for Global Policy Management. It's a simple rational of setting the policy correctly once in UCS Central, and having your registered UCS Domains adopt that policy.

Backup & Export Policies – UCS Central provides great assistance in scheduling and maintaining proper backups for registered UCS Domains and UCS Central itself. Since UCS Central 1.3, administrators can create custom schedules and have UCS Domain Backups occur at any date and time they wish. This affords greater flexibility over what is natively available configuration-wise within UCS Manager. Another distinction, Backups managed by UCS Central afford the option for Remote Copy offline, to insure the safety of Backup Files. It has always been a UCS Best Practice to ensure daily backups are taken for each UCS Domain…. Backups (Full State-binary Database as well as Configuration Export-xml). This same exact best practice extends to UCS Central. When UCS Central is configured to backup a UCS Domain, those Backup files are stored in the UCS Central database. As such, you can define the number of backup files to keep (typically 3-5 copies), before they are written over by subsequent backups. This allows a mechanism to limit the amount of space used within the UCS Central database and disk, and prevents uncontrolled growth. Additionally, please make sure that ALL Backups and Exports are properly configured to be copied remotely offline of UCS and UCS Central (Remote Copy).

UCS Central – UCS Domain Backup Schedules



Domain Backup Schedule

Domain Group *: DG-NYC

Schedule *: BACKUP-0300

Maximum No. of Backup Files: 3

Remote Copy: [✓ Enabled] Disabled

Transfer Protocol: [✓ FTP] SFTP TFTP SCP

Absolute Remote Path *: /ucs_backups

Remote Server Host Name/IP Address *: XXX.XXX.XXX.XXX

User Name *: root

Password *

DG-NYC
root/DG-Americas/DG-NYC

Circle of Influence

2

0 Not subscribed
0 Not managed
2 Impacted

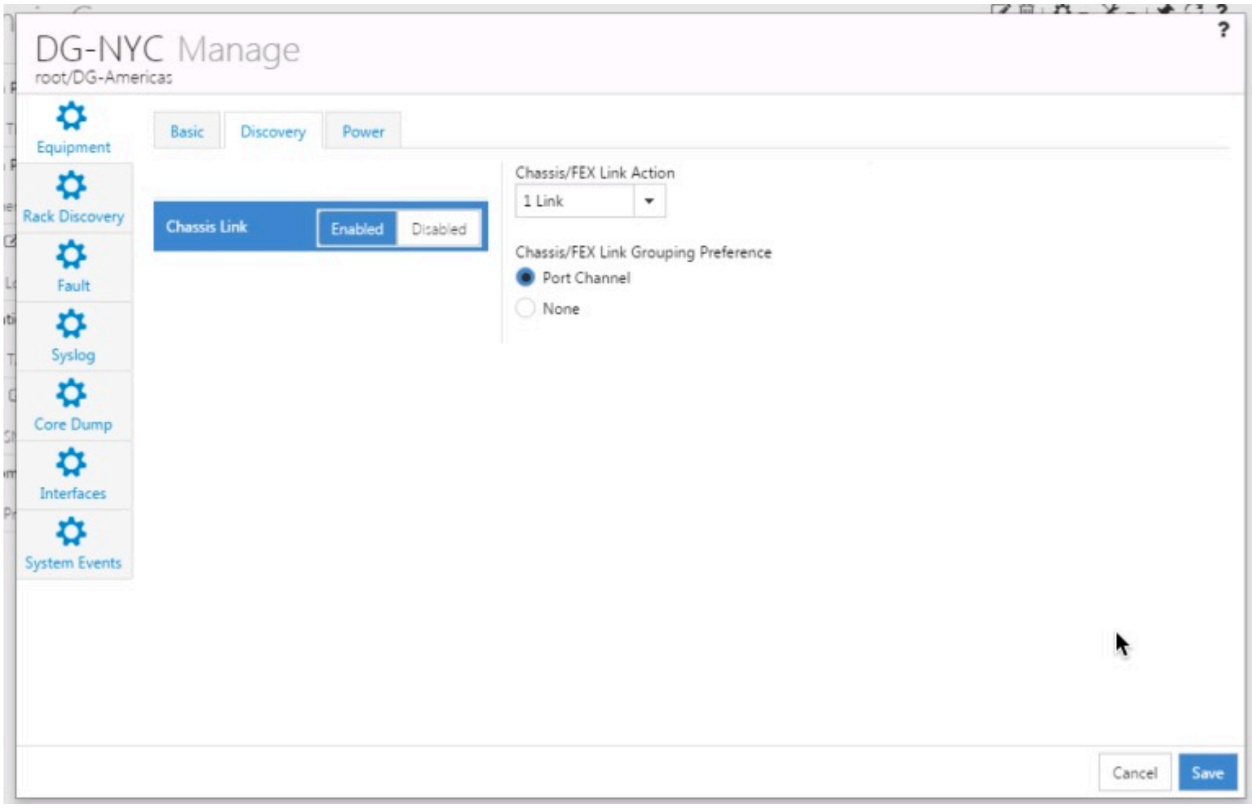
Domains included in DG-NYC group backup

Domain Group	Impacted Domains
root/DG-Americas/DG-NYC	2

1-1 of 1

New for UCS Central 1.4 (refer to the Release Notes for UCS Manager Version Support) is the ability to set Global Equipment Policies. In UCSM 3.1.0, you will notice a new Global Policy that allows for UCS Central to control Chassis Discovery Policy, Rack Management Action, MAC address Table Aging Time, VLAN Port Optimization, and Firmware Auto Server Sync State.

UCS Central – Equipment Policies



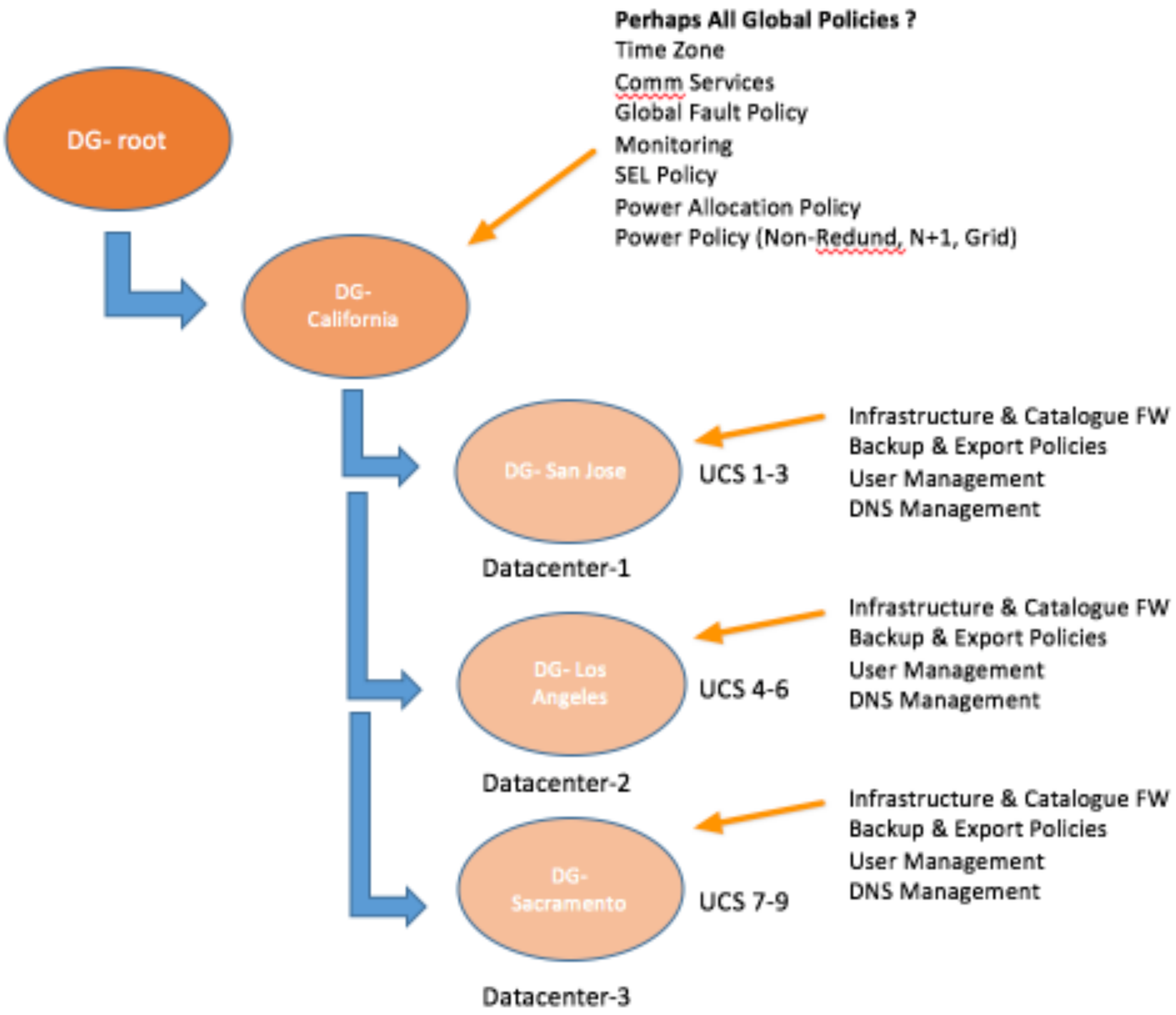
DG-NYC Manage
root/DG-Americas

Chassis Link: [✓ Enabled] Disabled

Chassis/FEX Link Action: 1 Link

Chassis/FEX Link Grouping Preference
● Port Channel
○ None

Medium UCS Central Environment: 4-12 Registered UCS Domains (example)



Medium UCS Central Environments:

For a medium size deployment of UCS Domains registered to UCS Central, a larger Domain Group (DG) hierarchy should be considered. With upwards of 12 UCS Domains, there's a good chance those UCS Domains might be in different geographic areas, and consequently it's best if your Domain Group structure reflects that. While it's hard to say it's an absolute "Best Practice", more than often the major influence behind architecting your UCS Central Domain Group structure are the geographic locations of the registered UCS Domains. Global Operational Policies such as Time Zone, User Authentication Settings, Backups, Firmware etc. tend to lend themselves to crafting Domain Groups with geography in mind. Of course, doing what is best for your unique situation and implementation is always the first consideration, there are few "absolutes".

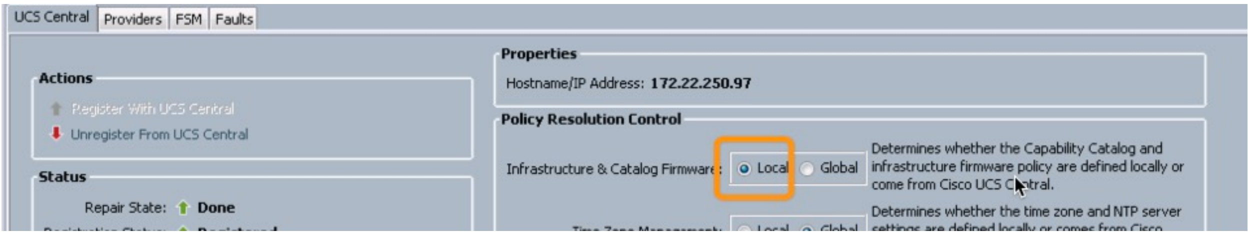
An example of the importance of Domain Group hierarchy at-scale can be understood from crafting the necessary Backup Schedules and Policies in UCS Central for registered UCS Domains. If the registered UCS Domains are geographically dispersed, then it's likely best that the Remote Copy functionality of a UCS Central Backup Job is actually copying those Backups to a specific FTP Server located close to the UCS Domains that could potentially leverage those backups, especially in a DR scenario where the Backup (Full State binary) is injected from the console-connected UCS Manager Setup Script on the new/replacement FI's. Consequently, you would not want to ideally perform a DR Restore on a San Jose pair of FI's from an FTP Server in New York. With UCS Central Domain Group Policies, the actual remote copy FTP server can maintain the proper backups of the UCS Domains is close proximity, or part of that specific Domain Group.

Some organizations have adopted a separation of Domain Groups by business group to support multi-tenancy. Another consideration for Domain Group setup is the creation of your Global VLANs. When you create Global VLANs in UCS Central, you must define the Domain Group structure of that Global VLAN…and the hierarchy can be top level "DG-root" or a lower sub-DG. The purpose of this additional "property" attached to a Global VLAN is to support the UCS Central capability of VLAN ID Aliasing. An aliased name is used to define a given VLAN ID, and then, additional IDs can be created and given that same aliased name. The Aliased VLAN name is then called by a given Global Service Profile. With a feature known as "Sticky-Binding", the actual VLAN ID does not get assigned until you start the association process to a given UCS Domain that is a member of that specific Domain Group. Since the underlying VLAN ID is attached to a Domain Group, if you use workload mobility to change the location of a Global Service Profile from one UCS Domain to another UCS Domain, in a different Domain Group, then the proper VLAN ID is assigned per the policy design. This ability can potential decrease the total number of Service Profile Templates required. One should consider all aspects and adopt the model and Domain Group structure that makes the most sense for their operational needs. The exact same aliasing concept applies also to named VSANS. For further details, refer to the section later in this document VLAN/VSAN ID Aliasing.

Domain Group hierarchy certainly effects the Operational Policies used in UCS, and we know that Organizational Units effect the multi-tenancy and “access” of ID Pools, Policies, VLANs, VSANs, Templates, and Service Profiles. Org Permissions are optional in Locally defined VLANs in UCS Manager, however, Global VLANs in UCS Central must have Org Permissions Defined. They are mandatory. One can define “root” as a single Org Permission, effectively giving the entire organization access to a given VLAN, or you can be more granular for security reasons in allowing sub-orgs access to only specific VLANs.

With Infrastructure & Catalog Firmware, there’s less of a tendency to construct individual Domain Groups for UCS Domains based on scale, just to segment the possibility of more than one User-Ack on a UCS Domain that you wish to upgrade. As such, consider still putting this potentially disruptive policy lower in the Domain Group Hierarchy, perhaps in a sub-Domain Group with just a couple UCS Domains registered as to minimize the amount of User-Acks on your registered UCS Domains. As previously mentioned, one can always make sure that the Operational Policy for Infrastructure and Catalogue Firmware within each UCS Domain is set to “Local” for normal operations and then at time of upgrade for a specific UCS Domain, simply “Opt-In” to the Global Policy, thus causing a single User-Ack on that specific UCS Domain. This seems like a very reasonable and efficient way of addressing Global Firmware management, leveraging the benefits of Global Management but yet the conservative safety of individual “opt-in” policies within the registered UCS Domains. It’s imperative to understand that No Global Policy applies to a UCS Domain, unless that UCS Domain “opts-in” for that Global Policy.

UCS Central Registration in UCS Manager – Infrastructure FW Resolution Control



Properties

Hostname/IP Address: 172.22.250.97

Status

Repair State: Done

Policy Resolution Control

Infrastructure & Catalog Firmware: ● Local ○ Global — Determines whether the Capability Catalog and infrastructure firmware policy are defined locally or come from Cisco UCS Central.

Determines whether the time zone and NTP server settings are defined locally or comes from Cisco

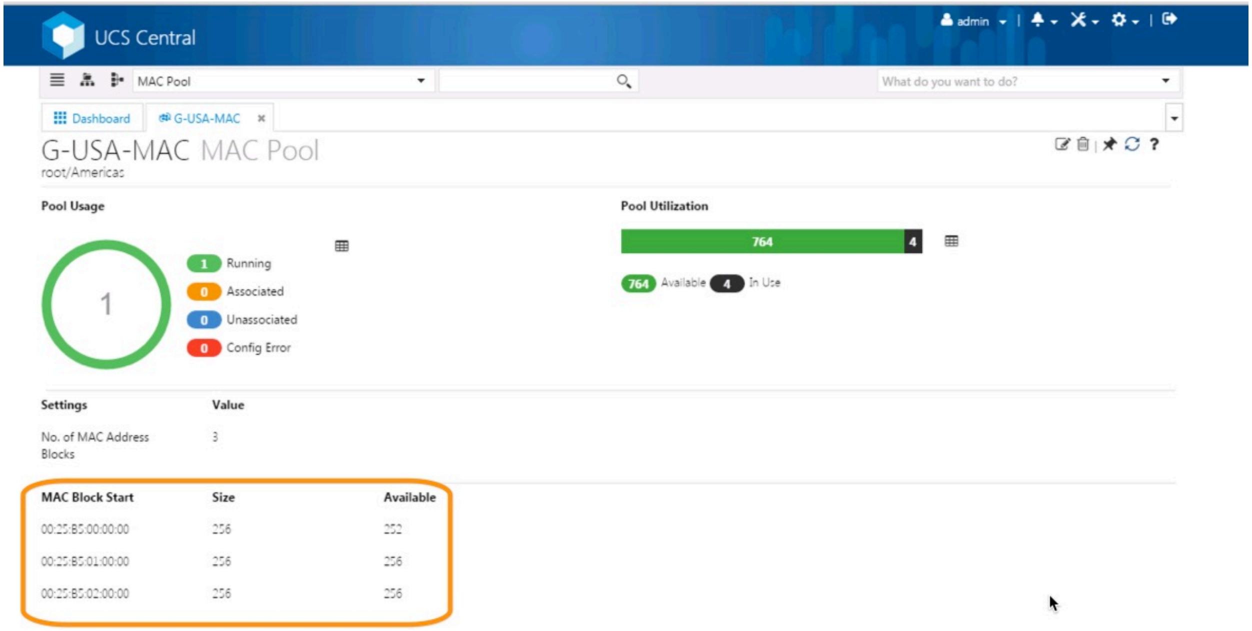
With Time Zone Management, and a larger more geographically dispersed number of registered UCS Domains, you would want to place this Domain Group operational policy as high in the Domain Group hierarchy as feasible, to reduce the amount of times you need to craft and maintain this policy. An organization that’s entirely contained within a single Time Zone can configured this policy once at the highest levels, while conversely, another organization that spans several time zones will need to make sub Domain Group policies that correspond to a specific subset of registered UCS Domains in a particular time zone.

Medium Size Greenfield Deployments of UCS Central:

In a Medium size Greenfield Deployment, setting-up a logical Domain Group and Organization hierarchy is very important from the beginning. Certainly, multiple levels of hierarchy should be considered to accommodate the different requirements for operational policies amongst the deployed UCS Domains. In addition to Firmware considerations as previously discussed, UCS Backups (Backup and Configuration Export) are likely scheduled in different time zones, and would likely have different remote-copy destinations. Additionally, there may be different User Authentication Settings…perhaps different LDAP integration points because upon organization and geographic dispersion.

With the creation of Global ID Pools for UUID, MAC Address, WWNN, WWPN and Management IPs, it is wise to plan in advance for not only the existing scope of the infrastructure but also future growth. Single Global Pools can be leveraged for each ID-type, and then Blocks of IDs can be added to their respective Pools for scale-out. Typically, it's more efficient for the internal DB to have fewer numbers of overall "pools" and smaller-size "blocks" but simply add additional blocks of IDs to accomplish the growth and scale. For instance, in the graphic below, we use a single Global MAC Pool "G-USA-MAC", and achieve growth and scale-out by adding 256-Blocks of ID's to the pool, making the 4th Octet Unique for each block.

Global MAC Pool – Blocks of IDs



G-USA-MAC MAC Pool

root/Americas

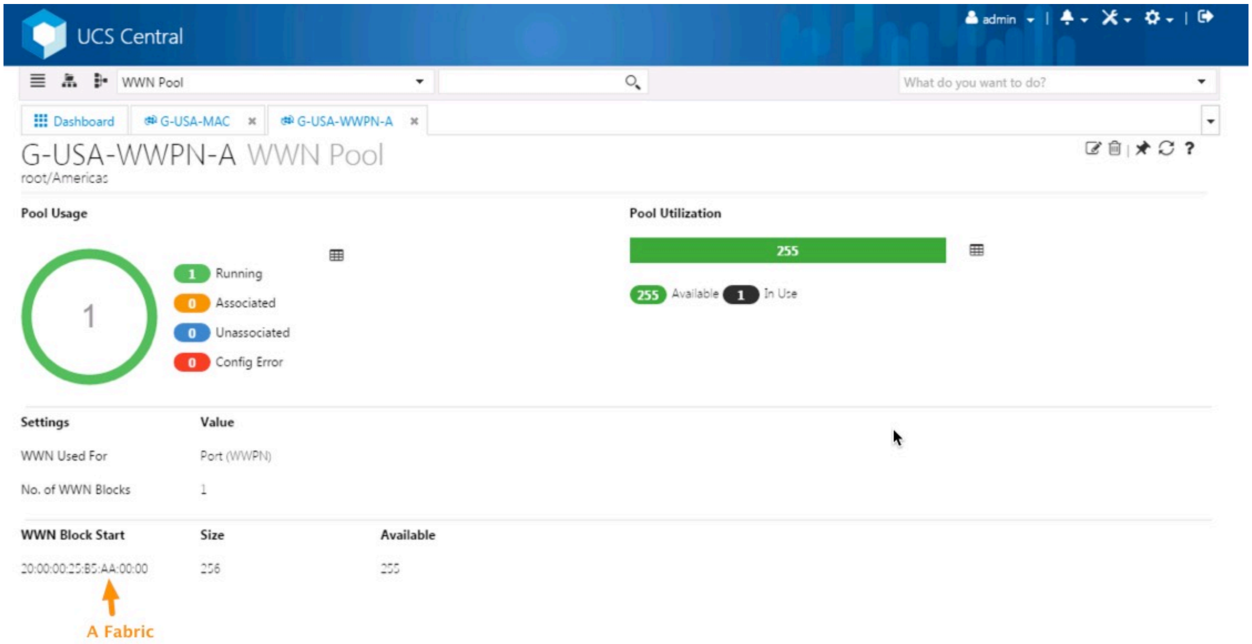
Settings	Value
No. of MAC Address Blocks	3

MAC Block Start	Size	Available
00:25:B5:00:00:00	256	252
00:25:B5:01:00:00	256	256
00:25:B5:02:00:00	256	256

Some clients prefer to segment their MAC Pools for their respective A & B Fabrics, verses using a simple single pool for both. This is purely individual preference…. if the network administrators care to know what fabric a certain MAC address is assigned to, then it could be helpful, however Best Practices architecture for all UCS Deployments recommend FI Ethernet up-linking to a clustered-switch technology, either vPC or VSS, and the MACs from the two fabrics will become meshed as a result.

For WWPNs, the universal tendency is to create two separate pools for A Fabric and B Fabric, using one of the fields in the WWPN format to define A and B Fabrics. This greatly benefits the SAN Administrator; as best practices dictate keep SAN Fabrics separated. With the respective fabric identifiers, SAN Administrators can quickly tell if they have a crossed-fiber to the uplinks of the Fabric Switches. The graphics below show an example of Global WWPN Pools for A Fabric and B Fabric.

Global WWPN Pool – Fabric A



G-USA-WWPN-A WWN Pool
root/Americas

Pool Usage

1

1 Running
0 Associated
0 Unassociated
0 Config Error

Pool Utilization

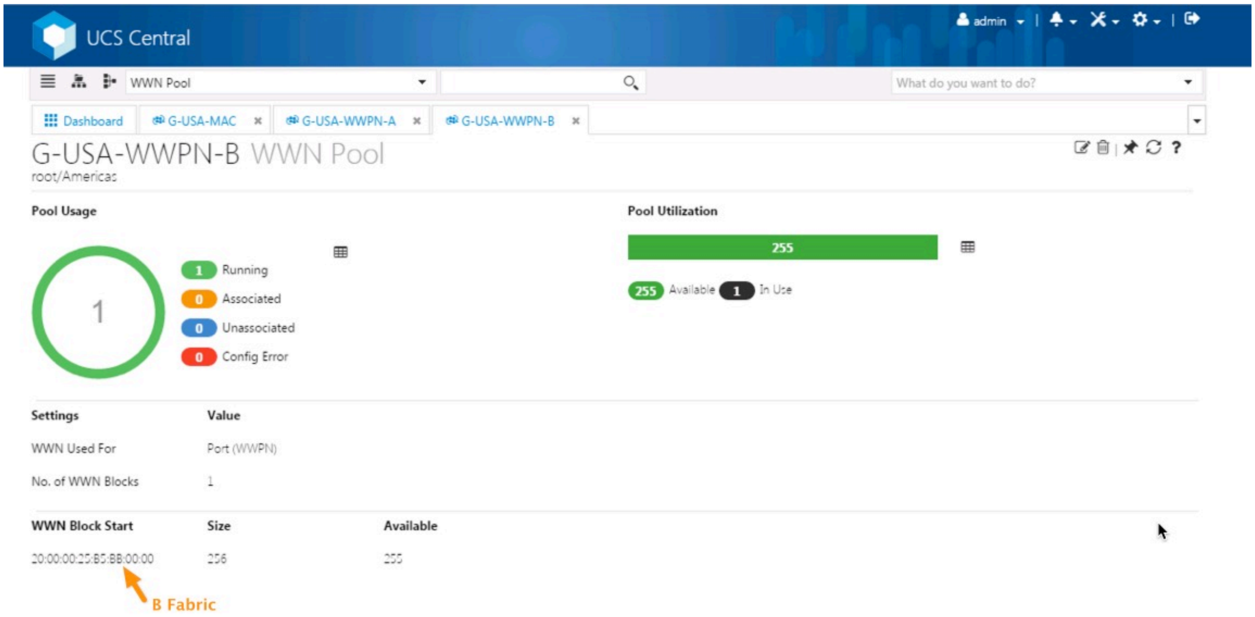
255

255 Available 1 In Use

Settings	Value
WWN Used For	Port (WWPN)
No. of WWN Blocks	1

WWN Block Start	Size	Available
20:00:00:25:B5:AA:00:00	256	255

Global WWPN Pool – B Fabric



G-USA-WWPN-B WWN Pool
root/Americas

Pool Usage

1

1 Running
0 Associated
0 Unassociated
0 Config Error

Pool Utilization

255

255 Available 1 In Use

Settings	Value
WWN Used For	Port (WWPN)
No. of WWN Blocks	1

WWN Block Start	Size	Available
20:00:00:25:B5:BB:00:00	256	255

With a Medium Size deployment of UCS Central, with up to 12 registered domains…. that can still take-on the scope of some average metrics of some 768+ servers (12 Domains x 8 Chassis x 8 Blades) with a maximum of (12 Domains x 20 Chassis x 8 Blades), 1920 B-Series Blades, plus potentially X-number of Manager C-Series Servers….so scale can be quite large with just 12 Registered Domains. The number of Global VLANs/VSANs, vNIC/vHBA Templates, LAN/SAN Connectivity Policies, corresponding Global Service Profile Templates and finally Global Service Profiles can be very significant.

Several great features of UCS Central that can assist in streamlining some of the "infrastructure" to manage that is discussed above is to use VLAN/VSAN "Aliasing" and ID Access Control Policies. These two powerful UCS Central functionalities can assist in reducing the overall amount of templates you need to manage in your infrastructure, yet provide the uniqueness required to manage different Blades/Servers in different network and fabric segments. Whether your goal is to reduce the number of managed objects, and/or achieve better Global SP Workload mobility, these functionalities can be a great asset. VLAN/VSAN ID Aliasing and ID Access Control Policies are discussed in-detail later in this document.

Medium Size Brownfield Deployments of UCS Central:

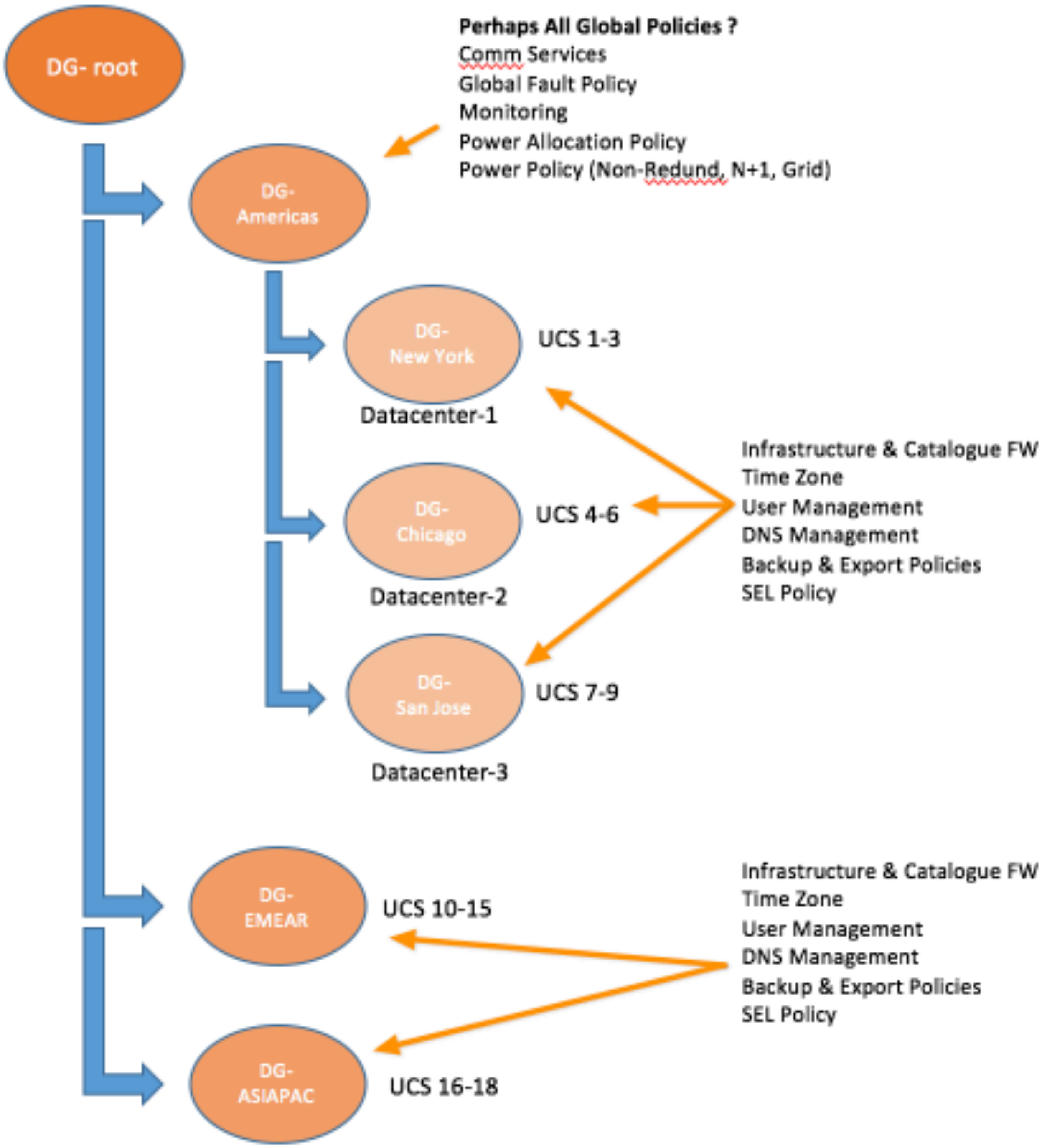
Medium Size deployments of UCS managed by UCS Central are much easier to manage than environments that lack UCS Central. With a medium size Brownfield deployment of UCS and UCS Central, it becomes much more manageable to eventually convert all existing Local Policies, VLANs, VSANs, ID Pools, vNIC Templates, vHBA Templates, LAN/SAN Connectivity Policies and Service Profile Templates/Service Profiles to a Global Infrastructure.

One can certainly register their existing UCS Domains to UCS Central on day-1, and take advantage of the first two Major User Cases, Dashboard and Operational Policies explained earlier in the document. With that great capability, there’s also the leisure of slowly defining and building-out of the Global Infrastructure…perhaps mirroring what exists exactly in the Local Domains, or making some desired, needed changes to policies and pools. The point is, there’s no time criticality to accomplish this conversion. Once can whiteboard, plan and finally build-out what makes sense in the Global Object context. Additionally, this can also be tested readily in a lab with an instance of UCS Central, test UCS H/W Domains, and/or the UCS Emulators.

The beautiful aspect is that the entire Global Object infrastructure can be built-out and tested well in advance of actually deploying Global Infrastructure to UCS Domains in production. It’s OK for Duplicate Pools to exist…one uniquely defined Locally within a UCS Domain, and its Global Counterpart defined within UCS Central. UCS Central will track exactly the status of each and every ID within all the Local and Global Pools, and while a particular ID may exist in multiple Pool Definitions, UCS Central will never all the issue of a duplicate ID to a UCS Domain.

Final migration of UCS Domains can take place Domain by Domain, leveraging existing scheduled maintenance periods to gracefully shut down blades/servers, remove and delete the Local Service Profile, and then replace that with the corresponding Global Service Profile. While this process is not as easy as “Pressing an Easy-Button”, the process is well defined and can planned, tested and successfully performed with little to minimum risk. The process of switching a Local Service Profile to a Global Service Profile is thoroughly discussed, and also shown in a Video on Demand (VOD) later in this document.

Large UCS Central Environment: >12 Registered UCS Domains (example)



Large UCS Central Environments:

Large scale deployments of UCS and UCS Central almost necessitate the registration and use of UCS Central. Cisco IT itself has well over 300 registered UCS Domains, with some 6000 plus servers. Internal Analysis by Cisco IT revealed that they save about 1-person/yr in OPEX workload by leveraging UCS Central. So, Yes Cisco is using their own tools…every UCS Domain within Cisco is managed by UCS Central.

The latest release of UCS Central, version 1.4.1a has been scale tested tested to support up to 10,000 servers in a single instance of UCS Central Server. Such possible scales are what really drove the complete redesign of the HTML-5 UI, and the deprecation of the older Flash UI. The HTML-5 UI is much more suited to manage UCS Domains and Servers at-scale, and the performance is there to support this. The older Flash based UI always suffered performance issues when used in very large environments.

With larger deployments, leveraging an efficient Domain Group hierarchy takes-on even greater importance. Perhaps in a very large environment, we are talking about UCS Domains dispersed all around a given country, and perhaps around the world, encompassing many differences in Time Zones, DNS Servers, User Authentication (LDAP) Domain Controllers, Backup remote FTP Servers, and certainly a more granular approach to Firmware Upgrades and management.

One can imagine the headache with separately managing the Backup Job Schedules for dozens of individual UCS Domains. This task is made simple with UCS Central, as custom schedules can be defined for Backup (Full State .bin) and Configuration Export (AllConfig .xml) as well as specific remote copy FTP servers to ensure proper safe-guard of those Backups.

Also, with LDAP Integration of UCS Domains with internal LDAP Servers, it becomes a real chore to replicate those granular settings, prone to human typing mistakes, in each an every UCS Domain. With UCS Central, this task becomes much easier as LDAP Configurations are set as a part of Domain Group hierarchical policy, and can be defined as broad, or as granular as required.

The graphic above to introduce this section is a simply example of how you might consider placing those Domain Group Operational Policies within the hierarchy. Policies such as Timezone and DNS can be places as high-up in the Domain Group hierarchy as applicable for the UCS Domains registered in a given geographic Domain Group. Whereas, Infrastructure and Catalog Firmware certainly can be more granularly placed, lower in the Sub-Domain Group structure.

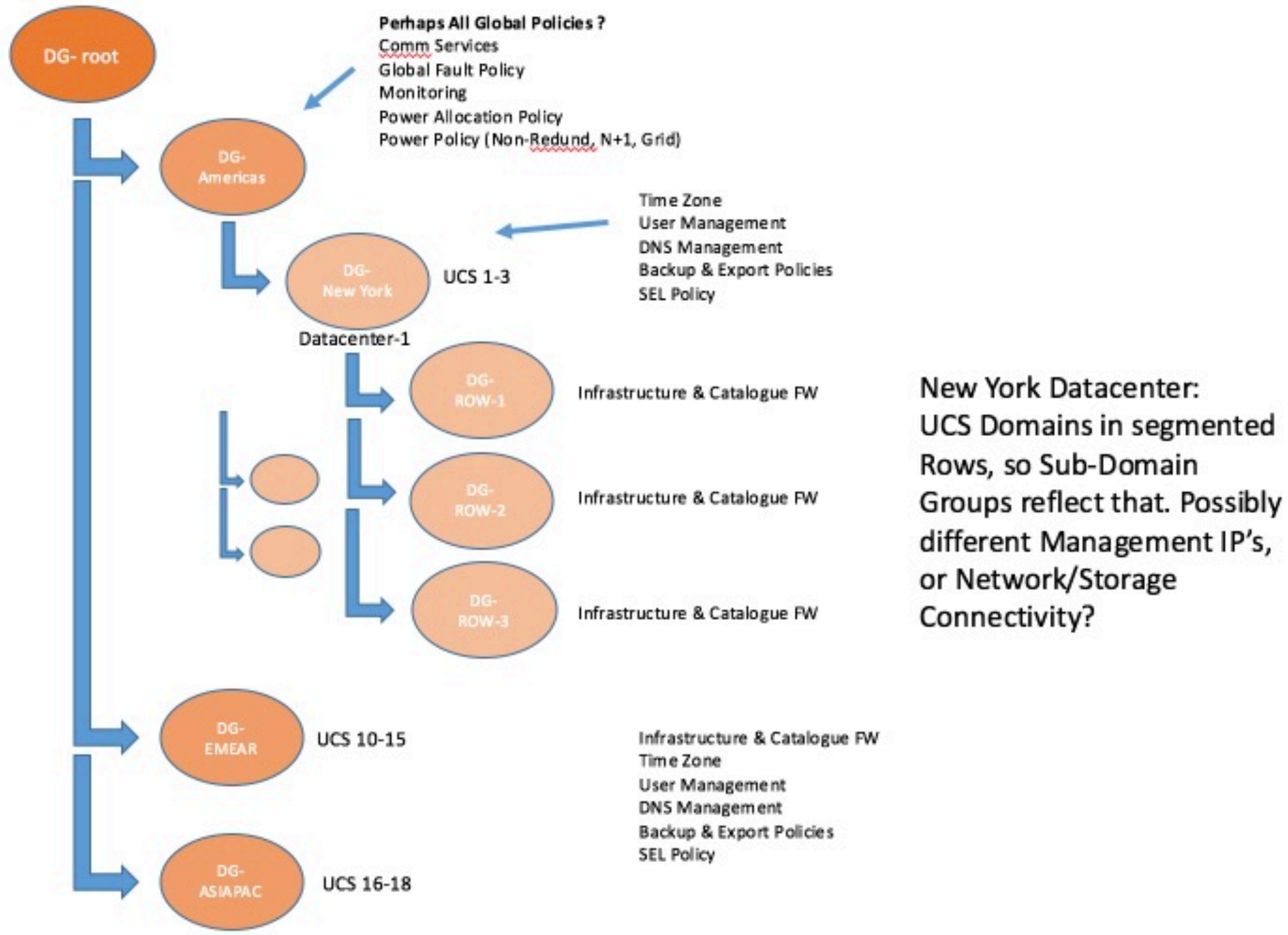
It's important to stress, there is no "right or wrong" and it would be foolish to try to dictate a "Best Practice" …. Ultimately, what works "best" for you and your organization becomes the Best Practice. Additionally, you can always opt for the simple-approach and make changes, or "expand" your sub-Domain Group structure in the future as necessary. It's not something that is “in-stone”, and it is infinitely easier to make changes to Domain Group hierarchy structure as compared to making changes to the Organization Structure which deals with the access to all Blade/Server related Pools, Policies, Templates and Service Profiles. Changes to Org Structure are mostly changes that result in a disruption of some kind in the environment.

Large Size Greenfield Deployments of UCS Central:

For large planned Greenfield deployments of UCS, please by-all-means considering adopting UCS Central from the very beginning, and design your Global Policy and Object infrastructure correctly from the beginning. Having everything built-out Globally within UCS Central will make it so much easier and less time to manage day to day operations and also less time consuming to scale-out and bring additional UCS Domains online. UCS Central 1.4.1a has come very close to closing the “gap” that has existed between UCS Central and UCS Manager in the Day-1 setup of a UCS Domain. UCS Central now includes the ability to define Equipment Policies, Unified Port Configurations, Port Roles, and Port-Channel configurations.

In addition to Domain Group hierarchy for Operational Policies, the Organizational Hierarchy for Global ID Pools, Policies, VLANs/VSANs, Templates and Service Profiles should also be strongly planned and considered before deploying the final architecture. As previously demonstrated with Advanced UCS/UCS Central Policy Resolution, as explained in-detail later in this document, the ability to smartly create Organizational boundaries not only serves the Use Case of Multi-Tenancy, but it also provides a way of potentially decreasing the over amount of Global Service Profiles Templates needed to support the environment. Other advanced functionalities of UCS Central Management such as VLAN/VSAN Aliasing and ID Range Access Control Policies can also certainly support decreasing the overall number of G-SP Templates to Manage. There’s absolutely no requirement to “Manage Less”, however with extremely large deployments, with hundreds and thousands of Blades/Servers, and with Dozens and Hundreds of G-SP Templates, then being able to markedly reduce those number only server to reduce the OPEX related to managing the environment.

An Alternative possibility to constructing Domain Group Hierarchy, is the case below where you have UCS Domains in a datacenter that perhaps occupy specific Rows, and have some level of segmentation. In this scenario, perhaps the Management Network is a different subnet, or upstream Network and Storage Connectivity for data traffic is different. Remember that in addition to the Operational Policies that can be defined per Domain Group, or Sub-Domain Group you also set Domain Group properties on all Global VLANs and VSANs…and can leverage advanced UCS Central capabilities such as VLAN/VSAN ID Aliasing and ID Range Access Control Policies for Management IP addresses addressed later in this document.



New York Datacenter:
UCS Domains in segmented Rows, so Sub-Domain Groups reflect that. Possibly different Management IP's, or Network/Storage Connectivity?

Large Size Brownfield Deployments of UCS Central:

With the largest scale-out architectures of UCS and UCS Central, you could easily be dealing with Hundreds or Thousands of Service Profiles assigned to blades/servers, so the move to UCS Central is certainly one that requires careful planning and calculation, particularly if considering moving the object repository to UCS Central and converting Local Service Profiles to Global Service Profiles. As previously explained, you can build-out the entire Global Infrastructure to mirror all the local infrastructure in all your UCS Domains, but the actual "exchange" of a Local Service Profile for it's Global Service Profile counterpart is a disruptive action. One truly has the weigh the convenience of managing everything globally from a single interface, and also the possibility of gaining workload mobility amongst multiple UCS Domains to truly weigh the work involved to convert.

Some very large Brownfield Clients have opted for the "eventual" move of the object repository and Local Service Profile conversion as a defined process over-time…. taking advantage of future maintenance windows to sequentially migrate completely over UCS Central. Sooner or later, clients will upgrade the Firmware on UCS Domains, and while Infrastructure Firmware Upgrades can be performed without completely disrupting the network and fabrics, the actual upgrade of Host Firmware, Controller Firmware, BIOS, Network Adapter, CIMC, and Storage Controller are all disruptive actions, so the Hosts will need maintenance windows to gracefully shut-down, and essentially "Re-Associate" the Service Profile containing the newly updated Host Firmware Policy to the blade/server to perform the upgrades. It is during this time that a new Global Service Profile could easily replace the existing Local Service Profile.

Other large Brownfield Clients have adopted a model of operating a Brownfield and Greenfield environments in parallel. What this means is that existing UCS infrastructure will remain Brownfield, locally managed within the respective UCS Managers, while anything "New" coming into the environment will be deployed as Global objects from UCS Central. As time passes, and local infrastructure has reached end-of-life and retired, more and more of the total environment will be global. Even with the decision of keeping Local Service Profiles, one can still take advantage of Global Objects and Policies by simply "switching" from Domain to Global from within the Local Service Profile Template or Local Service Profile. With that, policies can be global, fewer, and managed from one place within UCS Central. Further information about this can be read in later in the document in the section Brownfield – Accessing Global ID's and Policies with Local SP's.

Finally, automation with PowerTools and scripts with the XML-API can greatly facilitate the conversion process. If not already consulted, please see the section later in the document Migrating Brownfield Local Service Profiles to Global Service Profiles in UCS Central.

UCS Central Sizing Considerations

Sizing the UCS Central VM Resources

Some UCS Central Customers have scaled their UCS Environments from literally Dozens to Hundreds of Domains and from Hundreds to Thousands of servers. As previously mentioned in this document, the scaling metric to focus-upon is not so much the number of registered UCS Domains, but rather number of Blades and Servers. Currently, UCS Central 1.4.1a has been QA Tested to support up to 10,000 Servers…. however, there's no real software limit.

Very Large customers should take a look at the performance of their UCS Central VMs and gauge whether or not to increase cpu and memory resources to the UCS Central Server VM. In the UCS Central Install Guide, you can easily see the minimum requirements for running UCS Central. You'll notice that the deployment of the OVA File, will actually carve-out 2 x 40 GB Disks, allocate 4 x vCPUs and 16 GB RAM. It's important to realize that these parameters are the absolute minimum requirements….and for small to medium size environments, they should provide sufficient performance, however…. for large environments, it's wise to increase those resources by a factor of two. Cisco IT internally runs at least 4 vCPUs and 24 GB Ram for their instance of UCS Central, which exceeds 200 UCS Domains and close to 6,000 Servers. Bottom line, it's recommended to monitor the performance metrics of the UCS Central VM in new or growing infrastructures, and adjust CPU and RAM resources accordingly. If performance is noticeably lacking, please verify vCPU and Memory usage and make needed changes with your virtualization administrator.

Scaling Global Service Profiles and Global Service Profile Templates

I'd like to express that there's no software hard-limit to the number of Global Service Profile's that can be attached-to a Global Service Template. While the OPEX benefits of leveraging Templates to make wide-spread changes is beneficial to many customers and many architectures, I want to also express and bring attention to the fact that too much of anything is likely not a good.

One has to consider the "Fault Domain" of a single disruptive change to the environment. Fault Domain in the context of "How Much" is affected by a single disruptive error or change. This is something that's difficult to place an exact number upon, or claim an absolute "Best Practice", however in architecting your environment. How many resources (Global Service Profiles & Servers) are you willing to attach to an updating Global Service Profile Template, where a single wrong/disastrous change can cause a wide-spread outage? Sure, there are "User-Ack" Maintenance Policies…and Cisco absolutely recommends using Maintenance Policies as a Best Practice, but regardless one should consider leveling the playing field and reducing the potential Fault Domain…. aside, does anyone want to see the majority of their environment (servers) have User-Acks pending? Perhaps a scale of 100 Global Service Profiles to a single Global Profile Template should be considered the very max. Again, there's no hard fast limits. I've heard of architectures that have 1000's of Global Service Profiles attached to a single Global Service Profile Template, but that is beyond extreme and certainly would not be considered a Best Practice.

In addition to the scaling of GSPs to GSP Templates, another important aspect to consider is the quantity of a given policy. For instance, if you have 10 Global Service Profile Templates…with 100 Global Service Profiles attached…that's 1000 Blades or Servers. As such, perhaps you have ALL 10 Templates accessing the same Disruptive Policy (Boot/FW/BIOS/LAN-SAN Connectivity Policy) in your environment. Now, irrespective of Global Maintenance Policies (User-Ack), you have a single policy that can potentially disrupt 1000 Blades/Servers (same policy is being used by all your Global Service Profile Templates) if something is done incorrectly, administratively in editing that policy. As with spreading or balancing some of the scale across multiple Service Profile Templates, you can also create multiple Policies…perhaps with the same exact settings, but different names, so those policies can be consumed by their respective Global Service Profile Templates. Again, all in the spirit of reducing the Fault Domain.

Perhaps the given numbers are somewhat extreme….and certainly User-Ack Maintenance Policies will be your friend…. however, it's still unnerving to receive wide-spread User-Acks on all your Blades/Servers just because an Admin incorrectly edited a disruptive policy…perhaps a Boot Policy, or a LAN/SAN Connectivity Policy.

If you are in a situation of having too many Global Service Profiles attached to Too-Few Templates, you can easily Clone the Global Service Profile Template and Unbind-Bind a percentage of the Global Service Profiles to the Cloned Templates (Test First!) The entire system is so flexible in design and operations, that It's easy to balance and scale according to refined designs. But remember, it really does no good to increase the spread of your GSPs-Templates, if they are all accessing the same policy on the backend.

You might we thinking, in some sections of this document, I showed you ways of reducing the number of Global Service Profile Templates…. certainly, VLAN/VSAN ID Aliasing, Advanced Policy Resolution and ID Access Control Policies can all be used to reduce the numbers of required Global Service Profile Templates…but then, I warn or guard you against putting "all your eggs in one basket" so-to-speak by attaching too many Global Service Profiles to a given Template, or using a single policy for too many Global Service Profile Templates/Global Service Profiles. This sounds contradictory….and in a sense, it is…however, what I am trying to communicate to you are the techniques to reduce-down the number of Global Service Profile Templates to make them manageable…. but also keep in mind your desired size of your "Fault Domain" as discussed above. There's no magic or easy concrete answer…. I cannot provide a spreadsheet with numbers…but taking all that's been discussed in consideration, I am sure you are armed with enough detailed information to make the right design decisions, and changes, for your business and environment. Frankly, you could ask 5 different architects about how to do this, and probably get 5 different answers. I think the important thing is you realize the capabilities of the system, and the consequences for doing things a certain way, and you work towards mitigating the overall risk just like everywhere else in your IT environment.

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

Link to VOD: Converting a Local Service Profile to a Global Service Profile

https://youtu.be/cOMxNu91VG8

In the above VOD, and below procedure, we assume the most challenging Use Case, Boot from SAN with Remote Storage Boot LUNs, that are already Zoned to Target Initiators (WWPN's) within each Service Profile. ID's Must remain the same during migration.

- Register existing UCS Domain to UCS Central
- Create Global Pools, Policies, VLANS, VSANS, vNIC Templates, vHBA Templates, LAN Connectivity Policies, SAN Connectivity Policies, Global Service Profile Templates, and Global Service Profiles.
- When creating Global VSANs that have the Same IDs as Locally defined VSANs in UCS Manager, make sure the Global Name is Unique, consider a "G-" in front of the VSAN Name, and also make sure that the FCoE VLAN ID on the newly created Global VSAN MATCHES Exactly the FCoE VLAN ID configured on the corresponding Local VSAN. If the VSAN ID is the same, and the FCoE ID is different, then a Fault will be raised upon Global Service Profile Association.
- Creation of the Global SP's will allocate new UUID, MACs, WWNN, and WWPNs from their respective Global ID Pools.
- Leverage simple UCS Central PowerTool script to "swap" or "assign" the original (Correctly Zoned) WWPNs and other IDs. These ID's are part of the created Global Pools, and ID Universe will reflect "In-Use" status once these IDs are properly assigned.

Steps: **Local Service Profile (L-SP) to Global Service Profile (G-SP) Conversion**

1. Document Pool IDs/Policies/VLANs/VSANs/Templates of Local SPs.
2. Re-create all IDs/Policies/VLANs/VSANs/Templates and G-SPs in UCS Central.
3. Gracefully Shut down Server with L-SP
4. Disassociate L-SP
5. Delete L-SP (restores allocated IDs back into pool with unused status)
6. Execute UCS Central PowerTools Script to swap IDs for the specific G-SP (Making the G-SP look "Exactly" like it's corresponding, predecessor L-SP)
7. Verify IDs are the correct ones for the specific Zoned Server in the new G-SP
8. Associate the G-SP to the designated Server
9. Boot Server from SAN LUN.

Below UCS Central PowerTools Script is just an example, and is not an officially supported product of Cisco. Please use at your own risk, and test first in a lab before using in production. Please edit script according to your G-SP setup, Orgs, IDs, Policies, etc.

Assume:

Global Service Profile Name: G-SP-TEST-2 (with global pool derived IDs)
Org: root
Global WWNN Pool: G-USA-WWNN
Global UUID Pool: G-USA-UUID
Global MAC Pool: G-USA-MAC
Change To (from Local SP) UUID: dc81c8de-3b00-11e5-0000-000000000025
Change To (from Local SP) MAC for vnic0: 00:25:B5:00:00:25
Change To (from Local SP) MAC for vnic1: 00:25:B5:00:00:26
Change To (from Local SP) WWNN ID: 20:00:00:25:B5:00:00:25
Change To (from Local SP) WWPN for A Fabric: 20:00:00:25:B5:AA:00:25
Change To (from Local SP) WWPN for B Fabric: 20:00:00:25:B5:BB:00:25

```
Start-UcsCentralTransaction
$mo = Get-UcsCentralOrg -Name root | Add-UcsCentralServiceProfile -Name “G-SP-TEST-2”
-ModifyPresent -Uuid "0909ac8a-2411-11e4-0000-181401000099”
$mo_1 = $mo | Add-UcsCentralVnic -ModifyPresent  -Name “eth0" -Addr
"00:25:B5:14:A1:99”
$mo_2 = $mo | Add-UcsCentralVnic -ModifyPresent  -Name “eth1" -Addr
"00:25:B5:14:B1:99”
$mo_3 = $mo | Add-UcsCentralVhba -ModifyPresent -Name “fc0" -Addr
"20:00:00:25:B5:14:01:98”
$mo_4 = $mo | Add-UcsCentralVhba -ModifyPresent -Name “fc1" -Addr
"20:00:00:25:B5:14:01:99”
$mo_5 = $mo | Add-UcsCentralVnicFcNode -ModifyPresent -Addr "20:01:00:25:B5:14:01:99”
Complete-UcsCentralTransaction

Start-UcsCentralTransaction
$mo = Get-UcsCentralOrg -Name root | Add-UcsCentralServiceProfile -Name “G-SP-TEST-2”
-ModifyPresent -Uuid derived
$mo_1 = $mo | Add-UcsCentralVnic -ModifyPresent  -Name “eth0" -Addr derived
$mo_2 = $mo | Add-UcsCentralVnic -ModifyPresent  -Name “eth1" -Addr derived
$mo_3 = $mo | Add-UcsCentralvhba -ModifyPresent  -Name “fc0" -Addr derived
$mo_4 = $mo | Add-UcsCentralvhba -ModifyPresent  -Name “fc1" -Addr derived
$mo_5 = $mo | Add-UcsCentralVnicFcNode -ModifyPresent -Addr pool-derived
Complete-UcsCentralTransaction
```

UCS Central Upgrade Recommended Process Steps

1. Verify Upgrade compatibility – Consult and Read Release Notes of UCS Manager and UCS Central.

2. Verify No operations are being performed with UCS Central. Ensure no administrators are performing actions.

3. Verify no “Pending” acknowledgements within UCS Central.

4. Take Full State and Configuration Exports of UCS Central and remotely Store Offline.

5. In the CLI, gracefully shut-down UCS Central. “shutdown” Command.

6. Once UCS Central is gracefully shutdown, take a Hypervisor “snapshot” of existing UCS Central state.

7. Download new version of UCS Central (.ISO)

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

9. Edit the Boot Order as required.

10. Boot UCS Central to the .ISO

11. Select Option #2 to Upgrade UCS Central

12. Complete Upgrade and automatic reboot.

13. Verify UCS Central has been upgraded.

14. Take Full State and Configuration Exports of UCS Central and remotely Store Offline.

Advanced UCS & UCS Central Policy Resolution

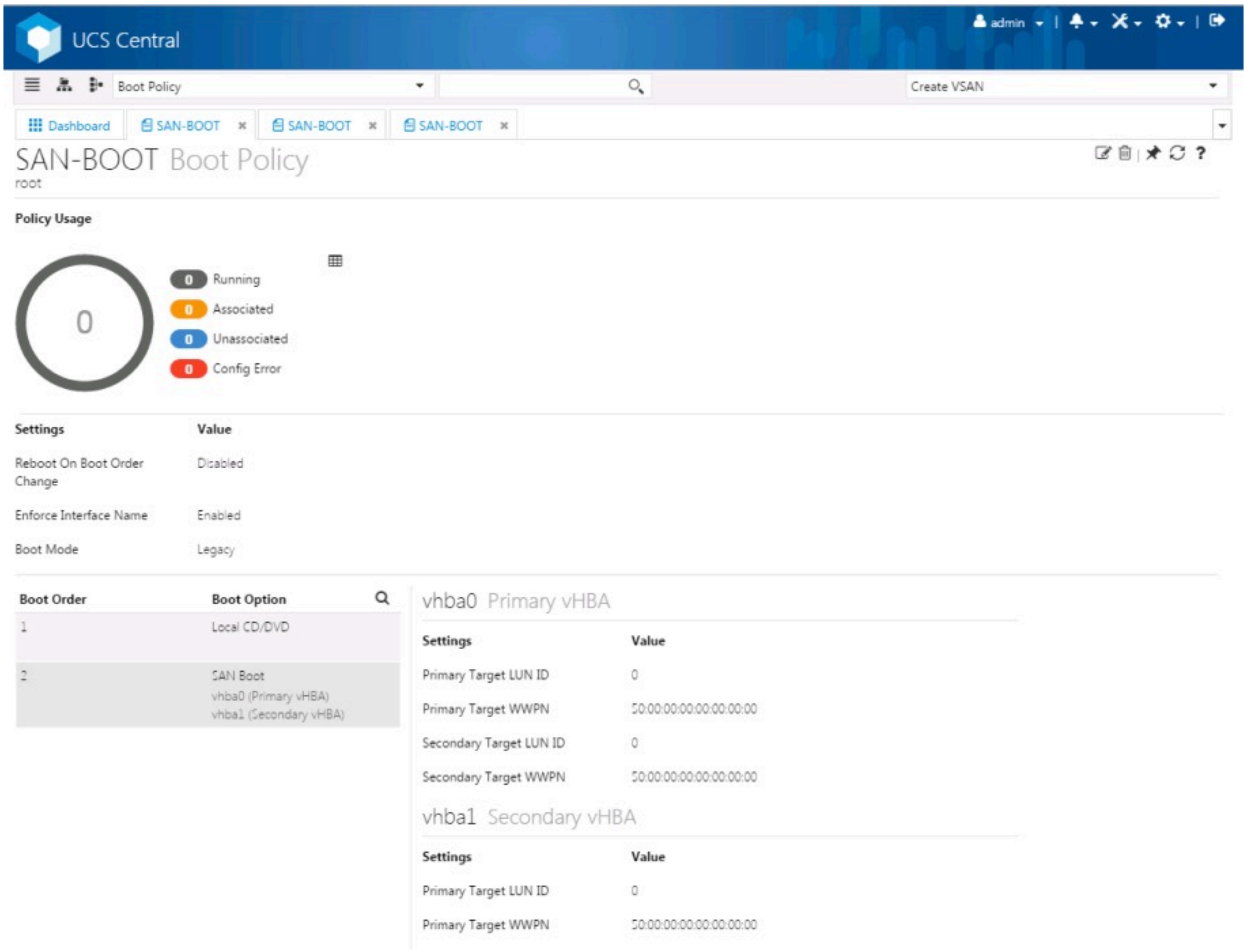
Link to VOD: UCS Advanced Policy Resolution

https://youtu.be/bQlBYUfAJeM

Use SAN-BOOT in different Orgs as an Example. Replicate the “SAN-BOOT” policy in different Orgs, with different policy settings…and then use a Single Global SP Template to instantiate resulting G-SPs down into those different Sub-Orgs, taking-on the desired boot policy at that level of the Sub-Org.

For instance, it our example. We’ve created a SAN-BOOT policy at the /root Org with generic (fake) target initiators. No Blade/Server is going to boot to SAN with this boot policy…but it’s acting as a placeholder to be consumed in the Global Service Profile Template.

Global Boot Policy



SAN-BOOT Boot Policy
root

Policy Usage

Settings	Value
Reboot On Boot Order Change	Disabled
Enforce Interface Name	Enabled
Boot Mode	Legacy

Boot Order	Boot Option
1	Local CD/DVD
2	SAN Boot vhba0 (Primary vHBA) vhba1 (Secondary vHBA)

vhba0 Primary vHBA

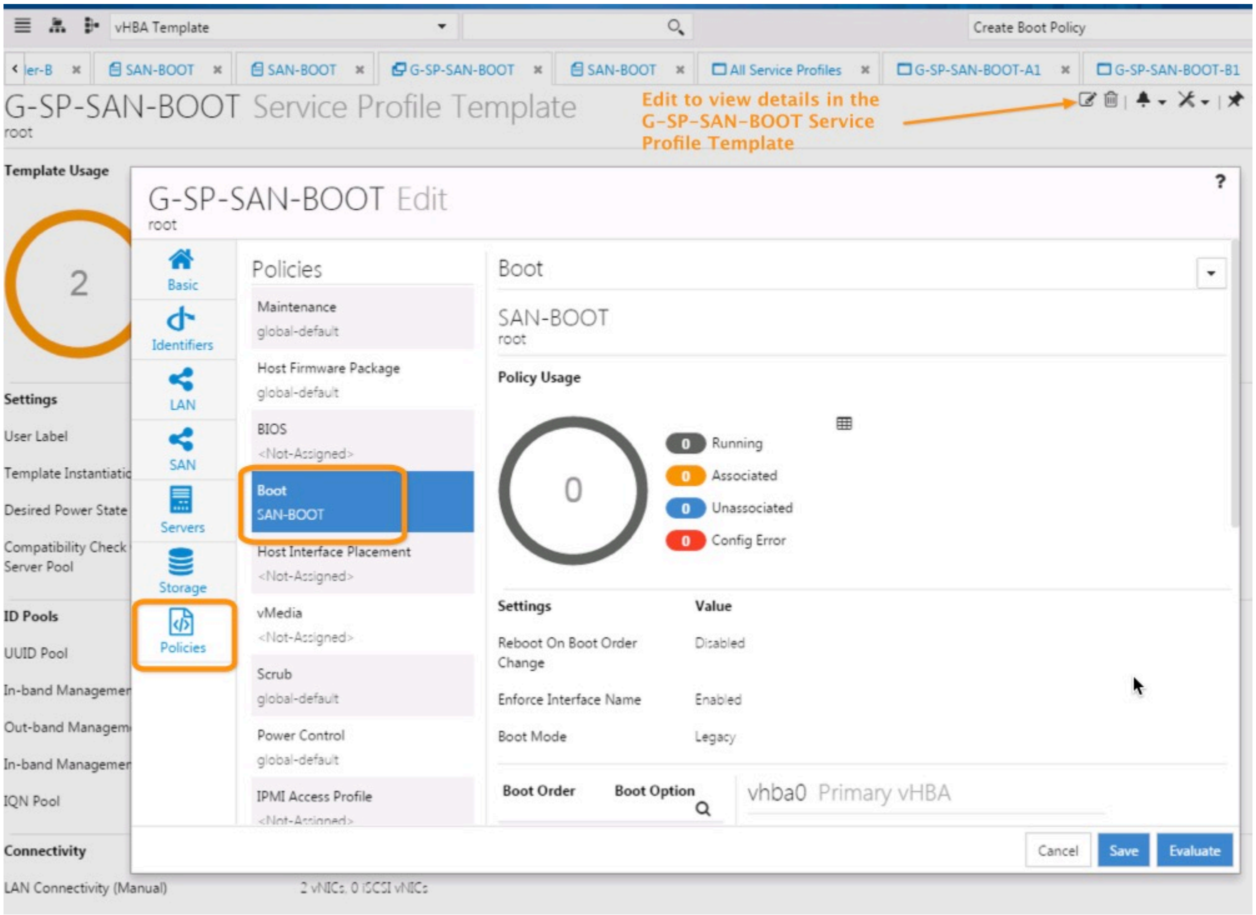
Settings	Value
Primary Target LUN ID	0
Primary Target WWPN	50:00:00:00:00:00:00:00
Secondary Target LUN ID	0
Secondary Target WWPN	50:00:00:00:00:00:00:00

vhba1 Secondary vHBA

Settings	Value
Primary Target LUN ID	0
Primary Target WWPN	50:00:00:00:00:00:00:00

As you can see, when you actually edit the Service Profile Template, and then Select Policies, Boot Policy, you can then see the details of the newly created SAN-BOOT policy.

Editing Global Boot Policy



G-SP-SAN-BOOT Service Profile Template
root

Edit to view details in the G-SP-SAN-BOOT Service Profile Template

Template Usage
2

Settings
User Label
Template Instantiatio
Desired Power State
Compatibility Check
Server Pool

ID Pools
UUID Pool
In-band Managemen
Out-band Managem
In-band Managemen
IQN Pool

Connectivity
LAN Connectivity (Manual) 2 vNICs, 0 iSCSI vNICs

G-SP-SAN-BOOT Edit
root

Policies

Policy	Value
Maintenance	global-default
Host Firmware Package	global-default
BIOS	<Not-Assigned>
Boot	SAN-BOOT
Host Interface Placement	<Not-Assigned>
vMedia	<Not-Assigned>
Scrub	global-default
Power Control	global-default
IPMI Access Profile	<Not-Assigned>

Boot

SAN-BOOT
root

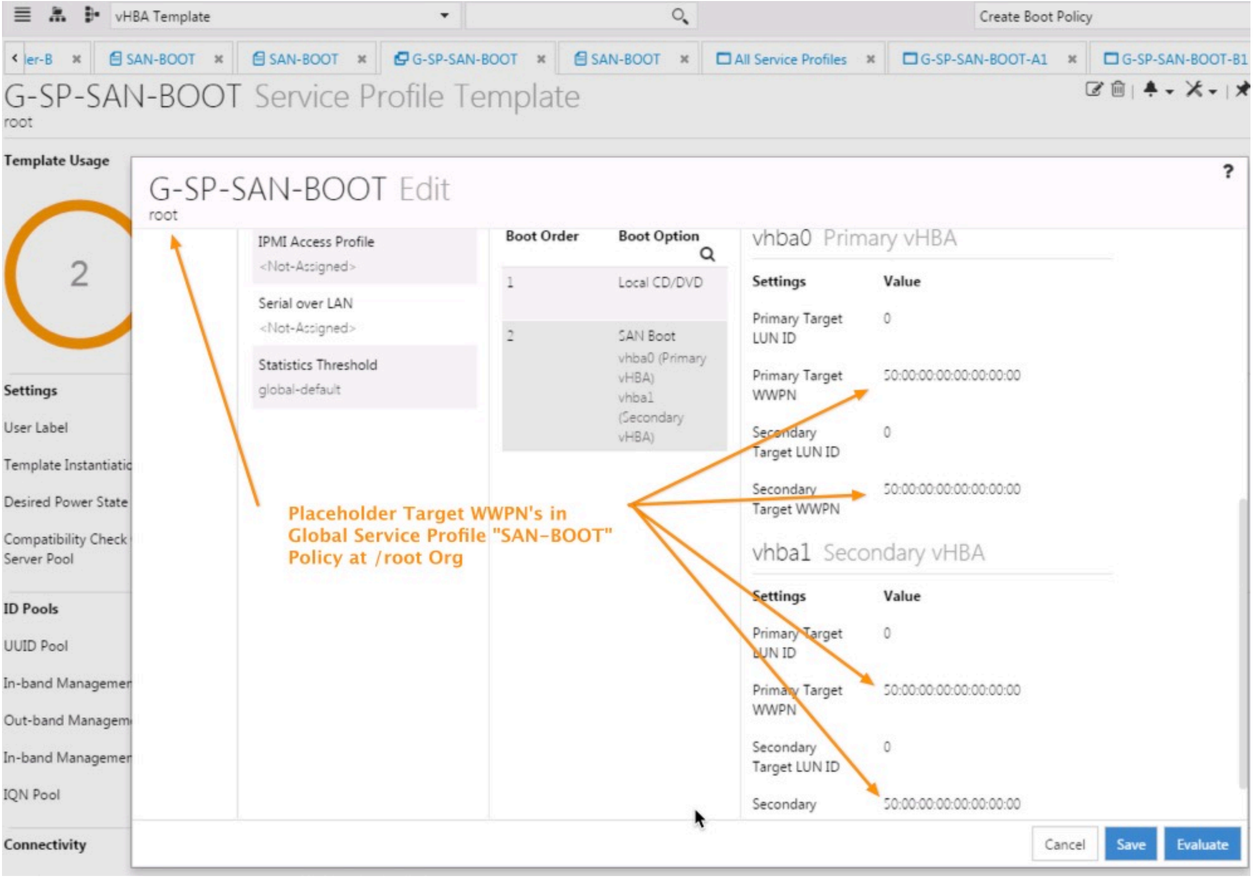
Policy Usage
0
0 Running
0 Associated
0 Unassociated
0 Config Error

Settings	Value
Reboot On Boot Order Change	Disabled
Enforce Interface Name	Enabled
Boot Mode	Legacy

Boot Order Boot Option
vhba0 Primary vHBA

Upon investigation of the SAN-BOOT Policy in detail in the /root Org, you can see the “Fake” initiators that have been created for the 4-possible Boot Paths of a UCS/UCS Central SAN Boot Policy. 2 possible vhba’s, 1-Primary and 1-Secondary, and in-turn, each vhba has its own Primary and Secondary target initiators.

Editing Global Boot Policy - Details



IPMI Access Profile
<Not-Assigned>

Serial over LAN
<Not-Assigned>

Statistics Threshold
global-default

Boot Order	Boot Option
1	Local CD/DVD
2	SAN Boot vhba0 (Primary vHBA) vhba1 (Secondary vHBA)

vhba0 Primary vHBA

Settings	Value
Primary Target LUN ID	0
Primary Target WWPN	50:00:00:00:00:00:00:00
Secondary Target LUN ID	0
Secondary Target WWPN	50:00:00:00:00:00:00:00

vhba1 Secondary vHBA

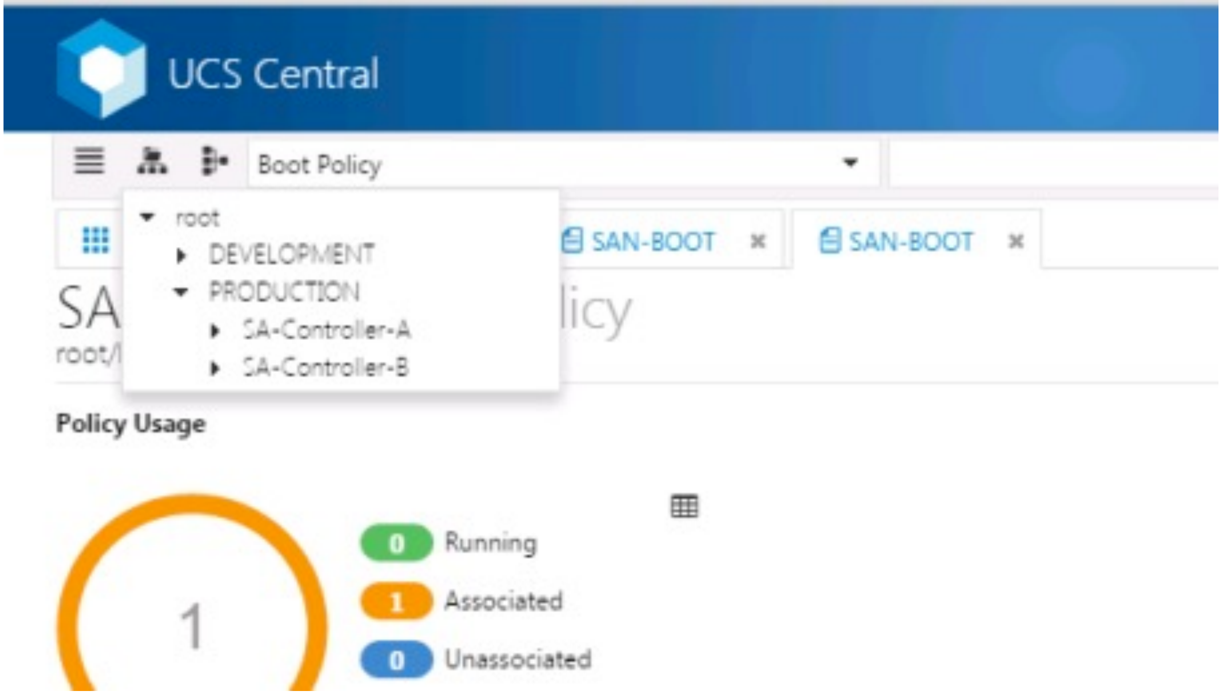
Settings	Value
Primary Target LUN ID	0
Primary Target WWPN	50:00:00:00:00:00:00:00
Secondary Target LUN ID	0
Secondary	50:00:00:00:00:00:00:00

Placeholder Target WWPN's in Global Service Profile "SAN-BOOT" Policy at /root Org

In our scenario, we have an Organizational Structure that reflects "how" the Blades/Servers will boot to the SAN, for instance I want half of my Global Service Profiles booting from one Storage Array Controller and the other half of my Global Service Profiles booting from another, in order to spread the boot-load on my Storage Array.

Under the /root Org, I've created a Sub-Org for Production, and then two Sub-Orgs under Production, one called SA-Controller-A and the other SA-Controller-B.

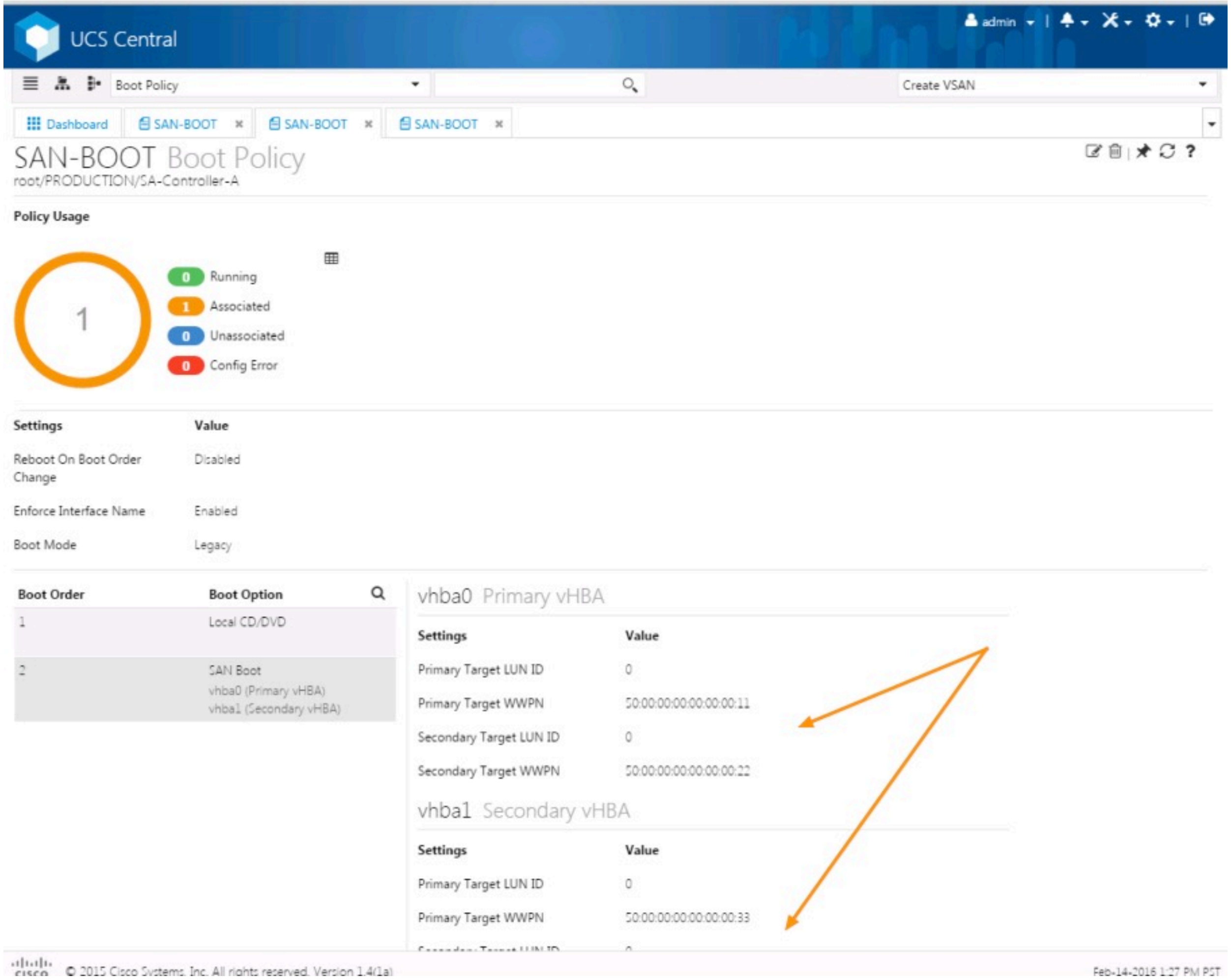
Organizational Structure



I then created boot-controller specific SAN-BOOT policies down within each of the SA-Controller Sub-Orgs. The SAN-BOOT Policies in these Sub-Orgs will contain the valid, true target initiators to Boot the the Storage Array, except they will contain different Initiators/order to separate the boot-load when all the Global Service Profiles boot to the Storage Array.

You can see that the SAN-BOOT policy that lives in the SA-Controller-A Sub-Org, contains the boot target initiator values below. The WWPNs end in 11, 22, 33, 44 for the 4 target initiators.

Global Boot Policy – Details root/PRODUCTION/SA-Controller-A



SAN-BOOT Boot Policy
root/PRODUCTION/SA-Controller-A

Policy Usage

Settings	Value
Reboot On Boot Order Change	Disabled
Enforce Interface Name	Enabled
Boot Mode	Legacy

Boot Order	Boot Option
1	Local CD/DVD
2	SAN Boot vhba0 (Primary vHBA) vhba1 (Secondary vHBA)

vhba0 Primary vHBA

Settings	Value
Primary Target LUN ID	0
Primary Target WWPN	50:00:00:00:00:00:00:11
Secondary Target LUN ID	0
Secondary Target WWPN	50:00:00:00:00:00:00:22

vhba1 Secondary vHBA

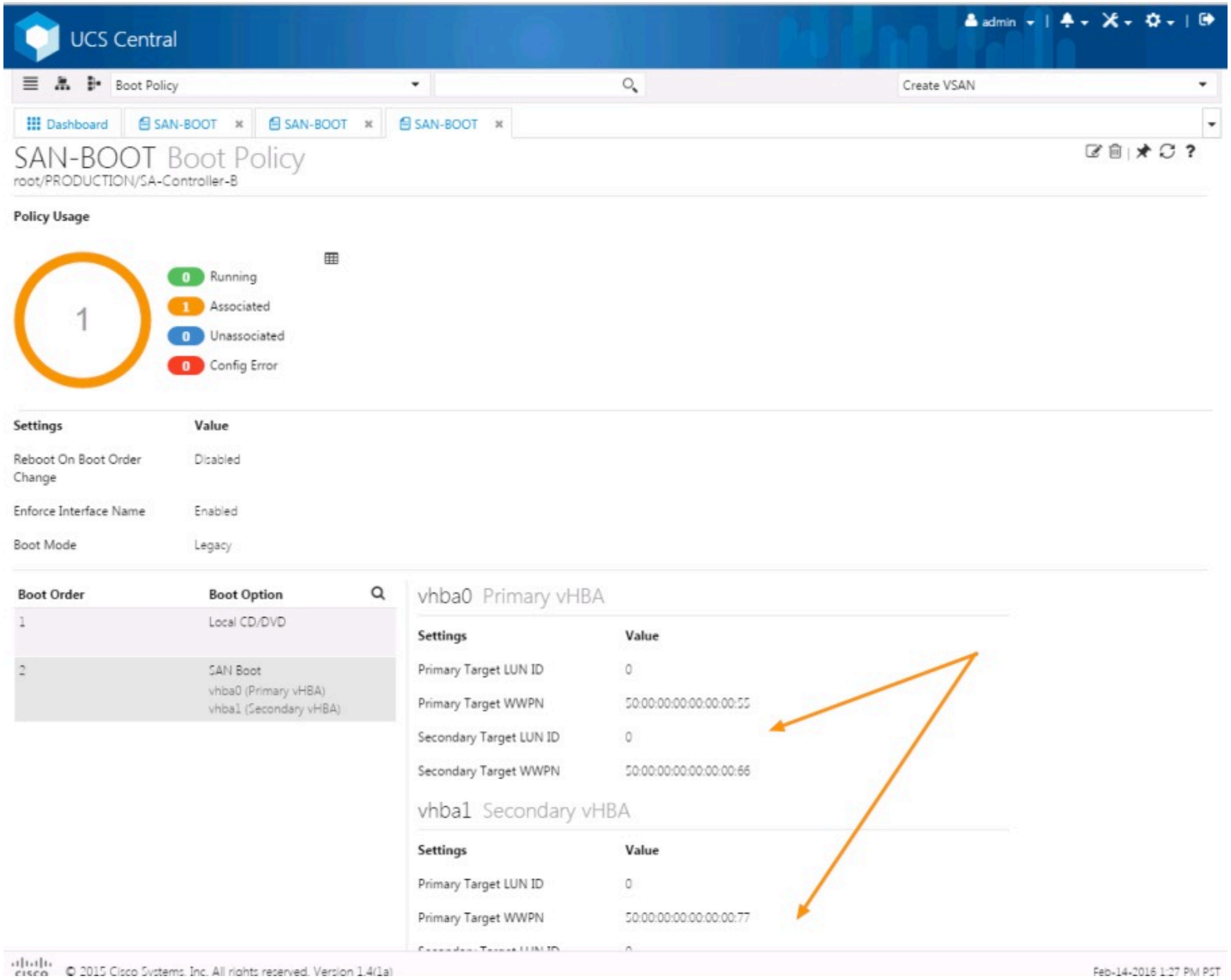
Settings	Value
Primary Target LUN ID	0
Primary Target WWPN	50:00:00:00:00:00:00:33
Secondary Target LUN ID	0

© 2015 Cisco Systems, Inc. All rights reserved. Version 1.4(1a)

Feb-14-2016 1:27 PM PST

You can see that the SAN-BOOT policy that lives in the SA-Controller-B Sub-Org, contains the boot target initiator values below. The WWPNs end in 55, 66, 77, 88 for the 4 target initiators.

Global Boot Policy – Details root/PRODUCTION/SA-Controller-B



SAN-BOOT Boot Policy
root/PRODUCTION/SA-Controller-B

Policy Usage

Settings	Value
Reboot On Boot Order Change	Disabled
Enforce Interface Name	Enabled
Boot Mode	Legacy

Boot Order	Boot Option
1	Local CD/DVD
2	SAN Boot vhba0 (Primary vHBA) vhba1 (Secondary vHBA)

vhba0 Primary vHBA

Settings	Value
Primary Target LUN ID	0
Primary Target WWPN	50:00:00:00:00:00:00:55
Secondary Target LUN ID	0
Secondary Target WWPN	50:00:00:00:00:00:00:66

vhba1 Secondary vHBA

Settings	Value
Primary Target LUN ID	0
Primary Target WWPN	50:00:00:00:00:00:00:77
Secondary Target LUN ID	0

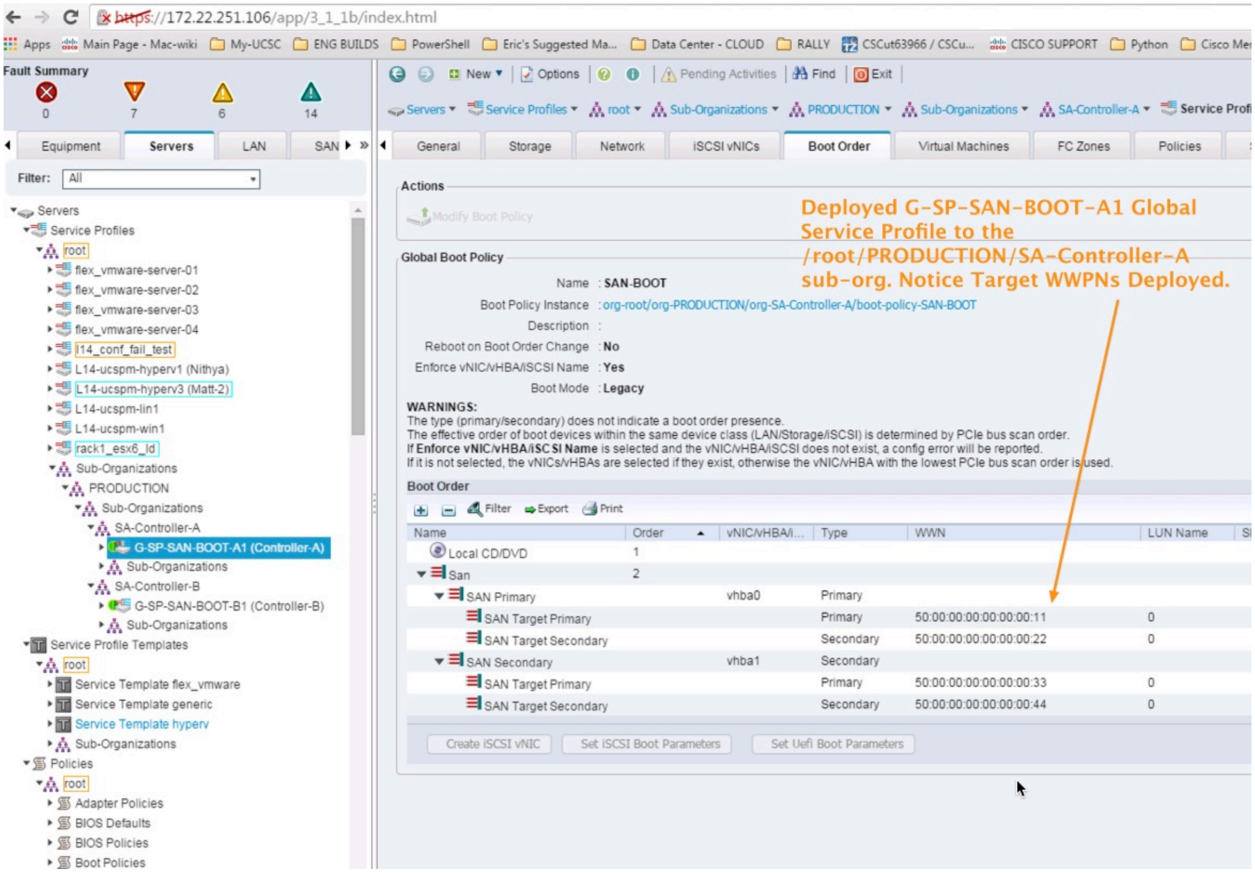
© 2015 Cisco Systems, Inc. All rights reserved. Version 1.4(1a)

Feb-14-2016 1:27 PM PST

From the Single Global Service Profile Template (G-SP-SAN-BOOT), located in the /root Org consuming the “SAN-BOOT” boot from SAN policy, you can then “Create Service Profile from Template” and instantiate those Global Service Profiles down into their respective SA-Controller Sub-Orgs.

Upon creation of G-SP-SAN-BOOT-A1 Global Service Profile, and subsequent association to a blade in a UCS Domain, you can see the Global Service Profile Deployment and the actual SAN-BOOT policy and initiators that are copied down to the Domain. The target initiators precisely match those configured in the SAN-BOOT policy in the SA-Controller-A Sub-Org.

UCS Manager – Viewing Deployed Global Service Profile



Deployed G-SP-SAN-BOOT-A1 Global Service Profile to the /root/PRODUCTION/SA-Controller-A sub-org. Notice Target WWPNs Deployed.

Global Boot Policy

Name : SAN-BOOT
Boot Policy Instance : org-root/org-PRODUCTION/org-SA-Controller-A/boot-policy-SAN-BOOT
Description :
Reboot on Boot Order Change : No
Enforce vNIC/vHBA/iSCSI Name : Yes
Boot Mode : Legacy

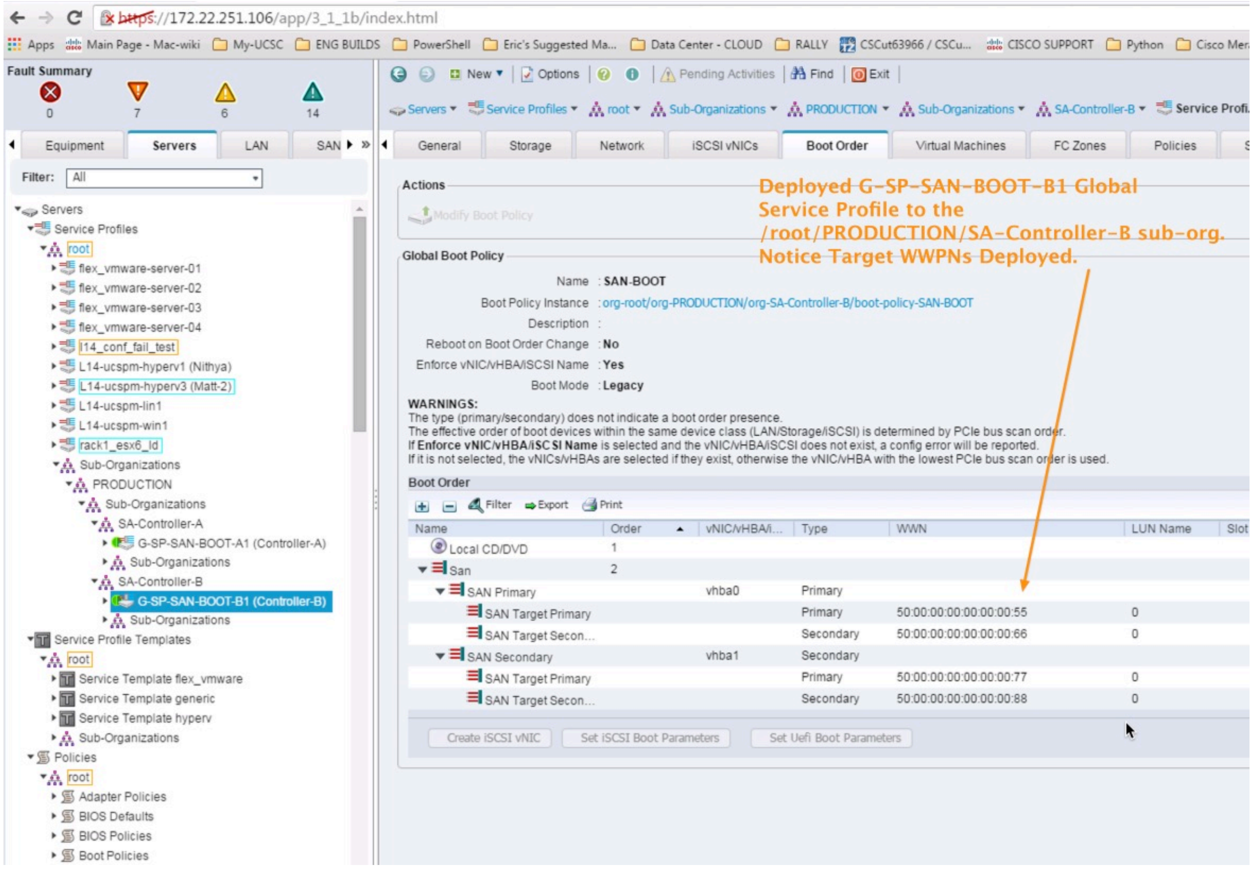
WARNINGS:
The type (primary/secondary) does not indicate a boot order presence.
The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.
If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.
If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

Boot Order

Name	Order	vNIC/vHBA/i...	Type	WWN	LUN Name	Sl
Local CD/DVD	1					
San	2					
SAN Primary		vhba0	Primary			
SAN Target Primary			Primary	50:00:00:00:00:00:00:11	0	
SAN Target Secondary			Secondary	50:00:00:00:00:00:00:22	0	
SAN Secondary		vhba1	Secondary			
SAN Target Primary			Primary	50:00:00:00:00:00:00:33	0	
SAN Target Secondary			Secondary	50:00:00:00:00:00:00:44	0	

Also, upon creation of G-SP-SAN-BOOT-B1 Global Service Profile, and subsequent association to a blade in a UCS Domain, you can see the Global Service Profile Deployment and the actual SAN-BOOT policy and initiators that are copied down to the Domain. The target initiators precisely match those configured in the SAN-BOOT policy in the SA-Controller-B Sub-Org.

UCS Manager – Viewing Deployed Global Service Profile



Deployed G-SP-SAN-BOOT-B1 Global Service Profile to the /root/PRODUCTION/SA-Controller-B sub-org. Notice Target WWPNs Deployed.

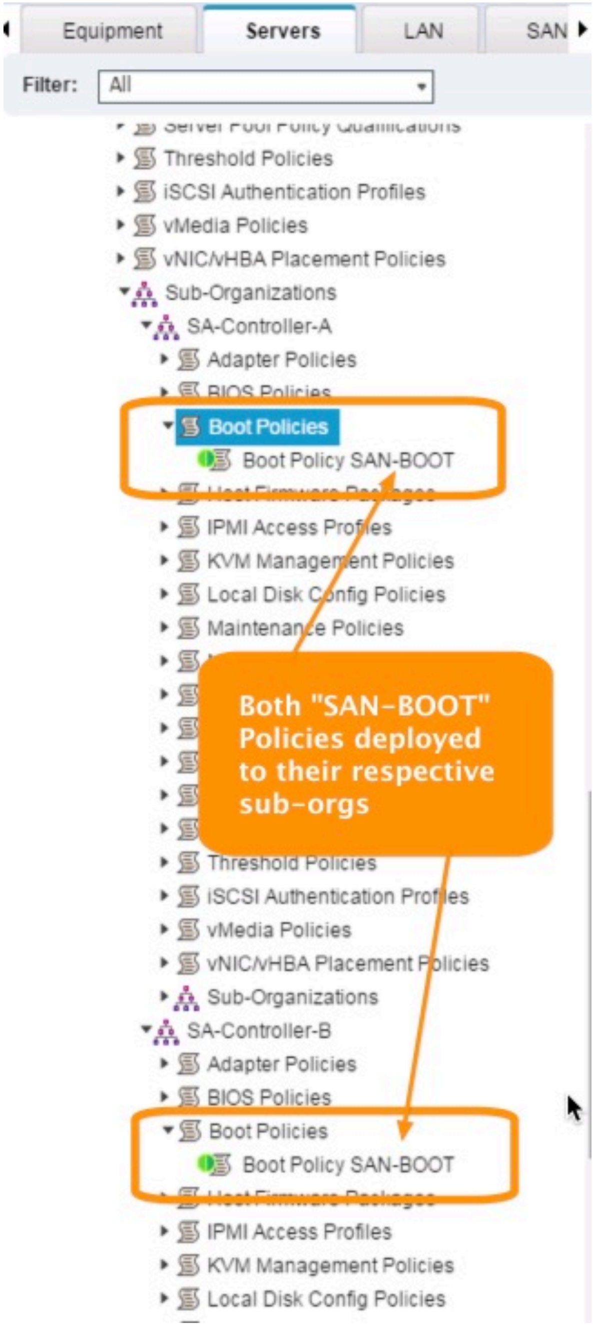
Name : **SAN-BOOT**
Boot Policy Instance : org-root/org-PRODUCTION/org-SA-Controller-B/boot-policy-SAN-BOOT
Description :
Reboot on Boot Order Change : **No**
Enforce vNIC/vHBA/iSCSI Name : **Yes**
Boot Mode : **Legacy**

WARNINGS:
The type (primary/secondary) does not indicate a boot order presence.
The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.
If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.
If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

Name	Order	vNIC/vHBA/i...	Type	WWN	LUN Name	Slot
Local CD/DVD	1					
San	2					
SAN Primary		vhba0	Primary			
SAN Target Primary			Primary	50:00:00:00:00:00:00:55	0	
SAN Target Secon...			Secondary	50:00:00:00:00:00:00:66	0	
SAN Secondary		vhba1	Secondary			
SAN Target Primary			Primary	50:00:00:00:00:00:00:77	0	
SAN Target Secon...			Secondary	50:00:00:00:00:00:00:88	0	

Finally, you can actually see that both “SAN-BOOT” policies were deployed to the UCS Domain as expected. There’s no object-name conflict because the two policies with the same exact name are contained in different Sub-Org structures.

UCS Manager – Viewing Deployed Global Boot Policies in different Sub-Orgs



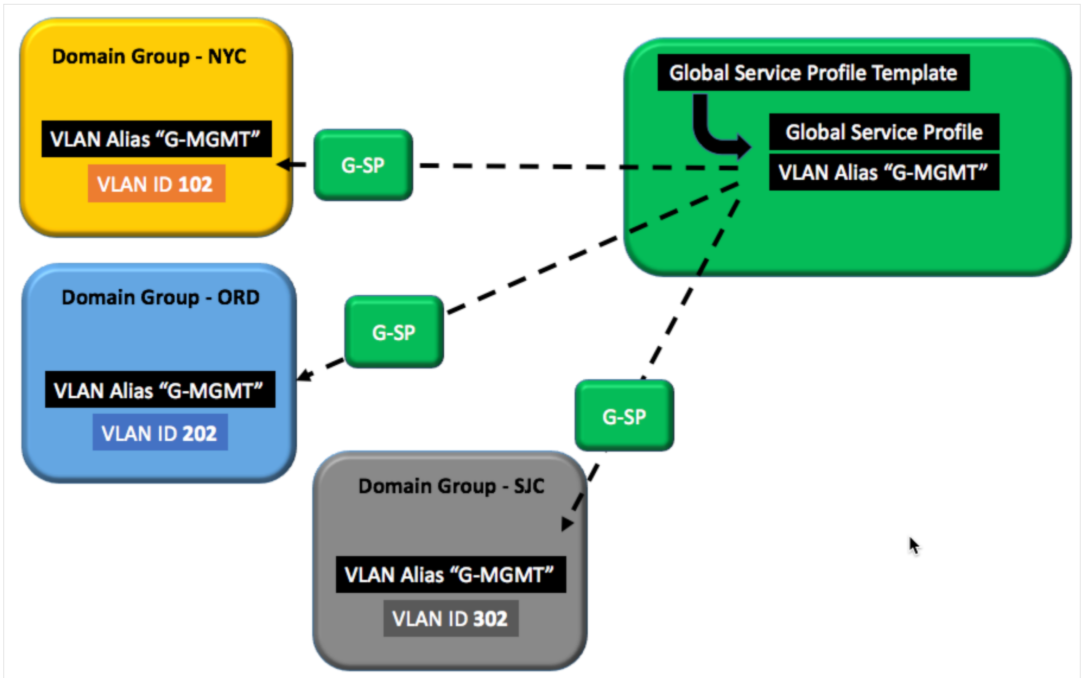
Both "SAN-BOOT" Policies deployed to their respective sub-orgs

In summary, this scenario demonstrated how a single Global Service Profile Template can actually be used to support multiple policies that contain unique values but use the same-name. I am using one Global SP Template, but ultimately consuming one of two unique SAN-BOOT Policies, in their respective and separate Sub-Orgs for my Global Service Profiles. This policy resolution process is fundamental to UCS and UCS Central.

VLAN/VSAN ID Aliasing

Link to VOD: UCS Central VLAN ID Aliasing

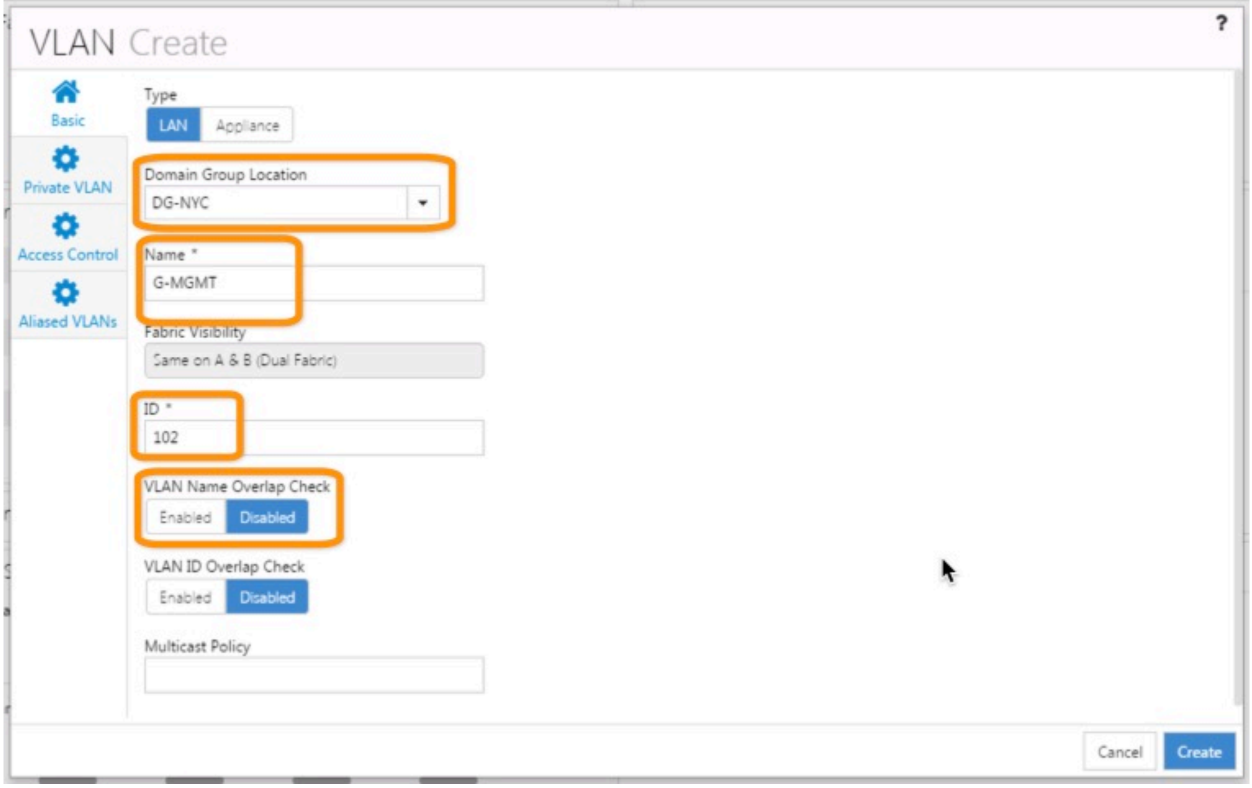
https://youtu.be/SJpizfV4wkY



VLAN ID Aliasing is a powerful functionality of UCS Central, that can assist clients in potentially reducing the overall number of Global Service Profile Templates to maintain in their UCS Central Environment. Traditionally, as in creating Local VLANs/VSANs within UCS Manager, you need to create a new VLAN/VSAN for ever single ID in your network or fabric. For example, if you have different VLAN IDs for Hypervisor Mgmt in different subnets…. that perhaps coincide with the physical locations of those network subnets, then you would need to construct those VLANs separately, which in turn would require separate vNIC Templates and the resulting LAN Connectivity Policies, and Service Profile Templates. The exact same scenario would be true for VSANs. With UCS Central and Global Objects and Policies, this process can be made much more efficient, and the resulting number of Global Service Profiles Templates decreased. Whenever there is "less" to manage in the infrastructure, then it generally becomes "easier" to manage overall.

Let's consider our graphic above. I have a Single Global Service Profile, instantiated from it's corresponding Global Service Profile Template. In the graphic below, when I create a Global VLAN in UCS Central "G-MGMT", I notice there's an additional property that I must designate when creating the Global VLAN. That property is "Domain Group Location". This designation "ties" the use of the VLAN, and corresponding ID to that specific Domain Group.

UCS Central – Creating Global VLANs



VLAN Create

Type: LAN

Domain Group Location: DG-NYC

Name *: G-MGMT

Fabric Visibility: Same on A & B (Dual Fabric)

ID *: 102

VLAN Name Overlap Check: Disabled

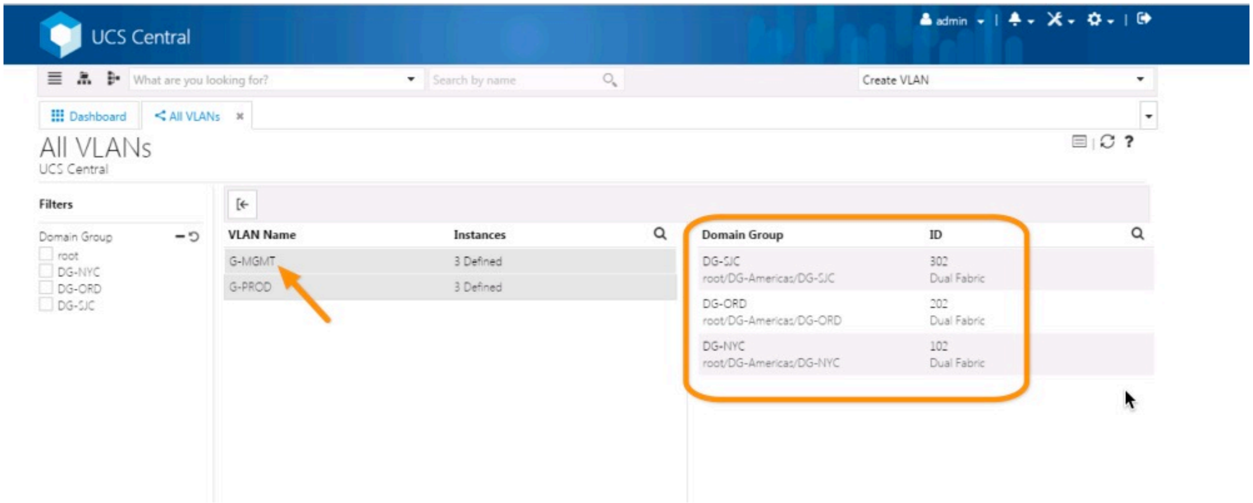
VLAN ID Overlap Check: Disabled

Multicast Policy:

Notice in the graphic we've selected DG-NYC as our Domain Group, with the VLAN Name of "G-MGMT", ID of "102" and we've ensured we disabled VLAN Name Overlap Check, which would prevent us from using "Aliasing". Not shown in the graphic is the Access Control tab where you define your Organizational Privileges, (***root*** for example). Setting Org Permissions is a requirement in UCS Central for all Global VLANs.

In our scenario, after creating the first 'G-MGMT" VLAN for the NYC Domain Group, we can simply repeat the creation process two additional times…. using the exact same NAME of "G-MGMT", but of course using the different VLAN IDs (202, 302) and Domain-Groups (DG-ORD, DG-SJC) respectively. After creating three G-MGMT VLANs, you can see from the form selecting G-MGMT in the ALL VLANs Tab what this Aliased G-MGMT VLAN looks like, and the resulting VLAN IDs that are associated with the Single G-MGMT VLAN name.

UCS Central – Viewing All VLANs



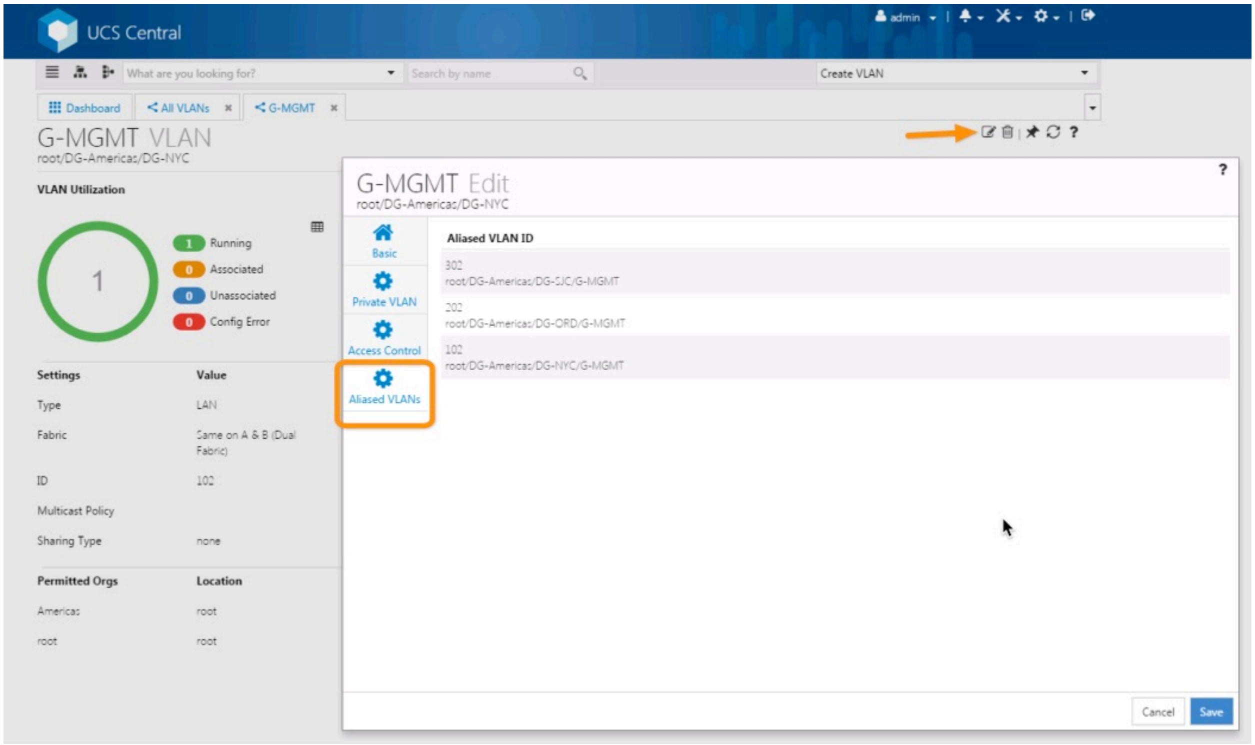
All VLANs
UCS Central

VLAN Name	Instances
G-MGMT	3 Defined
G-PROD	3 Defined

Domain Group	ID
DG-SJC root/DG-Americas/DG-SJC	302 Dual Fabric
DG-ORD root/DG-Americas/DG-ORD	202 Dual Fabric
DG-NYC root/DG-Americas/DG-NYC	102 Dual Fabric

Once you select the G-MGMT VLAN, you can edit the VLAN, and go to the Aliased VLANs tab within and see the corresponding VLAN IDs.

UCS Central – Viewing Aliased VLANs



G-MGMT VLAN
root/DG-Americas/DG-NYC

Settings	Value
Type	LAN
Fabric	Same on A & B (Dual Fabric)
ID	102
Multicast Policy	
Sharing Type	none

Permitted Orgs	Location
Americas	root
root	root

G-MGMT Edit
root/DG-Americas/DG-NYC

Aliased VLAN ID
302 root/DG-Americas/DG-SJC/G-MGMT
202 root/DG-Americas/DG-ORD/G-MGMT
102 root/DG-Americas/DG-NYC/G-MGMT

What is achieved in this scenario with Global VLAN ID Aliasing? I now have a single Global Service Profile Template, that can provide Global Service Profiles for all my Domain Groups. When those Global Service Profiles are "Associated" with the UCS Domain (Blade/Server), that are members of one of those Domain Groups, then UCS Central will pick the appropriate VLAN

ID to deploy with that Global Service Profile. We've made the VLAN Name "Generic" with an aliased name of "G-MGMT" and allowed the intelligence of the UCS Central software to deploy the correct VLAN ID to the UCS Domain.

ID Range Access Control Policy – UCS KVM Management IPs

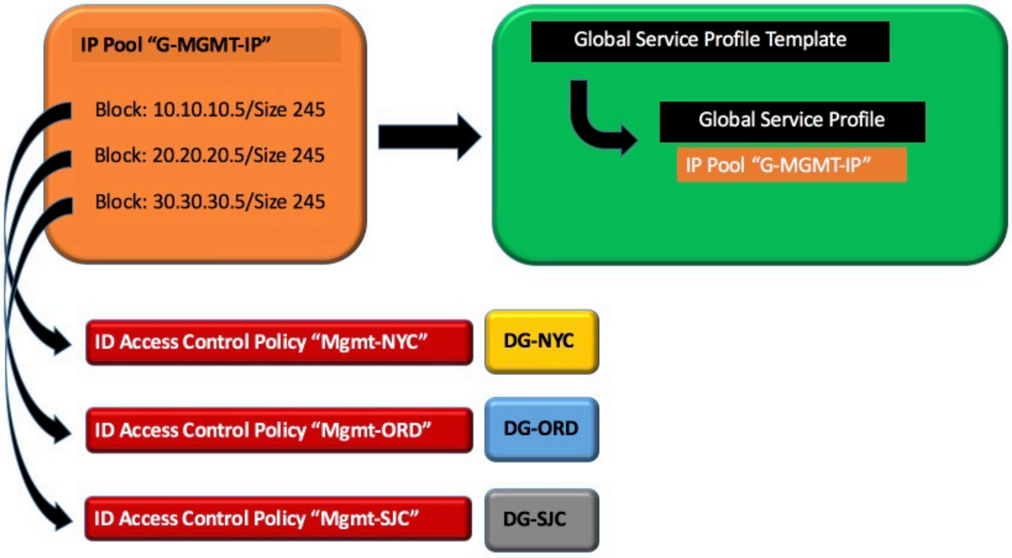
Link to VOD: UCS Central ID Access Control Policies

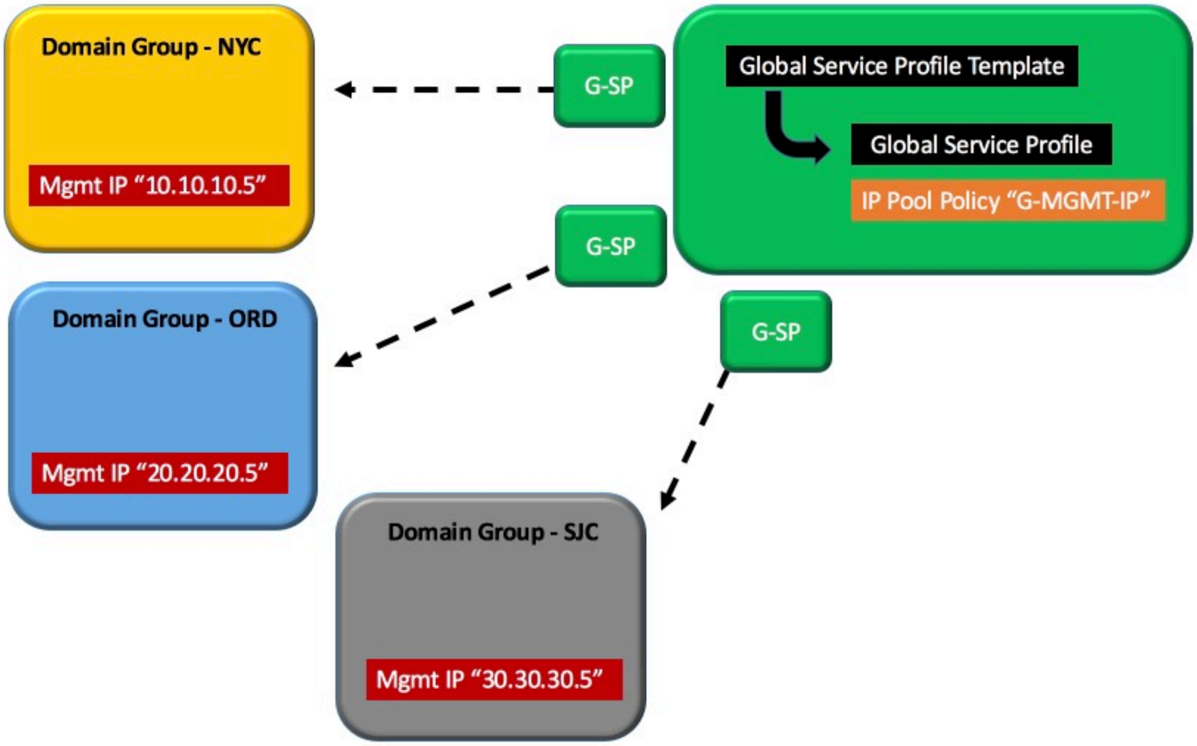
https://youtu.be/OgF5GejzJFM

But Wait !!! Some of you might think that VLAN/VSAN ID Aliasing is "*all great and all*", being able to reduce my Global Service Profile Templates, and also being able to move Global Service Profiles from UCS Domain to UCS Domain, and have the VLANs/VSANs adjust to the proper IDs…..BUT….What about Management IP Addresses for the Blade/Server KVMs? What about those?

ID Range Access Control Policies to the Rescue! This policy, part of UCS Central, can be applied to any ID Pool, but really takes-on a significant importance with managing IP Management Pool IDs in large UCS-UCS Central Infrastructures. Management IPs for UCS Blades and Servers, whether In-Band, or Out-of-Band will likely be on different IP Subnets when UCS Domains are dispersed across the enterprise. Like VLAN/VSAN ID Aliasing, ID Range Access Control Policies can provide the needed flexibility to allow for Mgmt IPs to "adjust" when Global Service Profiles are associated to UCS Domains. The actual process is slightly different however….as there are actual policies that need to be created to act as pointers between Blocks of Mgmt IPs (subnet specific) and the deploying Global Service Profile.

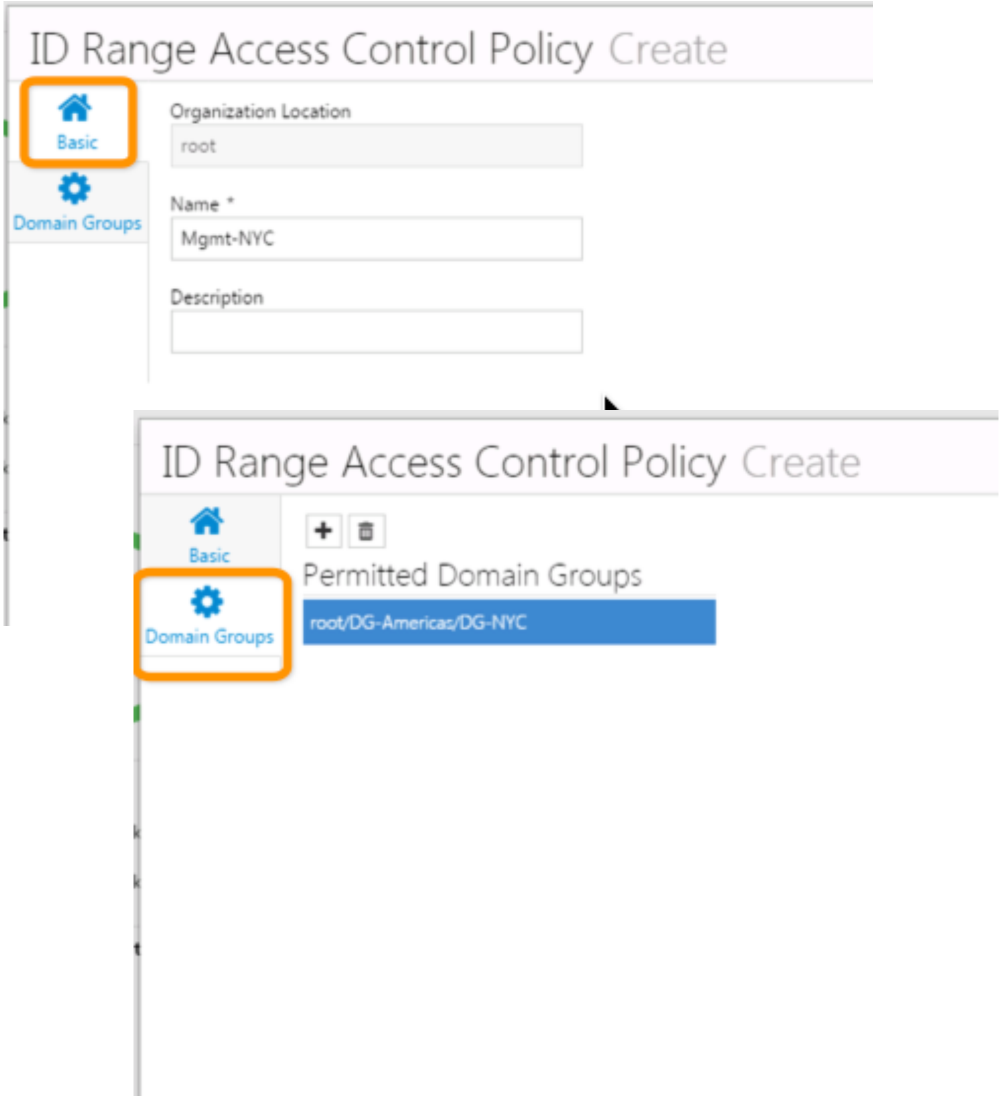
In our example below, we can see that we've created a Global IP Management Pool "G-MGMT-IP" with corresponding Blocks of Management IPs that match the management subnets of our different UCS Domains.


IP Pool "G-MGMT-IP"
Block: 10.10.10.5/Size 245
Block: 20.20.20.5/Size 245
Block: 30.30.30.5/Size 245
Global Service Profile Template
Global Service Profile
IP Pool "G-MGMT-IP"
ID Access Control Policy "Mgmt-NYC"
DG-NYC
ID Access Control Policy "Mgmt-ORD"
DG-ORD
ID Access Control Policy "Mgmt-SJC"
DG-SJC


Domain Group - NYC
Mgmt IP "10.10.10.5"
G-SP
Global Service Profile Template
Global Service Profile
IP Pool Policy "G-MGMT-IP"
G-SP
Domain Group - ORD
Mgmt IP "20.20.20.5"
G-SP
Domain Group - SJC
Mgmt IP "30.30.30.5"

Creating the actual ID Range Access Control Policies themselves is very simply, since they coincide with a particular Domain Group.

UCS Central – Creating ID Access Control Policy



ID Range Access Control Policy Create

Organization Location: root

Name *: Mgmt-NYC

Description:

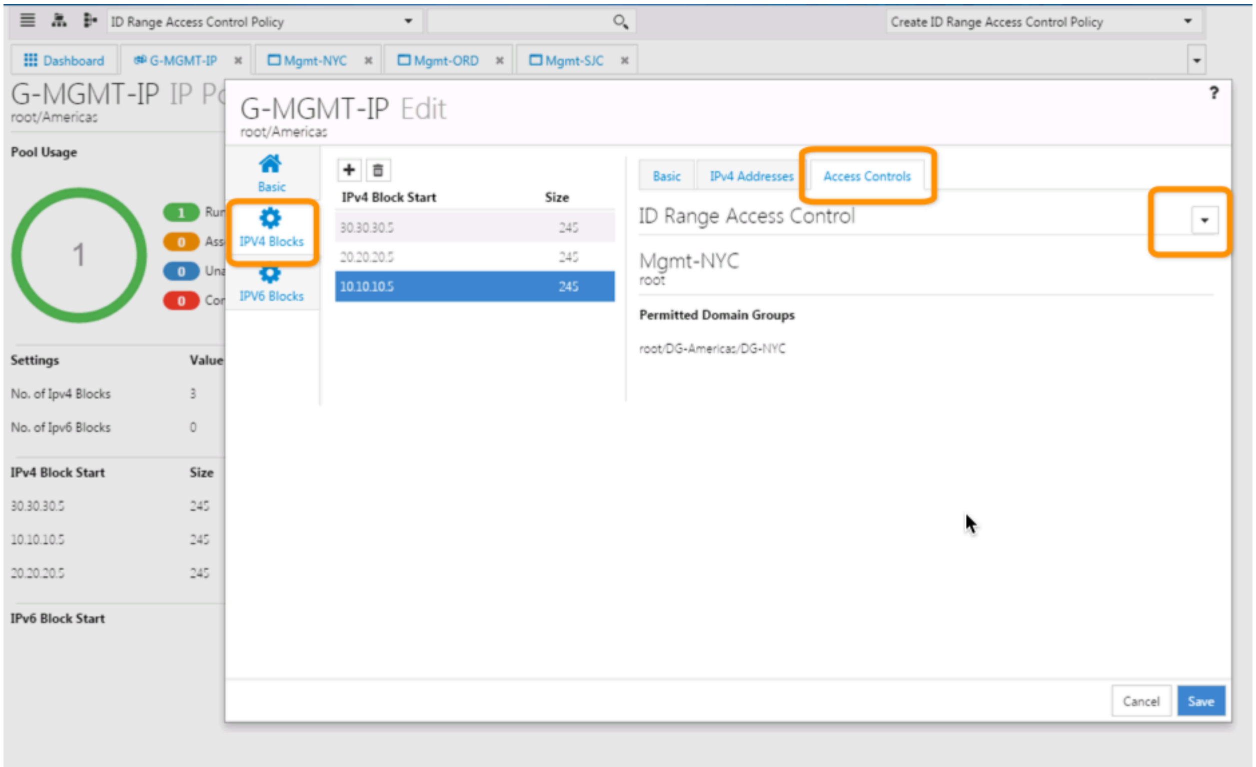
ID Range Access Control Policy Create

Permitted Domain Groups

root/DG-Americas/DG-NYC

Once the policies are created, accessing them is just a matter of selecting the correct policy, per the specific Block of management addresses in the Management IP Pool “G-MGMT-IP”

UCS Central – Pointing IP ID Blocks to Access Control Policy



G-MGMT-IP
root/Americas

Settings	Value
No. of Ipv4 Blocks	3
No. of Ipv6 Blocks	0

IPv4 Block Start	Size
30.30.30.5	245
10.10.10.5	245
20.20.20.5	245

IPv6 Block Start

G-MGMT-IP Edit
root/Americas

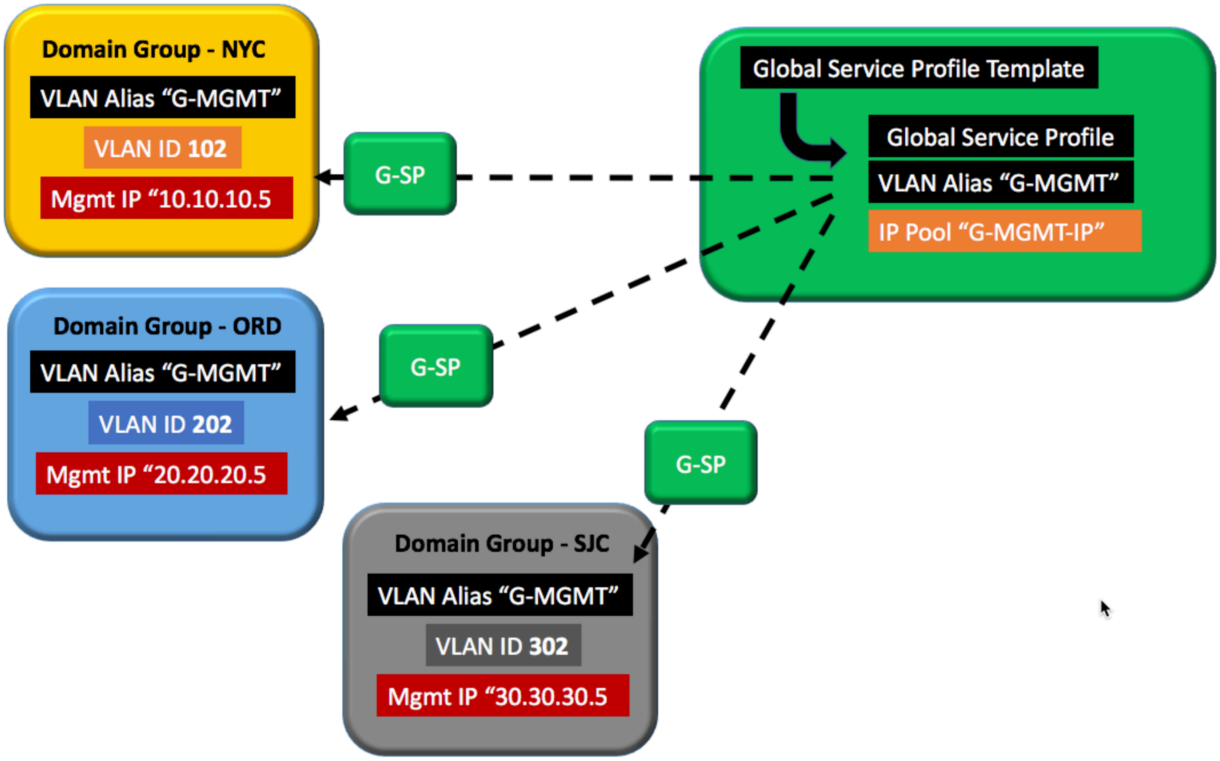
IPv4 Block Start	Size
30.30.30.5	245
20.20.20.5	245
10.10.10.5	245

ID Range Access Control: Mgmt-NYC
root

Permitted Domain Groups
root/DG-Americas/DG-NYC

Sequentially, you select the appropriate ID Access Control Policy for each of the created Management IP Pool subnet blocks. In our example, we can see that the 10.10.10.5 subnet block, is “tied” to the Mgmt-NYC ID Access Control Policy. As such, any Global Service Profile, that is using the “G-MGMT-IP” Pool, and is being associated to a UCS Domain in the DG-NYC Domain Group, will only be issued Management IP Addresses starting with 10.10.10.5. If that Global Service Profile is moved to another UCS Domain, in another Domain Group, or…if another Global Service Profile itself is associated with a UCS Domain in another Domain Group, then the corresponding Management IP for that Domain Group/IP Block will be issued.

In the graphic below, we can see that our Single Global Service Profile Template, and resulting Global Service Profile is leveraging ID Access Control Policies with the “G-MGMT-IP” IP Management Pool. As depicted, we can see that a Global Service Profile associates to the different UCS Domains, that are part of the separate Domain Groups, will “take-on” the correct Management IP Addresses for the assigned Blades/Servers.



Section(s) Summary:

In the last two sections, we discussed and showed VLAN/VSAN ID Aliasing and ID Access Control Policies. In the above graphic, we were able to reduce the number of Global Service Profile Templates down from from what normally would require 3 different Global Service Profile Templates to single Template, 3:1. Even though we have 3 UCS Sites, with different UCS Domains and with 3 Different VLAN IDs, and 3 different Management Subnets, we can still architect all of our Global Service Profiles from a single Global Service Profile Template.

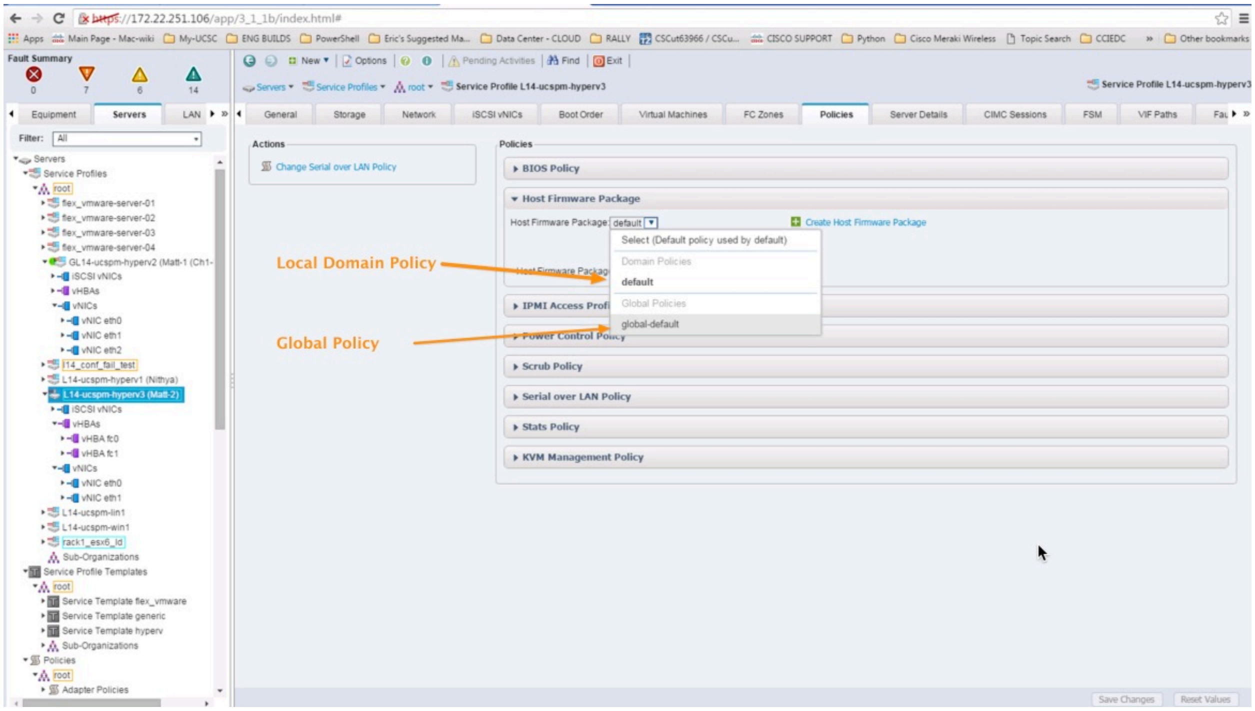
I could have still combined the above functionalities with the before mentioned Advanced Policy Resolution, namely utilizing the "same" given policy name for uniquely configured policies in separate sub-orgs and achieved the reduction in required templates for Boot Policies, as the "SAN-BOOT" example before.

Brownfield – Accessing Global ID's and Policies with Local SP's

From the time you register a UCS Domain to UCS Central, you will have "visibility" of any and all Global ID Pools and Policies from within UCS Manager. A stepping-stone in the direction of going from a Brownfield to a Greenfield (Global) implementation, is to create Global Policies within UCS Central and accessing those policies from UCS Manager, specifically your Local Service Templates and Local Service Profiles. The graphic below shows a Local Service Profile that has the easy capability of "switching" from "default" Host Firmware Package (local policy) to a "global-default" (global policy) that exists in UCS Central.

Any Policy and ID can be switched. Local UUID, MAC, IP, WWNN, and WWPN Pools can be switched from Local Domain to their Global counterparts. Any Local Policy can be switched to it's Global counterpart. Is this disruptive you may ask? The answer is, it depends. If the Global Policy has the EXACT SAME configuration as the Local Policy…then there's no disruption to running workloads. If you are switching an ID Pool from Local to Global, then the Global Pool MUST CONTAIN the exact same ID format as defined locally in the UCS Domain, and the specific ID must be available to allocate. Anything outside of these guidelines will cause a disruption (re-association) of the Service Profile, or by best practice, a User-Ack from a Maintenance Policy to confirm the disruption. Such changes should always be tested in a lab before attempting in Production, or at the very least, choosing a single Service Profile assigned to a blade/server that is not running production workloads, perhaps a hypervisor host that has been placed into Maintenance Mode with guest VMs evacuated.

UCS Manager – Accessing Global Policies from Local Service Profile



Host Firmware Package: default

Local and Global Maintenance Policies – "User-Ack" Behavior Explained

- Global Service Profiles with Global Maintenance Policy
  - Show's Pending Activities Alert in UCS Manager, CANNOT Ack in UCS Manager.
  - Show's in UCS Central Pending Activities…..Ack in UCS Central.

- Local Service Profiles with Global Maintenance Policy
  - Show's Pending Activities in UCS Manager…CANNOT Ack in UCS Manager.
  - Show's in UCS Central Pending Activities…..Must Ack in UCS Central.

- Local Service Profile with Local Maintenance Policy (UCS Domain Registered with UCS Central)
  - Show's Pending Activities in UCS Manager…Can Ack in UCS Manager.
  - Show's in UCS Central Pending Activities…..Can Ack in UCS Central.

Note: If administrators wish to limit the acknowledgement of UCS Blades/Servers to UCS Central (In Brownfield UCS Environments with Local Service Profiles, but registered to UCS Central) make sure All Local Service Profiles have a Global Maintenance Policy of "User-Ack".

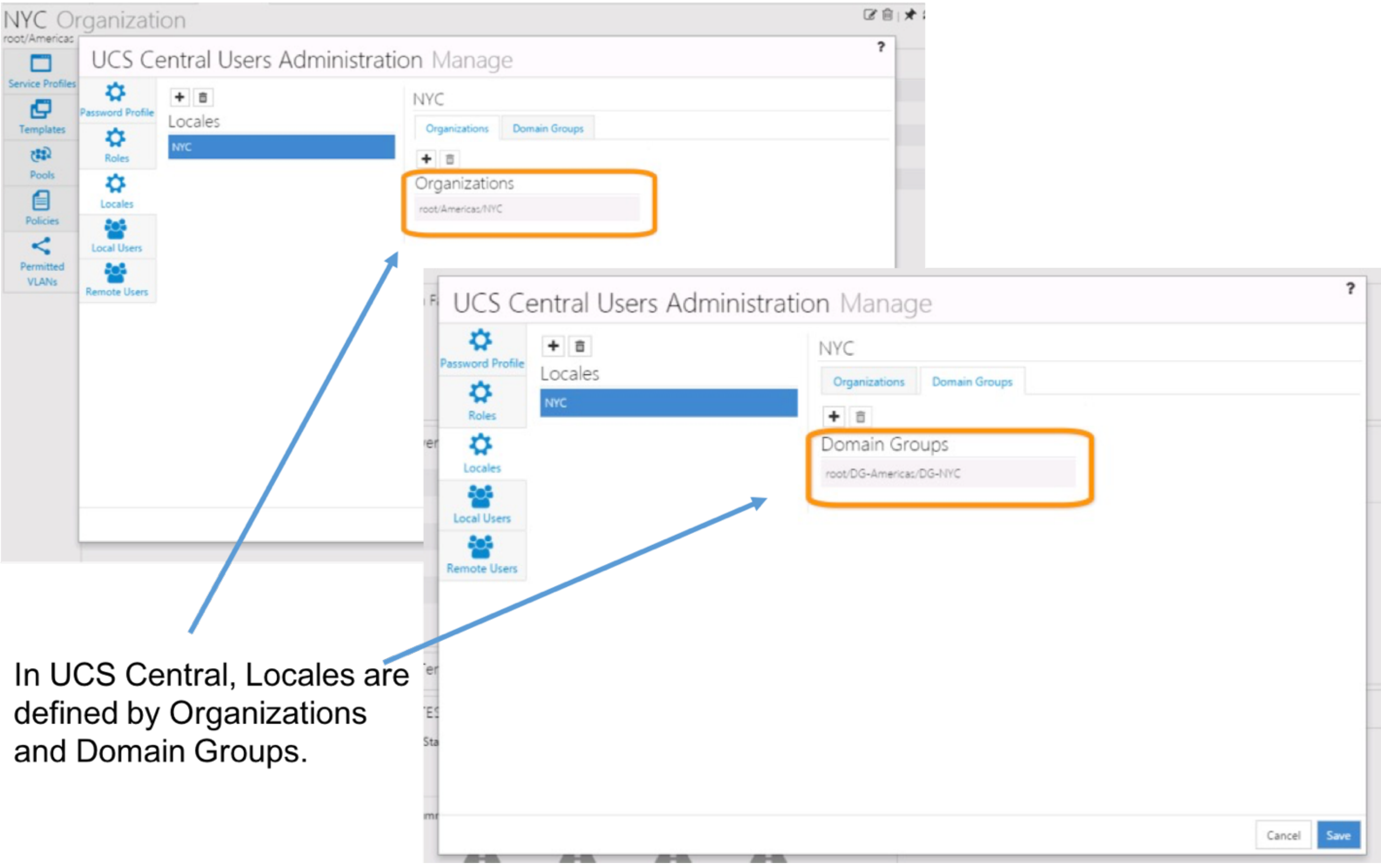
Role-Based Access Control (RBAC) and UCS Central Custom Views

An important distinction in managing a UCS Domain with UCS Manager, and managing a UCS Domain with UCS Central is the ability to create a customized view of what a user can see and manage as part of Role Based Access Control (RBAC).

With UCS Central, Locales are used to “filter” what a user can see and manage. The UCs Central Locale is defined not only with organizational permissions but also UCS Central Domain Group permissions.

In the example below, we have created a Locale called “NYC”, with Organizational Permissions set to *root/Americas/NYC* and Domain Group permissions of *root/DG-Americas/DG-NYC*.

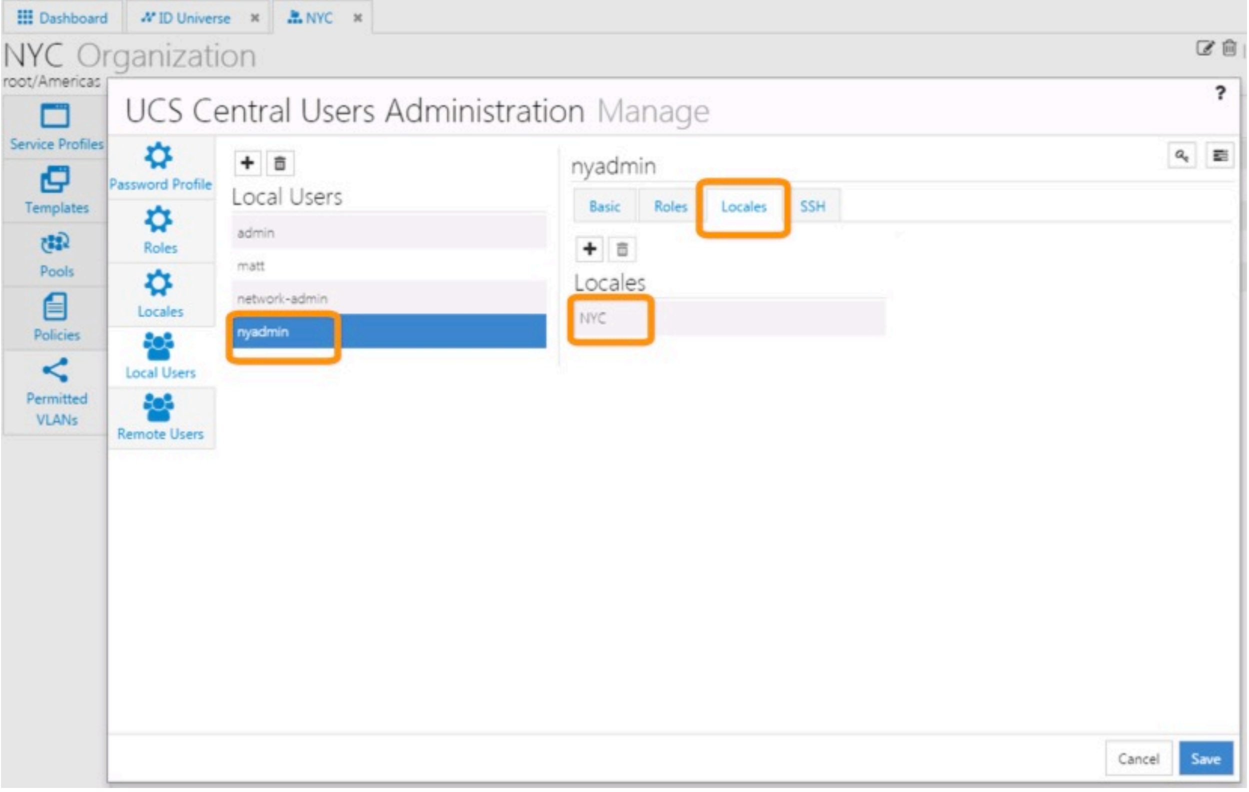
UCS Central – Configuring Locales



In UCS Central, Locales are defined by Organizations and Domain Groups.

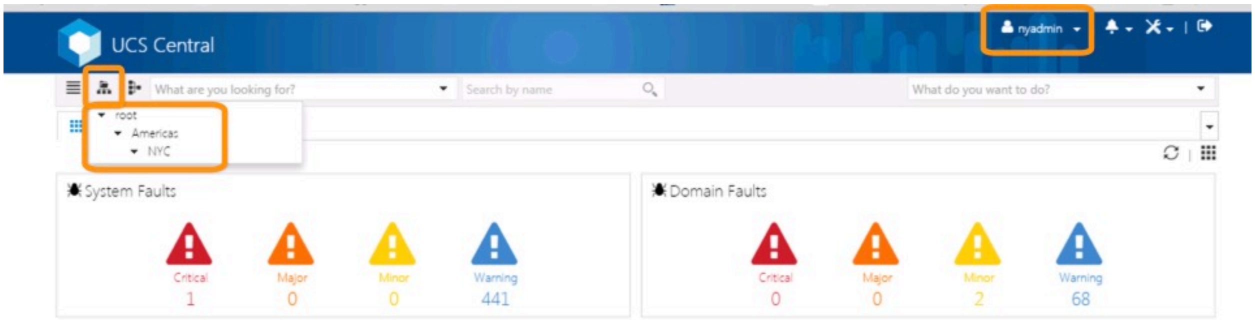
Once we created the Locale, we created a user called "*nyadmin*" and assigned the NYC Locate to the account *nyadmin*.

UCS Central – Specifying Local for Use Account

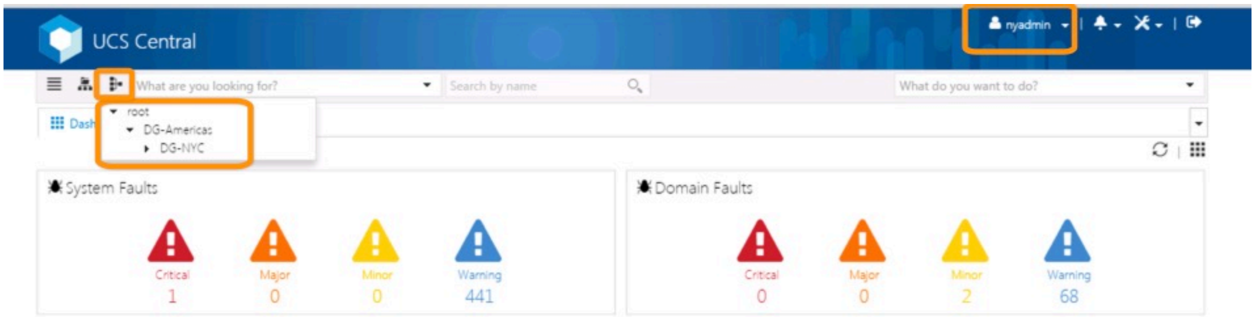


When we log off of *Admin*, and Login as *nyadmin*, we can see the following results…. a narrowed view of Organizational Structure as well as Domain Group Structure.

UCS Central – Custom View (Org Structure) for User Account



UCS Central – Custom View (Domain Group Structure) for User Account



Global UCS Firmware Management in UCS Central

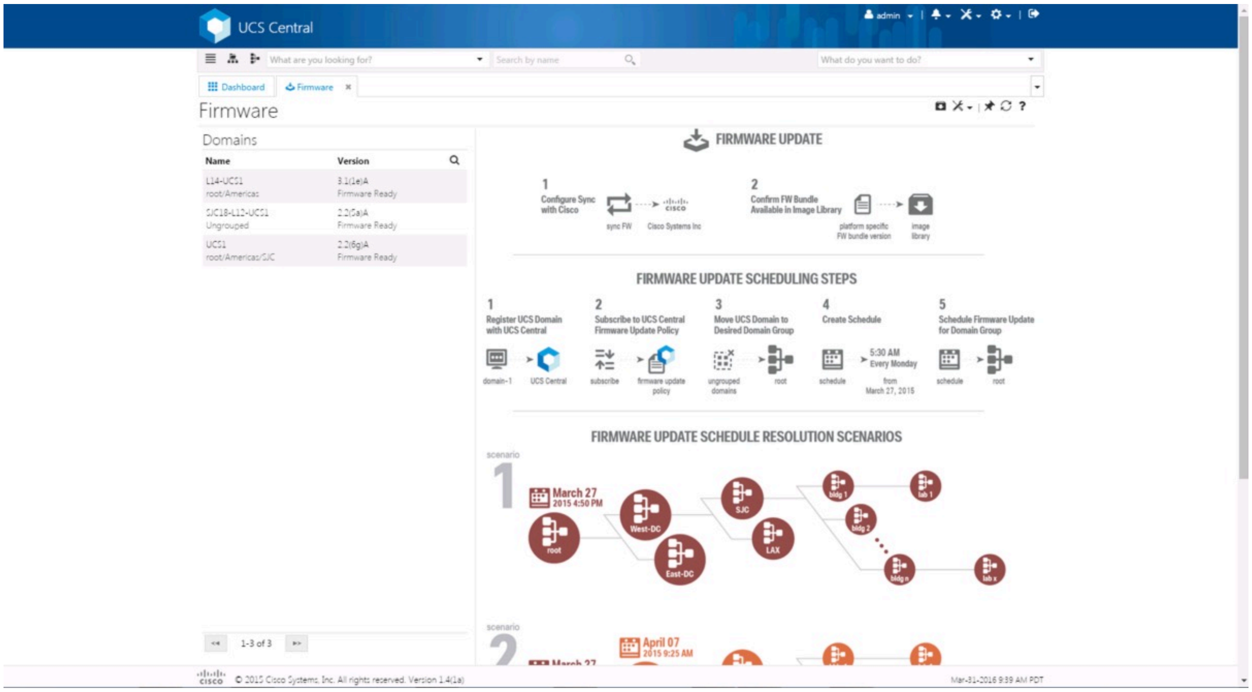
Link to VOD: UCS Central Infrastructure Firmware Upgrades

https://youtu.be/u7f6U6F8cWU

Current versions of UCS Central manage Infrastructure Firmware (FI System/bootstrap, UCSM, IOM) Upgrades Globally using an existing Domain Group, or Sub-Domain Group Policy to either schedule the upgrade at a future time, or apply the firmware immediately. UCS Central affords the ability to register the application with the Cisco Support website, supply a valid CCO Account and schedule regular firmware version updates to UCS Central. Manual Sync is also supported. UCS Central does not automatically download the actual Firmware Bundles, but rather downloads the meta-data for the firmware bundles, and then affords the ability to decide which firmware bundle version to completely download at the click of a button. Best practices mentioned previously about max latency (500ms) and minimum bandwidth for remote connections to UCS Domains (1.5Mbps) should be strictly adhered-to with managing Infrastructure firmware upgrades from UCS Central.

Global Infrastructure Firmware upgrades are actually "pulled" from UCS Central by each targeted UCS Domain. UCS Central simply communicates to the DME within UCS Manager to "curl-copy" the firmware from UCS Central to the UCS Domain. UCS Central will actually leverage the "Firmware Auto Install" capability of UCS Manager to perform the workload-based upgrades to the infrastructure of the specific UCS Domain.

UCS Central – Firmware Scheduling Guidance



Firmware

Domains

Name	Version
L14-UCS1 root/Americas	3.1(1e)A Firmware Ready
SJC18-L12-UCS1 Ungrouped	2.2(5a)A Firmware Ready
UCS1 root/Americas/SJC	2.2(6g)A Firmware Ready

1-3 of 3

FIRMWARE UPDATE

1 Configure Sync with Cisco

2 Confirm FW Bundle Available in Image Library

FIRMWARE UPDATE SCHEDULING STEPS

1 Register UCS Domain with UCS Central

2 Subscribe to UCS Central Firmware Update Policy

3 Move UCS Domain to Desired Domain Group

4 Create Schedule

5 Schedule Firmware Update for Domain Group

FIRMWARE UPDATE SCHEDULE RESOLUTION SCENARIOS

© 2015 Cisco Systems, Inc. All rights reserved. Version 1.4(1a)

Mar-31-2016 9:39 AM PDT

Current versions of UCS Central leverage a Domain Group Policy to attach a schedule to upgrade Infrastructure Firmware on a registered UCS Domain. As such, if there are multiple UCS Domains that are members of that particular Domain Group (with FW Schedule to upgrade), then there is potential for simultaneous upgrades to occur on more than one UCS Domain. To counter this, a simple way to control the upgrades, Domain-by-Domain is to simply "Opt-Out" of the Global Policy Resolution Control, within the Admin Tab of UCS Manager, and set the radio button to Local for Infrastructure & Catalog Firmware. With the Policy set to Local at the UCS Domain Level, there is not chance of a Global-Driven Infrastructure upgrade from UCS Central. As you wish to upgrade a particular domain, simply change the Policy Control from Local to Global.

Future versions of UCS Central will offer more flexibility with upgrading UCS Domains, specifically, afford the ability to identify an individual UCS Domain to upgrade, outside it's Domain Group hierarchy/membership.

Upgrading Blade/Server firmware with UCS Central utilizes the Host Firmware Policy and subsequent associations of a Service Profile to upgrade the host blade/server. Currently, there's no direct-endpoint upgrade ability of a blade/server, however this capability is also being "discussed" as being supported in a future UCS Central version.

Unregistering a UCS Domain from UCS Central:

In UCS Manager, there is the ability to "Unregister" a UCS Domain from UCS Central at any time, thus the need for security with the UCS Manager Admin Account. It is strongly advised by Cisco to consult Cisco TAC before unregistering a production UCS Domain.

The process of unregistering a UCS Domain from UCS Central immediately establishes Local UCS Manager Ownership for all the former Global VLANs/VSANs, Policies, and Service Profiles pushed down to that Domain. The icons will revert from Global Icons to Local Icons for these objects. The action of unregistering a UCS Domain will not directly effect any workloads running on UCS Blades/Servers, and new "localized" global objects will retain their exact names as created in UCS Central.

The design was to have no operational impact to existing workloads, and while that is a great thing, the difficulties come later if and when you decide to re-register that Domain back to UCS Central.

Here are several important points to consider:

- If your intent is to never re-register with UCS Central, then there's really no impact to un-registering a UCS Domain from UCS Central. Global Objects will become Local Objects with absolute object control restored to UCS Manager.
- If your intent is to re-register, please consult Cisco TAC before deciding to un-register a production UCS Domain.
- If you unregister, all Global Objects pushed-down to the UCS Domain will become Local Objects. You'll see Global "default" policies, and custom policies that retain their names as Local Objects, and the same with VLANs, VSANs, vHBA Templates, vNIC Templates, and Service Profiles.
- If you decide to re-register that UCS Domain with UCS Central, the fact that a myriad of these Local Objects (that retained their original Global Names) exist in the UCS Domain, will cause a Fault when trying to push another Global Service Profile down to that domain. The Fault is a naming-resource conflict, because a Local Object and Global Object cannot have the same name in the same Organizational level. This is a common error for those that have unregistered, and re-registered a UCS Domain, and does require some time to clean-up…combing through all the Org Levels of the Servers Tab, LAN Tab, SAN Tab, Admin Tab and Storage Tab of UCS Manager.

CLI - Deploying Global VLANs and VSANs to a UCS Domain

UCS Central 1.3 introduced the ability to deploy Global VLANs and VSANs to a UCS Domain without the use of a Global Service Profile as the "delivery" mechanism. This ability, only available with the CLI can benefit those customers using Local Service Profiles, but want to utilize and access Global Objects from UCS Central.

The below "publish" command assumes the Global VLAN/VSAN has already been created within UCS Central.

Manually Publishing a Global VLAN:

```
UCSC-131S7-TRAIN# connect resource-mgr
```

```
UCSC-131S7-TRAIN(resource-mgr)# scope domain-mgmt
```

```
UCSC-131S7-TRAIN(resource-mgr) /domain-mgmt # show ucs-domain
```

(Shows the UCS Domain ID's to be used with the next command)

```
UCSC-131S7-TRAIN(resource-mgr) /domain-mgmt # scope ucs-domain 1008
```

```
UCSC-131S7-TRAIN(resource-mgr) /domain-mgmt/ucs-domain # publish vlan vlan1000
```

Manually Publishing a Global VSAN:

```
UCSC-131S7-TRAIN# connect resource-mgr
```

```
UCSC-131S7-TRAIN(resource-mgr)# scope domain-mgmt
```

```
UCSC-131S7-TRAIN(resource-mgr) /domain-mgmt # show ucs-domain
```

(Shows the UCS Domain ID's to be used with the next command)

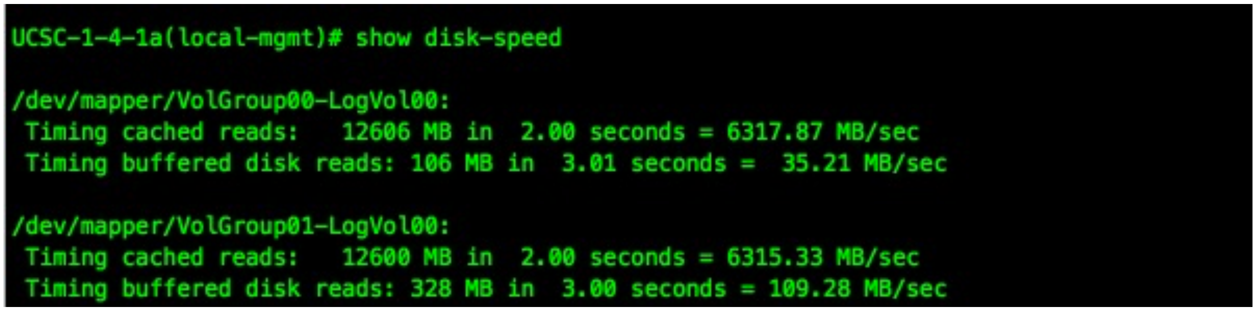
```
UCSC-131S7-TRAIN(resource-mgr) /domain-mgmt # scope ucs-domain 1008
```

```
UCSC-131S7-TRAIN(resource-mgr) /domain-mgmt/ucs-domain # publish vsan vsan100 a
```

(Be sure to designate the intended Fabric with either an "a" or "b" at the end of the command)

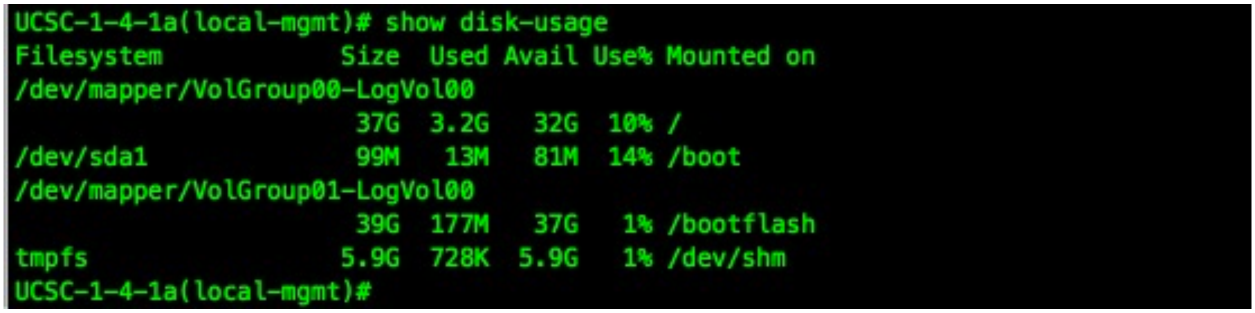
Some CLI Troubleshooting Commands

Show Disk Speed



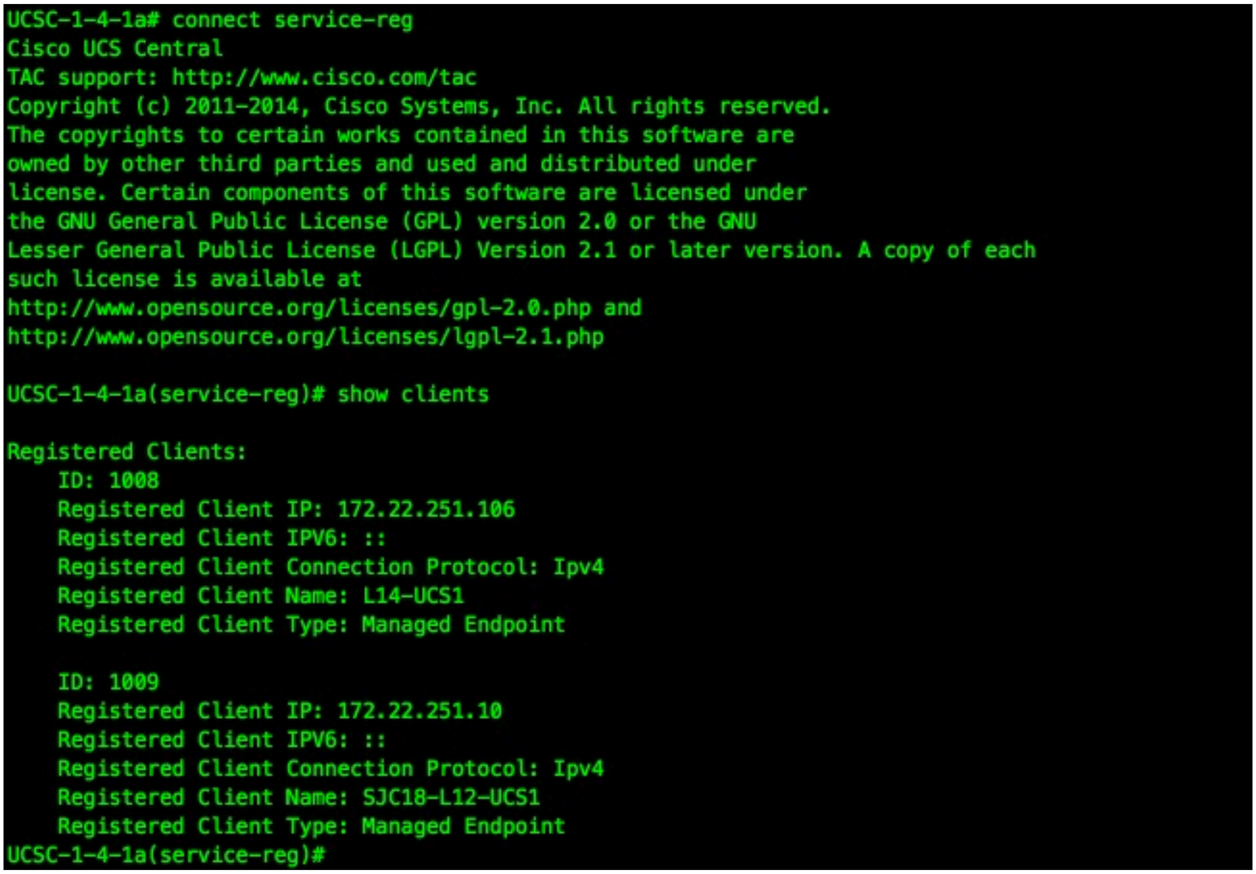
```
UCSC-1-4-1a(local-mgmt)# show disk-speed

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

/dev/mapper/VolGroup01-LogVol00:
 Timing cached reads:   12600 MB in  2.00 seconds = 6315.33 MB/sec
 Timing buffered disk reads: 328 MB in  3.00 seconds = 109.28 MB/sec
```

Show Disk Usage



```
UCSC-1-4-1a(local-mgmt)# show disk-usage
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/VolGroup00-LogVol00
                       37G  3.2G   32G  10% /
/dev/sda1              99M   13M   81M  14% /boot
/dev/mapper/VolGroup01-LogVol00
                       39G  177M   37G   1% /bootflash
tmpfs                 5.9G  728K  5.9G   1% /dev/shm
UCSC-1-4-1a(local-mgmt)#
```

Show registered Domain ID's



```
UCSC-1-4-1a# connect service-reg
Cisco UCS Central
TAC support: http://www.cisco.com/tac
Copyright (c) 2011-2014, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or later version. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCSC-1-4-1a(service-reg)# show clients

Registered Clients:
    ID: 1008
    Registered Client IP: 172.22.251.106
    Registered Client IPV6: ::
    Registered Client Connection Protocol: Ipv4
    Registered Client Name: L14-UCS1
    Registered Client Type: Managed Endpoint

    ID: 1009
    Registered Client IP: 172.22.251.10
    Registered Client IPV6: ::
    Registered Client Connection Protocol: Ipv4
    Registered Client Name: SJC18-L12-UCS1
    Registered Client Type: Managed Endpoint
UCSC-1-4-1a(service-reg)#
```

UCS Central Internal Processes Defined

Service Name	Description
core-svc_cor_secAG	Implement authentication related feature, such as local auth and remote auth
identifier-mgr-svc_idm_dme	Manage ID pool and allocate ID uniquely in the system
core-solr.sh	SOLR process
resource-mgr-svc_sam_snmpTrapAG	Send SNMP traps from resource-mgr
central-mgr-svc_centralMgr_dme	UCS Central NBAPI provider, forward the NBAPI to a specific DME
policy-mgr-svc_pol_dme	Manage UCS Central policies
identifier-mgr-svc_sam_snmpTrapAG	Send SNMP traps from identifier-mgr
core-svc_cor_snmpTrapAG	Send SNMP traps from mgmt.-controller
operation-mgr-svc_ops_dme	Operation manager DME
policy-mgr-svc_sam_pkiAG	Provide PKI related service for policy-mgr DME
core-httpd.sh	Start httpd process
gch-call_home	Cisco GCH call home process, which forwards the callhome/smartlicense message to Cisco Cloud Smartlicense Manager
service-reg-svc_sam_snmpTrapAG	Send SNMP trap from service-reg
core-svc_cor_sessionmgrAG	Session auditing for UCS Central HA implementation
core-svc_cor_dme	mgmt-control DME, manage the configuration for UCS Central VM
resource-mgr-svc_sam_cloudAG	GCH callhome/smartlicense application gateway
stats-mgr-svc_sam_snmpTrapAG	Send SNMP trap from stats-mgr
service-reg-svc_reg_dme	Implement registration service for different DME and UCSM
operation-mgr-svc_ops_imgMgmtAG	Image management Application gateway for operation manager
resource-mgr-svc_rsrcMgr_dme	resource-mgr DME where UCSM inventory is kept and which manages GSP
core-tomcat.sh	Controlling script for tomcat process
service-reg-svc_sam_controller	AG to implement UCS Central HA service
operation-mgr-svc_sam_snmpTrapAG	Send SNMP trap from operation manager
sam_cores_mon.sh	Script to monitor/manage UCS Central coredump file

core-svc_cor_controllerAG	AG to configure UCS Central VM policies
service-reg-svc_sam_licenseAG	License AG for domain base license.
core-sam_nfs_mon.sh	script to monitor NFS
gch-xosdsd	Infrastructure process for implementing GCH/smartlicense feature
policy-mgr-svc_sam_snmpTrapAG	Send SNMP Trap from policy-mgr
stats-mgr-svc_statsMgr_dme	stats-mgr which collects statistics from different UCSM and generates the statistics report

UCS Central Communications - Required Ports

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:

The ports below that need to be opened on UCS Central. These ports are accessed by UCS domains.

Note: If UCSM Domains version 2.2(1b) and below are registered with UCS Central, you need to open additional NFS ports. Below are the total ports that need to be opened on UCS Central.

LOCKD_TCPPORT=32803 – Linux NFS Lock
MOUNTD_PORT=892 – Linux NFS Mount
RQUOTAD_PORT=875 – Linux Remote Quota Server Port (NFS)
STATD_PORT=32805 – Linux – Used by NFS File Locking Service – Lock Recovery.
NFS_PORT="nfs"(2049) – Linux NFS Listening Port
RPC_PORT="sunrpc"(111) – Linux RPCBIND Listening Port (NFS)
HTTPS_PORT="https"(443) – Communications from UCS Central to UCS Domain(s) and UCS Central GUI.
HTTP_PORT="http"(80) – Communications from UCS Central to UCS Domain(s). This Port is configurable, and Only required for the Flash-based UCS Central UI.
PRIVATE_PORT=(843) – UCS Central communications from Flash UI to UCS Central VM. Not required for new HTML-5 UI.

Note: If UCSM Domains 2.2(2c) and above, including UCS-Mini, 3.0(1), 3.0(2) and beyond are registered to UCS Central, only the below ports need to be opened. Opening the additional NFS ports that appear above is not required.

HTTPS_PORT="https"(443) – Communications from UCS Central to UCS Domain(s) and UCS Central GUI. Always Required.
HTTP_PORT="http"(80) – Communications from UCS Central to UCS Domain(s). This Port is configurable, and Only required for the Flash-based UCS Central UI.
PRIVATE_PORT=(843) – UCS Central communications from Flash UI to UCS Central VM. and Only required for the Flash-based UCS Central UI.
The PRIVATE_PORT (843) is still required for communication between the UCS Central Flash-based UI and the UCS Central VM, but not between UCS Central VM and remote UCSM domains. Port 843 is Not Required if using the new HTML-5 UI.

The Ports below that need to be opened on UCSM in order to work with UCS Central. These ports are accessed by UCS Central.

HTTPS_PORT=”https”(443) – Communications from UCS Central to UCS Domain(s). Always Required.
HTTP_PORT=”http”(80) – Communications from UCS Central to UCS Domain(s). This Port is configurable, and Only required for the Flash-based UCS Central UI.

The Port below needs to be opened on AD server. This port is used by UCS Central for LDAP Integration with the AD Server.
LDAP Port - 389 (for UCS Central and MS AD LDAP Integration and communication)
UCS Central uses STARTTLS for supporting LDAP over SSL/TLS, this still uses port 389 only

A Note about Port 80: Port 80 is only required for the older Flash-Based UI communications. As of UCS Central release 1.4.1a, it is currently not possible to “turn-off” port 80 within UCS Central, however customers can deny port 80 traffic to and from UCS Central with Firewall Rules. Aside, in a future UCS Central release, the Flash-based UI will be deprecated, and the resulting Port-80 turned-off within UCS Central.

Testing & Development Environment

- Download UCS Emulators and install in Lab
- Download UCS Central and install in Lab
- Register Test Emulators to Test UCS Central
- Import “operational” Config Export, or Build-out UCS Central to Match Production.
- Import “operational” Config Export, or Build-out UCS Domains to Match Production.
- Test scenarios and operations…. such as migrating Local SPs to Global SPs.
- Test Automation, PowerTools Scripts against the API.

Online Resources

UCS Communities - Tech Talks
https://communities.cisco.com/docs/DOC-51417

UCS Emulator
https://communities.cisco.com/docs/DOC-37827

DEVnet Learning Labs
https://developer.cisco.com/site/devnet/learningLabs/overview.gsp

UCS / UCS Central PowerTools – Combo Release 2.0.1
https://software.cisco.com/download/release.html?mdfid=286305108&flowid=79283&softwareid=284574017&release=2.0.1&relind=AVAILABLE&rellifecycle=&reltype=latest

Cisco dCloud
https://dcloud.cisco.com/

UCS Central Documentation
http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-central-software/tsd-products-support-series-home.html

UCS Tech Talk - UCS Manager Documentation Videos
https://www.youtube.com/playlist?list=PLIlKAL_0d4Ew1rnSAnEuAoXenYnrctFjS

Summary

Some possible Futures:

Additional functionality is being considered for the future as well….as the possibility of having to "not touch" a UCS Domain to bring it online, with the exception of Racking, Cabling and Powering-on.

Another capability being considered is to have a "Fabric Profile" whereby all the settings necessary for the Fabric Configuration of a UCS Domain can be made into a policy and deployed.

There's no timeline or promise on these future functionalities, but Cisco Engineering is considering their utility.

About the Author:

Matt Faiello is a Technical Marketing Engineer (TME) in the UCS Engineering BU supporting UCS Central and emerging Data Center technologies. Matt is especially focused on UCS Central and managing large UCS Infrastructures "at-scale".

For the past 20+ years, Matt has supported large-scale operations and IT infrastructures. Matt is a graduate of the US Military Academy at West Point, NY, and subsequently served in combat in the First Gulf War.

Matt joined Cisco in January 2009, being part of the original Cisco Advanced Services Team supporting the new UCS Platform. Matt spent 6 years with Advanced Services, working a wide variety, and scale of UCS-related projects before joining the Engineering Team in January of 2015.

Matthew Faiello - UCS Technical Marketing Engineer - Cisco Systems, Inc.
mfaiello@cisco.com| Phone: 727-540-1432 | Twitter: @mfaiello
UCS Communities: http://communities.cisco.com/ucs
UCS Platform Emulator: http://communities.cisco.com/ucspe
UCS Developed Integrations: http://communities.cisco.com/ucsintegrations