

LAN and SAN Connectivity for a Cisco UCS Blade

Document ID: 110202

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Network Diagram
- Conventions

Background Information

Main Task

- Task
- Create Global VLAN
- Create Global VSAN
- Create vHBAs
- Create vNICs
- Associate Server to Service Profile

Verify

Troubleshoot

Related Information

Introduction

In order to understand blade management in the Cisco Unified Computing System (UCS), it is key to understand the Service Profile or *logical server*. The Service Profile represents a logical view of a single blade server, without the need to know exactly which blade you discuss. The profile object contains the server personality, for example, identity and network information and so forth. The profile can then be associated with a single blade at a time.

The concept of profiles was invented to support the notion of *logical server mobility* or the transfer of identity transparently from one blade to another, as well as pooling concept. Even if you intend to manage the blade server as a traditional individual server, and do not take advantage of mobility or pooling, you still have to create and manage a service profile for the blade. While you can boot a blade without a service profile, it does not have a network or SAN connectivity.

This is a summary of contents of a service profile in Cisco UCS:

- Identity information for Server (UUID)
- World-Wide Node Name (Server-wide)
- LAN/SAN configuration (through vNIC/vHBA configuration)
 - ◆ Identity of NIC/HBA (MAC/WWN)
 - ◆ Ethernet NIC Profile
 - ◆ VLAN/ VSAN configuration information
- Boot Order
- Various Policies

This document assumes Cisco UCS Manager connectivity works and all hardware was discovered correctly.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Cisco UCS Server Blade hardware administration.

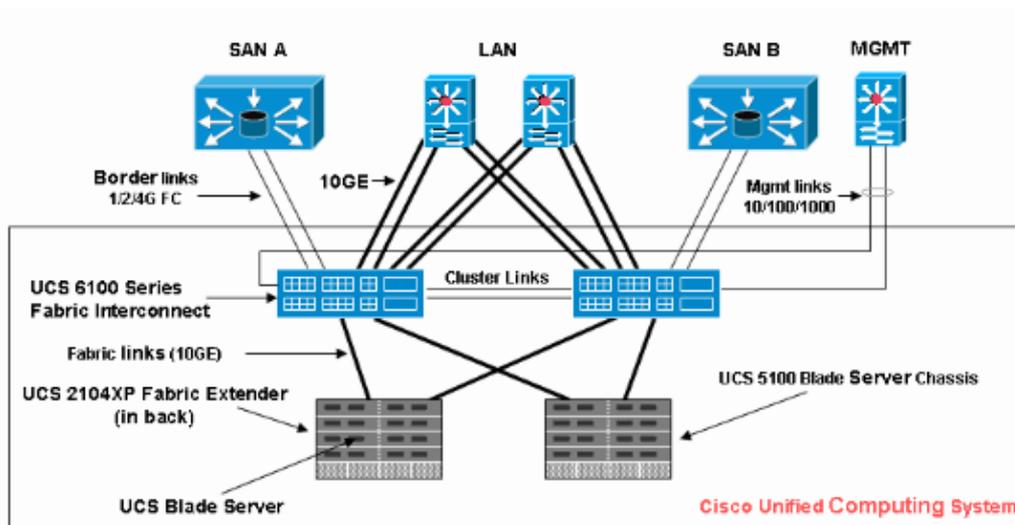
Components Used

The information in this document is based on the Cisco UCS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a default configuration. If your network is live, make sure that you understand the potential impact of any command.

Network Diagram

This document uses this network setup, which is a typical Cisco UCS topology:



Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

vNICs and vHBAs are the trickiest part of service profiles. vNICs are identified on MAC and vHBA are identified on WWN.

For adapters with only physical NICs, for example, Cisco UCS CNA M71KR and Cisco UCS 82598KR, you must create a vNIC for each NIC you want to make usable on the network within Cisco UCS. Then vNIC has a switch setting and a failover flag. For Cisco UCS 82598KR, you must match the physical setting so that the first adapter goes to Fabric Interconnect A and the second to Fabric Interconnect B, and you cannot choose failover. For Cisco UCS CNA M71KR, each vNIC is associated with a particular Fabric Interconnect, but you can enable failover.

Each vNIC must be associated with one or more VLANs, which means each VLAN must be globally configured, and the default VLAN (VLAN 1) must still be specifically associated with a vNIC if any default network traffic is to reach the adapter on the blade associated with the profile that contains the vNIC. The most typical simple configuration is a vNIC which supports only the default VLAN.

There is a flag, most often associated with the default VLAN, that declares a VLAN the *default network* for a particular vNIC. This flag indicates that traffic on that VLAN comes through to the NIC untagged, so in other words, the NIC in the OS can remain VLAN-unaware.

If a vNIC supports VLANs, which are not the *default network* for that particular vNIC, traffic for those VLANs come through to the NIC with VLAN tagging intact. This NIC must then be configured in its OS as VLAN-aware.

Physical Adapter For adapters with only physical NICs (Cisco UCS M71KR, Cisco UCS 82598KR), you must create a vNIC for each NIC you want to make usable on the network within Cisco UCS. Then, vNIC has a switch setting and a failover flag. For the Cisco UCS 82598KR, you must match the physical setting so that the first adapter goes to switch A and the second to switch B, and you cannot choose failover. For the Cisco UCS M71KR, each vNIC is associated with a particular switch, but you can enable failover.

Virtualization Capable Adapter The Cisco UCS M81KR adapter supports NIC virtualization for either single OS or for VMware ESX. Inside a single OS, each Cisco UCS M81KR vNIC is presented as a physical adapter. For VMware, a special feature allows Cisco UCS M81KR vNICs to be presented directly to the guest OS, bypassing the VMWare virtual switch layer. This allows efficiency and also allows Cisco UCS to reconfigure network infrastructure if virtual machines migrate between ESX server instances on different blades.

Main Task

Task

No network or SAN connectivity for the blade server through Cisco UCS fabric exists without a service profile. This document shows how to configure basic LAN and SAN connectivity for a Cisco UCS blade with the creation of a Service Profile with these objects in order to enable a Cisco UCS blade for LAN and SAN connectivity:

1. Create global VLAN (Make sure this is already created before the creation of a Service Profile)
2. Create global VSAN (Make sure this is already created before the creation of a Service Profile)
3. Create vHBAs within this Service Profile
4. Create vNICs within this Service Profile
5. Associate the created Service Profile to a Cisco UCS blade

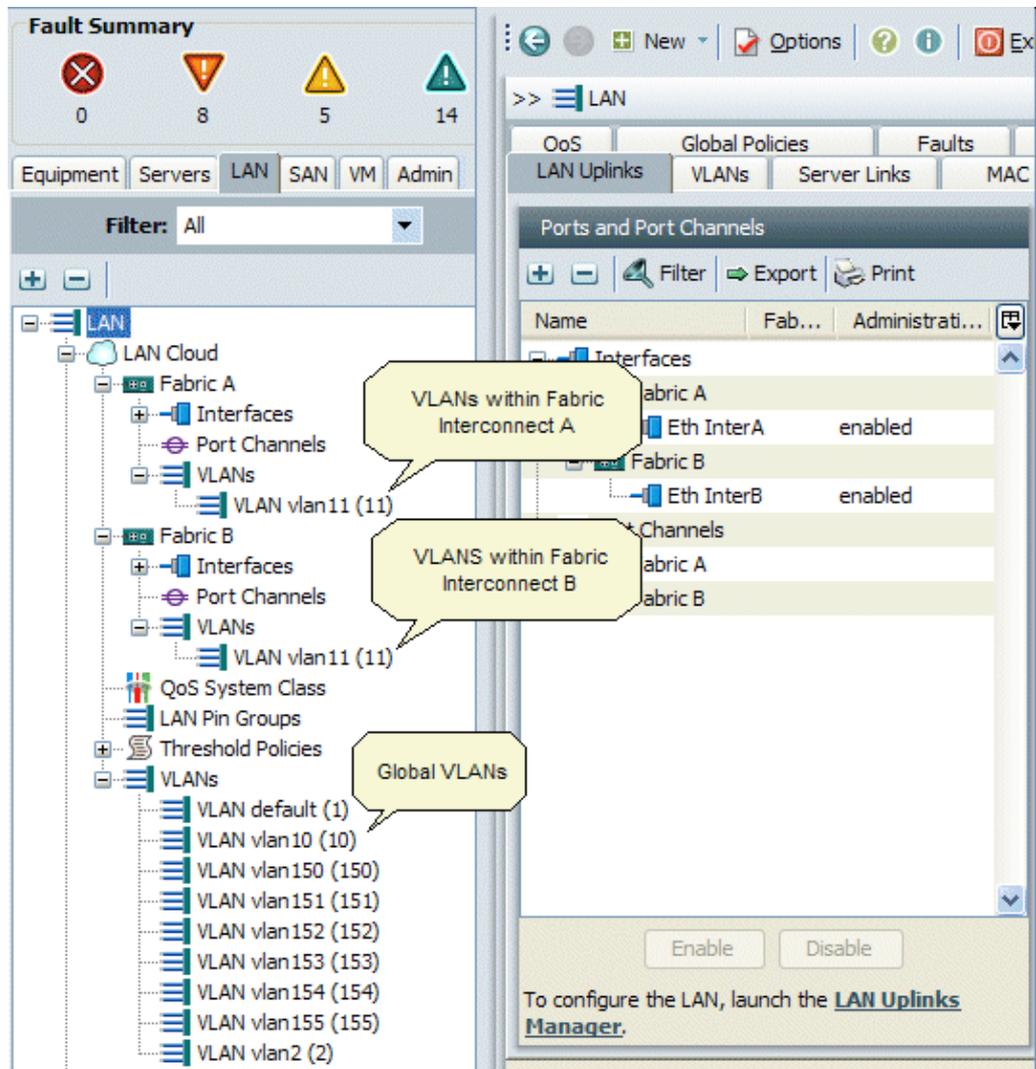
This document assumes that Cisco UCS Manager connectivity works and all hardware was discovered correctly.

Create Global VLAN

For any VLAN to be supported on any blade, a VLAN object must be created in the global Cisco UCS configuration in the LAN tab on the navigation panel. You can also create VLANs associated with only Fabric Interconnect A or only Fabric Interconnect B; but it is more flexible to just create them globally, and for the VLANs to be enabled on either Fabric Interconnect.

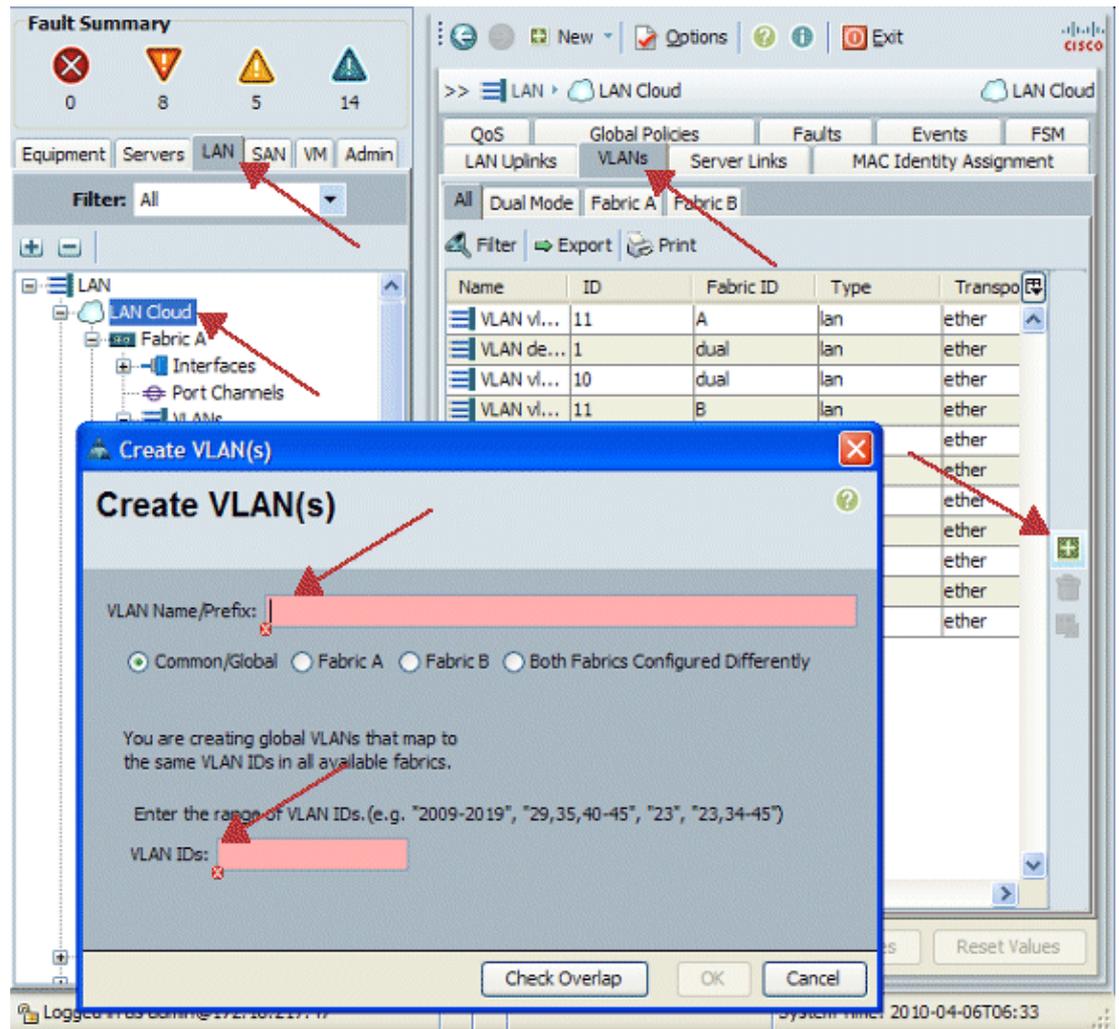
Note: You need a unique VLAN ID for each named VLAN that you create. You cannot create VLANs with IDs from 3968 to 4048. This range of VLAN IDs is reserved.

1. In the Navigation pane, choose the **LAN** tab.
2. Choose **LAN > LAN Cloud**.



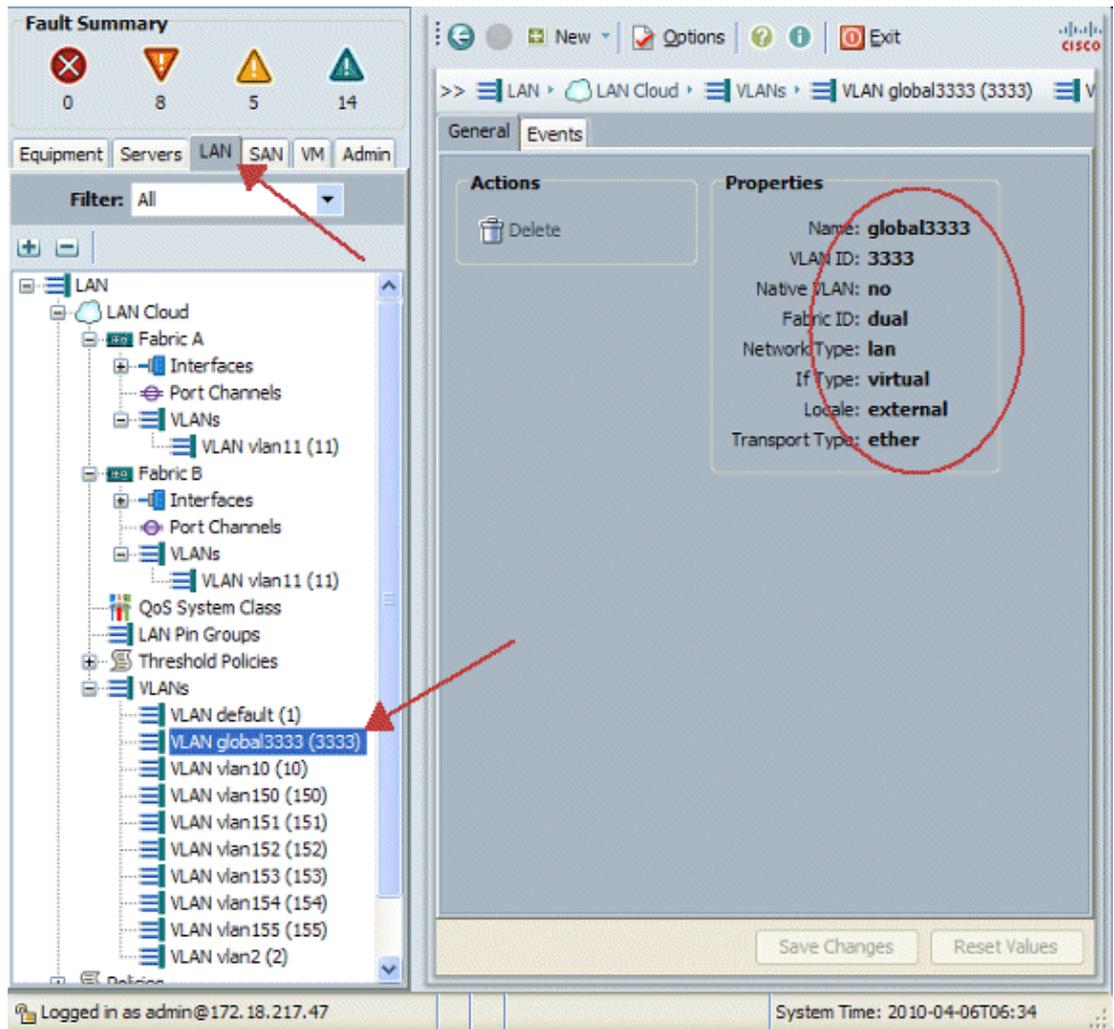
3. Choose the **VLANs** tab in Work Pane, choose **VLANs**, then choose + in order to begin the VLAN creation .
4. Enter this information in the Create VLAN dialog box and then click **OK**:
 - a. In the Name field, enter a unique name for the VLAN.
 - b. In the ID field, enter the network ID assigned to the VLAN.

Cisco UCS Manager GUI adds the VLAN to the VLANs node under LAN Cloud.



VLANs that are accessible to both Fabric Interconnects are visible only in LAN Cloud > VLANs node. You cannot see them under the Fabric Interconnect > VLANs node, which displays only the VLANs accessible to just that Fabric Interconnect. Verify that you have successfully created a global VLAN.

5. In the Navigation pane, choose the **LAN** tab.
6. In the LAN tab, choose **LAN > LAN Cloud**.
7. In the LAN Cloud, choose **VLAN**.
8. Choose the **Global VLAN** you created. Then confirm the VLAN property in the Work Pane to the right.



Create Global VSAN

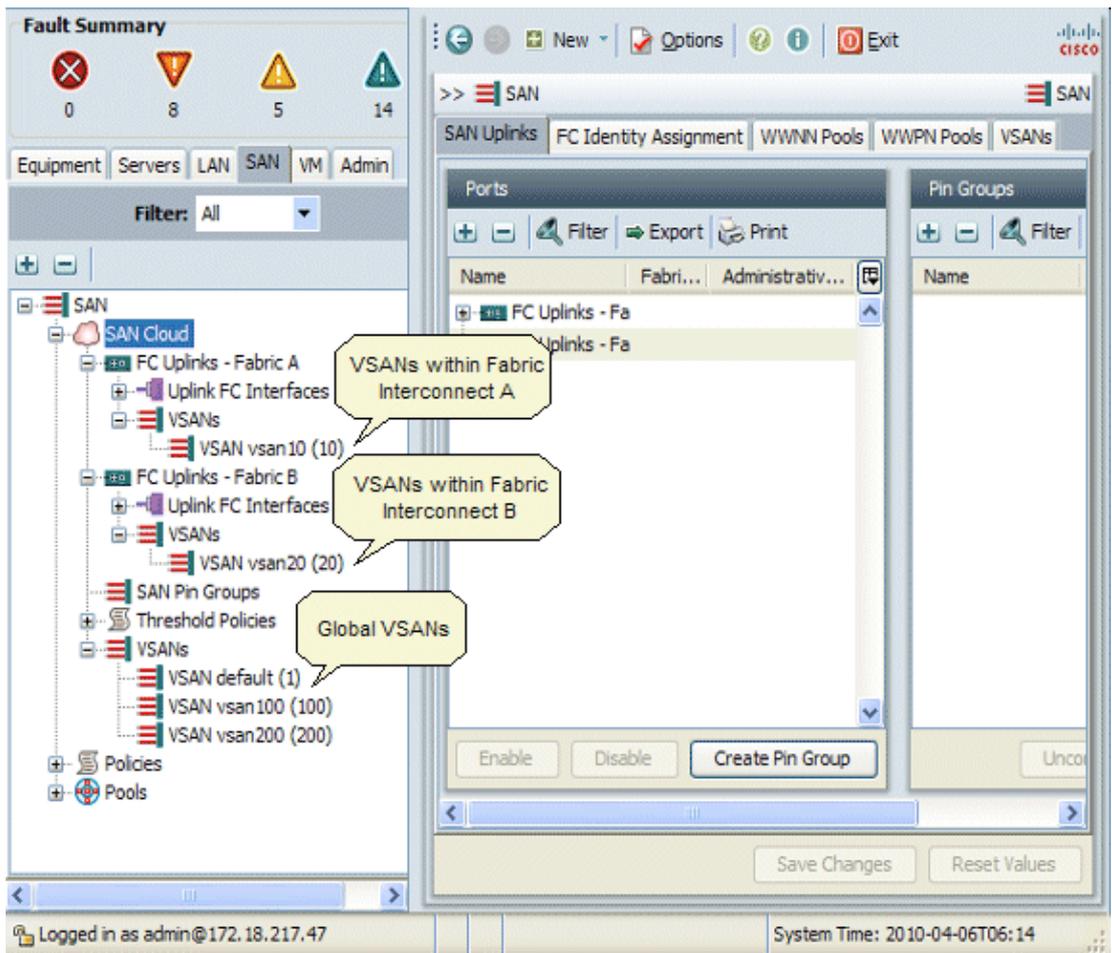
The VSAN/vHBA logic is mostly analogous to the VLAN/vNIC logic. If you want to support any VSAN, it needs to be configured globally into Cisco UCS Manager, and then it can be associated with a particular vHBA. The default VSAN is preconfigured into Cisco UCS Manager, and is automatically chosen as the default connectivity for each vHBA.

For VSAN, each fiber uplink from Cisco UCS to the distribution layer supports only one VSAN. This is specified as a property of the uplink. While vNIC can support multiple VLANs, each vHBA can support only one VSAN.

The configuration of VSAN:

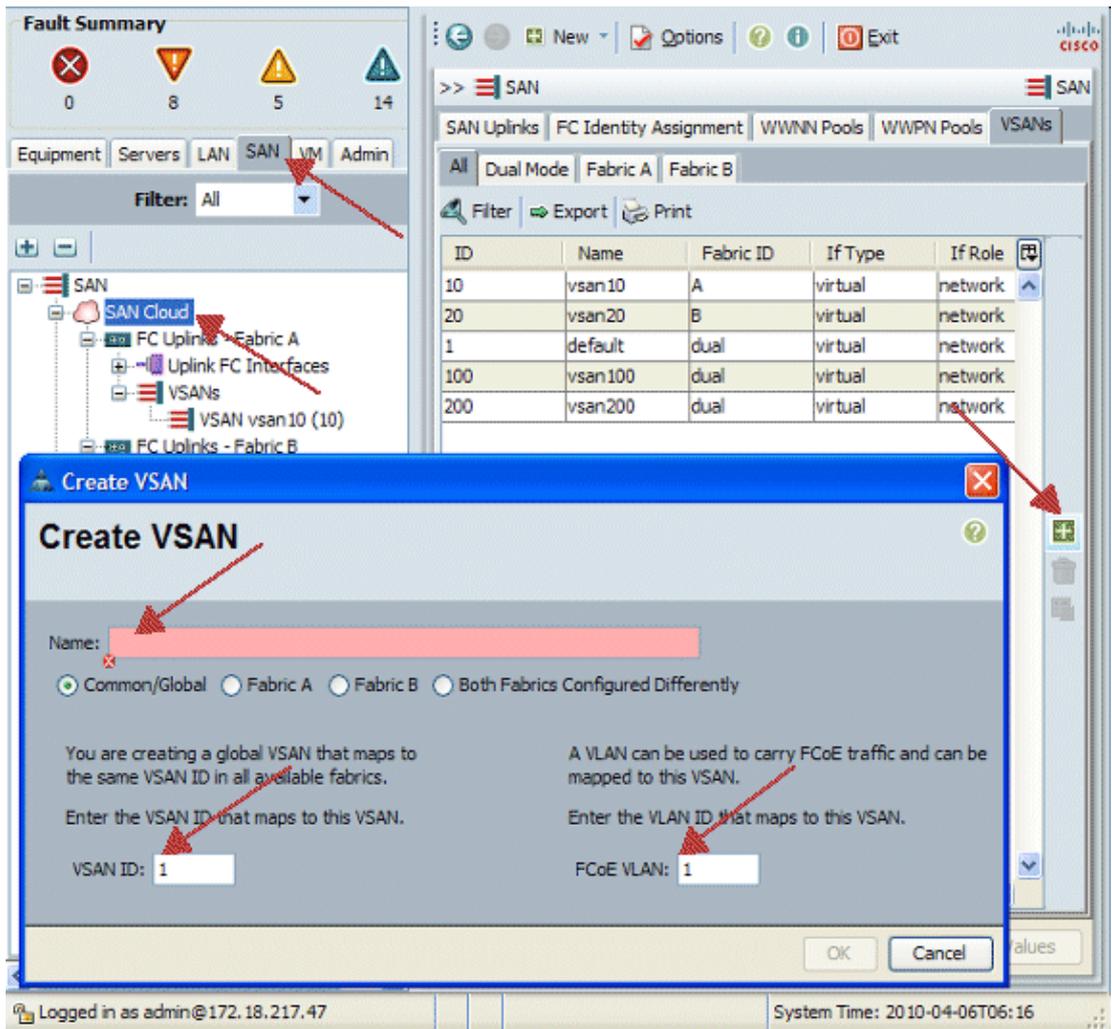
Complete these steps in order to configure a global VSAN to be used for vHBA.

1. Choose the **SAN** tab.
2. Choose **SAN > SAN Cloud**.



3. Choose the **VSANS** tab in Work Pane, choose **VSANS**, then choose + in order to begin the VSAN creation .

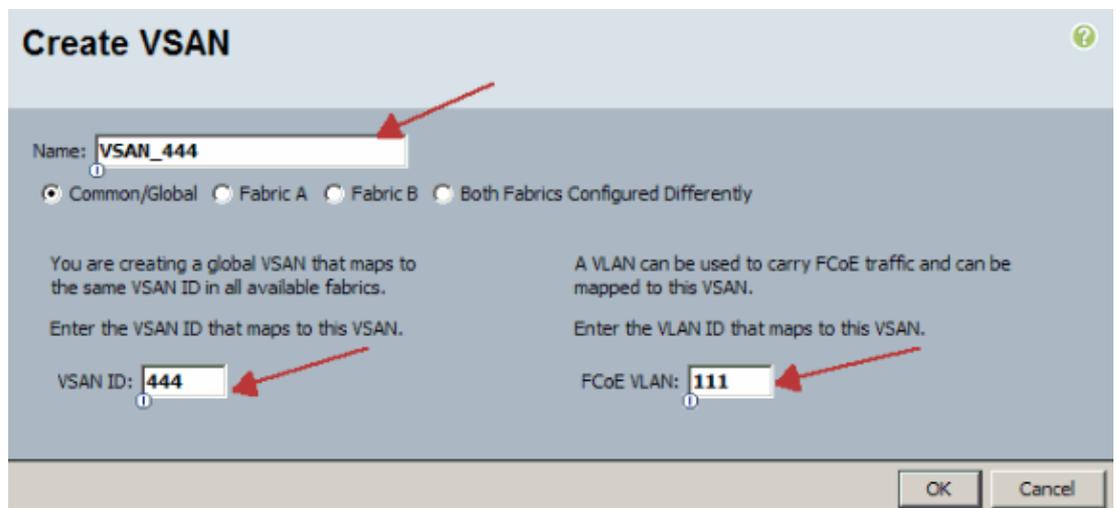
Cisco UCS Manager GUI adds the VSAN to the VSANS node under SAN Cloud.



4. Enter this information in the Create VSAN dialog box and complete these steps:

- In the Name field, create a meaningful name for your VSAN.
- In the ID field, enter a valid VSAN ID. This needs to match an ID in your Core SAN.
- Add a VLAN ID that is used internally in order to carry FCoE.

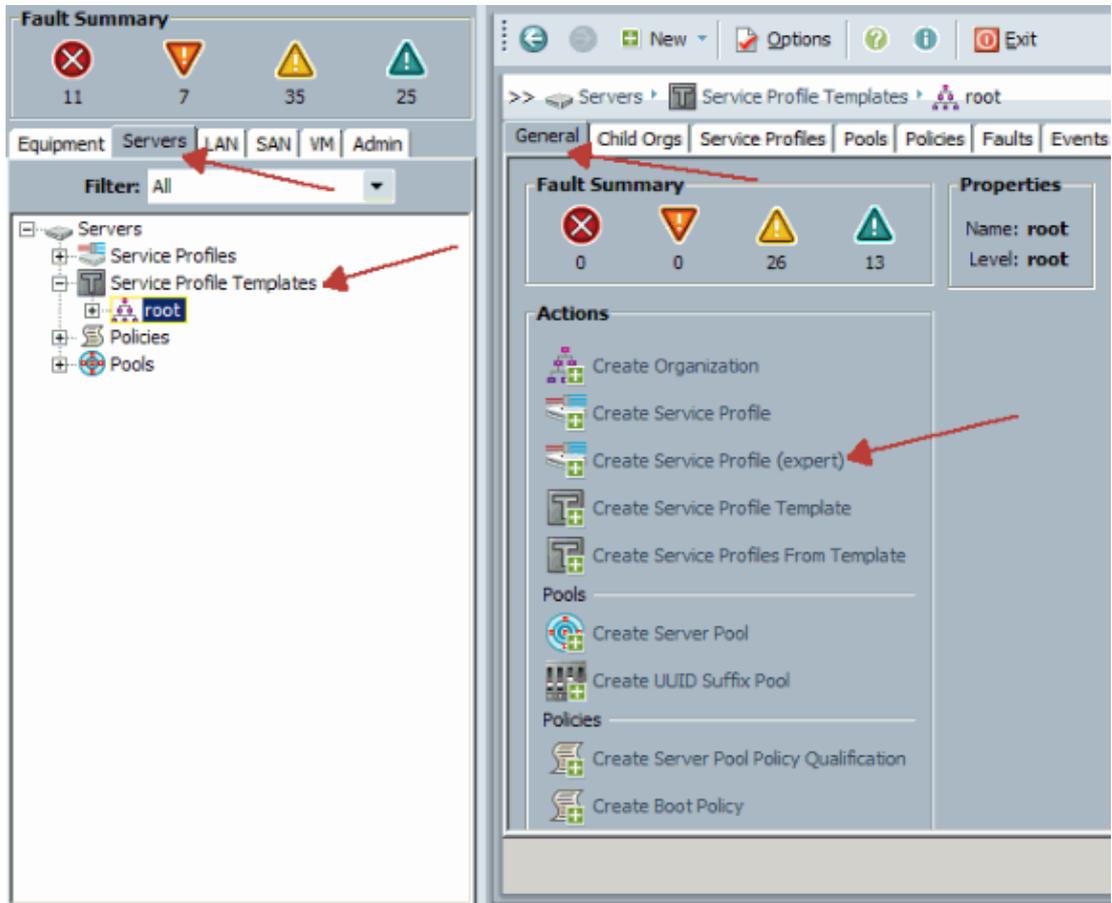
Cisco UCS Manager GUI adds the VSAN to the VSANs node under SAN Cloud.



Create vHBAs

Add the Virtual HBAs to your Profile if you are required to do FCoE for Fiber Channel access to storage. The vHBA is configured into each Service Profile in a manner analogous to vNIC.

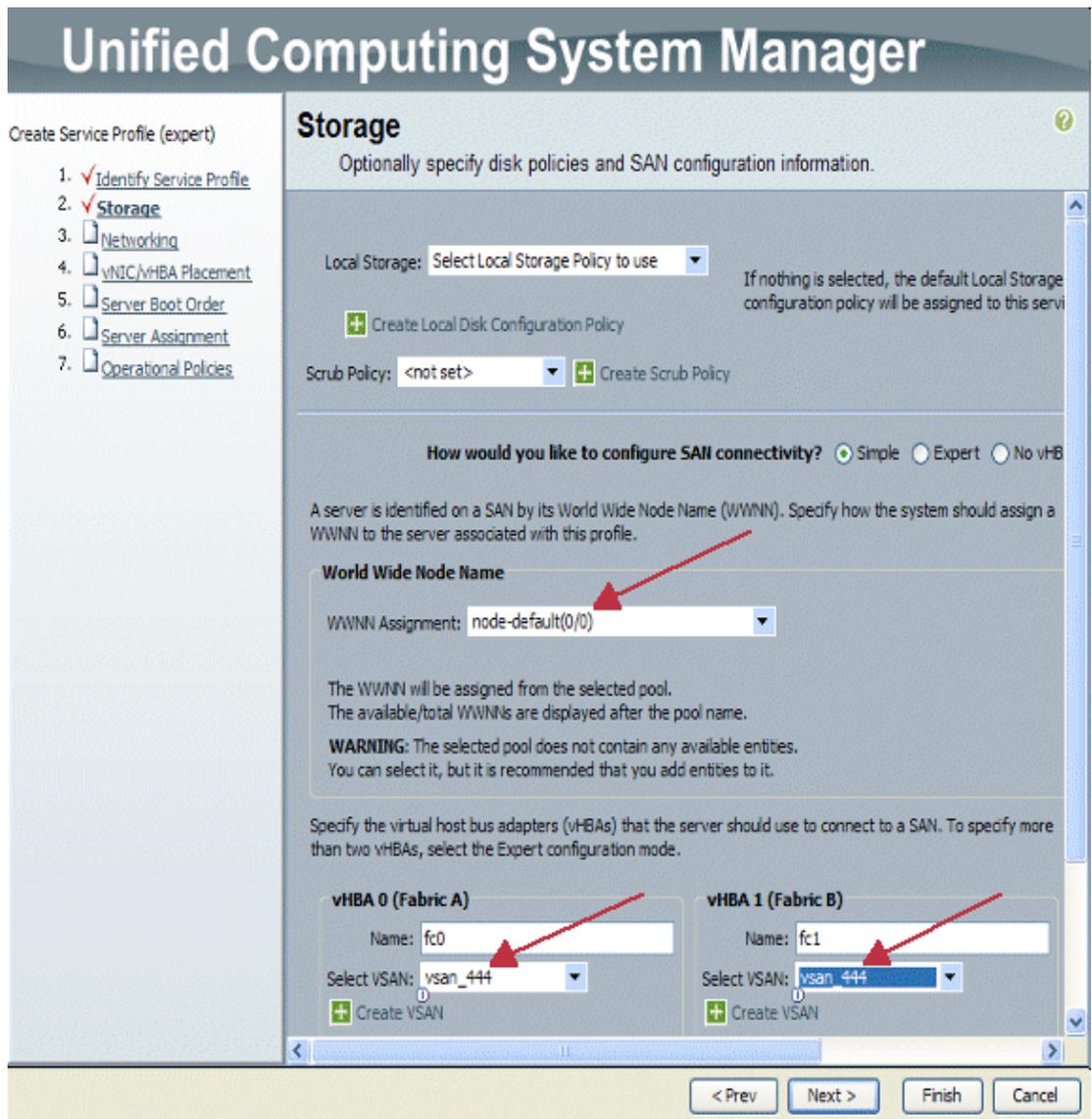
1. Log into Cisco UCS Manager GUI.
2. In the Navigation pane, choose the **Servers** tab.
3. Choose **Servers > Service Profile Templates**.
4. Choose **root**.
5. In the Work pane, select **General**.
6. Click **Create Service Profile (expert)** and a pop-up window appears.



7. Fill out the name, which is equal to something in general to this Profile when assigned to a Blade server. Add a description as required. Then click **Next**.



8. Select the method to assign WWN names to the vHBAs. Select the vSAN that was created in steps above and assign it to vHBAs.

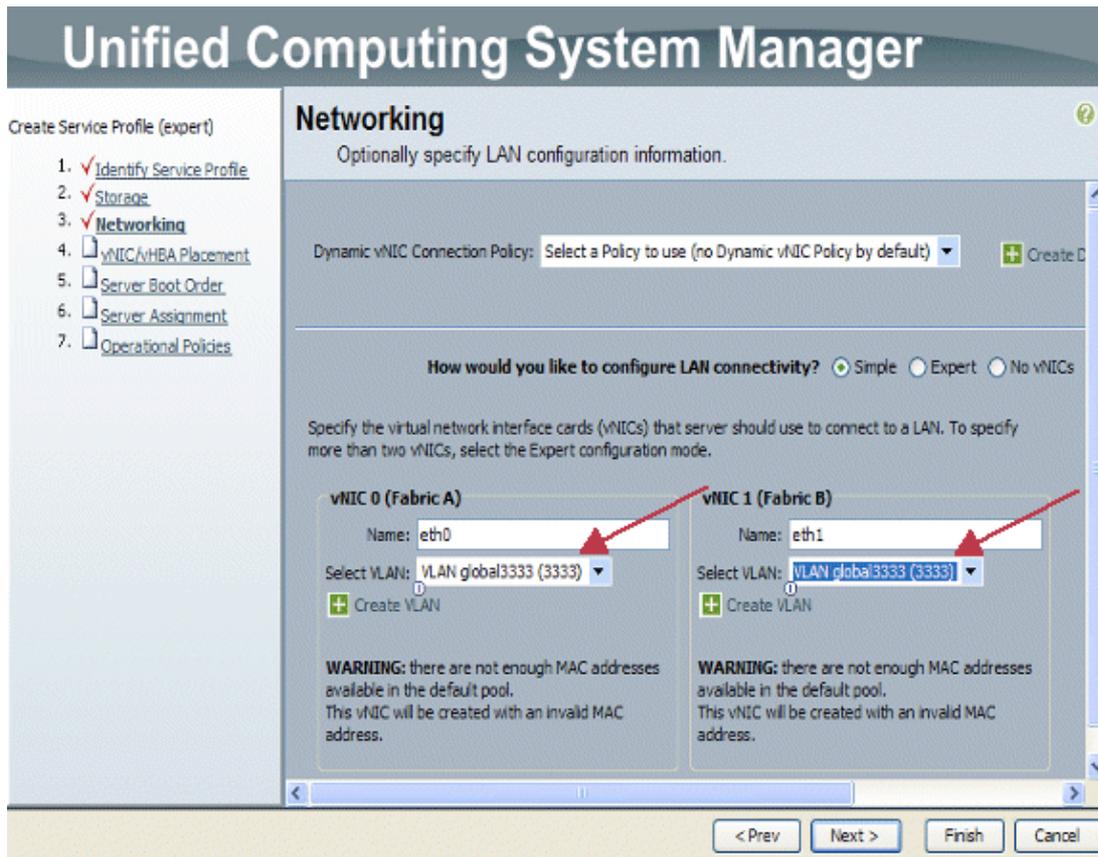


Create vNICs

Add vNICs to the profile as explained in the next steps as a continuation of the Service Profile creation process:

Complete these steps:

Choose the VLAN that was created in the previous step and assign it to the vNICs.

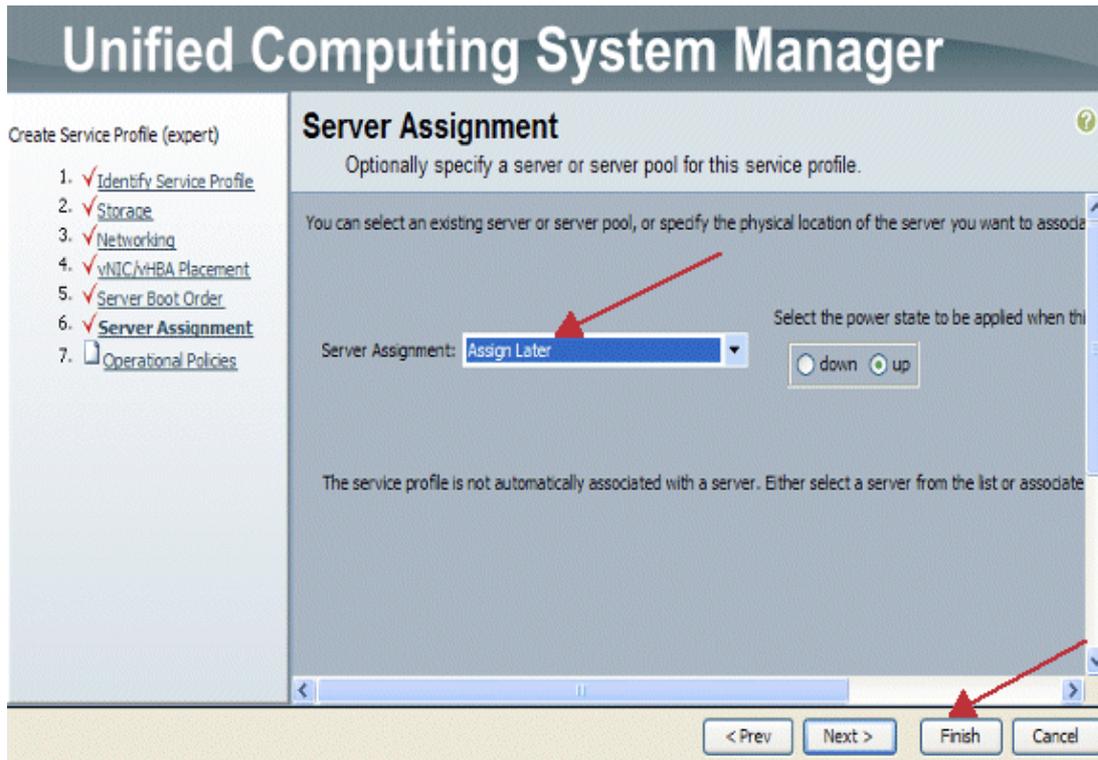


Associate Server to Service Profile

This step is Optional, which means you can choose to associate this Service Profile to servers in other part areas of Cisco UCS Manager.

When you associate a blade to a Service Profile, the Cisco UCS Manager first tries to assign the blade to the configuration. This does nothing to modify the blade itself, but the assignment still checks that a blade is compatible with a profile. If it is not compatible, it fails.

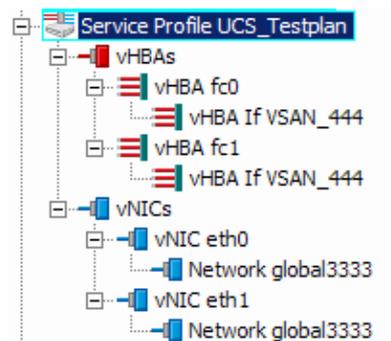
Once the blade is successfully assigned, the actual association process begins. This involves Cisco UCS Manager that causes a mini-OS called processing mode utility OS (PmuOS) to be booted on the blade.



Verify

Use this section in order to confirm that your configuration works properly.

Verify your created Adaptor interfaces in the Server Tab of UCS Manager.



Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [Technical Support & Documentation – Cisco Systems](#)

