# ılıılı cısco

# Use Cisco UCS Connectivity Policies to Achieve Strict Administrative Role Delineation

# What You Will Learn

As more customers deploy and expand their Cisco Unified Computing System<sup>™</sup> (Cisco UCS<sup>®</sup>) installations, they require a variety of methods for domain experts to construct and deploy service profiles. Many customers have expressed interest in dividing the responsibility and privilege for service profile construction among server, storage, and network administrators. This division would provide a more natural configuration process that is in concert with their data center's roles, responsibilities, and privileges.

Cisco UCS Manager 2.1 provides support for this clear delineation of responsibilities and privileges with LAN and SAN connectivity policies. Figure 1 contrasts (a) a simple service profile and (b) a service profile that references LAN and SAN connectivity policies. Note the clear division of server, storage and network components in the service profile, SAN connectivity policy, and LAN connectivity policy, respectively. Cisco UCS Manager 2.1 also provides a new role that can be used when configuring connectivity policies. An administrator with this role cannot configure network and storage resources; these resources are derived by referencing connectivity policies.





This document explains how to use LAN and SAN connectivity policies to deploy service profiles on Cisco UCS. It also discusses how connectivity policies, in conjunction with the Cisco UCS role-based access control (RBAC) system, can be used to provide a clear delineation of responsibilities and privileges for service profile configuration. Connectivity policies are introduced as part of Cisco UCS Manager Release 2.1 and are supported by all versions of Cisco UCS hardware.

# **Connectivity Policies**

LAN connectivity policies are used to configure a service profile's network resources. These resources include virtual network interface cards (vNICs), Small Computer System Interface over IP (iSCSI) vNICs, VLANs, network identities (MAC addresses), pinning, statistics, and adapter policies. A LAN connectivity policy can be used by one or many service profiles; therefore, its network identities must be pool or hardware derived. Typically, the network administrator configures the LAN connectivity policy.

SAN connectivity policies are used to configure a service profile's storage resources. These resources include virtual host bus adapters (vHBAs), virtual SANs (vSANs), storage identities (worldwide node names [WWNNs] and worldwide port names [WWPNs]), statistics, and adapter policies. A SAN connectivity policy can be used by one or more service profiles; therefore, its storage identities must be pool or hardware derived. Typically, the storage administrator configures the SAN connectivity policy.

To derive value from a connectivity policy, the policy must referenced by a service profile. During service profile construction, users can reference a LAN connectivity policy for network resources and a SAN connectivity policy for storage resources. After a policy is referenced, the connectivity policy's network or storage resources are configured on the service profile.

## **Configuration Flexibility**

A connectivity policy can be referenced by one or many service profiles or service profile templates. This approach provides a powerful and flexible foundation for service profile configuration and facilitates connectivity policy reuse. It also means that changes to a connectivity policy will affect (update) all referencing service profiles. Figure <u>2</u> illustrates several service profile configurations.

- a. Service profile DatabaseProf references LAN and SAN connectivity policies InternalNetLCP and SecureDataSCP.
- b. Service profile VDIProfile references LAN connectivity policy InternalNetLCP.
- c. Service profile template DbVMTemplate references LAN and SAN connectivity policies InternalNetLCP and SecureDataSCP.
- Figure 2. Logical View of Connectivity Policies Shared by Service Profiles



Even though the server administrator references a LAN or SAN connectivity policy, the administrator still can configure the device order and boot order.

#### **Configuration Flexibility**

Note the clear division of network, storage, and server components in the service profile and their connectivity policies. Cisco UCS Manager 2.1 also provides a new role, designed to be used in conjunction with connectivity policies.

### Server Administrator Privileges

Cisco UCS provides a RBAC system that allows administrators to control access to the actions and resources in Cisco UCS. Cisco UCS Manager 2.1 introduces a new role, **server-compute**, which allows administrators to limit a user's role to server administration only. A server administrator with this role will have the necessary privileges to create service profiles that reference LAN and SAN connectivity policies. However, the administrator will be prohibited from configuring network and storage resources. The following example demonstrates how this role can be used with Cisco UCS locales to implement a clear delineation of responsibilities and privileges among server, storage and network administrators.

# Sample Configuration

The following sections show the use of the Cisco UCS GUI to configure a service profile that references LAN and SAN connectivity policies. Configuration includes the following steps:

- 1. Create users and roles.
- 2. Create a LAN connectivity policy.
- 3. Create a SAN connectivity policy.
- 4. Create a service profile.

# **Create Users and Roles**

This example assumes that network and storage administrator users have already been created, and it shows how to create a new server administrator user using the new **server-compute** role. This example also limits the server administrator to configuration of the **finance** organization through creation of a Cisco UCS locale. To create a locale, launch the Create Locale wizard as illustrated in Figure 3.

Figure 3. Launch the Create Locale Wizard



You create a locale named **financial** and assign the **finance** organization to it, as shown in <u>Figure 4</u>. Users assigned this locale will be able to perform configuration operations in the **finance** organization.

Figure 4.	Create a Locale	That Includes	the Finance	Organization
				e.gaa.o

Organizations	8	
Grganizations     for root     finance     for h		 💝 financial
- A benents		♦ org-root/org-finance

Next, you launch the Create User wizard from the Admin tab, as shown in Figure  $5^{1}$ .

Figure 5. Launch the Create User Wizard



In the Create User wizard, you populate details about the new user. Choose the **server-compute** role and the **financial** locale as illustrated in Figure 6.

Roles	Locales
🔲 aaa	🔽 financial
🔄 admin	
facility-manager	
network	
operations	
read-only	
server-compute	
server-equipment	
server-profile	
server-security	
🔲 storage	

Figure 6. Create a User with the server-compute Role and Assign the Locale

<sup>&</sup>lt;sup>1</sup> This example creates a locally authenticated user. However, Cisco UCS provides a comprehensive set of RBAC options, including Lightweight Directory Access Protocol (LDAP) integration.

You have created a server administrator who can configure server resources only in the **financial** locale. The administrator will rely on the network and storage administrators to create LAN and SAN connectivity policies to create service profiles with network and storage connectivity.

# **Create a LAN Connectivity Policy**

Typically, the network administrator is responsible for creating LAN connectivity policies. To create a LAN connectivity policy, find the target organization (**finance**) on the Cisco UCS GUI's LAN tab, launch the wizard by right-clicking the LAN Connectivity Policy node, and select Create LAN Connectivity Policy, as shown in Figure 7.

Figure 7. Launch the Create LAN Connectivity Policy Wizard



The Create LAN Connectivity Policy wizard, shown in <u>Figure 8</u>, allows you to configure vNICs and iSCSI vNICs. Click the Add button to launch the Create vNIC wizard.

Figure 8. The Create LAN Connectivity Policy Wizard

Name: Inter		
0	nalNetLCP	
Û	cure access to internal networks	
	y one or more vNICs that the server should use to connect to the LAN	
Name	MAC Address	Native VLAN

The Create vNIC wizard, shown in Figure 9. allows you to configure the various characteristics of a vNIC, including its MAC address, maximum transmission unit (MTU), pin group, and adapter policy. You can create as many vNICs as required; however, vNICs must be configured to draw their MAC addresses from a pool or be hardware derived.<sup>2</sup>

<sup>&</sup>lt;sup>2</sup> This vNIC configuration process is similar to the process for vNIC configuration on a service profile. Many options are available, however, a detailed explanation of all options is beyond the scope of this document.

reate	VNIC			
abair TDa	<ul> <li>Fabric A <ul> <li>Fabric I</li> <li>Fabri</li></ul></li></ul>	C Foshla Esilovar	L	
VLANS				
Select	Name	Native	VLAN	1
	default	l	0	A
	finlan200		Õ	
<b>V</b>	finlan201		0	
<b>V</b>			0	-
	1500 <not set=""></not>	Create LAN Pin Group		
Occuratio	nal Parameters			8
operatio				~
	erformance Profile			~
		inux 💌 🖪	Create Ethernet Adapter	
lapter P	Adapter Policy:		Create Ethernet Adapter	Policy
dapter P	Adapter Policy: I IC Connection Policy:	<not set=""> 🔹 🛨</not>	Create Dynamic vNIC Con	Policy
dapter Po iynamic vN	Adapter Policy:	<not set=""></not>		Policy inection Policy

Figure 9. The Create vNIC Wizard Lets You Customize a vNIC's Characteristics

To complete the construction, select the VLANs that the vNIC should use and the policies that define the vNIC. After you finish construction of the LAN connectivity policy, you can view and modify its configuration on the LAN tab, as shown in <u>Figure 10</u>.

A Summary	💿 🖬 New - 😡 Options	0 0 APendra /	attrations   📵 Exit			1
0 3 10 8	> 🗐 LAN + 🚿 Policies + 🙏	root + 🚿 LAN Connectiv	Ry Policies + 🚿 DevLCP			SS Devi
pment Servers LAN SAN VM Admin	ieneral Events					
Filter: Al	Actions	Name: DevLCP				
=	H Delete Show Policy Usage	Description: For develop				
Em Febric A     A     Febric B	200 Scow Low S opply	Click Add to specify one	e or more vNICs that the server should	Juse to connect to the LAN.		
QoS System Class		Name		MAC Address	Native VLAN	
LAN Pin Groups		I viac etho		Derived	1.000 00000	
Threshold Policies				Dennes	0	
VLAN Groups		-S Network T			0	1
⊕ ≡ vlavs		- Network T			0	
E C Applances				Derived	0	
Internal LAN     Internal Fabric A		E - VILL COL				
<ul> <li>- Internal Fabric A</li> <li>- Internal Fabric 8</li> </ul>				Telete Add I Modfy		
Si Polices		Add ISCSLYNICS				0
Acolances		Accretest wates		the second s	the state of the second st	6
C LAN Cloud						
		Name	Overlay vNIC Name	ISCSI Adapter Policy	MAC Address	
⊖ A root			Stated the same	should margine makely		
- I Default vNIC Behavior						
Source of the Connection Policies						
In Flow Control Policies						
Si Flow Control Policies     Si def aut     Si LAN Connectivity Policies     Si LAN Connectivity Policies     Si Control						
Flow Control Policies     Softwart						
Single Control Policies     Softant     Softant						
Grico Control Policies     Grico Policies     Grico Policies				🖬 Add 👚 Delete 🖷 Modity		
Single Control Policies				Add 👚 Delete 📲 Modify		
File Control Polices     Set Aut     Set     Set Aut     Set				Add 🕆 Delete 🖷 Modify		
Por Control Polices     Series     Seri				🖬 Add 🕆 Delete 📲 Mosify,		
Brow Control Pilotos     Service Control Pilotos     Service     Service				🖬 Add 🏦 Delete 📑 Posty		
Por Control Polices     Series     Seri				🖬 Add 👚 Delete 🖷 Modily	Ster Charge	

Figure 10. View and Modify the LAN Connectivity Policy Configuration

#### **Create a SAN Connectivity Policy**

Typically, the storage administrator is responsible for creating the SAN connectivity policies. To create a SAN connectivity policy, find the target organization (**finance**) on the Cisco UCS GUI's SAN tab, launch the wizard by right-clicking the SAN Connectivity Policy node, and select Create SAN Connectivity Policy, as shown in Figure <u>11</u>.

Filter: Al ▼ Name	Filter: Al         Image: Start	Filter: Al	Equipment Servers LAN SAN VM Admin	SAN Connectivity Policies
SAN Connectivity Policies     L	A Sub-Organizations     A finance     S Fore Channel Adapter Policies     S Fore Channel Adapter Policies	Sub-Oracizations     Sub-Oracizations     Setup: Stree Channel Adapter Policies     Stree Channel Adapter Policies     Strenge Connectivity     SAN Connectivity Policies	Filter: Al	None

Figure 11. Launch the Create SAN Connectivity Policy Wizard

The Create SAN Connectivity Policy wizard is shown in <u>Figure 12</u>. It allows you to create and configure vHBAs. Click the Add button to launch the Create vHBA wizard.

Figure 12. The SAN Connectivity Policy Creation Wizard

Name: SecureData	SCP		
escription:			
server is identified on a ofile.	5AN by its World Wide Node Name (1	WWNN). Specify how the system should	l assign a WW
World Wide Node Nar	ne		
WWNN Assignment:	finpool(10/10)	•	
Create WWNN P	lool		
	gned from the selected pool. /NNs are displayed after the pool na	me.	

The Create vHBA wizard (Figure 13) allows you to configure the various characteristics of a vHBA, including the identity, VSAN, maximum data field size, pin group, and adapter policy. You can create as many vHBAs as required; however, the vHBAs must be configured to draw their WWPN from a pool or be hardware derived.<sup>3</sup>

<sup>&</sup>lt;sup>3</sup> This vHBA configuration process is similar to the process for vHBA configuration directly under a service profile. Many options are available; however, a detailed explanation of all options is beyond the scope of this document.

Figure 13. The vHBA Creation Wizard

Un vitis fordizz: Create vitis Template Patric ID:  A B Select Visiti, default  Create Visiti Patric ID:  Create Visiti Create Visiti C	Name: 1	rf)			-World Wide Port N	ame	
Select VSAN: Pin Group: dend set> Persstern Einding: Disabiled Max Data Field Stee: 2016					Create WWPN	Pool assigned from the selected pool.	
	Select VSAN: Pin Group: Persistent Binding:	default <not set=""> © Disabled</not>	٠				
	,			8			

To complete the construction, select the VSAN that the vNIC should use and the policies that define the vHBA. Note that you can create a number of different vHBAs.

After you finish construction of the SAN connectivity policy, you can view and modify its configuration on the SAN tab, as shown in Figure 14.

Figure 14. View and Modify the SAN Connectivity Policy Configuration

Equipment Servers LAN SAN VM Admin	General vHBA Initiator Groups Events			
Filter: Al 💌	Actions	Name: SecureDataSCP		
e =	- Change World Wide Node Name	Description:		
SAN     SAN     SAN Cloud	Show Policy Usage	Name	WWPN	10
E E Fabric A	The result of the		Derived	-
🕢 💷 Fabric B				
SAN Pin Groups				
E Storage Cloud				+
Eabric A     Eabric B		1	Delete 🔛 Add 🔤 Modify	
Har Patric B     Har Patric B     Har Patric B				
- S Policies				
SAN Cloud				
Threshold Policies     A root				
<ul> <li>         —</li></ul>				
Horizon Fibre Channel Adapter Policies				
SAN Connectivity Policies     SecureDataSCP				

## **Create a Service Profile**

The server administrator can now create a service profile using the LAN and SAN connectivity policies that were created in the previous sections. You can create a service profile by right-clicking the **finance** organization on the Server tab of the Cisco UCS GUI and selecting one of the Create Service Profile options. This example uses the Create Service Profile (expert) option, as shown in <u>Figure 15</u>.

quipment Servers LAN SAM	V VM Admin	General	Sub-Organization	s Service Profiles	P
Filter: All			t Summary		
Servers Service Profiles	tions		Create Organiza		
B-A finance B-S S -A S B-A hr	Suppression Task Prope Show Navigator	rties =		rofile (expert) rofiles From Templa rofile	ate
P ⊕ ▲ Si ⊕ Service Profile Te	Create Organization Create Service Profile (e			rofile Template ression	
⊕ _ ▲ Sub-Orga     ♥ Oilcies     ♥ Policies     ♥ for coot     ⊕ _ ⑤ Adapter F     ⊕ _ ⑤ BIOS Def.     ⊕ _ ⑤ BIOS Policies	Create Service Profile Create Service Profile Create Service Profile To Start Fault Suppression Stop Fault Suppression		e	ession : Properties	
<ul> <li>BIOS Point</li> <li>Boot Polic</li> <li>S Host Firm</li> <li>S Host Firm</li> <li>S Local Disk</li> <li>Maintenance</li> </ul>	Copy Copy XML Delete		Ctrl+C Ctrl+L Ctrl+D		

Figure 15. Launch the Create Service Profile Wizard

The Cisco UCS GUI will guide you through the steps for service profile configuration. Note that since you logged in as a user with only the **server-compute** role, the service profile creation process is streamlined. The wizard will provide only configuration options related to server administration. The connectivity settings are configured by selecting a LAN and SAN connectivity policy, as illustrated in <u>Figure 16</u>.

Figure 16. Select LAN and SAN Connectivity Policies

Treate Service Profile (expert) 1. √ <u>Identify Service Profile</u> 2. √ <u>Connectivity</u>	Connectivity Optionally specify disk p configuration information			0
3. <u>VNIC/VHBA Placement</u> 4. <u>Server Boot Order</u> 5. <u>Maintenance Policy</u> 6. <u>Server Assignment</u>	Dynamic vNIC Connection Policy: Local Storage: LAN Connectivity Policy:	<not set=""></not>	• •	
7. Doperational Policies	SAN Connectivity Policy:	U SecureDataSCP U	•	

The wizard will guide you through the other service profile configuration options, such as the NIC placement and server boot order and assignment. At the completion of service profile configuration, you can view and modify the service profile on the Server tab, as illustrated in <u>Figure 17</u>.

Figure 17. View and Modify the Service Profile

3     Y     ▲       3     0     9       ort     Servers     L Servers       Filter:     Ad	
er, Servers LAN SAN MI Adam Herr Al Server factor and Servery Herrork, BCS1 HBCs Box Order What Madrees Factor Sammary Source Sammary	
ext arrows (LAN ( 344)	
	Properties
0 0 1	Name: Scalability
@ vNCs & sub-Organizations Status	User Label:
B (Å dev)	Description:
Overal Status:      Unassociated	UUID: 3c70a7ea-78f3-11df-0000-0000000000a
-G GCST WRICE Status Details (2)	UUD Pool: DevPool
B VTEAS	UUID Pool Instance: org-root/uuid-pool-DevPool
U vHBA fr0     U vHBA If default     Desired Power State:      t     Up	Associated Server:
	Service Profile Template:
	Template Instance:
Unit Assigned State:      Unassigned	Assigned Server or Server Pool
D I vitC etho Note: The "Desired Power State" is the	Assigned Server of Server Pool
- Dynamic vNICs Power State of the server set via UCSM.	Instance in and
⊕ - € VLAVIS     It may be therefore different from the	Nothing Selected
	Management IP Address 🔗
A sub-Organizations	
Service Profile Templates Actions	Management IP Address Policy: None
B-A root	realityment of Hourss Foldy, Hours
A Sub-Organizations	
B A dev Change Initial Power State	
Sub-Organizations	Maintenance Policy
S Polcies ⊖ A root	
D- S Adapter Policies	Name: default
- S Eth Adapter Policy Linux Rename Service Profile	Maintenance Policy Instance: org-root/maint-default
CE Db Adveter Date: (D10)	Description:
- S Eth Adapter Policy Solaris Create a Clone	Reboot Policy: Immediate
- Sth Adapter Policy VMWare Create a Service Profile Template	
- 30 Eth Adapter Policy VMWarePassThru	
Seth Adapter Policy Windows     Set Adapter Policy default	
-S ECH Mageer Policy Units	
W. BC Advater Delay Salari	
-SFC Adapter Policy VMWare	
- SFC Adapter Policy Windows ST Bind to a Template	
- SFC Adapter Policy default	
SI ISCSI Adapter Policy default	
Stor Defaults	
	Save Changes Reset Values

# Conclusion

Cisco UCS provides a comprehensive RBAC system that allows administrators to control user access to the actions and resources in Cisco UCS. Cisco UCS Manager 2.1 introduces LAN and SAN connectivity policies that allow users to strictly control the network, storage, and server administrator roles in Cisco UCS.

# For More Information

Contact your local Cisco representative or visit:

- Cisco UCS: <u>http://www.cisco.com/go/unifiedcomputing</u>
- Cisco UCS: A Complete Reference Guide to the Cisco Data Center: <u>http://www.amazon.com/Cisco-Unified-</u> <u>Computing-System-Center/dp/1587141930</u>
- Virtualization server architecture: <u>http://www.amazon.com/Cisco-Unified-Computing-System-Center/dp/1587141930</u>
- Cisco Developer Network: <u>http://developer.cisco.com/web/unifiedcomputing/home</u>
- Cisco UCS Manager product page on Cisco.com: <u>http://www.cisco.com/en/US/products/ps10281/index.html</u>
- Cisco UCS Platform Emulator (UCSPE) download: http://developer.cisco.com/web/unifiedcomputing/ucsemulatordownload
- Cisco UCS Manager Advantage Video Series: <u>http://www.cisco.com/en/US/prod/ps10265/ucs\_advantage\_video\_library.html</u>
- Cisco IT Solutions: <a href="http://www.cisco.com/web/about/ciscoitatwork/data\_center/index.html">http://www.cisco.com/web/about/ciscoitatwork/data\_center/index.html</a>



Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA

C11-719521-00 11/12