



Cisco UCS Manager CLI Configuration Guide, Release 1.3(1)

First Published: June 04, 2010

Last Modified: August 25, 2010

Americas Headquarters

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

Text Part Number: OL-22881-04

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at <http://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. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface **xxi**

Audience **xxi**

New and Changed Information for this Release **xxi**

Organization **xxiii**

Conventions **xxiv**

Related Documentation **xxv**

Documentation Feedback **xxv**

Obtaining Documentation and Submitting a Service Request **xxv**

Introduction **1**

Overview of Cisco Unified Computing System **3**

About Cisco Unified Computing System **3**

Unified Fabric **4**

Fibre Channel over Ethernet **5**

Link-Level Flow Control **5**

Priority Flow Control **5**

Server Architecture and Connectivity **6**

Overview of Service Profiles **6**

Network Connectivity through Service Profiles **6**

Configuration through Service Profiles **6**

Service Profiles that Override Server Identity **7**

Service Profiles that Inherit Server Identity **8**

Service Profile Templates **8**

Policies **9**

Configuration Policies **9**

Boot Policy **9**

Chassis Discovery Policy **10**

Dynamic vNIC Connection Policy **11**

Ethernet and Fibre Channel Adapter Policies **12**

| | |
|--|----|
| Host Firmware Package | 13 |
| IPMI Access Profile | 14 |
| Local Disk Configuration Policy | 14 |
| Management Firmware Package | 14 |
| Network Control Policy | 15 |
| Power Policy | 15 |
| Quality of Service Policy | 15 |
| Server Autoconfiguration Policy | 16 |
| Server Discovery Policy | 16 |
| Server Inheritance Policy | 16 |
| Server Pool Policy | 16 |
| Server Pool Policy Qualifications | 17 |
| vHBA Template | 17 |
| VM Lifecycle Policy | 17 |
| vNIC Template | 18 |
| vNIC/vHBA Placement Policies | 18 |
| Operational Policies | 18 |
| Fault Collection Policy | 18 |
| Flow Control Policy | 19 |
| Scrub Policy | 19 |
| Serial over LAN Policy | 20 |
| Statistics Collection Policy | 20 |
| Statistics Threshold Policy | 20 |
| Pools | 21 |
| Server Pools | 21 |
| MAC Pools | 21 |
| UUID Suffix Pools | 21 |
| WWN Pools | 22 |
| Management IP Pool | 22 |
| Traffic Management | 23 |
| Oversubscription | 23 |
| Oversubscription Considerations | 23 |
| Guidelines for Estimating Oversubscription | 24 |
| Pinning | 24 |
| Pinning Server Traffic to Server Ports | 25 |

| | |
|--|-----------|
| Guidelines for Pinning | 26 |
| Quality of Service | 26 |
| System Classes | 26 |
| Quality of Service Policy | 27 |
| Flow Control Policy | 27 |
| Opt-In Features | 27 |
| Stateless Computing | 27 |
| Multi-Tenancy | 28 |
| Virtualization in Cisco UCS | 29 |
| Overview of Virtualization | 29 |
| Virtualization in Cisco UCS | 30 |
| Virtualization with Network Interface Cards and Converged Network Adapters | 30 |
| Virtualization with a Virtual Interface Card Adapter | 30 |
| Cisco VN-Link | 31 |
| VN-Link in Hardware | 31 |
| Extension File for Communication with VMware vCenter | 32 |
| Distributed Virtual Switches | 33 |
| Port Profiles | 33 |
| Port Profile Clients | 33 |
| VN-Link in Hardware Considerations | 33 |
| Overview of Cisco UCS Manager | 35 |
| About Cisco UCS Manager | 35 |
| Tasks You Can Perform in Cisco UCS Manager | 36 |
| Tasks You Cannot Perform in Cisco UCS Manager | 38 |
| Cisco UCS Manager in a Cluster Environment | 38 |
| Overview of Cisco UCS Manager CLI | 39 |
| Managed Objects | 39 |
| Command Modes | 39 |
| Object Commands | 41 |
| Complete a Command | 42 |
| Command History | 42 |
| Committing, Discarding, and Viewing Pending Commands | 42 |
| Online Help for the CLI | 43 |
| System Configuration | 45 |
| Configuring the Fabric Interconnects | 47 |

| | |
|---|-----------|
| Initial System Setup | 47 |
| Setup Mode | 48 |
| System Configuration Type | 48 |
| Management Port IP Address | 48 |
| Performing an Initial System Setup for a Standalone Configuration | 49 |
| Initial System Setup for a Cluster Configuration | 51 |
| Performing an Initial System Setup for the First Fabric Interconnect | 51 |
| Performing an Initial System Setup for the Second Fabric Interconnect | 53 |
| Enabling a Standalone Fabric Interconnect for Cluster Configuration | 54 |
| Changing the System Name | 54 |
| Changing the Management Subnet of a Cluster | 55 |
| Ethernet Switching Mode | 56 |
| Configuring Ethernet Switching Mode | 57 |
| Configuring Ports | 59 |
| Server and Uplink Ports on the Fabric Interconnect | 59 |
| Server Ports | 60 |
| Configuring a Server Port | 60 |
| Deleting a Server Port | 60 |
| Uplink Ethernet Ports | 61 |
| Configuring an Uplink Ethernet Port | 61 |
| Deleting an Uplink Ethernet Port | 61 |
| Uplink Ethernet Port Channels | 62 |
| Configuring an Uplink Ethernet Port Channel | 62 |
| Deleting an Uplink Ethernet Port Channel | 63 |
| Adding a Member Port to an Uplink Ethernet Port Channel | 64 |
| Deleting a Member Port from an Uplink Ethernet Port Channel | 64 |
| Configuring Communication Services | 67 |
| Communication Services | 67 |
| Configuring CIM XML | 68 |
| Configuring HTTP | 69 |
| Configuring HTTPS | 69 |
| Certificates, Key Rings, and Trusted Points | 69 |
| Creating a Key Ring | 70 |
| Creating a Certificate Request for a Key Ring | 70 |
| Creating a Trusted Point | 71 |

| | |
|--|-----------|
| Importing a Certificate into a Key Ring | 72 |
| Configuring HTTPS | 73 |
| Deleting a Key Ring | 74 |
| Deleting a Trusted Point | 75 |
| Configuring SNMP | 75 |
| Enabling SNMP and Configuring an SNMP Community | 75 |
| Creating an SNMP Trap Host | 76 |
| Deleting an SNMP Trap Host | 76 |
| Creating an SNMPv3 User | 77 |
| Deleting an SNMPv3 User | 78 |
| Disabling SNMP | 78 |
| Configuring Telnet | 78 |
| Disabling Communication Services | 79 |
| Configuring Primary Authentication | 81 |
| Primary Authentication | 81 |
| Remote Authentication Providers | 81 |
| Creating a Remote Authentication Provider | 83 |
| Configuring Properties for LDAP Providers | 83 |
| Creating an LDAP Provider | 84 |
| Configuring Properties for RADIUS Providers | 85 |
| Creating a RADIUS Provider | 86 |
| Configuring Properties for TACACS+ Providers | 87 |
| Creating a TACACS+ Provider | 87 |
| Selecting a Primary Authentication Service | 88 |
| Selecting the Console Authentication Service | 88 |
| Selecting the Default Authentication Service | 89 |
| Configuring Organizations | 91 |
| Organizations in a Multi-Tenancy Environment | 91 |
| Hierarchical Name Resolution in a Multi-Tenancy Environment | 92 |
| Configuring an Organization Under the Root Organization | 93 |
| Configuring an Organization Under an Organization that is not Root | 94 |
| Deleting an Organization | 95 |
| Configuring Role-Based Access Control | 97 |
| Role-Based Access Control | 97 |
| User Accounts for Cisco UCS Manager | 97 |

| | |
|---|------------|
| Guidelines for Cisco UCS Manager Usernames | 98 |
| Guidelines for Cisco UCS Manager Passwords | 98 |
| User Roles | 99 |
| Privileges | 100 |
| User Locales | 102 |
| Configuring User Roles | 102 |
| Creating a User Role | 102 |
| Adding Privileges to a User Role | 103 |
| Removing Privileges from a User Role | 103 |
| Deleting a User Role | 104 |
| Configuring Locales | 104 |
| Creating a Locale | 104 |
| Adding an Organization to a Locale | 105 |
| Deleting an Organization from a Locale | 105 |
| Deleting a Locale | 106 |
| Configuring User Accounts | 106 |
| Creating a User Account | 106 |
| Deleting a User Account | 108 |
| Assigning a Role to a User Account | 108 |
| Removing a Role from a User Account | 109 |
| Assigning a Locale to a User Account | 109 |
| Removing a Locale from a User Account | 110 |
| Monitoring User Sessions | 110 |
| Managing Firmware | 113 |
| Overview of Firmware | 113 |
| Firmware Image Management | 114 |
| Firmware Image Headers | 114 |
| Firmware Image Catalog | 114 |
| Firmware Upgrades | 115 |
| Guidelines and Cautions for Firmware Upgrades | 115 |
| Firmware Versions | 117 |
| Direct Firmware Upgrade at Endpoints | 118 |
| Stages of a Direct Firmware Upgrade | 118 |
| Recommended Order of Components for Firmware Activation | 120 |
| Outage Impacts of Direct Firmware Upgrades | 120 |

| | |
|---|-----|
| Firmware Upgrades through Service Profiles | 121 |
| Host Firmware Package | 122 |
| Management Firmware Package | 122 |
| Stages of a Firmware Upgrade through Service Profiles | 123 |
| Firmware Downgrades | 123 |
| Completing the Prerequisites for Upgrading the Firmware | 124 |
| Prerequisites for Upgrading and Downgrading Firmware | 124 |
| Creating an All Configuration Backup File | 124 |
| Verifying the Operability of a Fabric Interconnect | 125 |
| Verifying the High Availability Status and Roles of a Cluster Configuration | 125 |
| Verifying the Status of an I/O Module | 126 |
| Verifying the Status of a Server | 127 |
| Verifying the Status of an Adapter | 128 |
| Downloading and Managing Images | 128 |
| Obtaining Firmware Packages from Cisco | 128 |
| Downloading a Firmware Package to the Fabric Interconnect | 129 |
| Displaying the Firmware Package Download Status | 129 |
| Displaying All Available Software Images on the Fabric Interconnect | 130 |
| Directly Upgrading Firmware at Endpoints | 131 |
| Updating and Activating the Firmware on an Adapter | 131 |
| Updating and Activating the Firmware on a CIMC | 133 |
| Updating and Activating the Firmware on an I/O Module | 135 |
| Activating the Board Controller Firmware on a Server | 137 |
| Activating the Cisco UCS Manager Software | 138 |
| Activating the Firmware on a Fabric Interconnect | 139 |
| Updating Firmware through Service Profiles | 140 |
| Host Firmware Package | 140 |
| Creating and Updating a Host Firmware Package | 141 |
| Management Firmware Package | 142 |
| Creating and Updating a Management Firmware Package | 143 |
| Managing the Capability Catalog | 144 |
| Capability Catalog | 144 |
| Contents of the Capability Catalog | 144 |
| Updates to the Capability Catalog | 145 |
| Obtaining Capability Catalog Updates from Cisco | 145 |

| | |
|---|------------|
| Updating the Capability Catalog | 146 |
| Restarting a Capability Catalog Update | 147 |
| Viewing a Capability Catalog Provider | 148 |
| Configuring DNS Servers | 151 |
| DNS Servers in Cisco UCS | 151 |
| Configuring a DNS Server | 151 |
| Deleting a DNS Server | 152 |
| Configuring System-Related Policies | 153 |
| Configuring the Chassis Discovery Policy | 153 |
| Chassis Discovery Policy | 153 |
| Configuring the Chassis Discovery Policy | 154 |
| Configuring the Power Policy | 155 |
| Power Policy | 155 |
| Configuring the Power Policy | 155 |
| Configuring the Aging Time for the MAC Address Table | 156 |
| Aging Time for the MAC Address Table | 156 |
| Configuring the Aging Time for the MAC Address Table | 157 |
| Managing Port Licenses | 159 |
| Port Licenses | 159 |
| Obtaining the Host ID for a Fabric Interconnect | 159 |
| Obtaining a Port License | 160 |
| Installing a Port License on a Fabric Interconnect | 161 |
| Viewing the Port Licenses Installed on a Fabric Interconnect | 162 |
| Viewing Port License Usage for a Fabric Interconnect | 162 |
| Uninstalling a Port License from a Fabric Interconnect | 163 |
| Network Configuration | 165 |
| Configuring Named VLANs | 167 |
| Named VLANs | 167 |
| Creating a Named VLAN Accessible to Both Fabric Interconnects | 167 |
| Creating a Named VLAN Accessible to One Fabric Interconnect | 168 |
| Deleting a Named VLAN | 169 |
| Configuring LAN Pin Groups | 171 |
| LAN Pin Groups | 171 |
| Configuring a LAN Pin Group | 171 |
| Configuring MAC Pools | 173 |

| | |
|---|------------|
| MAC Pools | 173 |
| Configuring a MAC Pool | 173 |
| Configuring Quality of Service | 175 |
| Quality of Service | 175 |
| Configuring System Classes | 175 |
| System Classes | 175 |
| Configuring a System Class | 176 |
| Disabling a System Class | 177 |
| Configuring Quality of Service Policies | 178 |
| Quality of Service Policy | 178 |
| Configuring a QoS Policy | 178 |
| Deleting a QoS Policy | 180 |
| Configuring Flow Control Policies | 180 |
| Flow Control Policy | 180 |
| Configuring a Flow Control Policy | 181 |
| Deleting a Flow Control Policy | 182 |
| Configuring Network-Related Policies | 183 |
| Configuring vNIC Templates | 183 |
| vNIC Template | 183 |
| Configuring a vNIC Template | 183 |
| Deleting a vNIC Template | 185 |
| Configuring Ethernet Adapter Policies | 185 |
| Ethernet and Fibre Channel Adapter Policies | 185 |
| Configuring an Ethernet Adapter Policy | 186 |
| Deleting an Ethernet Adapter Policy | 188 |
| Configuring Network Control Policies | 188 |
| Network Control Policy | 188 |
| Configuring a Network Control Policy | 189 |
| Deleting a Network Control Policy | 190 |
| Storage Configuration | 191 |
| Configuring Named VSANs | 193 |
| Named VSANs | 193 |
| Creating a Named VSAN Accessible to Both Fabric Interconnects | 194 |
| Creating a Named VSAN Accessible to One Fabric Interconnect | 194 |
| Deleting a Named VSAN | 195 |

| | |
|--|------------|
| Configuring SAN Pin Groups | 197 |
| SAN Pin Groups | 197 |
| Configuring a SAN Pin Group | 197 |
| Configuring WWN Pools | 199 |
| WWN Pools | 199 |
| Configuring a WWN Pool | 200 |
| Configuring Storage-Related Policies | 203 |
| Configuring vHBA Templates | 203 |
| vHBA Template | 203 |
| Configuring a vHBA Template | 203 |
| Deleting a vHBA Template | 205 |
| Configuring Fibre Channel Adapter Policies | 205 |
| Ethernet and Fibre Channel Adapter Policies | 205 |
| Configuring a Fibre Channel Adapter Policy | 206 |
| Deleting a Fibre Channel Adapter Policy | 208 |
| Server Configuration | 209 |
| Configuring Server-Related Pools | 211 |
| Server Pool Configuration | 211 |
| Server Pools | 211 |
| Configuring a Server Pool | 211 |
| Deleting a Server Pool | 212 |
| UUID Suffix Pool Configuration | 212 |
| UUID Suffix Pools | 212 |
| Configuring a UUID Suffix Pool | 213 |
| Deleting a UUID Suffix Pool | 214 |
| Management IP Pool Configuration | 214 |
| Management IP Pool | 214 |
| Configuring an IP Address Block for the Management IP Pool | 214 |
| Deleting an IP Address Block from the Management IP Pool | 215 |
| Configuring Server-Related Policies | 217 |
| Configuring BIOS Settings | 217 |
| Server BIOS Settings | 217 |
| BIOS Policy | 219 |
| Default BIOS Settings | 219 |
| Creating a BIOS Policy | 219 |

| | |
|---|-----|
| Modifying BIOS Defaults | 225 |
| Viewing the Actual BIOS Settings for a Server | 232 |
| Configuring Boot Policies | 233 |
| Boot Policy | 233 |
| Configuring a Boot Policy | 234 |
| Configuring a LAN Boot for a Boot Policy | 236 |
| Configuring a Storage Boot for a Boot Policy | 237 |
| Configuring a Virtual Media Boot for a Boot Policy | 238 |
| Viewing a Boot Policy | 239 |
| Deleting a Boot Policy | 240 |
| Configuring IPMI Access Profiles | 240 |
| IPMI Access Profile | 240 |
| Configuring an IPMI Access Profile | 240 |
| Deleting an IPMI Access Profile | 242 |
| Adding an Endpoint User to an IPMI Access Profile | 242 |
| Deleting an Endpoint User from an IPMI Access Profile | 243 |
| Configuring Local Disk Configuration Policies | 243 |
| Local Disk Configuration Policy | 243 |
| Guidelines and Considerations for a Local Disk Configuration Policy | 244 |
| Creating a Local Disk Configuration Policy | 245 |
| Viewing a Local Disk Configuration Policy | 246 |
| Deleting a Local Disk Configuration Policy | 246 |
| Configuring Scrub Policies | 247 |
| Scrub Policy | 247 |
| Creating a Scrub Policy | 247 |
| Deleting a Scrub Policy | 248 |
| Configuring Serial over LAN Policies | 248 |
| Serial over LAN Policy | 248 |
| Configuring a Serial over LAN Policy | 249 |
| Viewing a Serial over LAN Policy | 250 |
| Deleting a Serial over LAN Policy | 250 |
| Configuring Server Autoconfiguration Policies | 251 |
| Server Autoconfiguration Policy | 251 |
| Configuring a Server Autoconfiguration Policy | 251 |
| Deleting a Server Autoconfiguration Policy | 252 |

| | |
|--|------------|
| Configuring Server Discovery Policies | 252 |
| Server Discovery Policy | 252 |
| Configuring a Server Discovery Policy | 253 |
| Deleting a Server Discovery Policy | 254 |
| Configuring Server Inheritance Policies | 254 |
| Server Inheritance Policy | 254 |
| Configuring a Server Inheritance Policy | 255 |
| Deleting a Server Inheritance Policy | 256 |
| Configuring Server Pool Policies | 256 |
| Server Pool Policy | 256 |
| Configuring a Server Pool Policy | 256 |
| Deleting a Server Pool Policy | 257 |
| Configuring Server Pool Policy Qualifications | 257 |
| Server Pool Policy Qualifications | 257 |
| Creating a Server Pool Policy Qualification | 258 |
| Deleting a Server Pool Policy Qualification | 259 |
| Creating an Adapter Qualification | 259 |
| Deleting an Adapter Qualification | 261 |
| Configuring a Chassis Qualification | 261 |
| Deleting a Chassis Qualification | 262 |
| Creating a CPU Qualification | 262 |
| Deleting a CPU Qualification | 264 |
| Creating a Memory Qualification | 264 |
| Deleting a Memory Qualification | 265 |
| Creating a Physical Qualification | 266 |
| Deleting a Physical Qualification | 266 |
| Creating a Storage Qualification | 267 |
| Deleting a Storage Qualification | 268 |
| Configuring vNIC/vHBA Placement Profiles | 268 |
| vNIC/vHBA Placement Policies | 268 |
| Configuring a vNIC/vHBA Placement Profile | 269 |
| Deleting a vNIC/vHBA Placement Profile | 270 |
| Configuring Service Profiles | 271 |
| Service Profiles that Inherit Server Identity | 271 |
| Service Profiles that Override Server Identity | 272 |

| | |
|--|------------|
| Service Profile Templates | 272 |
| Creating a Service Profile Template | 273 |
| Creating a Service Profile Instance from a Service Profile Template | 275 |
| Creating a Service Profile | 276 |
| Configuring a vNIC for a Service Profile | 278 |
| Configuring a vHBA for a Service Profile | 279 |
| Configuring a Local Disk for a Service Profile | 281 |
| Configuring Serial over LAN for a Service Profile | 282 |
| Service Profile Boot Definition Configuration | 283 |
| Configuring a Boot Definition for a Service Profile | 283 |
| Configuring a LAN Boot for a Service Profile Boot Definition | 284 |
| Configuring a Storage Boot for a Service Profile Boot Definition | 285 |
| Configuring a Virtual Media Boot for a Service Profile Boot Definition | 286 |
| Deleting a Boot Definition for a Service Profile | 287 |
| Associating a Service Profile with a Server or Server Pool | 288 |
| Disassociating a Service Profile from a Server or Server Pool | 288 |
| Resetting the UUID Assigned to a Service Profile from a Pool in a Service Profile Template | 289 |
| Resetting the MAC Address Assigned to a vNIC from a Pool in a Service Profile Template | 290 |
| Resetting the WWPN Assigned to a vHBA from a Pool in a Service Profile Template | 291 |
| Configuring Server Power Usage | 293 |
| Server Power Usage | 293 |
| Setting the Power Usage for a Server | 293 |
| Viewing Server Power Usage | 294 |
| VN-Link Configuration | 295 |
| Overview of VN-Link in Cisco UCS | 297 |
| Virtualization with a Virtual Interface Card Adapter | 297 |
| Cisco VN-Link | 297 |
| VN-Link in Hardware | 298 |
| Extension File for Communication with VMware vCenter | 298 |
| Distributed Virtual Switches | 299 |
| Port Profiles | 299 |
| Port Profile Clients | 300 |
| VN-Link in Hardware Considerations | 300 |
| Configuring Cisco UCS for VN-Link in Hardware | 300 |

| | |
|--|------------|
| Configuring VN-Link Components and Connectivity | 303 |
| Components of VN-Link in Hardware | 303 |
| Configuring a VMware ESX Host for VN-Link | 304 |
| Configuring a VMware vCenter Instance for VN-Link | 305 |
| Configuring a Certificate for VN-Link in Hardware | 306 |
| Certificate for VN-Link in Hardware | 306 |
| Copying a Certificate to the Fabric Interconnect | 306 |
| Creating a Certificate for VN-Link in Hardware | 307 |
| Deleting a Certificate for VN-Link in Hardware | 308 |
| Connecting Cisco UCS Manager to VMware vCenter Using the Extension Key | 308 |
| (Optional) Modifying the vCenter Extension Key | 308 |
| Exporting a vCenter Extension File from Cisco UCS Manager | 309 |
| Registering a vCenter Extension File in VMware vCenter | 310 |
| Configuring Distributed Virtual Switches in Cisco UCS | 311 |
| Distributed Virtual Switches | 311 |
| Configuring a Distributed Virtual Switch | 312 |
| Managing Distributed Virtual Switches | 313 |
| Adding a Folder to a vCenter | 313 |
| Deleting a Folder from a vCenter | 314 |
| Adding a Datacenter to a vCenter | 315 |
| Deleting a Datacenter from vCenter | 316 |
| Adding a Folder to a Datacenter | 316 |
| Deleting a Folder from a Datacenter | 317 |
| Adding a Distributed Virtual Switch to a Datacenter Folder | 318 |
| Deleting a Distributed Virtual Switch from a Datacenter Folder | 320 |
| Configuring Port Profiles | 323 |
| Port Profiles | 323 |
| Port Profile Clients | 323 |
| Configuring a Port Profile | 324 |
| Deleting a Port Profile | 326 |
| Adding a Named VLAN to a Port Profile | 326 |
| Deleting a Named VLAN from a Port Profile | 327 |
| Adding a Port Profile Client to a Port Profile | 328 |
| Deleting a Port Profile Client from a Port Profile | 329 |
| Configuring VN-Link Related Policies | 331 |

| | |
|--|------------|
| Dynamic vNIC Connection Policy | 331 |
| Configuring a Dynamic vNIC Connection Policy | 331 |
| Deleting a Dynamic vNIC Connection Policy | 332 |
| Managing Pending Deletions | 333 |
| Pending Deletions for VN-Link Tasks | 333 |
| Viewing Pending Deletions | 334 |
| Viewing Properties for a Pending Deletion | 334 |
| Deleting a Pending Deletion | 335 |
| Changing Properties for a Pending Deletion | 335 |
| System Management | 337 |
| Managing Time Zones | 339 |
| Time Zones | 339 |
| Setting the Time Zone | 339 |
| Configuring an NTP Server | 341 |
| Deleting an NTP Server | 341 |
| Setting the System Clock Manually | 342 |
| Managing the Chassis | 343 |
| Acknowledging a Chassis | 343 |
| Decommissioning a Chassis | 344 |
| Removing a Chassis | 344 |
| Recommissioning a Chassis | 345 |
| Toggling the Locator LED | 345 |
| Turning On the Locator LED for a Chassis | 345 |
| Turning Off the Locator LED for a Chassis | 346 |
| Managing the Servers | 347 |
| Booting a Server | 347 |
| Shutting Down a Server | 348 |
| Power Cycling a Server | 349 |
| Performing a Hard Reset on a Server | 349 |
| Acknowledging a Server | 350 |
| Removing a Server from a Chassis | 350 |
| Decommissioning a Server | 351 |
| Turning On the Locator LED for a Server | 351 |
| Turning Off the Locator LED for a Server | 351 |
| Resetting the CMOS for a Server | 352 |

| | |
|--|------------|
| Resetting the BMC for a Server | 352 |
| Recovering the Corrupt BIOS on a Server | 353 |
| Managing the I/O Modules | 355 |
| Resetting the IOM | 355 |
| Configuring Call Home | 357 |
| Call Home | 357 |
| Call Home Considerations and Guidelines | 359 |
| Cisco UCS Faults and Call Home Severity Levels | 360 |
| Cisco Smart Call Home | 361 |
| Configuring Call Home | 362 |
| Disabling Call Home | 363 |
| Enabling Call Home | 364 |
| Configuring System Inventory Messages | 364 |
| Configuring System Inventory Messages | 364 |
| Sending a System Inventory Message | 365 |
| Configuring Call Home Profiles | 366 |
| Call Home Profiles | 366 |
| Configuring a Call Home Profile | 366 |
| Deleting a Call Home Profile | 368 |
| Sending a Test Call Home Alert | 368 |
| Configuring Call Home Policies | 369 |
| Call Home Policies | 369 |
| Configuring a Call Home Policy | 370 |
| Disabling a Call Home Policy | 370 |
| Enabling a Call Home Policy | 371 |
| Deleting a Call Home Policy | 371 |
| Example: Configuring Call Home for Smart Call Home | 372 |
| Configuring Smart Call Home | 372 |
| Configuring the Default Cisco TAC-1 Profile | 374 |
| Configuring a System Inventory Message for Smart Call Home | 375 |
| Registering Smart Call Home | 376 |
| Backing Up and Restoring the Configuration | 377 |
| Backup and Export Configuration | 377 |
| Backup Types | 377 |
| Considerations and Recommendations for Backup Operations | 378 |

| | |
|--|------------|
| Import Configuration | 379 |
| Import Methods | 379 |
| System Restore | 379 |
| Required User Role for Backup and Import Operations | 379 |
| Backup Operations | 379 |
| Creating a Backup Operation | 379 |
| Running a Backup Operation | 381 |
| Modifying a Backup Operation | 381 |
| Deleting a Backup Operation | 383 |
| Import Operations | 383 |
| Creating an Import Operation | 383 |
| Running an Import Operation | 385 |
| Modifying an Import Operation | 385 |
| Deleting an Import Operation | 387 |
| Restoring the Configuration for a Fabric Interconnect | 387 |
| Erasing the Configuration | 389 |
| Managing the System Event Log | 391 |
| System Event Log | 391 |
| Viewing the System Event Log for a Server | 392 |
| Viewing the System Event Log from Exec Mode | 392 |
| Viewing the System Event Log from Chassis Server Mode | 392 |
| Configuring the SEL Policy | 393 |
| Backing Up the System Event Log for a Server | 395 |
| Backing Up the System Event Log from Exec Mode | 395 |
| Backing Up the System Event Log from Chassis Server Mode | 395 |
| Clearing the System Event Log for a Server | 396 |
| Clearing the System Event Log from Exec Mode | 396 |
| Clearing the System Event Log from Chassis Server Mode | 396 |
| Configuring Settings for Faults, Events, and Logs | 397 |
| Configuring Settings for the Fault Collection Policy | 397 |
| Fault Collection Policy | 397 |
| Configuring the Fault Collection Policy | 398 |
| Configuring Settings for the Core File Exporter | 398 |
| Core File Exporter | 398 |
| Configuring the Core File Exporter | 399 |

| | |
|---|------------|
| Disabling the Core File Exporter | 399 |
| Configuring the Syslog | 400 |
| Recovering a Lost Password | 403 |
| Password Recovery for the Admin Account | 403 |
| Determining the Leadership Role of a Fabric Interconnect | 403 |
| Recovering the Admin Account Password in a Standalone Configuration | 404 |
| Recovering the Admin Account Password in a Cluster Configuration | 405 |
| Configuring Statistics-Related Policies | 407 |
| Statistics Collection Policies | 407 |
| Statistics Collection Policy | 407 |
| Configuring a Statistics Collection Policy | 408 |
| Statistics Threshold Policies | 408 |
| Statistics Threshold Policy | 408 |
| Server and Server Component Statistics Threshold Policy Configuration | 409 |
| Configuring a Server and Server Component Statistics Threshold Policy | 409 |
| Deleting a Server and Server Component Statistics Threshold Policy | 410 |
| Configuring a Server and Server Component Statistics Threshold Policy Class | 410 |
| Deleting a Server and Server Component Statistics Threshold Policy Class | 412 |
| Uplink Ethernet Port Statistics Threshold Policy Configuration | 412 |
| Configuring an Uplink Ethernet Port Statistics Threshold Policy | 412 |
| Configuring an Uplink Ethernet Port Statistics Threshold Policy Class | 413 |
| Deleting an Uplink Ethernet Port Statistics Threshold Policy Class | 415 |
| Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Configuration | 415 |
| Configuring a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy | 415 |
| Configuring a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Class | 416 |
| Deleting a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Class | 417 |
| Fibre Channel Port Statistics Threshold Policy Configuration | 418 |
| Configuring a Fibre Channel Port Statistics Threshold Policy | 418 |
| Configuring a Fibre Channel Port Statistics Threshold Policy Class | 419 |
| Deleting an Uplink Fibre Channel Port Statistics Threshold Policy Class | 420 |



Preface

This preface includes the following sections:

- [Audience](#), page [xxi](#)
- [New and Changed Information for this Release](#), page [xxi](#)
- [Organization](#), page [xxiii](#)
- [Conventions](#), page [xxiv](#)
- [Related Documentation](#), page [xxv](#)
- [Documentation Feedback](#), page [xxv](#)
- [Obtaining Documentation and Submitting a Service Request](#), page [xxv](#)

Audience

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

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

New and Changed Information for this Release

The following tables provide an overview of the significant changes to this guide for this current release. The tables do not provide an exhaustive list of all changes made to the configuration guides or of the new features in this release. For information about new supported hardware in this release, see the *Release Notes for Cisco UCS Manager* available through the [Cisco UCS B-Series Servers Documentation Roadmap](#).

Table 1: New Features

| Feature | Description | Where Documented |
|---------------------------|--|---|
| Capability Catalog | The capability catalog is a set of tunable parameters, strings, and rules used to update the display and configurability of components such as newly qualified DIMMs and disk drives for servers. | Managing Firmware, page 113 |
| BIOS settings | Through Cisco UCS Manager you can create one or more BIOS policies that include a specific grouping of BIOS settings that match the needs of a server or set of servers, or you can configure the default BIOS settings for a specific server. | Configuring Server-Related Policies, page 217 |
| BIOS scrub | In the scrub policy, you can specify what happens to the BIOS settings on a server during discovery or service profile disassociation. | Configuring Server-Related Policies, page 217 |
| Server power usage | You can configure the level of power usage for each server in a Cisco UCS instance. | Configuring Server Power Usage, page 293 |
| Board controller firmware | Certain servers, such as the Cisco UCS B440 High Performance blade server, have board controller firmware that you can upgrade through host firmware packages in a service profile. | Managing Firmware, page 113 |
| Additional RAID options | The local disk configuration policy | Configuring Server-Related Policies, page 217 |

Table 2: Significant Changes in the June 2010 release

| Change | Description | Where Documented |
|---|--|---|
| BMC renamed to CIMC | The BMC component in the servers has been renamed Cisco Integrated Management Controller (CIMC). | Throughout the guide |
| Attribute for configuring remote authentication through RADIUS is now cisco-avpair. | The attribute you must create in the RADIUS remote authentication service and map to Cisco UCS user roles and locales is now cisco-avpair. | Configuring Primary Authentication, page 81 |

| Change | Description | Where Documented |
|----------------------------------|---|--|
| Chassis decommission and removal | The procedures to decommission and remove a chassis are now consistent with the equivalent server procedures. | Managing the Chassis, page 343 |
| Length of service profile name | A service profile name can be between 2 and 32 alphanumeric characters. | Configuring Service Profiles, page 271 |

Table 3: Significant Changes in the August 2010 release

| Change | Description | Where Documented |
|--|--|---|
| Uplink Ethernet port properties | The steps to configure the admin speed property of an uplink Ethernet port for 1Gbps or 10Gbps have been added. | Configuring Ports, page 59 |
| Local disk configuration policy guidelines | New guidelines for the Protect Configuration property of local disk configuration policies have been added. | Configuring Server-Related Policies, page 217 |
| MAC address table | Default value for the aging time in end-host mode has been changed to 14,500 seconds. | Configuring System-Related Policies, page 153 |
| Named VSANs | New guideline for the default FCoE VLAN when configuring a named VSAN for a FIP capable, converged network adapter has been added. | Configuring Named VSANs, page 193 |
| Viewing a boot policy | Command displays policy details. If you have not set a policy, the boot definition is displayed. | Configuring Server-Related Policies, page 217 |
| Viewing a local disk configuration policy | Command displays policy details. If you have not set a policy, the local disk configuration is displayed. | Configuring Server-Related Policies, page 217 |
| Viewing a serial over LAN policy | Command displays policy details. If you have not set a policy, the serial over LAN definition is displayed. | Configuring Server-Related Policies, page 217 |

Organization

This document includes the following parts:

| Part | Title | Description |
|--------|-----------------------|---|
| Part 1 | Introduction | Contains chapters that provide an overview of Cisco Unified Computing System (Cisco UCS) and Cisco UCS Manager. |
| Part 2 | System Configuration | Contains chapters that describe how to configure fabric interconnects, ports, communication services, primary authentication, and role-based access control configuration, and how to manage firmware and the capability catalog on a system. |
| Part 3 | Network Configuration | Contains chapters that describe how to configure named VLANs, LAN pin groups, MAC pools, and Quality of Service (QoS). |
| Part 4 | Storage Configuration | Contains chapters that describe how to configure named VSANs, SAN pin groups, and WWN pools. |
| Part 5 | Server Configuration | Contains chapters that describe how to configure server-related policies, server-related pools, service profiles, and server power usage. |
| Part 6 | System Management | Contains chapters that describe how to manage a Cisco UCS instance, including managing the chassis, servers, and I/O modules, and how to back up and restore the configuration. |

Conventions

This document uses the following conventions:

| Convention | Indication |
|---------------------------|---|
| bold font | Commands, keywords, GUI elements, and user-entered text appear in bold font . |
| <i>italic font</i> | Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> . |
| [] | Elements in square brackets are optional. |
| {x y z} | Required alternative keywords are grouped in braces and separated by vertical bars. |
| [x y z] | Optional alternative keywords are grouped in brackets and separated by vertical bars. |
| string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |
| <code>courier font</code> | Terminal sessions and information the system displays appear in <code>courier font</code> . |

| Convention | Indication |
|------------|---|
| < > | Nonprinting characters such as passwords are in angle brackets. |
| [] | Default responses to system prompts are in square brackets. |
| !, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line. |

**Note**

Means *reader take note*.

**Tip**

Means *the following information will help you solve a problem*.

**Caution**

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

**Timesaver**

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

**Warning**

Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.

Related Documentation

A roadmap that lists all documentation for Cisco Unified Computing System (Cisco UCS) is available at the following URL:

<http://www.cisco.com/go/unifiedcomputing/b-series-doc>

Documentation Feedback

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



PART **I**

Introduction

- [Overview of Cisco Unified Computing System, page 3](#)
- [Overview of Cisco UCS Manager, page 35](#)
- [Overview of Cisco UCS Manager CLI, page 39](#)



CHAPTER 1

Overview of Cisco Unified Computing System

This chapter includes the following sections:

- [About Cisco Unified Computing System](#) , page 3
- [Unified Fabric](#), page 4
- [Server Architecture and Connectivity](#), page 6
- [Traffic Management](#), page 23
- [Opt-In Features](#), page 27
- [Virtualization in Cisco UCS](#), page 29

About Cisco Unified Computing System

Cisco Unified Computing System (Cisco UCS) fuses access layer networking and servers. This high-performance, next-generation server system provides a data center with a high degree of workload agility and scalability.

The hardware and software components support Cisco's unified fabric, which runs multiple types of data center traffic over a single converged network adapter.

Architectural Simplification

The simplified architecture of Cisco UCS reduces the number of required devices and centralizes switching resources. By eliminating switching inside a chassis, network access-layer fragmentation is significantly reduced.

Cisco UCS implements Cisco unified fabric within racks and groups of racks, supporting Ethernet and Fibre Channel protocols over 10 Gigabit Cisco Data Center Ethernet and Fibre Channel over Ethernet (FCoE) links.

This radical simplification reduces the number of switches, cables, adapters, and management points by up to two-thirds. All devices in a Cisco UCS instance remain under a single management domain, which remains highly available through the use of redundant components.

High Availability

The management and data plane of Cisco UCS is designed for high availability and redundant access layer fabric interconnects. In addition, Cisco UCS supports existing high availability and disaster recovery solutions for the data center, such as data replication and application-level clustering technologies.

Scalability

A single Cisco UCS instance supports multiple chassis and their servers, all of which are administered through one Cisco UCS Manager. For more detailed information about the scalability, speak to your Cisco representative.

Flexibility

A Cisco UCS instance allows you to quickly align computing resources in the data center with rapidly changing business requirements. This built-in flexibility is determined by whether you choose to fully implement the stateless computing feature.

Pools of servers and other system resources can be applied as necessary to respond to workload fluctuations, support new applications, scale existing software and business services, and accommodate both scheduled and unscheduled downtime. Server identity can be abstracted into a mobile service profile that can be moved from server to server with minimal downtime and no need for additional network configuration.

With this level of flexibility, you can quickly and easily scale server capacity without having to change the server identity or reconfigure the server, LAN, or SAN. During a maintenance window, you can quickly do the following:

- Deploy new servers to meet unexpected workload demand and rebalance resources and traffic.
- Shut down an application, such as a database management system, on one server and then boot it up again on another server with increased I/O capacity and memory resources.

Optimized for Server Virtualization

Cisco UCS has been optimized to implement VN-Link technology. This technology provides improved support for server virtualization, including better policy-based configuration and security, conformance with a company's operational model, and accommodation for VMware's VMotion.

Unified Fabric

With unified fabric, multiple types of data center traffic can run over a single Data Center Ethernet (DCE) network. Instead of having a series of different host bus adapters (HBAs) and network interface cards (NICs) present in a server, unified fabric uses a single converged network adapter. This type of adapter can carry LAN and SAN traffic on the same cable.

Cisco UCS uses Fibre Channel over Ethernet (FCoE) to carry Fibre Channel and Ethernet traffic on the same physical Ethernet connection between the fabric interconnect and the server. This connection terminates at a converged network adapter on the server, and the unified fabric terminates on the uplink ports of the fabric interconnect. On the core network, the LAN and SAN traffic remains separated. Cisco UCS does not require that you implement unified fabric across the data center.

The converged network adapter presents an Ethernet interface and Fibre Channel interface to the operating system. At the server, the operating system is not aware of the FCoE encapsulation because it sees a standard Fibre Channel HBA.

At the fabric interconnect, the server-facing Ethernet port receives the Ethernet and Fibre Channel traffic. The fabric interconnect (using Ethertype to differentiate the frames) separates the two traffic types. Ethernet frames and Fibre Channel frames are switched to their respective uplink interfaces.

Fibre Channel over Ethernet

Cisco UCS leverages Fibre Channel over Ethernet (FCoE) standard protocol to deliver Fibre Channel. The upper Fibre Channel layers are unchanged, so the Fibre Channel operational model is maintained. FCoE network management and configuration is similar to a native Fibre Channel network.

FCoE encapsulates Fibre Channel traffic over a physical Ethernet link. FCoE is encapsulated over Ethernet with the use of a dedicated Ethertype, 0x8906, so that FCoE traffic and standard Ethernet traffic can be carried on the same link. FCoE has been standardized by the ANSI T11 Standards Committee.

Fibre Channel traffic requires a lossless transport layer. Instead of the buffer-to-buffer credit system used by native Fibre Channel, FCoE depends upon the Ethernet link to implement lossless service.

Ethernet links on the fabric interconnect provide two mechanisms to ensure lossless transport for FCoE traffic:

- Link-level flow control
- Priority flow control

Link-Level Flow Control

IEEE 802.3x link-level flow control allows a congested receiver to signal the endpoint to pause data transmission for a short time. This link-level flow control pauses all traffic on the link.

The transmit and receive directions are separately configurable. By default, link-level flow control is disabled for both directions.

On each Ethernet interface, the fabric interconnect can enable either priority flow control or link-level flow control (but not both).

Priority Flow Control

The priority flow control (PFC) feature applies pause functionality to specific classes of traffic on the Ethernet link. For example, PFC can provide lossless service for the FCoE traffic, and best-effort service for the standard Ethernet traffic. PFC can provide different levels of service to specific classes of Ethernet traffic (using IEEE 802.1p traffic classes).

PFC decides whether to apply pause based on the IEEE 802.1p CoS value. When the fabric interconnect enables PFC, it configures the connected adapter to apply the pause functionality to packets with specific CoS values.

By default, the fabric interconnect negotiates to enable the PFC capability. If the negotiation succeeds, PFC is enabled and link-level flow control remains disabled (regardless of its configuration settings). If the PFC negotiation fails, you can either force PFC to be enabled on the interface or you can enable IEEE 802.x link-level flow control.

Server Architecture and Connectivity

Overview of Service Profiles

Service profiles are the central concept of Cisco UCS. Each service profile serves a specific purpose: ensuring that the associated server hardware has the configuration required to support the applications it will host.

The service profile maintains configuration information about the server hardware, interfaces, fabric connectivity, and server and network identity. This information is stored in a format that you can manage through Cisco UCS Manager. All service profiles are centrally managed and stored in a database on the fabric interconnect.

Every server must be associated with a service profile.



Important At any given time, each server can be associated with only one service profile. Similarly, each service profile can be associated with only one server at a time.

After you associate a service profile with a server, the server is ready to have an operating system and applications installed, and you can use the service profile to review the configuration of the server. If the server associated with a service profile fails, the service profile does not automatically fail over to another server.

When a service profile is disassociated from a server, the identity and connectivity information for the server is reset to factory defaults.

Network Connectivity through Service Profiles

Each service profile specifies the LAN and SAN network connections for the server through the Cisco UCS infrastructure and out to the external network. You do not need to manually configure the network connections for Cisco UCS servers and other components. All network configuration is performed through the service profile.

When you associate a service profile with a server, the Cisco UCS internal fabric is configured with the information in the service profile. If the profile was previously associated with a different server, the network infrastructure reconfigures to support identical network connectivity to the new server.

Configuration through Service Profiles

A service profile can take advantage of resource pools and policies to handle server and connectivity configuration.

Hardware Components Configured by Service Profiles

When a service profile is associated with a server, the following components are configured according to the data in the profile:

- Server, including BIOS and CIMC
- Adapters
- Fabric interconnects

You do not need to configure these hardware components directly.

Server Identity Management through Service Profiles

You can use the network and device identities burned into the server hardware at manufacture or you can use identities that you specify in the associated service profile either directly or through identity pools, such as MAC, WWN, and UUID.

The following are examples of configuration information that you can include in a service profile:

- Profile name and description
- Unique server identity (UUID)
- LAN connectivity attributes, such as the MAC address
- SAN connectivity attributes, such as the WWN

Operational Aspects configured by Service Profiles

You can configure some of the operational functions for a server in a service profile, such as the following:

- Firmware packages and versions
- Operating system boot order and configuration
- IPMI and KVM access

vNIC Configuration by Service Profiles

A vNIC is a virtualized network interface that is configured on a physical network adapter and appears to be a physical NIC to the operating system of the server. The type of adapter in the system determines how many vNICs you can create. For example, a converged network adapter has two NICs, which means you can create a maximum of two vNICs for each adapter.

A vNIC communicates over Ethernet and handles LAN traffic. At a minimum, each vNIC must be configured with a name and with fabric and network connectivity.

vHBA Configuration by Service Profiles

A vHBA is a virtualized host bus adapter that is configured on a physical network adapter and appears to be a physical HBA to the operating system of the server. The type of adapter in the system determines how many vHBAs you can create. For example, a converged network adapter has two HBAs, which means you can create a maximum of two vHBAs for each of those adapters. In contrast, a network interface card does not have any HBAs, which means you cannot create any vHBAs for those adapters.

A vHBA communicates over FCoE and handles SAN traffic. At a minimum, each vHBA must be configured with a name and fabric connectivity.

Service Profiles that Override Server Identity

This type of service profile provides the maximum amount of flexibility and control. This profile allows you to override the identity values that are on the server at the time of association and use the resource pools and policies set up in Cisco UCS Manager to automate some administration tasks.

You can disassociate this service profile from one server and then associate it with another server. This re-association can be done either manually or through an automated server pool policy. The burned-in settings,

such as UUID and MAC address, on the new server are overwritten with the configuration in the service profile. As a result, the change in server is transparent to your network. You do not need to reconfigure any component or application on your network to begin using the new server.

This profile allows you to take advantage of and manage system resources through resource pools and policies, such as the following:

- Virtualized identity information, including pools of MAC addresses, WWN addresses, and UUIDs
- Ethernet and Fibre Channel adapter profile policies
- Firmware package policies
- Operating system boot order policies

Service Profiles that Inherit Server Identity

This hardware-based service profile is the simplest to use and create. This profile uses the default values in the server and mimics the management of a rack-mounted server. It is tied to a specific server and cannot be moved to another server.

You do not need to create pools or configuration policies to use this service profile.

This service profile inherits and applies the identity and configuration information that is present at the time of association, such as the following:

- MAC addresses for the two NICs
- For a converged network adapter or a virtual interface card, the WWN addresses for the two HBAs
- BIOS versions
- Server UUID



Important

The server identity and configuration information inherited through this service profile may not be the values burned into the server hardware at manufacture if those values were changed before this profile is associated with the server.

Service Profile Templates

With a service profile template, you can quickly create several service profiles with the same basic parameters, such as the number of vNICs and vHBAs, and with identity information drawn from the same pools.



Tip

If you need only one service profile with similar values to an existing service profile, you can clone a service profile in the Cisco UCS Manager GUI.

For example, if you need several service profiles with similar values to configure servers to host database software, you can create a service profile template, either manually or from an existing service profile. You then use the template to create the service profiles.

Cisco UCS supports the following types of service profile templates:

- Initial template** Service profiles created from an initial template inherit all the properties of the template. However, after you create the profile, it is no longer connected to the template. If you need to make changes to one or more profiles created from this template, you must change each profile individually.
- Updating template** Service profiles created from an updating template inherit all the properties of the template and remain connected to the template. Any changes to the template automatically update the service profiles created from the template.

Policies

Policies determine how Cisco UCS components will act in specific circumstances. You can create multiple instances of most policies. For example, you might want different boot policies, so that some servers can PXE boot, some can SAN boot, and others can boot from local storage.

Policies allow separation of functions within the system. A subject matter expert can define policies that are used in a service profile, which is created by someone without that subject matter expertise. For example, a LAN administrator can create adapter policies and quality of service policies for the system. These policies can then be used in a service profile that is created by someone who has limited or no subject matter expertise with LAN administration.

You can create and use two types of policies in Cisco UCS Manager:

- Configuration policies that configure the servers and other components
- Operational policies that control certain management, monitoring, and access control functions

Configuration Policies

Boot Policy

The boot policy determines the following:

- Configuration of the boot device
- Location from which the server boots
- Order in which boot devices are invoked

For example, you can choose to have associated servers boot from a local device, such as a local disk or CD-ROM (VMedia), or you can select a SAN boot or a LAN (PXE) boot.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect. If you do not include a boot policy in a service profile, the server uses the default settings in the BIOS to determine the boot order.



Important

Changes to a boot policy may be propagated to all servers created with an updating service profile template that includes that boot policy. Reassociation of the service profile with the server to rewrite the boot order information in the BIOS is auto-triggered.

Guidelines

When you create a boot policy, you can add one or more of the following to the boot policy and specify their boot order:

| Boot type | Description |
|--------------------|---|
| SAN boot | Boots from an operating system image on the SAN. You can specify a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary. We recommend that you use a SAN boot, because it offers the most service profile mobility within the system. If you boot from the SAN when you move a service profile from one server to another, the new server boots from the exact same operating system image. Therefore, the new server appears to be the exact same server to the network. |
| LAN boot | Boots from a centralized provisioning server. It is frequently used to install operating systems on a server from that server. |
| Local disk boot | If the server has a local drive, boots from that drive. Note Cisco UCS Manager does not differentiate between the types of local drives. If an operating system has been installed on more than one local drive or on an internal USB drive (eUSB), you cannot specify which of these local drives the server should use as the boot drive. |
| Virtual media boot | Mimics the insertion of a physical CD-ROM disk (read-only) or floppy disk (read-write) into a server. It is typically used to manually install operating systems on a server. |



Note The default boot order is as follows:

- 1 Local disk boot
- 2 LAN boot
- 3 Virtual media read-only boot
- 4 Virtual media read-write boot

Chassis Discovery Policy

The chassis discovery policy determines how the system reacts when you add a new chassis. Cisco UCS Manager uses the settings in the chassis discovery policy to determine the minimum threshold for the number of links between the chassis and the fabric interconnect. However, the configuration in the chassis discovery policy does not prevent you from connecting multiple chassis to the fabric interconnects in a Cisco UCS instance and wiring those chassis with a different number of links.

If you have a Cisco UCS instance that has some chassis wired with 1 link, some with 2 links, and some with 4 links, we recommend that you configure the chassis discovery policy for the minimum number links in the

instance so that Cisco UCS Manager can discover all chassis. After the initial discovery, you must reacknowledge the chassis that are wired for a greater number of links and Cisco UCS Manager configures the chassis to use all available links.

Cisco UCS Manager cannot discover any chassis that is wired for fewer links than are configured in the chassis discovery policy. For example, if the chassis discovery policy is configured for 4 links, Cisco UCS Manager cannot discover any chassis that is wired for 1 link or 2 links. Reacknowledgement of the chassis does not resolve this issue.

The following table provides an overview of how the chassis discovery policy works in a multi-chassis Cisco UCS instance:

Table 4: Chassis Discovery Policy and Chassis Links

| Number of Links Wired for the Chassis | 1-Link Chassis Discovery Policy | 2-Link Chassis Discovery Policy | 4-Link Chassis Discovery Policy |
|---|--|---|--|
| 1 link between IOM and fabric interconnects | Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 1 link. | Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS instance. | Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS instance. |
| 2 links between IOM and fabric interconnects | Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 1 link. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links. | Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 2 link. | Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS instance. |
| 4 links between IOM and fabric interconnects | Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 1 link. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links. | Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 2 links. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links. | Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 4 link. |

Dynamic vNIC Connection Policy

This policy determines how the VN-link connectivity between VMs and dynamic vNICs is configured. This policy is required for Cisco UCS instances that include servers with virtual interface card adapters on which you have installed VMs and configured dynamic vNICs.

Each Dynamic vNIC connection policy must include an adapter policy and designate the number of vNICs that can be configured for any server associated with a service profile that includes the policy.

Ethernet and Fibre Channel Adapter Policies

These policies govern the host-side behavior of the adapter, including how the adapter handles traffic. For example, you can use these policies to change default settings for the following:

- Queues
- Interrupt handling
- Performance enhancement
- RSS hash
- Failover in a cluster configuration with two fabric interconnects



Note

For Fibre Channel adapter policies, the values displayed by Cisco UCS Manager may not match those displayed by applications such as QLogic SANsurfer. For example, the following values may result in an apparent mismatch between SANsurfer and Cisco UCS Manager:

- Max LUNs Per Target—SANsurfer has a maximum of 256 LUNs and does not display more than that number. Cisco UCS Manager supports a higher maximum number of LUNs.
- Link Down Timeout—In SANsurfer, you configure the timeout threshold for link down in seconds. In Cisco UCS Manager, you configure this value in milliseconds. Therefore, a value of 5500 ms in Cisco UCS Manager displays as 5s in SANsurfer.
- Max Data Field Size—SANsurfer has allowed values of 512, 1024, and 2048. Cisco UCS Manager allows you to set values of any size. Therefore, a value of 900 in Cisco UCS Manager displays as 512 in SANsurfer.

Operating System Specific Adapter Policies

By default, Cisco UCS provides a set of Ethernet adapter policies and Fibre Channel adapter policies. These policies include the recommended settings for each supported server operating system. Operating systems are sensitive to the settings in these policies. Storage vendors typically require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.

**Important**

We recommend that you use the values in these policies for the applicable operating system. Do not modify any of the values in the default policies unless directed to do so by Cisco Technical Support.

However, if you are creating an Ethernet adapter policy for a Windows OS (instead of using the default Windows adapter policy), you must use the following formulas to calculate values that work with Windows:

$$\text{Completion Queues} = \text{Transmit Queues} + \text{Receive Queues}$$
$$\text{Interrupt Count} = (\text{Completion Queues} + 2) \text{ rounded up to nearest power of } 2$$

For example, if Transmit Queues = 1 and Receive Queues = 8 then:

$$\text{Completion Queues} = 1 + 8 = 9$$
$$\text{Interrupt Count} = (9 + 2) \text{ rounded up to the nearest power of } 2 = 16$$

Host Firmware Package

This policy enables you to specify a set of firmware versions that make up the host firmware package (also known as the host firmware pack). The host firmware includes the following firmware for server and adapter endpoints:

- **Adapter Firmware Packages**
- **Storage Controller Firmware Packages**
- **Fibre Channel Adapters Firmware Packages**
- **BIOS Firmware Packages**
- **HBA Option ROM Packages**
- **Board Controller Packages**

**Tip**

You can include more than one type of firmware in the same host firmware package. For example, a host firmware package can include both BIOS firmware and storage controller firmware or adapter firmware for two different models of adapters. However, you can only have one firmware version with the same type, vendor, and model number. The system recognizes which firmware version is required for an endpoint and ignores all other firmware versions.

The firmware package is pushed to all servers associated with service profiles that include this policy.

This policy ensures that the host firmware is identical on all servers associated with service profiles which use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained. Also, if you change the firmware version for an endpoint in the firmware package, new versions are applied to all the affected service profiles immediately, which could cause server reboots.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

Prerequisites

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect. If the firmware image is not available when Cisco UCS

Manager is associating a server with a service profile, Cisco UCS Manager ignores the firmware upgrade and completes the association.

IPMI Access Profile

This policy allows you to determine whether IPMI commands can be sent directly to the server, using the IP address. For example, you can send commands to retrieve sensor data from the CIMC. This policy defines the IPMI access, including a username and password that can be authenticated locally on the server, and whether the access is read-only or read-write.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Local Disk Configuration Policy

This policy configures any optional SAS local drives that have been installed on a server through the onboard RAID controller of the local drive. This policy enables you to set a local disk mode for all servers that are associated with a service profile that includes the local disk configuration policy.

The local disk modes include the following:

- **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes.
- **No Local Storage**—For a diskless server or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk.
- **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.
- **RAID 1 Mirrored**—Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives.
- **RAID10 Mirrored and Striped**—RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.
- **RAID 0 Stripes**—Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails.
- **RAID 6 Stripes Dual Parity**—Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.
- **RAID 5 Striped Parity**—Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.

You must include this policy in a service profile, and that service profile must be associated with a server for the policy to take effect.

Management Firmware Package

This policy enables you to specify a set of firmware versions that make up the management firmware package (also known as a management firmware pack). The management firmware package includes the Cisco Integrated Management Controller (CIMC) on the server. You do not need to use this package if you upgrade the CIMC directly.

The firmware package is pushed to all servers associated with service profiles that include this policy. This policy ensures that the CIMC firmware is identical on all servers associated with service profiles which use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Network Control Policy

This policy configures the network control settings for the Cisco UCS instance, including the following:

- Whether the Cisco Discovery Protocol (CDP) is enabled or disabled
- How the VIF behaves if no uplink port is available in end-host mode
- Whether the server can use different MAC addresses when sending packets to the fabric interconnect

The network control policy also determines the action that Cisco UCS Manager takes on the remote Ethernet port or the vEthernet interface when the associated border port fails. By default, the **Action on Uplink Fail** property in the network control policy is configured with a value of link-down. This default behavior directs Cisco UCS Manager to bring the remote Ethernet or vEthernet port down if the border port fails.



Note

The default behaviour of the **Action on Uplink Fail** property is optimal for most Cisco UCS that support link failover at the adapter level or only carry Ethernet traffic. However, for those converged network adapters that support both Ethernet and Fibre Channel traffic, such as the Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, the default behavior can affect and interrupt Fibre Channel traffic as well. Therefore, if the server includes one of those converged network adapters and the the adapter is expected to handle both Ethernet and Fibre Channel traffic, we recommend that you configure the **Action on Uplink Fail** property with a value of warning. Please note that this configuration may result in an Ethernet teaming driver not being able to detect a link failure when the border port goes down.

Power Policy

The power policy is a global policy that specifies the redundancy for power supplies in all chassis in the Cisco UCS instance. This policy is also known as the PSU policy.

For more information about power supply redundancy, see *Cisco UCS 5108 Server Chassis Hardware Installation Guide*.

Quality of Service Policy

A quality of service (QoS) policy assigns a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic. For certain adapters you can also specify additional controls on the outgoing traffic, such as burst and rate.

You must include a QoS policy in a vNIC policy or vHBA policy and then include that policy in a service profile to configure the vNIC or vHBA.

Server Autoconfiguration Policy

Cisco UCS Manager uses this policy to determine how to configure a new server. If you create a server autoconfiguration policy, the following occurs when a new server starts:

- 1 The qualification in the server autoconfiguration policy is executed against the server.
- 2 If the server meets the required qualifications, the server is associated with a service profile created from the service profile template configured in the server autoconfiguration policy. The name of that service profile is based on the name given to the server by Cisco UCS Manager.
- 3 The service profile is assigned to the organization configured in the server autoconfiguration policy.

Server Discovery Policy

This discovery policy determines how the system reacts when you add a new server. If you create a server discovery policy, you can control whether the system conducts a deep discovery when a server is added to a chassis, or whether a user must first acknowledge the new server. By default, the system conducts a full discovery.

If you create a server discovery policy, the following occurs when a new server starts:

- 1 The qualification in the server discovery policy is executed against the server.
- 2 If the server meets the required qualifications, Cisco UCS Manager applies the following to the server:
 - Depending upon the option selected for the action, either discovers the new server immediately or waits for a user to acknowledge the new server
 - Applies the scrub policy to the server

Server Inheritance Policy

This policy is invoked during the server discovery process to create a service profile for the server. All service profiles created from this policy use the values burned into the blade at manufacture. The policy performs the following:

- Analyzes the inventory of the server
- If configured, assigns the server to the selected organization
- Creates a service profile for the server with the identity burned into the server at manufacture

You cannot migrate a service profile created with this policy to another server.

Server Pool Policy

This policy is invoked during the server discovery process. It determines what happens if server pool policy qualifications match a server to the target pool specified in the policy.

If a server qualifies for more than one pool and those pools have server pool policies, the server is added to all those pools.

Server Pool Policy Qualifications

This policy qualifies servers based on the inventory of a server conducted during the discovery process. The qualifications are individual rules that you configure in the policy to determine whether a server meets the selection criteria. For example, you can create a rule that specifies the minimum memory capacity for servers in a data center pool.

Qualifications are used in other policies to place servers, not just by the server pool policies. For example, if a server meets the criteria in a qualification policy, it can be added to one or more server pools or have a service profile automatically associated with it.

You can use the server pool policy qualifications to qualify servers according to the following criteria:

- Adapter type
- Chassis location
- Memory type and configuration
- CPU cores, type, and configuration
- Storage configuration and capacity
- Server model

Depending upon the implementation, you may configure several policies with server pool policy qualifications including the following:

- Autoconfiguration policy
- Chassis discovery policy
- Server discovery policy
- Server inheritance policy
- Server pool policy

vHBA Template

This template is a policy that defines how a vHBA on a server connects to the SAN. It is also referred to as a vHBA SAN connectivity template.

You need to include this policy in a service profile for it to take effect.

VM Lifecycle Policy

The VM lifecycle policy determines how long Cisco UCS Manager retains offline VMs and offline dynamic vNICs in its database. If a VM or dynamic vNIC remains offline after that period, Cisco UCS Manager deletes the object from its database.

All virtual machines (VMs) on Cisco UCS servers are managed by vCenter. Cisco UCS Manager cannot determine whether an inactive VM is temporarily shutdown, has been deleted, or is in some other state that renders it inaccessible. Therefore, Cisco UCS Manager considers all inactive VMs to be in an offline state.

Cisco UCS Manager considers a dynamic vNIC to be offline when the associated VM is shutdown, or the link between the fabric interconnect and the I/O module fails. On rare occasions, an internal error can also cause Cisco UCS Manager to consider a dynamic vNIC to be offline.

The default VM and dynamic vNIC retention period is 15 minutes. You can set that for any period of time between 1 minute and 7200 minutes (or 5 days).

**Note**

The VMs that Cisco UCS Manager displays are for information and monitoring only. You cannot manage VMs through Cisco UCS Manager. Therefore, when you delete a VM from the Cisco UCS Manager database, you do not delete the VM from the server or from vCenter.

vNIC Template

This policy defines how a vNIC on a server connects to the LAN. This policy is also referred to as a vNIC LAN connectivity policy.

You need to include this policy in a service profile for it to take effect.

vNIC/vHBA Placement Policies

vNIC/vHBA placement policies are used to assign vNICs or vHBAs to the physical adapters on a server. Each vNIC/vHBA placement policy contains two virtual network interface connections (vCons) that are virtual representations of the physical adapters. When a vNIC/vHBA placement policy is assigned to a service profile, and the service profile is associated to a server, the vCons in the vNIC/vHBA placement policy are assigned to the physical adapters. For servers with only one adapter, both vCons are assigned to the adapter; for servers with two adapters, one vCon is assigned to each adapter.

You can assign vNICs or vHBAs to either of the two vCons, and they are then assigned to the physical adapters based on the vCon assignment during server association. Additionally, vCons use the following selection preference criteria to assign vHBAs and vNICs:

| | |
|---------------------------|---|
| All | The vCon is used for vNICs or vHBAs assigned to it, vNICs or vHBAs not assigned to either vCon, and dynamic vNICs or vHBAs. |
| Assigned-Only | The vCon is reserved for only vNICs or vHBAs assigned to it. |
| Exclude-Dynamic | The vCon is not used for dynamic vNICs or vHBAs. |
| Exclude-Unassigned | The vCon is not used for vNICs or vHBAs not assigned to the vCon. The vCon is used for dynamic vNICs and vHBAs. |

For servers with two adapters, if you do not include a vNIC/vHBA placement policy in a service profile, or you do not configure vCons for a service profile, Cisco UCS equally distributes the vNICs and vHBAs between the two adapters.

Operational Policies**Fault Collection Policy**

The fault collection policy controls the lifecycle of a fault in a Cisco UCS instance, including when faults are cleared, the flapping interval (the length of time between the fault being raised and the condition being cleared), and the retention interval (the length of time a fault is retained in the system).

A fault in Cisco UCS has the following lifecycle:

- 1 A condition occurs in the system and Cisco UCS Manager raises a fault. This is the active state.
- 2 When the fault is alleviated, it is cleared if the time between the fault being raised and the condition being cleared is greater than the flapping interval, otherwise, the fault remains raised but its status changes to soaking-clear. Flapping occurs when a fault is raised and cleared several times in rapid succession. During the flapping interval the fault retains its severity for the length of time specified in the fault collection policy.
- 3 If the condition reoccurs during the flapping interval, the fault remains raised and its status changes to flapping. If the condition does not reoccur during the flapping interval, the fault is cleared.
- 4 When a fault is cleared, it is deleted if the clear action is set to delete, or if the fault was previously acknowledged; otherwise, it is retained until either the retention interval expires, or if the fault is acknowledged.
- 5 If the condition reoccurs during the retention interval, the fault returns to the active state. If the condition does not reoccur, the fault is deleted.

Flow Control Policy

Flow control policies determine whether the uplink Ethernet ports in a Cisco UCS instance send and receive IEEE 802.3x pause frames when the receive buffer for a port fills. These pause frames request that the transmitting port stop sending data for a few milliseconds until the buffer clears.

For flow control to work between a LAN port and an uplink Ethernet port, you must enable the corresponding receive and send flow control parameters for both ports. For Cisco UCS, the flow control policies configure these parameters.

When you enable the send function, the uplink Ethernet port sends a pause request to the network port if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels. If you enable the receive function, the uplink Ethernet port honors all pause requests from the network port. All traffic is halted on that uplink port until the network port cancels the pause request.

Because you assign the flow control policy to the port, changes to the policy have an immediate effect on how the port reacts to a pause frame or a full receive buffer.

Scrub Policy

This policy determines what happens to local data and to the BIOS settings on a server during the discovery process and when the server is disassociated from a service profile. Depending upon how you configure a scrub policy, the following can occur at those times:

Disk Scrub

One of the following occurs to the data on any local drives on disassociation:

- If enabled, destroys all data on any local drives
- If disabled, preserves all data on any local drives, including local storage configuration

BIOS Settings Scrub

One of the following occurs to the BIOS settings when a service profile containing the scrub policy is disassociated from a server:

- If enabled, erases all BIOS settings for the server and resets them to the BIOS defaults for that server type and vendor
- If disabled, preserves the existing BIOS settings on the server

Serial over LAN Policy

This policy sets the configuration for the serial over LAN connection for all servers associated with service profiles that use the policy. By default, the serial over LAN connection is disabled.

If you implement a serial over LAN policy, we recommend that you also create an IPMI profile.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Statistics Collection Policy

A statistics collection policy defines how frequently statistics are to be collected (collection interval) and how frequently the statistics are to be reported (reporting interval). Reporting intervals are longer than collection intervals so that multiple statistical data points can be collected during the reporting interval, which provides Cisco UCS Manager with sufficient data to calculate and report minimum, maximum, and average values.

For NIC statistics, Cisco UCS Manager displays the average, minimum, and maximum of the change since the last collection of statistics. If the values are 0, there has been no change since the last collection.

Statistics can be collected and reported for the following five functional areas of the Cisco UCS system:

- Adapter—statistics related to the adapters
- Chassis—statistics related to the blade chassis
- Host—this policy is a placeholder for future support
- Port—statistics related to the ports, including server ports, uplink Ethernet ports, and uplink Fibre Channel ports
- Server—statistics related to servers



Note

Cisco UCS Manager has one default statistics collection policy for each of the five functional areas. You cannot create additional statistics collection policies and you cannot delete the existing default policies. You can only modify the default policies.

Statistics Threshold Policy

A statistics threshold policy monitors statistics about certain aspects of the system and generates an event if the threshold is crossed. You can set both minimum and maximum thresholds. For example, you can configure the policy to raise an alarm if the CPU temperature exceeds a certain value, or if a server is overutilized or underutilized.

These threshold policies do not control the hardware or device-level thresholds enforced by endpoints, such as the CIMC. Those thresholds are burned in to the hardware components at manufacture.

Cisco UCS enables you to configure statistics threshold policies for the following components:

- Servers and server components
- Uplink Ethernet ports
- Ethernet server ports, chassis, and fabric interconnects
- Fibre Channel port

**Note**

You cannot create or delete a statistics threshold policy for Ethernet server ports, uplink Ethernet ports, or uplink Fibre Channel ports. You can only configure the existing default policy.

Pools

Pools are collections of identities, or physical or logical resources, that are available in the system. All pools increase the flexibility of service profiles and allow you to centrally manage your system resources.

You can use pools to segment unconfigured servers or available ranges of server identity information into groupings that make sense for the data center. For example, if you create a pool of unconfigured servers with similar characteristics and include that pool in a service profile, you can use a policy to associate that service profile with an available, unconfigured server.

If you pool identifying information, such as MAC addresses, you can pre-assign ranges for servers that will host specific applications. For example, all database servers could be configured within the same range of MAC addresses, UUIDs, and WWNs.

Server Pools

A server pool contains a set of servers. These servers typically share the same characteristics. Those characteristics can be their location in the chassis, or an attribute such as server type, amount of memory, local storage, type of CPU, or local drive configuration. You can manually assign a server to a server pool, or use server pool policies and server pool policy qualifications to automate the assignment.

If your system implements multi-tenancy through organizations, you can designate one or more server pools to be used by a specific organization. For example, a pool that includes all servers with two CPUs could be assigned to the Marketing organization, while all servers with 64 GB memory could be assigned to the Finance organization.

A server pool can include servers from any chassis in the system. A given server can belong to multiple server pools.

MAC Pools

A MAC pool is a collection of network identities, or MAC addresses, that are unique in their layer 2 environment and are available to be assigned to vNICs on a server. If you use MAC pools in service profiles, you do not have to manually configure the MAC addresses to be used by the server associated with the service profile.

In a system that implements multi-tenancy, you can use the organizational hierarchy to ensure that MAC pools can only be used by specific applications or business services. Cisco UCS Manager uses the name resolution policy to assign MAC addresses from the pool.

To assign a MAC address to a server, you must include the MAC pool in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server.

You can specify your own MAC addresses or use a group of MAC addresses provided by Cisco.

UUID Suffix Pools

A UUID suffix pool is a collection of SMBIOS UUIDs that are available to be assigned to servers. The first number of digits that constitute the prefix of the UUID are fixed. The remaining digits, the UUID suffix, are

variable. A UUID suffix pool ensures that these variable values are unique for each server associated with a service profile which uses that particular pool to avoid conflicts.

If you use UUID suffix pools in service profiles, you do not have to manually configure the UUID of the server associated with the service profile.

WWN Pools

A WWN pool is a collection of WWNs for use by the Fibre Channel vHBAs in a Cisco UCS instance. You create separate pools for the following:

- WW node names assigned to the server
- WW port names assigned to the vHBA



Important

A WWN pool can include only WWNNs or WWPNS in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNS in the SAN fabric, we recommend that you use the following WWN prefix for all blocks in a pool:
20:00:00:25:B5:XX:XX:XX

If you use WWN pools in service profiles, you do not have to manually configure the WWNs that will be used by the server associated with the service profile. In a system that implements multi-tenancy, you can use a WWN pool to control the WWNs used by each organization.

You assign WWNs to pools in blocks. For each block or individual WWN, you can assign a boot target.

WWNN Pools

A WWNN pool is a WWN pool that contains only WW node names. If you include a pool of WWNNs in a service profile, the associated server is assigned a WWNN from that pool.

WWPN Pools

A WWPN pool is a WWN pool that contains only WW port names. If you include a pool of WWPNS in a service profile, the port on each vHBA of the associated server is assigned a WWPN from that pool.

Management IP Pool

The management IP pool is a collection of external IP addresses. Cisco UCS Manager reserves each block of IP addresses in the management IP pool for external access that terminates in the Cisco Integrated Management Controller (CIMC) on a server.

Cisco UCS Manager uses the IP addresses in a management IP pool for external access to a server through the following:

- KVM console
- Serial over LAN
- IPMI

Traffic Management

Oversubscription

Oversubscription occurs when multiple network devices are connected to the same fabric interconnect port. This practice optimizes fabric interconnect use, since ports rarely run at maximum speed for any length of time. As a result, when configured correctly, oversubscription allows you to take advantage of unused bandwidth. However, incorrectly configured oversubscription can result in contention for bandwidth and a lower quality of service to all services that use the oversubscribed port.

For example, oversubscription can occur if four servers share a single uplink port, and all four servers attempt to send data at a cumulative rate higher than available bandwidth of uplink port.

Oversubscription Considerations

The following elements can impact how you configure oversubscription in a Cisco UCS instance:

Ratio of Server-Facing Ports to Uplink Ports

You need to know what how many server-facing ports and uplink ports are in the system, because that ratio can impact performance. For example, if your system has twenty ports that can communicate down to the servers and only two ports that can communicate up to the network, your uplink ports will be oversubscribed. In this situation, the amount of traffic created by the servers can also affect performance.

Number of Uplink Ports from Fabric Interconnect to Network

You can choose to add more uplink ports between the Cisco UCS fabric interconnect and the upper layers of the LAN to increase bandwidth. In Cisco UCS, you must have at least one uplink port per fabric interconnect to ensure that all servers and NICs to have access to the LAN. The number of LAN uplinks should be determined by the aggregate bandwidth needed by all Cisco UCS servers.

FC uplink ports are available on the expansion slots only. You must add more expansion slots to increase number of available FC uplinks. Ethernet uplink ports can exist on the fixed slot and on expansion slots.

For example, if you have two Cisco UCS 5100 series chassis that are fully populated with half width Cisco UCS B200-M1 servers, you have 16 servers. In a cluster configuration, with one LAN uplink per fabric interconnect, these 16 servers share 20GbE of LAN bandwidth. If more capacity is needed, more uplinks from the fabric interconnect should be added. We recommend that you have symmetric configuration of the uplink in cluster configurations. In the same example, if 4 uplinks are used in each fabric interconnect, the 16 servers are sharing 80 GB of bandwidth, so each has approximately 5 GB of capacity. When multiple uplinks are used on a Cisco UCS fabric interconnect the network design team should consider using a port channel to make best use of the capacity.

Number of Uplink Ports from I/O Module to Fabric Interconnect

You can choose to add more bandwidth between I/O module and fabric interconnect by using more uplink ports and increasing the number of cables. In Cisco UCS, you can have one, two, or four cables connecting a I/O module to a Cisco UCS fabric interconnect. The number of cables determines the number of active uplink ports and the oversubscription ratio. For example, one cable results in 8:1 oversubscription for one I/O module. If two I/O modules are in place, each with one cable, and you have 8 half-width blades, the 8 blades will be sharing two uplinks (one left IOM and one right IOM). This results in 8 blades sharing an aggregate bandwidth of 20 GB of Unified Fabric capacity. If two cables are used, this results in 4:1 oversubscription

per IOM (assuming all slots populated with half width blades), and four cables result in 2:1 oversubscription. The lower oversubscription ratio gives you higher performance, but is also more costly as you consume more fabric interconnect ports.

Number of Active Links from Server to Fabric Interconnect

The amount of non-oversubscribed bandwidth available to each server depends on the number of I/O modules used and the number of cables used to connect those I/O modules to the fabric interconnects. Having a second I/O module in place provides additional bandwidth and redundancy to the servers. This level of flexibility in design ensures that you can provide anywhere from 80 Gbps (two I/O modules with four links each) to 10 Gbps (one I/O module with one link) to the chassis.

With 80 Gbps to the chassis, each half-width server in the Cisco UCS instance can get up to 10 Gbps in a non-oversubscribed configuration, with an ability to use up to 20 Gbps with 2:1 oversubscription.

Guidelines for Estimating Oversubscription

When you estimate the optimal oversubscription ratio for a fabric interconnect port, consider the following guidelines:

Cost/Performance Slider

The prioritization of cost and performance is different for each data center and has a direct impact on the configuration of oversubscription. When you plan hardware usage for oversubscription, you need to know where the data center is located on this slider. For example, oversubscription can be minimized if the data center is more concerned with performance than cost. However, cost is a significant factor in most data centers, and oversubscription requires careful planning.

Bandwidth Usage

The estimated bandwidth that you expect each server to actually use is important when you determine the assignment of each server to a fabric interconnect port and, as a result, the oversubscription ratio of the ports. For oversubscription, you must consider how many GBs of traffic the server will consume on average, the ratio of configured bandwidth to used bandwidth, and the times when high bandwidth use will occur.

Network Type

The network type is only relevant to traffic on uplink ports, because FCoE does not exist outside Cisco UCS. The rest of the data center network only differentiates between LAN and SAN traffic. Therefore, you do not need to take the network type into consideration when you estimate oversubscription of a fabric interconnect port.

Pinning

Pinning in Cisco UCS is only relevant to uplink ports. You can pin Ethernet or FCoE traffic from a given server to a specific uplink Ethernet port or uplink FC port.

When you pin the NIC and HBA of both physical and virtual servers to uplink ports, you give the fabric interconnect greater control over the unified fabric. This control ensures more optimal utilization of uplink port bandwidth.

Cisco UCS uses pin groups to manage which NICs, vNICs, HBAs, and vHBAs are pinned to an uplink port. To configure pinning for a server, you can either assign a pin group directly, or include a pin group in a vNIC

policy, and then add that vNIC policy to the service profile assigned to that server. All traffic from the vNIC or vHBA on the server travels through the I/O module to the same uplink port.

Pinning Server Traffic to Server Ports

All server traffic travels through the I/O module to server ports on the fabric interconnect. The number of links for which the chassis is configured determines how this traffic is pinned.

The pinning determines which server traffic goes to which server port on the fabric interconnect. This pinning is fixed. You cannot modify it. As a result, you must consider the server location when you determine the appropriate allocation of bandwidth for a chassis.



Note

You must review the allocation of ports to links before you allocate servers to slots. The cabled ports are not necessarily port 1 and port 2 on the I/O module. If you change the number of links between the fabric interconnect and the I/O module, you must reacknowledge the chassis to have the traffic rerouted.

All port numbers refer to the fabric interconnect-side ports on the I/O module.

Chassis with One I/O Module

| Links on Chassis | Servers Pinned to Link 1 | Servers Pinned to Link 2 | Servers Pinned to Link 3 | Servers Pinned to Link 4 |
|------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| 1 link | All server slots | None | None | None |
| 2 links | Slots 1, 3, 5, and 7 | Slots 2, 4, 6, and 8 | None | None |
| 4 links | Slots 1 and 5 | Slots 2 and 6 | Slots 3 and 7 | Slots 4 and 8 |

Chassis with Two I/O Modules

If a chassis has two I/O modules, traffic from one I/O module goes to one of the fabric interconnects and traffic from the other I/O module goes to the second fabric interconnect. You cannot connect two I/O modules to a single fabric interconnect.

| Fabric Interconnect Configured in vNIC | Server Traffic Path |
|--|---|
| A | Server traffic goes to fabric interconnect A. If A fails, the server traffic does not fail over to B. |
| B | All server traffic goes to fabric interconnect B. If B fails, the server traffic does not fail over to A. |
| A-B | All server traffic goes to fabric interconnect A. If A fails, the server traffic fails over to B. |
| B-A | All server traffic goes to fabric interconnect B. If B fails, the server traffic fails over to A. |

Guidelines for Pinning

When you determine the optimal configuration for pin groups and pinning for an uplink port, consider the estimated bandwidth usage for the servers. If you know that some servers in the system will use a lot of bandwidth, ensure that you pin these servers to different uplink ports.

Quality of Service

Cisco UCS provides the following methods to implement quality of service:

- System classes that specify the global configuration for certain types of traffic across the entire system
- QoS policies that assign system classes for individual vNICs
- Flow control policies that determine how uplink Ethernet ports handle pause frames

System Classes

Cisco UCS uses Data Center Ethernet (DCE) to handle all traffic inside a Cisco UCS instance. This industry standard enhancement to Ethernet divides the bandwidth of the Ethernet pipe into eight virtual lanes. Two virtual lanes are reserved for internal system and management traffic. You can configure quality of service for the other six virtual lanes. System classes determine how the DCE bandwidth in these six virtual lanes is allocated across the entire Cisco UCS instance.

Each system class reserves a specific segment of the bandwidth for a specific type of traffic. This provides a level of traffic management, even in an oversubscribed system. For example, you can configure the Fibre Channel Priority system class to determine the percentage of DCE bandwidth allocated to FCoE traffic.

The following table describes the system classes that you can configure:

Table 5: System Classes

| System Class | Description |
|--------------------------------------|--|
| Platinum Gold Silver Bronze | A configurable set of system classes that you can include in the QoS policy for a service profile. Each system class manages one lane of traffic. All properties of these system classes are available for you to assign custom settings and policies. |
| Best Effort | A system class that sets the quality of service for the lane reserved for Basic Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a drop policy that allows it to drop data packets if required. You cannot disable this system class. |
| Fibre Channel | A system class that sets the quality of service for the lane reserved for Fibre Channel over Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a no-drop policy that ensures it never drops data packets. You cannot disable this system class. |

Quality of Service Policy

A quality of service (QoS) policy assigns a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic. For certain adapters you can also specify additional controls on the outgoing traffic, such as burst and rate.

You must include a QoS policy in a vNIC policy or vHBA policy and then include that policy in a service profile to configure the vNIC or vHBA.

Flow Control Policy

Flow control policies determine whether the uplink Ethernet ports in a Cisco UCS instance send and receive IEEE 802.3x pause frames when the receive buffer for a port fills. These pause frames request that the transmitting port stop sending data for a few milliseconds until the buffer clears.

For flow control to work between a LAN port and an uplink Ethernet port, you must enable the corresponding receive and send flow control parameters for both ports. For Cisco UCS, the flow control policies configure these parameters.

When you enable the send function, the uplink Ethernet port sends a pause request to the network port if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels. If you enable the receive function, the uplink Ethernet port honors all pause requests from the network port. All traffic is halted on that uplink port until the network port cancels the pause request.

Because you assign the flow control policy to the port, changes to the policy have an immediate effect on how the port reacts to a pause frame or a full receive buffer.

Opt-In Features

Each Cisco UCS instance is licensed for all functionality. Depending upon how the system is configured, you can decide to opt in to some features or opt out of them for easier integration into existing environment. If a process change happens, you can change your system configuration and include one or both of the opt-in features.

The opt-in features are as follows:

- Stateless computing, which takes advantage of mobile service profiles with pools and policies where each component, such as a server or an adapter, is stateless.
- Multi-tenancy, which uses organizations and role-based access control to divide the system into smaller logical segments.

Stateless Computing

Stateless computing allows you to use a service profile to apply the personality of one server to a different server in the same Cisco UCS instance. The personality of the server includes the elements that identify that server and make it unique in the instance. If you change any of these elements, the server could lose its ability to access, use, or even achieve booted status.

The elements that make up a server's personality include the following:

- Firmware versions
- UUID (used for server identification)

- MAC address (used for LAN connectivity)
- World Wide Names (used for SAN connectivity)
- Boot settings

Stateless computing creates a dynamic server environment with highly flexible servers. Every physical server in a Cisco UCS instance remains anonymous until you associate a service profile with it, then the server gets the identity configured in the service profile. If you no longer need a business service on that server, you can shut it down, disassociate the service profile, and then associate another service profile to create a different identity for the same physical server. The "new" server can then host another business service.

To take full advantage of the flexibility of statelessness, the optional local disks on the servers should only be used for swap or temp space and not to store operating system or application data.

You can choose to fully implement stateless computing for all physical servers in a Cisco UCS instance, to not have any stateless servers, or to have a mix of the two types.

If You Opt In to Stateless Computing

Each physical server in the Cisco UCS instance is defined through a service profile. Any server can be used to host one set of applications, then reassigned to another set of applications or business services, if required by the needs of the data center.

You create service profiles that point to policies and pools of resources that are defined in the instance. The server pools, WWN pools, and MAC pools ensure that all unassigned resources are available on an as-needed basis. For example, if a physical server fails, you can immediately assign the service profile to another server. Because the service profile provides the new server with the same identity as the original server, including WWN and MAC address, the rest of the data center infrastructure sees it as the same server and you do not need to make any configuration changes in the LAN or SAN.

If You Opt Out of Stateless Computing

Each server in the Cisco UCS instance is treated as a traditional rack mount server.

You create service profiles that inherit the identify information burned into the hardware and use these profiles to configure LAN or SAN connectivity for the server. However, if the server hardware fails, you cannot reassign the service profile to a new server.

Multi-Tenancy

Multi-tenancy allows you to divide up the large physical infrastructure of an instance into logical entities known as organizations. As a result, you can achieve a logical isolation between organizations without providing a dedicated physical infrastructure for each organization.

You can assign unique resources to each tenant through the related organization, in the multi-tenant environment. These resources can include different policies, pools, and quality of service definitions. You can also implement locales to assign or restrict user privileges and roles by organization, if you do not want all users to have access to all organizations.

If you set up a multi-tenant environment, all organizations are hierarchical. The top-level organization is always root. The policies and pools that you create in root are system-wide and are available to all organizations in the system. However, any policies and pools created in other organizations are only available to organizations that are above it in the same hierarchy. For example, if a system has organizations named Finance and HR that are not in the same hierarchy, Finance cannot use any policies in the HR organization, and HR cannot

access any policies in the Finance organization. However, both Finance and HR can use policies and pools in the root organization.

If you create organizations in a multi-tenant environment, you can also set up one or more of the following for each organization or for a sub-organization in the same hierarchy:

- Resource pools
- Policies
- Service profiles
- Service profile templates

If You Opt In to Multi-Tenancy

Each Cisco UCS instance is divided into several distinct organizations. The types of organizations you create in a multi-tenancy implementation depends upon the business needs of the company. Examples include organizations that represent the following:

- Enterprise groups or divisions within a company, such as marketing, finance, engineering, or human resources
- Different customers or name service domains, for service providers

You can create locales to ensure that users have access only to those organizations that they are authorized to administer.

If You Opt Out of Multi-Tenancy

The Cisco UCS instance remains a single logical entity with everything in the root organization. All policies and resource pools can be assigned to any server in the instance.

Virtualization in Cisco UCS

Overview of Virtualization

Virtualization allows the creation of multiple virtual machines to run in isolation, side-by-side on the same physical machine.

Each virtual machine has its own set of virtual hardware (RAM, CPU, NIC) upon which an operating system and fully configured applications are loaded. The operating system sees a consistent, normalized set of hardware regardless of the actual physical hardware components.

In a virtual machine, both hardware and software are encapsulated in a single file for rapid copying, provisioning, and moving between physical servers. You can move a virtual machine, within seconds, from one physical server to another for zero-downtime maintenance and continuous workload consolidation.

The virtual hardware makes it possible for many servers, each running in an independent virtual machine, to run on a single physical server. The advantages of virtualization include better use of computing resources, greater server density, and seamless server migration.

Virtualization in Cisco UCS

Cisco UCS provides hardware-level server virtualization. Hardware-level server virtualization allows a server to be simulated at the physical level and cannot be detected by existing software, including the operating system, drivers, and management tools. If underlying hardware faults require you to recreate the virtual server in another location, the network and existing software remain unaware that the physical server has changed.

Server virtualization allows networks to rapidly adapt to changing business and technical conditions. The lower level integration with the virtualized environment in Cisco UCS improves visibility and control of the virtual machine environment, and enhances the overall agility of the system. In addition, this virtualization ensures that there is no performance penalty or overhead for applications while running.

The virtualized environment available in a Cisco UCS server depends upon the type of adapter installed in the server. For example, a virtual interface card (VIC) adapter provides a unique and flexible virtualized environment and support for virtual machines. The other adapters support the standard integration and virtualized environment with VMWare.

Virtualization with Network Interface Cards and Converged Network Adapters

Network interface card (NIC) and converged network adapters support virtualized environments with the standard VMware integration with ESX installed on the server and all virtual machine management performed through the VC.

Portability of Virtual Machines

If you implement service profiles you retain the ability to easily move a server identity from one server to another. After you image the new server, the ESX treats that server as if it were the original.

Communication between Virtual Machines on the Same Server

These adapters implement the standard communications between virtual machines on the same server. If an ESX host includes multiple virtual machines, all communications must go through the virtual switch on the server.

If the system uses the native VMware drivers, the virtual switch is out of the network administrator's domain and is not subject to any network policies. As a result, for example, QoS policies on the network are not applied to any data packets traveling from VM1 to VM2 through the virtual switch.

If the system includes another virtual switch, such as the Nexus 1000, that virtual switch is subject to the network policies configured on that switch by the network administrator.

Virtualization with a Virtual Interface Card Adapter

Virtual interface card (VIC) adapters support virtualized environments with VMware. These environments support the standard VMware integration with ESX installed on the server and all virtual machine management performed through the VMware vCenter.

This virtualized adapter supports the following:

- Dynamic vNICs in a virtualized environment with VM software, such as vSphere. This solution enables you to divide a single physical blade server into multiple logical PCIE instances.
- Static vNICs in a single operating system installed on a server.

With a VIC adapter, the solution you choose determines how communication works. This type of adapter supports the following communication solutions:

- Cisco VN-Link in hardware, which is a hardware-based method of handling traffic to and from a virtual machine. Details of how to configure this solution are available in this document.
- Cisco VN-Link in software, which is a software-based method of handling traffic to and from a virtual machine and uses the Nexus 1000v virtual switch. Details of how to configure this solution are available in the Nexus 1000v documentation.
- Single operating system installed on the server without virtualization, which uses the same methods of handling traffic as the other Cisco UCS adapters.

Cisco VN-Link

Cisco Virtual Network Link (VN-Link) is a set of features and capabilities that enable you to individually identify, configure, monitor, migrate, and diagnose virtual machine interfaces in a way that is consistent with the current network operation models for physical servers. VN-Link literally indicates the creation of a logical link between a vNIC on a virtual machine and a Cisco UCS fabric interconnect. This mapping is the logical equivalent of using a cable to connect a NIC with a network port on an access-layer switch.

VN-Link in Hardware

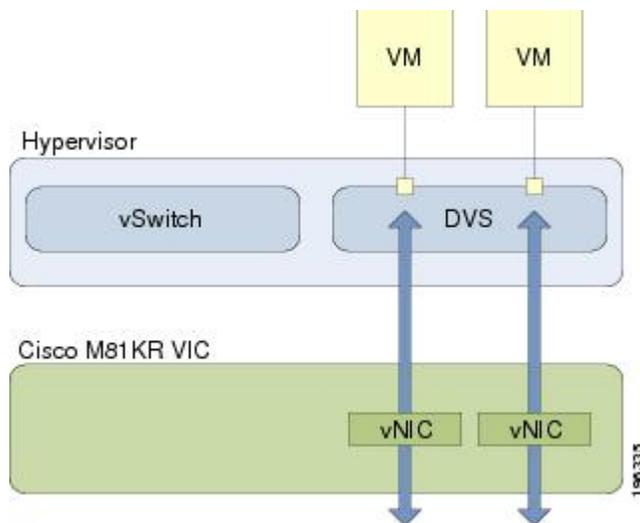
Cisco VN-Link in hardware is a hardware-based method of handling traffic to and from a virtual machine on a server with a VIC adapter. This method is sometimes referred to as pass-through switching. This solution replaces software-based switching with ASIC-based hardware switching and improves performance.

The distributed virtual switch (DVS) framework delivers VN-Link in hardware features and capabilities for virtual machines on Cisco UCS servers with VIC adapters. This approach provides an end-to-end network solution to meet the new requirements created by server virtualization.

With VN-Link in hardware, all traffic to and from a virtual machine passes through the DVS and the hypervisor, and then returns to the virtual machine on the server. Switching occurs in the fabric interconnect (hardware). As a result, network policies can be applied to traffic between virtual machines. This capability provides consistency between physical and virtual servers.

The following figure shows the traffic paths taken by VM traffic on a Cisco UCS server with a VIC adapter:

Figure 1: Traffic Paths for VM traffic with VN-Link in Hardware



Extension File for Communication with VMware vCenter

For Cisco UCS instances that use VIC adapters to implement VN-Link in hardware, you must create and install an extension file to establish the relationship and communications between Cisco UCS Manager and the VMware vCenter. This extension file is an XML file that contains vital information, including the following:

- Extension key
- Public SSL certificate

If you need to have two Cisco UCS instances share the same set of distributed virtual switches in a vCenter, you can create a custom extension key and import the same SSL certificate in the Cisco UCS Manager for each Cisco UCS instance.

Extension Key

The extension key includes the identity of the Cisco UCS instance. By default, this key has the value Cisco UCS GUID, as this value is identical across both fabric interconnects in a cluster configuration.

When you install the extension, vCenter uses the extension key to create a distributed virtual switch (DVS).

Public SSL Certificate

Cisco UCS Manager generates a default, self-signed SSL certificate to support communication with vCenter. You can also provide your own custom certificate.

Custom Extension Files

You can create a custom extension file for a Cisco UCS instance that does not use either or both of the default extension key or SSL certificate. For example, you can create the same custom key in two different Cisco UCS instances when they are managed by the same VMware vCenter instance.

**Important**

You cannot change an extension key that is being used by a DVS or vCenter. If you want to use a custom extension key, we recommend that you create and register the custom key before you create the DVS in Cisco UCS Manager to avoid any possibility of having to delete and recreate the associated DVS.

Distributed Virtual Switches

Each VMware ESX host has its own software-based virtual switch (vSwitch) in its hypervisor that performs the switching operations between its virtual machines (VMs). The Cisco UCS distributed virtual switch (DVS) is a software-based virtual switch that runs alongside the vSwitch in the ESX hypervisor, and can be distributed across multiple ESX hosts. Unlike vSwitch, which uses its own local port configuration, a DVS associated with multiple ESX hosts uses the same port configuration across all ESX hosts.

After associating an ESX host to a DVS, you can migrate existing VMs from the vSwitch to the DVS, and you can create VMs to use the DVS instead of the vSwitch. With the hardware-based VN-Link implementation, when a VM uses the DVS, all VM traffic passes through the DVS and ASIC-based switching is performed by the fabric interconnect.

In Cisco UCS Manager, DVSES are organized in the following hierarchy:

```

vCenter
  Folder (optional)
    Datacenter
      Folder (required)
        DVS
  
```

At the top of the hierarchy is the vCenter, which represents a VMware vCenter instance. Each vCenter contains one or more datacenters, and optionally vCenter folders with which you can organize the datacenters. Each datacenter contains one or more required datacenter folders. Datacenter folders contain the DVSES.

Port Profiles

Port profiles contain the properties and settings used to configure virtual interfaces in Cisco UCS for VN-Link in hardware. The port profiles are created and administered in Cisco UCS Manager. There is no clear visibility into the properties of a port profile from VMware vCenter.

In VMware vCenter, a port profile is represented as a port group. Cisco UCS Manager pushes the port profile names to vCenter, which displays the names as port groups. None of the specific networking properties or settings in the port profile are visible in VMware vCenter.

After a port profile is created, assigned to, and actively used by one or more DVSES, any changes made to the networking properties of the port profile in Cisco UCS Manager are immediately applied to those DVSES.

You must configure at least one port profile client for a port profile, if you want Cisco UCS Manager to push the port profile to VMware vCenter.

Port Profile Clients

The port profile client determines the DVSES to which a port profile is applied. By default, the port profile client specifies that the associated port profile applies to all DVSES in the vCenter. However, you can configure the client to apply the port profile to all DVSES in a specific datacenter or datacenter folder, or only to one DVS.

VN-Link in Hardware Considerations

How you configure a Cisco UCS instance for VN-Link in hardware has several dependencies. The information you need to consider before you configure VN-Link in hardware includes the following:

- A Cisco UCS instance can have a maximum of 4 vCenters

- Each vCenter can have a maximum of 8 distributed virtual switches
- Each distributed virtual switch can have a maximum of 4096 ports
- Each port profile can have a maximum of 4096 ports
- Each Cisco UCS instance can have a maximum of 256 port profiles



CHAPTER 2

Overview of Cisco UCS Manager

This chapter includes the following sections:

- [About Cisco UCS Manager](#) , page 35
- [Tasks You Can Perform in Cisco UCS Manager](#) , page 36
- [Tasks You Cannot Perform in Cisco UCS Manager](#) , page 38
- [Cisco UCS Manager in a Cluster Environment](#), page 38

About Cisco UCS Manager

Cisco UCS Manager is the management service for all components in a Cisco UCS instance. Cisco UCS Manager runs within the fabric interconnect. You can use any of the interfaces available with this management service to access, configure, administer, and monitor the network and server resources for all chassis connected to the fabric interconnect.

Multiple Management Interfaces

Cisco UCS Manager includes the following interfaces you can use to manage a Cisco UCS instance:

- Cisco UCS Manager GUI
- Cisco UCS Manager CLI
- XML API

Almost all tasks can be performed in any of the interfaces, and the results of tasks performed in one interface are automatically displayed in another.

However, you cannot do the following:

- Use Cisco UCS Manager GUI to invoke Cisco UCS Manager CLI
- View the results of a command invoked through Cisco UCS Manager CLI in Cisco UCS Manager GUI
- Generate CLI output from Cisco UCS Manager GUI

Centralized Management

Cisco UCS Manager centralizes the management of resources and devices, rather than using multiple management points. This centralized management includes management of the following devices in a Cisco UCS instance:

- Fabric interconnects
- Software switches for virtual servers
- Power and environmental management for chassis and servers
- Configuration and firmware updates for Ethernet NICs and Fibre Channel HBAs
- Firmware and BIOS settings for servers

Support for Virtual and Physical Servers

Cisco UCS Manager abstracts server state information—including server identity, I/O configuration, MAC addresses and World Wide Names, firmware revision, and network profiles—into a service profile. You can apply the service profile to any server resource in the system, providing the same flexibility and support to physical servers, virtual servers, and virtual machines connected to a virtual device provided by a VIC adapter.

Role-Based Administration and Multi-Tenancy Support

Cisco UCS Manager supports flexibly defined roles so that data centers can use the same best practices with which they manage discrete servers, storage, and networks to operate a Cisco UCS instance. You can create user roles with privileges that reflect user responsibilities in the data center. For example, you can create the following:

- Server administrator roles with control over server-related configurations
- Storage administrator roles with control over tasks related to the SAN
- Network administrator roles with control over tasks related to the LAN

In a multi-tenancy environment, Cisco UCS Manager enables you to create locales for user roles that can limit the scope of a user to a particular organization.

Tasks You Can Perform in Cisco UCS Manager

You can use Cisco UCS Manager to perform management tasks for all physical and virtual devices within a Cisco UCS instance.

Cisco UCS Hardware Management

You can use Cisco UCS Manager to manage all hardware within a Cisco UCS instance, including the following:

- Chassis
- Servers
- Fabric interconnects
- Fans
- Ports

- Cards
- Slots
- I/O modules

Cisco UCS Resource Management

You can use Cisco UCS Manager to create and manage all resources within a Cisco UCS instance, including the following:

- Servers
- WWN addresses
- MAC addresses
- UUIDs
- Bandwidth

Server Administration in a Cisco UCS Instance

A server administrator can use Cisco UCS Manager to perform server management tasks within a Cisco UCS instance, including the following:

- Create server pools and policies related to those pools, such as qualification policies
- Create policies for the servers, such as discovery policies, scrub policies, and IPMI policies
- Create service profiles and, if desired, service profile templates
- Apply service profiles to servers
- Monitor faults, alarms, and the status of equipment

Network Administration in a Cisco UCS Instance

A network administrator can use Cisco UCS Manager to perform tasks required to create LAN configuration for a Cisco UCS instance, including the following:

- Configure uplink ports, port channels, and LAN PIN groups
- Create VLANs
- Configure the quality of service classes and definitions
- Create the pools and policies related to network configuration, such as MAC address pools and Ethernet adapter profiles

Storage Administration in a Cisco UCS Instance

A storage administrator can use Cisco UCS Manager to perform tasks required to create SAN configuration for a Cisco UCS instance, including the following:

- Configure ports, port channels, and SAN PIN groups
- Create VSANs
- Configure the quality of service classes and definitions

- Create the pools and policies related to the network configuration, such as WWN pools and Fibre Channel adapter profiles

Tasks You Cannot Perform in Cisco UCS Manager

You cannot use Cisco UCS Manager to perform certain system management tasks that are not specifically related to device management within a Cisco UCS instance

No Cross-System Management

You cannot use Cisco UCS Manager to manage systems or devices that are outside the Cisco UCS instance where Cisco UCS Manager is located. For example, you cannot manage heterogeneous environments, such as non-Cisco UCS x86 systems, SPARC systems, or PowerPC systems.

No Operating System or Application Provisioning or Management

Cisco UCS Manager provisions servers and, as a result, exists below the operating system on a server. Therefore, you cannot use it to provision or manage operating systems or applications on servers. For example, you cannot do the following:

- Deploy an OS, such as Windows or Linux
- Deploy patches for software, such as an OS or an application
- Install base software components, such as anti-virus software, monitoring agents, or backup clients
- Install software applications, such as databases, application server software, or web servers
- Perform operator actions, including restarting an Oracle database, restarting printer queues, or handling non-Cisco UCS user accounts
- Configure or manage external storage on the SAN or NAS storage

Cisco UCS Manager in a Cluster Environment

In a cluster Cisco UCS instance with two fabric interconnects, you can run a separate instance of Cisco UCS Manager on each fabric interconnect. The Cisco UCS Manager on the primary fabric interconnect acts as the primary management instance, and the Cisco UCS Manager on the other fabric interconnect is the subordinate management instance.

The two instances of Cisco UCS Manager communicate across a private network between the L1 and L2 Ethernet ports on the fabric interconnects. Configuration and status information is communicated across this private network to ensure that all management information is replicated. This ongoing communication ensures that the management information for Cisco UCS persists even if the primary fabric interconnect fails. In addition, the "floating" management IP address that runs on the primary Cisco UCS Manager ensures a smooth transition in the event of a failover to the subordinate fabric interconnect.



CHAPTER 3

Overview of Cisco UCS Manager CLI

This chapter includes the following sections:

- [Managed Objects, page 39](#)
- [Command Modes, page 39](#)
- [Object Commands, page 41](#)
- [Complete a Command, page 42](#)
- [Command History, page 42](#)
- [Committing, Discarding, and Viewing Pending Commands, page 42](#)
- [Online Help for the CLI, page 43](#)

Managed Objects

Cisco UCS uses a managed object model, where managed objects are abstract representations of physical or logical entities that can be managed. For example, servers, chassis, I/O cards, and processors are physical entities represented as managed objects, and resource pools, user roles, service profiles, and policies are logical entities represented as managed objects.

Managed objects may have one or more associated properties that can be configured.

Command Modes

The CLI is organized into a hierarchy of command modes, with the EXEC mode being the highest-level mode of the hierarchy. Higher-level modes branch into lower-level modes. You use **create**, **enter**, and **scope** commands to move from higher-level modes to modes in the next lower level, and you use the **exit** command to move up one level in the mode hierarchy.

**Note**

Most command modes are associated with managed objects, so you must create an object before you can access the mode associated with that object. You use **create** and **enter** commands to create managed objects for the modes being accessed. The **scope** commands do not create managed objects and can only access modes for which managed objects already exist.

Each mode contains a set of commands that can be entered in that mode. Most of the commands available in each mode pertain to the associated managed object. Depending on your assigned role and locale, you may have access to only a subset of the commands available in a mode; commands to which you do not have access are hidden.

The CLI prompt for each mode shows the full path down the mode hierarchy to the current mode. This helps you to determine where you are in the command mode hierarchy, and it can be an invaluable tool when you need to navigate through the hierarchy.

The following table lists the main command modes, the commands used to access each mode, and the CLI prompt associated with each mode.

Table 6: Main Command Modes and Prompts

| Mode Name | Commands Used to Access | Mode Prompt |
|------------------------------|---|------------------------|
| EXEC | top command from any mode | # |
| adapter | scope adapter command from EXEC mode | /adapter # |
| chassis | scope chassis command from EXEC mode | /chassis # |
| Ethernet server | scope eth-server command from EXEC mode | /eth-server # |
| Ethernet uplink | scope eth-uplink command from EXEC mode | /eth-uplink # |
| fabric-interconnect | scope fabric-interconnect command from EXEC mode | /fabric-interconnect # |
| Fibre Channel uplink | scope fc-uplink command from EXEC mode | /fc-uplink # |
| firmware | scope firmware command from EXEC mode | /firmware # |
| Host Ethernet interface | scope host-eth-if command from EXEC mode | /host-eth-if # |
| Host Fibre Channel interface | scope host-fc-if command from EXEC mode | /host-fc-if # |

| Mode Name | Commands Used to Access | Mode Prompt |
|-----------------|---|--------------------|
| monitoring | scope monitoring command from EXEC mode | /monitoring # |
| organization | scope org command from EXEC mode | /org # |
| security | scope security command from EXEC mode | /security # |
| server | scope server command from EXEC mode | /server # |
| service-profile | scope service-profile command from EXEC mode | /service-profile # |
| system | scope system command from EXEC mode | /system # |
| virtual HBA | scope vhba command from EXEC mode | /vhba # |
| virtual NIC | scope vnic command from EXEC mode | /vnic # |

Object Commands

Four general commands are available for object management:

- **create** *object*
- **delete** *object*
- **enter** *object*
- **scope** *object*

You can use the **scope** command with any managed object, whether a permanent object or a user-instantiated object. The other commands allow you to create and manage user-instantiated objects. For every **create** *object* command, a corresponding **delete** *object* and **enter** *object* command exists.

In the management of user-instantiated objects, the behavior of these commands depends on whether the object exists, as described in the following tables:

Table 7: Command behavior if the object does not exist

| Command | Behavior |
|-----------------------------|--|
| create <i>object</i> | The object is created and its configuration mode, if applicable, is entered. |

| Command | Behavior |
|-----------------------------|--|
| delete <i>object</i> | An error message is generated. |
| enter <i>object</i> | The object is created and its configuration mode, if applicable, is entered. |
| scope <i>object</i> | An error message is generated. |

Table 8: Command behavior if the object exists

| Command | Behavior |
|-----------------------------|--|
| create <i>object</i> | An error message is generated. |
| delete <i>object</i> | The object is deleted. |
| enter <i>object</i> | The configuration mode, if applicable, of the object is entered. |
| scope <i>object</i> | The configuration mode of the object is entered. |

Complete a Command

You can use the Tab key in any mode to complete a command. Partially typing a command name and pressing Tab causes the command to be displayed in full, or to the point where another keyword must be chosen or an argument value must be entered.

Command History

The CLI stores all previously used commands in the current session. You can step through the previously used commands by using the Up Arrow or Down Arrow keys. The Up Arrow key steps to the previous command in the history, and the Down Arrow key steps to the next command in the history. If you get to the end of the history, pressing the Down Arrow key does nothing.

All commands in the history can be entered again by simply stepping through the history to recall the desired command and pressing Enter. The command is entered as if you had manually typed it. You can also recall a command and change it before you enter it.

Committing, Discarding, and Viewing Pending Commands

When you enter a configuration command in the CLI, the command is not applied until you enter the **commit-buffer** command. Until committed, a configuration command is pending and can be discarded by entering a **discard-buffer** command.

You can accumulate pending changes in multiple command modes and apply them together with a single **commit-buffer** command. You can view the pending commands by entering the **show configuration pending** command in any command mode.

**Note**

Committing multiple commands together is not an atomic operation. If any command fails, the successful commands are applied despite the failure. Failed commands are reported in an error message.

While any commands are pending, an asterisk (*) appears before the command prompt. The asterisk disappears when you enter the **commit-buffer** command, as shown in this example:

```
switch-1# scope chassis 1
switch-1 /chassis # enable locator-led
switch-1 /chassis* # show configuration pending
  scope chassis 1
+   enable locator-led
  exit
switch-1 /chassis* # commit-buffer
switch-1 /chassis #
```

Online Help for the CLI

At any time, you can type the ? character to display the options available at the current state of the command syntax. If you have not typed anything at the prompt, typing ? lists all available commands for the mode you are in. If you have partially typed a command, typing ? lists all available keywords and arguments available at your current position in the command syntax.



PART II

System Configuration

- [Configuring the Fabric Interconnects, page 47](#)
- [Configuring Ports, page 59](#)
- [Configuring Communication Services, page 67](#)
- [Configuring Primary Authentication, page 81](#)
- [Configuring Organizations, page 91](#)
- [Configuring Role-Based Access Control, page 97](#)
- [Managing Firmware, page 113](#)
- [Configuring DNS Servers, page 151](#)
- [Configuring System-Related Policies, page 153](#)
- [Managing Port Licenses, page 159](#)



CHAPTER 4

Configuring the Fabric Interconnects

This chapter includes the following sections:

- [Initial System Setup, page 47](#)
- [Performing an Initial System Setup for a Standalone Configuration, page 49](#)
- [Initial System Setup for a Cluster Configuration, page 51](#)
- [Enabling a Standalone Fabric Interconnect for Cluster Configuration, page 54](#)
- [Changing the System Name, page 54](#)
- [Changing the Management Subnet of a Cluster, page 55](#)
- [Ethernet Switching Mode, page 56](#)
- [Configuring Ethernet Switching Mode, page 57](#)

Initial System Setup

The first time that you access a fabric interconnect in a Cisco UCS instance, a setup wizard prompts you for the following information required to configure the system:

- Installation method (GUI or CLI)
- Setup mode (restore from full system backup or initial setup)
- System configuration type (standalone or cluster configuration)
- System name
- Admin password
- Management port IP address and subnet mask
- Default gateway IP address
- DNS Server IP address
- Default domain name

Setup Mode

You can choose to either restore the system configuration from an existing backup file, or manually set up the system by going through the setup wizard. If you choose to restore the system, the backup file must be reachable from the management network.

System Configuration Type

You can configure a Cisco UCS instance to use a single fabric interconnect in a standalone configuration or to use a redundant pair of fabric interconnects in a cluster configuration.

A cluster configuration provides high availability. If one fabric interconnect becomes unavailable, the other takes over. Only one management port (Mgmt0) connection is required to support a cluster configuration; however, both Mgmt0 ports should be connected to provide link-level redundancy.

**Note**

The cluster configuration only provides redundancy for the management plane. Data redundancy is dependent on the user configuration and may require a third-party tool to support data redundancy.

To use the cluster configuration, the two fabric interconnects must be directly connected together using Ethernet cables between the L1 (L1-to-L1) and L2 (L2-to-L2) high availability ports, with no other fabric interconnects in between. This allows the two fabric interconnects to continuously monitor the status of each other and quickly know when one has failed.

Both fabric interconnects in a cluster configuration must go through the initial setup process. The first fabric interconnect to be set up must be enabled for a cluster configuration, then when the second fabric interconnect is set up, it detects the first fabric interconnect as a peer fabric interconnect in the cluster.

For more information, refer to the *Cisco UCS 6100 Series Fabric Interconnect Hardware Installation Guide*.

Management Port IP Address

In a standalone configuration, you must specify only one IP address and the subnet mask for the single management port on the fabric interconnect.

In a cluster configuration, you must specify the following three IP addresses in the same subnet:

- Management port IP address for fabric interconnect A
- Management port IP address for fabric interconnect B
- Cluster IP address

**Tip**

After the initial configuration, you can change the management IP port and the related subnet mask in the Cisco UCS Manager CLI. You cannot make this change in the Cisco UCS Manager GUI.

Performing an Initial System Setup for a Standalone Configuration

Before You Begin

1 Verify the following physical connections on the fabric interconnect:

- The console port is physically connected to a computer terminal or console server
- The management Ethernet port (mgmt0) is connected to an external hub, switch, or router

For more information, refer to the *Cisco UCS Hardware Installation Guide* for your fabric interconnect.

2 Verify that the console port parameters on the computer terminal (or console server) attached to the console port are as follows:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

3 Collect the following information that you will need to supply during the initial setup:

- System name.
- Password for the admin account. Choose a strong password that meets the guidelines for Cisco UCS Manager passwords. This password cannot be blank.
- Management port IP address and subnet mask.
- Default gateway IP address.
- DNS server IP address (optional).
- Domain name for the system (optional).

Procedure

Step 1 Connect to the console port.

Step 2 Power on the fabric interconnect.

You will see the power on self-test messages as the fabric interconnect boots.

- Step 3** When the unconfigured system boots, it prompts you for the setup method to be used. Enter **console** to continue the initial setup using the console CLI.
- Step 4** Enter **setup** to continue as an initial system setup.
- Step 5** Enter **y** to confirm that you want to continue the initial setup.
- Step 6** Enter the password for the admin account.
- Step 7** To confirm, re-enter the password for the admin account.
- Step 8** Enter **no** to continue the initial setup for a standalone configuration.
- Step 9** Enter the system name.
- Step 10** Enter the IP address for the management port on the fabric interconnect.
- Step 11** Enter the subnet mask for the management port on the fabric interconnect.
- Step 12** Enter the IP address for the default gateway.
- Step 13** Enter **yes** if you want to specify the IP address for the DNS server, or **no** if you do not.
- Step 14** (Optional) Enter the IP address for the DNS server.
- Step 15** Enter **yes** if you want to specify the default domain name, or **no** if you do not.
- Step 16** (Optional) Enter the default domain name.
- Step 17** Review the setup summary and enter **yes** to save and apply the settings, or enter **no** to go through the Setup wizard again to change some of the settings.
If you choose to go through the Setup wizard again, it provides the values you previously entered, and the values appear in brackets. To accept previously entered values, press **Enter**.

The following example sets up a standalone configuration using the console:

```

Enter the installation method (console/gui)? console
Enter the setup mode (restore from backup or initial setup) [restore/setup]? setup
You have chosen to setup a new switch. Continue? (y/n): y
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Do you want to create a new cluster on this switch (select 'no' for standalone setup or if
you want this switch to be added to an existing cluster)? (yes/no) [n]: no
Enter the system name: foo
Mgmt0 IPv4 address: 192.168.10.10
Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Configure the DNS Server IPv4 address? (yes/no) [n]: yes
DNS IPv4 address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: yes
Default domain name: domainname.com
Following configurations will be applied:
Switch Fabric=A
System Name=foo
Management IP Address=192.168.10.10
Management IP Netmask=255.255.255.0
Default Gateway=192.168.10.1
DNS Server=20.10.20.10
Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

```

Initial System Setup for a Cluster Configuration

Performing an Initial System Setup for the First Fabric Interconnect

Before You Begin

- 1 Verify the following physical connections on the fabric interconnect:
 - A console port on the first fabric interconnect is physically connected to a computer terminal or console server
 - The management Ethernet port (mgmt0) is connected to an external hub, switch, or router
 - The L1 ports on both fabric interconnects are directly connected to each other
 - The L2 ports on both fabric interconnects are directly connected to each other

For more information, refer to the *Cisco UCS Hardware Installation Guide* for your fabric interconnect.

- 2 Verify that the console port parameters on the computer terminal (or console server) attached to the console port are as follows:
 - 9600 baud
 - 8 data bits
 - No parity
 - 1 stop bit
- 3 Collect the following information that you will need to supply during the initial setup:
 - System name.
 - Password for the admin account. Choose a strong password that meets the guidelines for Cisco UCS Manager passwords. This password cannot be blank.
 - Three static IP addresses: two for the management port on both fabric interconnects (one per fabric interconnect), and one for the cluster IP address used by Cisco UCS Manager.
 - Subnet mask for the three static IP addresses.
 - Default gateway IP address.
 - DNS server IP address (optional).
 - Domain name for the system (optional).

Procedure

- Step 1** Connect to the console port.
- Step 2** Power on the fabric interconnect.

You will see the power on self-test messages as the fabric interconnect boots.

- Step 3** When the unconfigured system boots, it prompts you for the setup method to be used. Enter **console** to continue the initial setup using the console CLI.
- Step 4** Enter **setup** to continue as an initial system setup.
- Step 5** Enter **y** to confirm that you want to continue the initial setup.
- Step 6** Enter the password for the admin account.
- Step 7** To confirm, re-enter the password for the admin account.
- Step 8** Enter **yes** to continue the initial setup for a cluster configuration.
- Step 9** Enter the fabric interconnect fabric (either **A** or **B**).
- Step 10** Enter the system name.
- Step 11** Enter the IP address for the management port on the fabric interconnect.
- Step 12** Enter the subnet mask for the management port on the fabric interconnect.
- Step 13** Enter the IP address for the default gateway.
- Step 14** Enter the virtual IP address.
- Step 15** Enter **yes** if you want to specify the IP address for the DNS server, or **no** if you do not.
- Step 16** (Optional) Enter the IP address for the DNS server.
- Step 17** Enter **yes** if you want to specify the default domain name, or **no** if you do not.
- Step 18** (Optional) Enter the default domain name.
- Step 19** Review the setup summary and enter **yes** to save and apply the settings, or enter **no** to go through the Setup wizard again to change some of the settings.

If you choose to go through the Setup wizard again, it provides the values you previously entered, and the values appear in brackets. To accept previously entered values, press **Enter**.

The following example sets up the first fabric interconnect for a cluster configuration using the console:

```

Enter the installation method (console/gui)? console
Enter the setup mode (restore from backup or initial setup) [restore/setup]? setup
You have chosen to setup a new switch. Continue? (y/n): y
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Do you want to create a new cluster on this switch (select 'no' for standalone setup or if
you want this switch to be added to an existing cluster)? (yes/no) [n]: yes
Enter the switch fabric (A/B): A
Enter the system name: foo
Mgmt0 IPv4 address: 192.168.10.10
Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Virtual IPv4 address : 192.168.10.12
Configure the DNS Server IPv4 address? (yes/no) [n]: yes
DNS IPv4 address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: yes
Default domain name: domainname.com
Following configurations will be applied:
Switch Fabric=A
System Name=foo
Management IP Address=192.168.10.10
Management IP Netmask=255.255.255.0
Default Gateway=192.168.10.1
Cluster Enabled=yes
Virtual Ip Address=192.168.10.12
DNS Server=20.10.20.10
Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

```

Performing an Initial System Setup for the Second Fabric Interconnect

Before You Begin

1 Verify the following physical connections on the fabric interconnect:

- A console port on the second fabric interconnect is physically connected to a computer terminal or console server
- The management Ethernet port (mgmt0) is connected to an external hub, switch, or router
- The L1 ports on both fabric interconnects are directly connected to each other
- The L2 ports on both fabric interconnects are directly connected to each other

For more information, refer to the *Cisco UCS Hardware Installation Guide* for your fabric interconnect.

2 Verify that the console port parameters on the computer terminal (or console server) attached to the console port are as follows:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

3 Collect the following information that you will need to supply during the initial setup:

- Password for the admin account of the peer fabric interconnect. Choose a strong password that meets the guidelines for Cisco UCS Manager passwords. This password cannot be blank.
- Management port IP address in the same subnet as the peer fabric interconnect.

Procedure

Step 1 Connect to the console port.

Step 2 Power on the fabric interconnect.

You will see the power on self-test messages as the fabric interconnect boots.

Step 3 When the unconfigured system boots, it prompts you for the setup method to be used. Enter **console** to continue the initial setup using the console CLI.

Note The fabric interconnect should detect the peer fabric interconnect in the cluster. If it does not, check the physical connections between the L1 and L2 ports, and verify that the peer fabric interconnect has been enabled for a cluster configuration.

Step 4 Enter **y** to add the subordinate fabric interconnect to the cluster.

Step 5 Enter the admin password of the peer fabric interconnect.

Step 6 Enter the IP address for the management port on the subordinate fabric interconnect.

Step 7 Review the setup summary and enter **yes** to save and apply the settings, or enter **no** to go through the Setup wizard again to change some of the settings.

If you choose to go through the Setup wizard again, it provides the values you previously entered, and the values appear in brackets. To accept previously entered values, press **Enter**.

The following example sets up the second fabric interconnect for a cluster configuration using the console:

```
Enter the installation method (console/gui)? console
Installer has detected the presence of a peer switch. This switch will be added to the
cluster. Continue?[y/n] y
Enter the admin password of the peer switch: adminpassword%958
Mgmt0 IPv4 address: 192.168.10.11
Management Ip Address=192.168.10.11
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

Enabling a Standalone Fabric Interconnect for Cluster Configuration

You can add a second fabric interconnect to an existing Cisco UCS instance that uses a single standalone fabric interconnect. To do this, you must enable the standalone fabric interconnect for cluster operation, and then add the second fabric interconnect to the cluster.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# connect local-mgmt | Enters local management mode. |
| Step 2 | UCS-A(local-mgmt) # enable cluster ip-addr | Enables cluster operation on the standalone fabric interconnect with the specified IP address. When you enter this command, you are prompted to confirm that you want to enable cluster operation. Type yes to confirm. |

The following example enables a standalone fabric interconnect with IP address 192.168.1.101 for cluster operation:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# enable cluster 192.168.1.101
This command will enable cluster mode on this setup. You cannot change it
back to stand-alone. Are you sure you want to continue? (yes/no): yes
UCS-A(local-mgmt)#
```

What to Do Next

Add the second fabric interconnect to the cluster.

Changing the System Name

Procedure

| | Command or Action | Purpose |
|---------------|--------------------------------------|--|
| Step 1 | UCS-A # scope system | Enters system mode. |
| Step 2 | UCS-A /system # set name name | Sets the system name. |
| Step 3 | UCS-A /system # commit-buffer | Commits the transaction to the system configuration. |

The name is updated on both fabric interconnects within about 30 seconds after the transaction is committed.

The following example changes the system name and commits the transaction:

```
UCS-A# scope system
UCS-A /system* # set name SanJose5
UCS-A /system* # commit-buffer
UCS-A /system #
```

Changing the Management Subnet of a Cluster

When changing the management subnet in a cluster configuration, you must change the following three IP addresses simultaneously and you must configure all three in the same subnet:

- Management port IP address for fabric interconnect A
- Management port IP address for fabric interconnect B
- Cluster IP (virtual IP) address

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope fabric-interconnect a | Enters fabric interconnect mode for fabric A. |
| Step 2 | UCS-A /fabric-interconnect # set out-of-band ip ip-address netmask netmask gw gateway-ip-address | Sets the IP address, netmask, and gateway IP address of the fabric interconnect. |
| Step 3 | UCS-A /fabric-interconnect # scope fabric-interconnect b | Enters fabric interconnect mode for fabric B. |
| Step 4 | UCS-A /fabric-interconnect # set out-of-band ip ip-address netmask netmask gw gateway-ip-address | Sets the IP address, netmask, and gateway IP address of the fabric interconnect. |
| Step 5 | UCS-A /fabric-interconnect # scope system | Enters system mode. |
| Step 6 | UCS-A /system # set virtual-ip vip-address | Sets the virtual IP address for the cluster. |
| Step 7 | UCS-A /system # commit-buffer | Commits the transaction to the system configuration. |

When you commit the transaction, you are disconnected from the management session. Reconnect at the new management IP address.

This example changes both fabric-interconnect IP addresses, changes the virtual IP address, and commits the transaction, disconnecting the session:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask 255.255.255.0 gw 192.0.2.1
UCS-A /fabric-interconnect* # scope fabric-interconnect b
UCS-A /fabric-interconnect* # set out-of-band ip 192.0.2.112 netmask 255.255.255.0 gw
192.0.2.1
UCS-A /fabric-interconnect* # scope system
UCS-A /system* # set virtual-ip 192.0.2.113
UCS-A /system* # commit-buffer
```

Ethernet Switching Mode

The Ethernet switching mode determines how the fabric interconnect behaves as a switching device between the servers and the network. The fabric interconnect operates in either of the following Ethernet switching modes:

End-Host Mode

End-host mode allows the fabric interconnect to act as an end host to the network, representing all server (hosts) connected to it through vNICs. This is achieved by pinning (either dynamically pinned or hard pinned) vNICs to uplink ports, which provides redundancy toward the network, and makes the uplink ports appear as server ports to the rest of the fabric. When in end-host mode, the fabric interconnect does not run the Spanning Tree Protocol (STP) and avoids loops by denying uplink ports from forwarding traffic to each other, and by denying egress server traffic on more than one uplink port at a time. End-host mode is the default Ethernet switching mode and should be used if either of the following are used upstream:

- Layer 2 switching for L2 Aggregation
- Virtual Switching System (VSS) aggregation layer

**Note**

When end-host mode is enabled, if a vNIC is hard pinned to an uplink port and this uplink port goes down, the system cannot re-pin the vNIC, and the vNIC remains down.

Switch Mode

Switch mode is the traditional Ethernet switching mode. The fabric interconnect runs STP to avoid loops, and broadcast and multicast packets are handled in the traditional way. Switch mode is not the default Ethernet switching mode, and should be used only if the fabric interconnect is directly connected to a router, or if either of the following are used upstream:

- Layer 3 aggregation
- VLAN in a box

**Note**

For both Ethernet switching modes, even when vNICs are hard pinned to uplink ports, all server-to-server unicast traffic in the server array is sent only through the fabric interconnect and is never sent through uplink ports. Server-to-server multicast and broadcast traffic is sent through all uplink ports in the same VLAN.

Configuring Ethernet Switching Mode



Important

When you change the Ethernet switching mode, Cisco UCS Manager logs you out and restarts the fabric interconnect. For a cluster configuration, Cisco UCS Manager restarts both fabric interconnects sequentially. The second fabric interconnect can take several minutes to complete the change in Ethernet switching mode and become system ready.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # set mode {end-host switch} | Sets the fabric interconnect to the specified switching mode. |
| Step 3 | UCS-A /eth-uplink # commit-buffer | Commits the transaction to the system configuration. |

The following example sets the fabric interconnect to end-host mode and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # set mode end-host
Warning: When committed, this change will cause the switch to reboot
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink #
```




CHAPTER 5

Configuring Ports

This chapter includes the following sections:

- [Server and Uplink Ports on the Fabric Interconnect, page 59](#)
- [Server Ports, page 60](#)
- [Uplink Ethernet Ports, page 61](#)
- [Uplink Ethernet Port Channels, page 62](#)

Server and Uplink Ports on the Fabric Interconnect

Each fabric interconnect has a set of ports in a fixed port module that you can configure as either server ports or uplink Ethernet ports. These ports are not reserved. They cannot be used by a Cisco UCS instance until you configure them. You can add expansion modules to increase the number of uplink ports on the fabric interconnect, or to add uplink Fibre Channel ports to the fabric interconnect.

You need to create LAN pin groups and SAN pin groups to pin traffic from servers to an uplink port.

Each fabric interconnect can include the following types of ports:

| | |
|-----------------------------------|--|
| Server Ports | Server ports handle data traffic between the fabric interconnect and the adapter cards on the servers. You can only configure server ports on the fixed port module. Expansion modules do not include server ports. |
| Uplink Ethernet Ports | Uplink Ethernet ports handle Ethernet traffic between the fabric interconnect and the next layer of the network. All network-bound Ethernet traffic is pinned to one of these ports. You can configure uplink Ethernet ports on either the fixed module or an expansion module. You can also configure the admin speed as 1Gbps or 10Gbps and assign a flow control policy to the port. |
| Uplink Fibre Channel Ports | Uplink Fibre Channel ports handle FCoE traffic between the fabric interconnect and the next layer of the network. All network-bound FCoE traffic is pinned to one of these ports. |

You can only configure uplink Fibre Channel ports on an expansion module. The fixed module does not include uplink Fibre Channel ports.

Server Ports

Configuring a Server Port

You can only configure server ports on the fixed port module. Expansion modules do not include server ports.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope eth-server | Enters Ethernet server mode. |
| Step 2 | UCS-A /eth-server # scope fabric {a b} | Enters Ethernet server fabric mode for the specified fabric. |
| Step 3 | UCS-A /eth-server/fabric # create interface slot-num port-num | Creates an interface for the specified Ethernet server port. |
| Step 4 | UCS-A /eth-server/fabric # commit-buffer | Commits the transaction to the system configuration. |

The following example creates an interface for Ethernet server port 12 on slot 1 of fabric B and commits the transaction:

```
UCS-A# scope eth-server
UCS-A /eth-server # scope fabric b
UCS-A /eth-server/fabric # create interface 1 12
UCS-A /eth-server/fabric* # commit-buffer
UCS-A /eth-server/fabric #
```

Deleting a Server Port

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope eth-server | Enters Ethernet server mode. |
| Step 2 | UCS-A /eth-server # scope fabric {a b} | Enters Ethernet server fabric mode for the specified fabric. |
| Step 3 | UCS-A /eth-server/fabric # delete interface slot-num port-num | Deletes the interface for the specified Ethernet server port. |
| Step 4 | UCS-A /eth-server/fabric # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the interface for Ethernet server port 35 on slot 3 of fabric B and commits the transaction:

```
UCS-A# scope eth-server
UCS-A /eth-server # scope fabric b
UCS-A /eth-server/fabric # delete interface 1 12
UCS-A /eth-server/fabric* # commit-buffer
UCS-A /eth-server/fabric #
```

Uplink Ethernet Ports

Configuring an Uplink Ethernet Port

You can configure uplink Ethernet ports on either the fixed module or an expansion module. You can also configure the admin speed as 1Gbps or 10Gbps and assign a flow control policy to the port.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # scope fabric {a b} | Enters Ethernet uplink fabric mode for the specified fabric. |
| Step 3 | UCS-A /eth-uplink/fabric # create interface slot-num port-num | Creates an interface for the specified Ethernet uplink port. |
| Step 4 | UCS-A /eth-uplink/fabric # set speed {10gbps 1gbps} | (Optional) Sets the speed for the specified Ethernet uplink port. |
| Step 5 | UCS-A /eth-uplink/fabric # commit-buffer | Commits the transaction to the system configuration. |

The following example creates an interface for Ethernet uplink port 3 on slot 2 of fabric B, sets the speed to 10 gbps, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric b
UCS-A /eth-uplink/fabric # create interface 2 3
UCS-A /eth-uplink/fabric # set speed 10gbps
UCS-A /eth-uplink/fabric* # commit-buffer
UCS-A /eth-uplink/fabric #
```

Deleting an Uplink Ethernet Port

Procedure

| | Command or Action | Purpose |
|---------------|--------------------------------|------------------------------|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 2 | UCS-A /eth-uplink # scope fabric {a b} | Enters Ethernet uplink fabric mode for the specified fabric. |
| Step 3 | UCS-A /eth-uplink/fabric # delete interface <i>slot-num port-num</i> | Deletes the interface for the specified Ethernet uplink port. |
| Step 4 | UCS-A /eth-uplink/fabric # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the interface for Ethernet uplink port 3 on slot 2 of fabric B and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric b
UCS-A /eth-uplink/fabric # delete interface 2 3
UCS-A /eth-uplink/fabric* # commit-buffer
UCS-A /eth-uplink/fabric #
```

Uplink Ethernet Port Channels

An uplink Ethernet port channel allows you to group several physical uplink Ethernet ports (link aggregation) to create one logical Ethernet link for the purpose of providing fault-tolerance and high-speed connectivity. In Cisco UCS Manager, you create a port channel first and then add uplink Ethernet ports to the port channel. You can add up to eight uplink Ethernet ports to a port channel.



Note

Cisco UCS uses Link Aggregation Control Protocol (LACP), not Port Aggregation Protocol (PAgP), to group the uplink Ethernet ports into a port channel.

Configuring an Uplink Ethernet Port Channel

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # scope fabric {a b} | Enters Ethernet uplink fabric mode for the specified fabric. |
| Step 3 | UCS-A /eth-uplink/fabric # create port-channel <i>port-num</i> | Creates a port channel on the specified Ethernet uplink port, and enters Ethernet uplink fabric port channel mode. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 4 | UCS-A /eth-uplink/fabric/port-channel # { enable disable } | (Optional) Enables or disables the administrative state of the port channel. The port channel is disabled by default. |
| Step 5 | UCS-A /eth-uplink/fabric/port-channel # set name <i>port-chan-name</i> | (Optional) Specifies the name for the port channel. |
| Step 6 | UCS-A /eth-uplink/fabric/port-channel # set flow-control-policy <i>policy-name</i> | (Optional) Assigns the specified flow control policy to the port channel. |
| Step 7 | UCS-A /eth-uplink/fabric/port-channel # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a port channel on port 13 of fabric A, sets the name to portchan13a, enables the administrative state, assigns the flow control policy named flow-con-pol432 to the port channel, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create port-channel 13
UCS-A /eth-uplink/fabric/port-channel* # enable
UCS-A /eth-uplink/fabric/port-channel* # set name portchan13a
UCS-A /eth-uplink/fabric/port-channel* # set flow-control-policy flow-con-pol432
UCS-A /eth-uplink/fabric/port-channel* # commit-buffer
UCS-A /eth-uplink/fabric/port-channel #
```

Deleting an Uplink Ethernet Port Channel

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # scope fabric { a b } | Enters Ethernet uplink fabric mode for the specified fabric. |
| Step 3 | UCS-A /eth-uplink/fabric # delete port-channel <i>port-num</i> | Deletes the port channel on the specified Ethernet uplink port. |
| Step 4 | UCS-A /eth-uplink/fabric # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the port channel on port 13 of fabric A and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # delete port-channel 13
UCS-A /eth-uplink/fabric* # commit-buffer
UCS-A /eth-uplink/fabric #
```

Adding a Member Port to an Uplink Ethernet Port Channel

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # scope fabric {a b } | Enters Ethernet uplink fabric mode for the specified fabric. |
| Step 3 | UCS-A /eth-uplink/fabric # scope port-channel port-num | Enters Ethernet uplink fabric port channel mode for the specified port channel. |
| Step 4 | UCS-A /eth-uplink/fabric/port-channel # create member-port slot-num port-num | Creates the specified member port from the port channel and enters Ethernet uplink fabric port channel member port mode. |
| Step 5 | UCS-A /eth-uplink/fabric/port-channel # commit-buffer | Commits the transaction to the system configuration. |

The following example adds the member port on slot 1, port 7 to the port channel on port 13 of fabric A and commits the transaction.

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope port-channel 13
UCS-A /eth-uplink/fabric # create member-port 1 7
UCS-A /eth-uplink/fabric/port-channel* # commit-buffer
UCS-A /eth-uplink/fabric/port-channel #
```

Deleting a Member Port from an Uplink Ethernet Port Channel

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # scope fabric {a b } | Enters Ethernet uplink fabric mode for the specified fabric. |
| Step 3 | UCS-A /eth-uplink/fabric # scope port-channel port-num | Enters Ethernet uplink fabric port channel mode for the specified port channel. |
| Step 4 | UCS-A /eth-uplink/fabric/port-channel # delete member-port slot-num port-num | Deletes the specified member port from the port channel. |
| Step 5 | UCS-A /eth-uplink/fabric/port-channel # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes a member port from the port channel on port 13 of fabric A and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # scope port-channel 13
UCS-A /eth-uplink/fabric/port-channel # delete member-port 1 7
UCS-A /eth-uplink/fabric/port-channel* # commit-buffer
UCS-A /eth-uplink/fabric/port-channel #
```




CHAPTER 6

Configuring Communication Services

This chapter includes the following sections:

- [Communication Services, page 67](#)
- [Configuring CIM XML, page 68](#)
- [Configuring HTTP, page 69](#)
- [Configuring HTTPS, page 69](#)
- [Configuring SNMP, page 75](#)
- [Configuring Telnet, page 78](#)
- [Disabling Communication Services, page 79](#)

Communication Services

You can use the following communication services to interface third-party applications with Cisco UCS:

| Communication Service | Description |
|-----------------------|---|
| CIM XML | This service is disabled by default and is only available in read-only mode. The default port is 5988. This common information model is one of the standards defined by the Distributed Management Task Force. |
| HTTP | This service is enabled on port 80 by default. You must enable either HTTP or HTTPS to run Cisco UCS Manager GUI. If you select HTTP, all data is exchanged in clear text mode. For security purposes, we recommend that you enable HTTPS and disable HTTP. |
| HTTPS | This service is enabled on port 443 by default. You must enable either HTTP or HTTPS to run Cisco UCS Manager GUI. If you select HTTPS, all data is exchanged in encrypted mode through a secure server. |

| Communication Service | Description |
|-----------------------|--|
| | For security purposes, we recommend that you enable HTTPS and disable HTTP. |
| SMASH CLP | This service is enabled for read-only access and supports a limited subset of the protocols, such as the show command. You cannot disable it. This shell service is one of the standards defined by the Distributed Management Task Force. |
| SNMP | This service is disabled by default. If enabled, the default port is 161. You must configure the community and at least one SNMP trap. Enable this service only if your system includes integration with an SNMP server. |
| SSH | This service is enabled on port 22. You cannot disable it, nor can you change the default port. This service provides access to the Cisco UCS Manager CLI. |
| Telnet | This service is disabled by default. This service provides access to the Cisco UCS Manager CLI. |

Configuring CIM XML

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope services | Enters system services mode. |
| Step 3 | UCS-A /system/services # enable cimxml | Enables the CIM XML service. |
| Step 4 | UCS-A /system/services # set cimxml port <i>port-num</i> | Specifies the port to be used for the CIM XML connection. |
| Step 5 | UCS-A /system/services # commit-buffer | Commits the transaction to the system configuration. |

The following example enables CIM XML, sets the port number to 5988, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # enable cimxml
UCS-A /system/services* # set cimxml port 5988
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

Configuring HTTP

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope services | Enters system services mode. |
| Step 3 | UCS-A /system/services # enable http | Enables the HTTP service. |
| Step 4 | UCS-A /system/services # set http port <i>port-num</i> | Specifies the port to be used for the HTTP connection. |
| Step 5 | UCS-A /system/services # commit-buffer | Commits the transaction to the system configuration. |

The following example enables HTTP, sets the port number to 80, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # enable http
UCS-A /system/services* # set http port 80
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

Configuring HTTPS

Certificates, Key Rings, and Trusted Points

HTTPS uses components of the Public Key Infrastructure (PKI) to establish secure communications between two devices, such as a client's browser and Cisco UCS Manager.

Encryption Keys and Key Rings

Each PKI device holds a pair of asymmetric Rivest-Shamir-Adleman (RSA) encryption keys, one kept private and one made public, stored in an internal key ring. A message encrypted with either key can be decrypted with the other key. To send an encrypted message, the sender encrypts the message with the receiver's public key, and the receiver decrypts the message using its own private key. A sender can also prove its ownership of a public key by encrypting (also called 'signing') a known message with its own private key. If a receiver can successfully decrypt the message using the public key in question, the sender's possession of the corresponding private key is proven. Encryption keys can vary in length, with typical lengths from 512 bits to 2048 bits. In general, a longer key is more secure than a shorter key. Cisco UCS Manager provides a default key ring with an initial 1024-bit key pair, and allows you to create additional key rings.

Certificates

To prepare for secure communications, two devices first exchange their digital certificates. A certificate is a file containing a device's public key along with signed information about the device's identity. To merely support encrypted communications, a device can generate its own key pair and its own self-signed certificate. When a remote user connects to a device that presents a self-signed certificate, the user has no easy method

to verify the identity of the device, and the user's browser will initially display an authentication warning. By default, Cisco UCS Manager contains a built-in self-signed certificate containing the public key from the default key ring.

Trusted Points

To provide stronger authentication for Cisco UCS Manager, you can obtain and install a third-party certificate from a trusted source, or trusted point, that affirms the identity of your device. The third-party certificate is signed by the issuing trusted point, which can be a root certificate authority (CA) or an intermediate CA or trust anchor that is part of a trust chain that leads to a root CA. To obtain a new certificate, you must generate a certificate request through Cisco UCS Manager and submit the request to a trusted point.

Creating a Key Ring

Procedure

| | Command or Action | Purpose |
|---------------|---|----------------------------------|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # create keyring <i>keyring-name</i> | Creates and names the key ring. |
| Step 3 | UCS-A /security/keyring # set modulus { mod1024 mod1536 mod2048 mod512 } | Sets the SSL key length in bits. |
| Step 4 | UCS-A /security/keyring # commit-buffer | Commits the transaction. |

The following example creates a keyring with a key size of 1024 bits:

```
UCS-A# scope security
UCS-A /security # create keyring kr220
UCS-A /security/keyring* # set modulus mod1024
UCS-A /security/keyring* # commit-buffer
UCS-A /security/keyring #
```

What to Do Next

Create a certificate request for this key ring.

Creating a Certificate Request for a Key Ring

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # scope keyring <i>keyring-name</i> | Enters configuration mode for the key ring. |
| Step 3 | UCS-A /security/keyring # create certreq { ip <i>ip-address</i> subject-name <i>name</i> } | Creates a certificate request using the IP address or name of the fabric interconnect. You are prompted to enter a password for the certificate request. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 4 | UCS-A /security/keyring # commit-buffer | Commits the transaction. |
| Step 5 | UCS-A /security/keyring # show certreq | Displays the certificate request, which you can copy and send to a trust anchor or certificate authority. |

The following example creates and displays a certificate request for a key ring:

```
UCS-A# scope security
UCS-A /security # scope keyring kr220
UCS-A /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04
Certificate request password:
Confirm certificate request password:
UCS-A /security/keyring* # commit-buffer
UCS-A /security/keyring # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYWw1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF80PhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHO4SwccAUXQ5Zngf45YtX1WsyLwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWwNIcECSsEiXjAN
BgkqhkiG9w0BAQQFAA0BgQCxsN0qUHYGFoQw56RwQueLTNPnrndqUuwZHU003Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWicTWgHhH8BimOb/0OKuG8kwfIGGsED1Av
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGx1DNqon+odCXpC5kjoXD01ZTL09H
BA==
-----END CERTIFICATE REQUEST-----
UCS-A /security/keyring #
```

What to Do Next

- Copy the text of the certificate request, including the BEGIN and END lines, and save it in a file. Send the file with the certificate request to a trust anchor or certificate authority to obtain a certificate for the key ring.
- Create a trusted point and set the certificate chain for the certificate of trust received from the trust anchor.

Creating a Trusted Point

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # create trustpoint <i>name</i> | Creates and names a trusted point. |
| Step 3 | UCS-A /security/trustpoint # set certchain [<i>certchain</i>] | Specifies certificate information for this trusted point. If you do not specify certificate information in the command, you are prompted to enter a certificate or a list of trustpoints defining a certification path to the root |

| | Command or Action | Purpose |
|---------------|--|---|
| | | certificate authority (CA). On the next line following your input, type ENDOFBUF to finish. |
| Step 4 | UCS-A /security/trustpoint # commit-buffer | Commits the transaction. |

The following example creates a trusted point and provides a certificate for the trusted point:

```
UCS-A# scope security
UCS-A /security # create trustpoint tPoint10
UCS-A /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwyDVQQKEwxFeGFtcGx1IE1uYy4xEzARBGNVBASt
> CLRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWElHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCCyU
> ZgAMivYCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GMbkPayV1QjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bf5wZVNAgMBAAGGJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzC1903O6Mg51zq1zXcz75+VFj2I6rH9asckClD3mkOVx5gJU
> Ptt5CVQpNgNldvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtlv1WvfhevskV0j6
> jtcEMyZ+f7+3yh42lido3nO4MIGeBgNVHSMGZyYwgZOAFLlNjtcEMyZ+f7+3yh42
> lido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0EwFDASBgNVBAcT
> ClNhbnRhIENsYXJhMRswGQYDVQQKEwJ0dW92YSBTeXN0ZW1zIE1uYy4xZDASBgNV
> BAsTC0VuZ21uZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwdAYDVR0TBAAUwAEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
UCS-A /security/trustpoint* # commit-buffer
UCS-A /security/trustpoint #
```

What to Do Next

Obtain a key ring certificate from the trust anchor or certificate authority and import it into the key ring.

Importing a Certificate into a Key Ring

Before You Begin

- Obtain a key ring certificate from a trust anchor or certificate authority.
- A trusted point must be configured that contains the certificate chain for the key ring certificate.

Procedure

| | Command or Action | Purpose |
|---------------|------------------------------|-----------------------|
| Step 1 | UCS-A# scope security | Enters security mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 2 | UCS-A /security # scope keyring <i>keyring-name</i> | Enters configuration mode for the key ring that will receive the certificate. |
| Step 3 | UCS-A /security/keyring # set trustpoint <i>name</i> | Specifies the trusted point for the trust anchor or certificate authority from which the key ring certificate was obtained. |
| Step 4 | UCS-A /security/keyring # set cert | Launches a dialog for entering and uploading the key ring certificate. At the prompt, paste the certificate text that you received from the trust anchor or certificate authority. On the next line following the certificate, type ENDOFBUF to complete the certificate input. |
| Step 5 | UCS-A /security/keyring # commit-buffer | Commits the transaction. |

The following example specifies the trust point and imports a certificate into a key ring:

```
UCS-A# scope security
UCS-A /security # scope keyring kr220
UCS-A /security/keyring # set trustpoint tPoint10
UCS-A /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwZkxkCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENEMRUwEwYDVQQKEwxFeGFtcGx1IEluYy4xEzARBgNVBASt
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivYCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBKOND1
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bf5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJavMhzC190306Mg51zqlzXcz75+VFj2I6rH9asckCl1d3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtv1WvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L4317IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
UCS-A /security/keyring* # commit-buffer
UCS-A /security/keyring #
```

What to Do Next

Configure your HTTPS service with the key ring.

Configuring HTTPS

Procedure

| | Command or Action | Purpose |
|---------------|----------------------------|---------------------|
| Step 1 | UCS-A# scope system | Enters system mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 2 | UCS-A /system # scope services | Enters system services mode. |
| Step 3 | UCS-A /system/services # enable https | Enables the HTTPS service. |
| Step 4 | UCS-A /system/services # set https port <i>port-num</i> | Specifies the port to be used for the HTTPS connection. |
| Step 5 | UCS-A /system/services # set https keyring <i>keyring-name</i> | Specifies the name for the HTTPS keyring. Caution When the HTTPS keyring is modified using the set https keyring command, all current HTTP and HTTPS sessions are closed without warning. |
| Step 6 | UCS-A /system/services # commit-buffer | Commits the transaction to the system configuration. |

The following example enables HTTPS, sets the port number to 443, sets the key ring name to kring7984, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # enable https
UCS-A /system/services* # set https port 443
UCS-A /system/services* # set https keyring kring7984
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

Deleting a Key Ring

Procedure

| | Command or Action | Purpose |
|---------------|---|-----------------------------|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # delete keyring <i>name</i> | Deletes the named key ring. |
| Step 3 | UCS-A /security # commit-buffer | Commits the transaction. |

The following example deletes a key ring:

```
UCS-A# scope security
UCS-A /security # delete keyring key10
UCS-A /security* # commit-buffer
UCS-A /security #
```

Deleting a Trusted Point

Procedure

| | Command or Action | Purpose |
|---------------|---|----------------------------------|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # delete trustpoint name | Deletes the named trusted point. |
| Step 3 | UCS-A /security # commit-buffer | Commits the transaction. |

The following example deletes a trusted point:

```
UCS-A# scope security
UCS-A /security # delete trustpoint tPoint10
UCS-A /security* # commit-buffer
UCS-A /security #
```

Configuring SNMP

Enabling SNMP and Configuring an SNMP Community

SNMP messages from a Cisco UCS instance display the fabric interconnect name rather than the system name.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # enable snmp | Enables SNMP. |
| Step 3 | UCS-A /monitoring # set snmp community community-name | Specifies SNMP community. The community name can be any alphanumeric string up to 32 characters. |
| Step 4 | UCS-A /monitoring # commit-buffer | Commits the transaction to the system configuration. |

The following example enables SNMP, configures an SNMP community named SnmpCommSystem2, and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # set snmp community SnmpCommSystem2
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

What to Do Next

Create SNMP trap hosts and users.

Creating an SNMP Trap Host

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # enable snmp | Enables SNMP. |
| Step 3 | UCS-A /monitoring # create snmp-trap {hostname ip-addr} | Creates an SNMP trap host with the specified hostname or IP address. |
| Step 4 | UCS-A /monitoring/snmp-trap # set community community-name | Specifies the SNMP community name to be used for the SNMP trap. |
| Step 5 | UCS-A /monitoring/snmp-trap # set port port-num | Specifies the port to be used for the SNMP trap. |
| Step 6 | UCS-A /monitoring/snmp-trap # commit-buffer | Commits the transaction to the system configuration. |

The following example enables SNMP, creates an SNMP trap, specifies that the trap will use the SnmpCommSystem2 community on port 2, and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # create snmp-trap 192.168.100.112
UCS-A /monitoring/snmp-trap* # set community SnmpCommSystem2
UCS-A /monitoring/snmp-trap* # set port 2
UCS-A /monitoring/snmp-trap* # commit-buffer
UCS-A /monitoring/snmp-trap #
```

Deleting an SNMP Trap Host

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # delete snmp-trap {hostname ip-addr} | Deletes the specified SNMP trap host with the specified hostname or IP address. |
| Step 3 | UCS-A /monitoring # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the SNMP trap at IP address 192.168.100.112 and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # delete snmp-trap 192.168.100.112
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

Creating an SNMPv3 User

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # enable snmp | Enables SNMP. |
| Step 3 | UCS-A /monitoring # create snmp-user <i>user-name</i> | Creates the specified SNMPv3 user. An SNMP user name cannot be the same as a local user name. Choose an SNMP user name that does not match a local user name. |
| Step 4 | UCS-A /monitoring/snmp-user # set aes-128 {no yes} | Enables or disables the use of AES-128 encryption. |
| Step 5 | UCS-A /monitoring/snmp-user # set auth {md5 sha} | Specifies the use of MD5 or DHA authentication. |
| Step 6 | UCS-A /monitoring/snmp-user # set password | Specifies the user password. After you enter the set password command, you are prompted to enter and confirm the password. |
| Step 7 | UCS-A /monitoring/snmp-user # set priv-password | Specifies the user privacy password. After you enter the set priv-password command, you are prompted to enter and confirm the privacy password. |
| Step 8 | UCS-A /monitoring/snmp-user # commit-buffer | Commits the transaction to the system configuration. |

The following example enables SNMP, creates an SNMPv3 user named snmp-user14, disables AES-128 encryption, specifies the use of MD5 authentication, sets the password and privacy password, and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # enable snmp
UCS-A /monitoring* # create snmp-user snmp-user14
UCS-A /monitoring/snmp-user* # set aes-128 no
UCS-A /monitoring/snmp-user* # set auth md5
UCS-A /monitoring/snmp-user* # set password
Enter a password:
Confirm the password:
UCS-A /monitoring/snmp-user* # set priv-password
Enter a password:
Confirm the password:
UCS-A /monitoring/snmp-user* # commit-buffer
UCS-A /monitoring/snmp-user #
```

Deleting an SNMPv3 User

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # delete snmp-user <i>user-name</i> | Deletes the specified SNMPv3 user. |
| Step 3 | UCS-A /monitoring # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the SNMPv3 user named snmp-user14 and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # delete snmp-user snmp-user14
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

Disabling SNMP

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # disable snmp | Disables the SNMP service. |
| Step 3 | UCS-A //monitoring # commit-buffer | Commits the transaction to the system configuration. |

The following example disables SNMP and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # disable snmp
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```

Configuring Telnet

Procedure

| | Command or Action | Purpose |
|---------------|---------------------------------------|------------------------------|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope services | Enters system services mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 3 | UCS-A /services # enable telnet-server | Enables the Telnet service. |
| Step 4 | UCS-A /services # commit-buffer | Commits the transaction to the system configuration. |

The following example enables Telnet and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /services # enable telnet-server
UCS-A /services* # commit-buffer
UCS-A /services #
```

Disabling Communication Services

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope services | Enters system services mode. |
| Step 3 | UCS-A /system/services # disable <i>service-name</i> | Disables the specified service, where the <i>service-name</i> argument is one of the following keywords: <ul style="list-style-type: none"> • <i>cimxml</i>—Disables CIM XML service • http—Disables HTTP service • https—Disables HTTPS service • telnet-server—Disables Telnet service |
| Step 4 | UCS-A /system/services # commit-buffer | Commits the transaction to the system configuration. |

The following example disables CIM XML and commits the transaction:

```
UCS-A# scope system
UCS-A# scope services
UCS-A /system/services # disable cimxml
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```




CHAPTER 7

Configuring Primary Authentication

This chapter includes the following sections:

- [Primary Authentication, page 81](#)
- [Remote Authentication Providers, page 81](#)
- [Creating a Remote Authentication Provider, page 83](#)
- [Selecting a Primary Authentication Service, page 88](#)

Primary Authentication

Cisco UCS supports two methods to authenticate user logins:

- Local to Cisco UCS Manager
- Remote through one of the following protocols:
 - LDAP
 - RADIUS
 - TACACS+



Note

You can only use one authentication method. For example, if you select LDAP as your authentication provider, you cannot use RADIUS or TACACS+ for authentication. However, if the user account in the remote authentication provider does not have at least one Cisco UCS role, Cisco UCS Manager checks the local database to determine whether an account with the same name exists in the local database.

Remote Authentication Providers

If a system is configured for one of the supported remote authentication services, you must create a provider for that service to ensure that Cisco UCS Manager can communicate with it. In addition, you need to be aware of the following guidelines that impact user authorization:

User Accounts in Remote Authentication Services

You can create user accounts in Cisco UCS Manager or in the remote authentication server.

The temporary sessions for users who log in through remote authentication services can be viewed through Cisco UCS Manager GUI or Cisco UCS Manager CLI.

User Roles in Remote Authentication Services

If you create user accounts in the remote authentication server, you must ensure that the accounts include the roles those users require for working in Cisco UCS Manager and that the names of those roles match the names used in Cisco UCS Manager. If an account does not have the required roles, the user is granted only read-only privileges.

User Attribute for LDAP

If a Cisco UCS instance uses LDAP as the remote authentication provider, you can do one of the following:

- Map an existing attribute to the user roles and locale for the Cisco UCS instance.
- Create a CiscoAVPair or other unique attribute in the LDAP service and map that attribute to the user roles and locale for the Cisco UCS instance.

You must configure the LDAP provider in Cisco UCS Manager with the attribute that holds the user roles and locales. When a user logs in, Cisco UCS Manager checks for the value of this attribute when it queries the remote authentication service and validates the user.

If you create a CiscoAVPair attribute for the Cisco UCS instance, use the following definition for the OID:

```
CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
LDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

Required User Attribute for RADIUS

If a Cisco UCS instance uses RADIUS as the remote authentication provider, you must create a cisco-avpair attribute in the remote authentication service and map that attribute to the user roles and locale for the Cisco UCS instance. When a user logs in, Cisco UCS Manager checks for the value of this attribute when it queries the remote authentication service and validates the user.



Note

You cannot use any other attribute in RADIUS for the Cisco UCS roles. You must create the required attribute in RADIUS.

Required User Attribute for TACACS+

If a Cisco UCS instance uses either RADIUS or TACACS+ as the remote authentication provider, you must create a `cisco-av-pair` attribute in the remote authentication service and map that attribute to the user roles and locale for the Cisco UCS instance. When a user logs in, Cisco UCS Manager checks for the value of this attribute when it queries the remote authentication service and validates the user.

**Note**

You cannot use any other attribute in RADIUS or TACACS+ for the Cisco UCS roles. You must create the attribute required for that specific remote authentication service.

Creating a Remote Authentication Provider

Configuring Properties for LDAP Providers

The properties that you configure in this task apply to all LDAP provider connections.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # scope ldap | Enters security LDAP mode. |
| Step 3 | UCS-A /security/ldap # set attribute attribute | Restricts database searches to records that contain the specified attribute. |
| Step 4 | UCS-A /security/ldap # set basedn distinguished-name | Restricts database searches to records that contain the specified distinguished name. |
| Step 5 | UCS-A /security/ldap # set filter filter | Restricts database searches to records that contain the specified filter. |
| Step 6 | UCS-A /security/ldap # set timeout seconds | (Optional) Sets the time interval the system waits for a response from the LDAP server before noting the server as down. |
| Step 7 | UCS-A /security/ldap # commit-buffer | Commits the transaction to the system configuration. |

The following example sets the LDAP attribute to `CiscoAvPair`, the base distinguished name to `"DC=cisco-ucsm-aaa3,DC=qalab,DC=com"`, the filter to `sAMAccountName=$userid`, and the timeout interval to 5 seconds, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # set attribute CiscoAvPair
UCS-A /security/ldap* # set basedn "DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCS-A /security/ldap* # set filter sAMAccountName=$userid
UCS-A /security/ldap* # set timeout 5
```

```
UCS-A /security/ldap* # commit-buffer
UCS-A /security/ldap #
```

What to Do Next

Create an LDAP provider.

Creating an LDAP Provider

Before You Begin

Perform the following configuration in the LDAP server:

- Configure users with the attribute that holds the user role and locale information for Cisco UCS Manager. You can use an existing LDAP attribute that is mapped to the Cisco UCS user roles and locales or create a custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 1.3.6.1.4.1.9.287247.1.
- For a cluster configuration, add the management port IP addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.

Configure the properties for the LDAP provider connections in Cisco UCS Manager.

If SSL will be enabled, create a trustpoint in Cisco UCS Manager containing the certificate chain of the certificate authority (CA) that signed the LDAP server's certificate.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # scope ldap | Enters security LDAP mode. |
| Step 3 | UCS-A /security/ldap # create server <i>server-name</i> | Creates an LDAP server instance and enters security LDAP server mode. If SSL is enabled, the <i>server-name</i> , typically an IP address or FQDN, must exactly match a Common Name (CN) in the LDAP server's security certificate. Unless an IP address is specified, a DNS server must be configured in Cisco UCS Manager. |
| Step 4 | UCS-A /security/ldap/server # set ssl { yes no } | Enables or disables the use of encryption when communicating with the LDAP server. The options are as follows: <ul style="list-style-type: none"> • yes—Encryption is required. If encryption cannot be negotiated, the connection fails. • no—Encryption is disabled. Authentication information is sent as clear text. |
| Step 5 | UCS-A /security/ldap/server # set binddn <i>bind-dist-name</i> | Specifies the distinguished name (DN) for the LDAP database superuser account. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 6 | UCS-A /security/ldap/server # set key | Specifies the password for the LDAP database superuser account. To set the key value, press Enter after typing the set key command and enter the key value at the prompt. |
| Step 7 | UCS-A /security/ldap/server # set port <i>port-num</i> | (Optional) Specifies the port used to communicate with the LDAP server. The standard port number is 389. |
| Step 8 | UCS-A /security/ldap/server # commit-buffer | Commits the transaction to the system configuration. |

The following example configures the properties for all LDAP provider connections, then creates an LDAP server instance named 10.193.169.246 and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope ldap
UCS-A /security/ldap # set attribute CiscoAVPair
UCS-A /security/ldap # set filter sAccountName=$userid
UCS-A /security/ldap* # set basedn "DC=qalab,DC=com"
UCS-A /security/ldap* # create server 10.193.169.246
UCS-A /security/ldap/server* # set ssl yes
UCS-A /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCS-A /security/ldap/server* # set key
Enter the key:
Confirm the key:
UCS-A /security/ldap/server* # set port 389
UCS-A /security/ldap/server* # commit-buffer
UCS-A /security/ldap/server #
```

What to Do Next

Select LDAP as the primary authentication service.

Configuring Properties for RADIUS Providers

The properties that you configure in this task apply to all RADIUS provider connections.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # scope radius | Enters security RADIUS mode. |
| Step 3 | UCS-A /security/radius # set retries <i>retry-num</i> | (Optional) Sets the number of times to retry communicating with the RADIUS server before noting the server as down. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 4 | UCS-A /security/radius # set timeout <i>seconds</i> | (Optional) Sets the time interval the system waits for a response from the RADIUS server before noting the server as down. |
| Step 5 | UCS-A /security/radius # commit-buffer | Commits the transaction to the system configuration. |

The following example sets the RADIUS retries to 4, sets the timeout interval to 30 seconds, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # set retries 4
UCS-A /security/radius* # set timeout 30
UCS-A /security/radius* # commit-buffer
UCS-A /security/radius #
```

What to Do Next

Create a RADIUS provider.

Creating a RADIUS Provider

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # scope radius | Enters security RADIUS mode. |
| Step 3 | UCS-A /security/radius # create server <i>server-name</i> | Creates a RADIUS server instance and enters security RADIUS server mode |
| Step 4 | UCS-A /security/radius/server # set authport <i>authport-num</i> | Specifies the port used to communicate with the RADIUS server. |
| Step 5 | UCS-A /security/radius/server # set key | (Optional) Sets the RADIUS server key. To set the key value, press Enter after typing the set key command and enter the key value at the prompt. |
| Step 6 | UCS-A /security/radius/server # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a server instance named radiusserv7, sets the authentication port to 5858, sets the key to radiuskey321, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope radius
UCS-A /security/radius # create server radiusserv7
UCS-A /security/radius/server* # set authport 5858
UCS-A /security/radius/server* # set key
```

```

Enter the key: radiuskey321
Confirm the key: radiuskey321
UCS-A /security/radius/server* # commit-buffer
UCS-A /security/radius/server #

```

Configuring Properties for TACACS+ Providers

The properties that you configure in this task apply to all TACACS+ provider connections.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # scope tacacs | Enters security TACACS+ mode. |
| Step 3 | UCS-A /security/tacacs # set timeout <i>seconds</i> | (Optional) Sets the time interval the system waits for a response from the TACACS+ server before noting the server as down. |
| Step 4 | UCS-A /security/tacacs # commit-buffer | Commits the transaction to the system configuration. |

The following example sets the TACACS+ timeout interval to 45 seconds and commits the transaction:

```

UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # set timeout 45
UCS-A /security/tacacs* # commit-buffer
UCS-A /security/tacacs #

```

What to Do Next

Create a TACACS+ provider.

Creating a TACACS+ Provider

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # scope tacacs | Enters security TACACS+ mode. |
| Step 3 | UCS-A /security/tacacs # create server <i>server-name</i> | Creates an TACACS+ server instance and enters security TACACS+ server mode |
| Step 4 | UCS-A /security/tacacs/server # set key | (Optional) Sets the TACACS+ server key. To set the key value, press Enter after typing the set key command and enter the key value at the prompt. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 5 | UCS-A /security/tacacs/server # set port <i>port-num</i> | Specifies the port used to communicate with the TACACS+ server. |
| Step 6 | UCS-A /security/tacacs/server # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a server instance named tacacsserv680, sets the key to tacacskey321, sets the authentication port to 5859, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope tacacs
UCS-A /security/tacacs # create server tacacsserv680
UCS-A /security/tacacs/server* # set key
Enter the key: tacacskey321
Confirm the key: tacacskey321
UCS-A /security/tacacs/server* # set port 5859
UCS-A /security/tacacs/server* # commit-buffer
UCS-A /security/tacacs/server #
```

Selecting a Primary Authentication Service

Selecting the Console Authentication Service

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # set authentication console <i>auth-type</i> | Specifies the console authentication, where the <i>auth-type</i> argument is one of the following keywords: <ul style="list-style-type: none"> • ldap—Specifies LDAP authentication • local—Specifies local authentication • none—Allows local users to log on without specifying a password • radius—Specifies RADIUS authentication • tacacs—Specifies TACACS+ authentication |
| Step 3 | UCS-A /security # commit-buffer | Commits the transaction to the system configuration. |

The following example sets the console to use local authentication and commits the transaction:

```
UCS-A# scope security
UCS-A /security # set authentication console local
UCS-A /security* # commit-buffer
UCS-A /security #
```

Selecting the Default Authentication Service

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # set authentication default <i>auth-type</i> | Specifies the default authentication, where the <i>auth-type</i> argument is one of the following keywords: <ul style="list-style-type: none"> • ldap—Specifies LDAP authentication • local—Specifies local authentication • none—Allows local users to log on without specifying a password • radius—Specifies RADIUS authentication • tacacs—Specifies TACACS+ authentication |
| Step 3 | UCS-A /security # commit-buffer | Commits the transaction to the system configuration. |

The following example sets the default authentication to LDAP and commits the transaction:

```
UCS-A# scope security
UCS-A /security # set authentication default ldap
UCS-A /security* # commit-buffer
UCS-A /security #
```




CHAPTER 8

Configuring Organizations

This chapter includes the following sections:

- [Organizations in a Multi-Tenancy Environment, page 91](#)
- [Hierarchical Name Resolution in a Multi-Tenancy Environment, page 92](#)
- [Configuring an Organization Under the Root Organization, page 93](#)
- [Configuring an Organization Under an Organization that is not Root, page 94](#)
- [Deleting an Organization, page 95](#)

Organizations in a Multi-Tenancy Environment

Multi-tenancy allows you to divide up the large physical infrastructure of an instance into logical entities known as organizations. As a result, you can achieve a logical isolation between organizations without providing a dedicated physical infrastructure for each organization.

You can assign unique resources to each tenant through the related organization, in the multi-tenant environment. These resources can include different policies, pools, and quality of service definitions. You can also implement locales to assign or restrict user privileges and roles by organization, if you do not want all users to have access to all organizations.

If you set up a multi-tenant environment, all organizations are hierarchical. The top-level organization is always root. The policies and pools that you create in root are system-wide and are available to all organizations in the system. However, any policies and pools created in other organizations are only available to organizations that are above it in the same hierarchy. For example, if a system has organizations named Finance and HR that are not in the same hierarchy, Finance cannot use any policies in the HR organization, and HR cannot access any policies in the Finance organization. However, both Finance and HR can use policies and pools in the root organization.

If you create organizations in a multi-tenant environment, you can also set up one or more of the following for each organization or for a sub-organization in the same hierarchy:

- Resource pools
- Policies
- Service profiles

- Service profile templates

The root organization is always the top level organization.

Hierarchical Name Resolution in a Multi-Tenancy Environment

In a multi-tenant environment, Cisco UCS uses the hierarchy of an organization to resolve the names of policies and resource pools. When Cisco UCS Manager searches for details of a policy or a resource assigned to a pool, the following occurs:

- 1 Cisco UCS Manager checks for policies and pools with the specified name within the organization assigned to the service profile or policy.
- 2 If a policy is found or an available resource is inside a pool, Cisco UCS Manager uses that policy or resource. If the pool does not have any available resources at the local level, Cisco UCS Manager moves up in the hierarchy to the parent organization and searches for a pool with the same name. Cisco UCS Manager repeats this step until the search reaches the root organization.
- 3 If the search reaches the root organization and has not found an available resource or policy, Cisco UCS Manager returns to the local organization and begins to search for a default policy or available resource in the default pool.
- 4 If an applicable default policy or available resource in a default pool is found, Cisco UCS Manager uses that policy or resource. If the pool does not have any available resources, Cisco UCS Manager moves up in the hierarchy to the parent organization and searches for a default pool. Cisco UCS Manager repeats this step until the search reaches the root organization.
- 5 If Cisco UCS Manager cannot find an applicable policy or available resource in the hierarchy, it returns an allocation error.

Example: Server Pool Name Resolution in a Single-Level Hierarchy

In this example, all organizations are at the same level below the root organization. For example, a service provider creates separate organizations for each customer. In this configuration, organizations only have access to the policies and resource pools assigned to that organization and to the root organization.

In this example, a service profile in the XYZcustomer organization is configured to use servers from the XYZcustomer server pool. When resource pools and policies are assigned to the service profile, the following occurs:

- 1 Cisco UCS Manager checks for an available server in the XYZcustomer server pool.
- 2 If the XYZcustomer server pool has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the pool does not have an available server, Cisco UCS Manager checks the root organization for a server pool with the same name.
- 3 If the root organization includes an XYZcustomer server pool and that pool has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the pool does not have an available server, Cisco UCS Manager returns to the XYZcustomer organization to check the default server pool.
- 4 If the default pool in the XYZcustomer organization has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the default pool does not have an available server, Cisco UCS Manager checks the default server pool in the root organization.

- 5 If the default server pool in the root organization has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the default pool does not have an available server, Cisco UCS Manager returns an allocation error.

Example: Server Pool Name Resolution in a Multi-Level Hierarchy

In this example, each organization includes at least one suborganization. For example, a company could create organizations for each major division in the company and for subdivisions of those divisions. In this configuration, each organization has access to its local policies and resource pools and to the resource pools in the parent hierarchy.

In this example, the Finance organization includes two sub-organizations, AccountsPayable and AccountsReceivable. A service profile in the AccountsPayable organization is configured to use servers from the AP server pool. When resource pools and policies are assigned to the service profile, the following occurs:

- 1 Cisco UCS Manager checks for an available server in the AP server pool defined in the service profile.
- 2 If the AP server pool has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the pool does not have an available server, Cisco UCS Manager moves one level up the hierarchy and checks the Finance organization for a pool with the same name.
- 3 If the Finance organization includes a pool with the same name and that pool has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the pool does not have an available server, Cisco UCS Manager moves one level up in the hierarchy and checks the root organization for a pool with the same name.
- 4 If the root organization includes a pool with the same name and that pool has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the pool does not have an available server, Cisco UCS Manager returns to the AccountsPayable organization to check the default server pool.
- 5 If the default pool in the AccountsPayable organization has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the default pool does not have an available server, Cisco UCS Manager moves one level up in the hierarchy and checks the default server pool in the Finance organization.
- 6 If the default pool in the Finance organization has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the default pool does not have an available server, Cisco UCS Manager moves one level up in the hierarchy and checks the default server pool in the root organization.
- 7 If the default server pool in the root organization has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the default pool does not have an available server, Cisco UCS Manager returns an allocation error.

Configuring an Organization Under the Root Organization

Procedure

| | Command or Action | Purpose |
|--------|---------------------------------|------------------------------------|
| Step 1 | UCS-A# <code>scope org /</code> | Enters the root organization mode. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 2 | UCS-A /org # create org <i>org-name</i> | Creates the specified organization under the root organization and enters organization mode for the specified organization. Note When you move from one organization mode to another, the command prompt does not change. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example creates an organization named Finance under the root organization and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create org Finance
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring an Organization Under an Organization that is not Root

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope org / | Enters the root organization mode. |
| Step 2 | UCS-A /org # scope org <i>org-name</i> | Enters organization mode for the specified organization. Note When you move from one organization mode to another, the command prompt does not change. |
| Step 3 | UCS-A /org # create org <i>org-name</i> | Creates the specified organization under the previously configured non-root organization and enters organization mode for the specified organization. |
| Step 4 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example creates an organization named Finance under the NorthAmerica organization and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope org NorthAmerica
UCS-A /org # create org Finance
UCS-A /org* # commit-buffer
UCS-A /org #
```

Deleting an Organization

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope org / | Enters the root organization mode. |
| Step 2 | UCS-A /org # delete org <i>org-name</i> | Deletes the specified organization. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the organization under the root organization named Finance and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete org Finance
UCS-A /org* # commit-buffer
UCS-A /org #
```




CHAPTER 9

Configuring Role-Based Access Control

This chapter includes the following sections:

- [Role-Based Access Control, page 97](#)
- [User Accounts for Cisco UCS Manager, page 97](#)
- [User Roles, page 99](#)
- [Privileges, page 100](#)
- [User Locales, page 102](#)
- [Configuring User Roles, page 102](#)
- [Configuring Locales, page 104](#)
- [Configuring User Accounts, page 106](#)
- [Monitoring User Sessions, page 110](#)

Role-Based Access Control

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the privileges of a user in the system and the locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and locales.

A user is granted write access to desired system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the Server Administrator role in the Engineering organization could update server configurations in the Engineering organization but could not update server configurations in the Finance organization unless the locales assigned to the user include the Finance organization.

User Accounts for Cisco UCS Manager

User accounts are used to access the system. Up to 48 user accounts can be configured in each Cisco UCS instance. Each user account must have a unique username and password.

A user account can be set with a SSH public key. The public key can be set in either of the two formats: OpenSSH and SECSH.

Default User Account

Each Cisco UCS instance has a default user account, admin, which cannot be modified or deleted. This account is the system administrator or superuser account and has full privileges. There is no default password assigned to the admin account; you must choose the password during the initial system setup.

Expiration of User Accounts

User accounts can be configured to expire at a predefined time. When the expiration time is reached the user account is disabled.

By default, user accounts do not expire.

Guidelines for Cisco UCS Manager Usernames

The username is also used as the login ID for Cisco UCS Manager. When you assign usernames to Cisco UCS Manager user accounts, consider the following guidelines and restrictions:

- The login ID can contain between 1 and 32 characters, including the following:
 - Any alphabetic character
 - Any digit
 - _ (underscore)
 - - (dash)
 - @
- The unique username for each user account cannot be all-numeric. You cannot create a local user with an all-numeric username.
- The unique username cannot start with a number.
- If an all-numeric username exists on an AAA server (RADIUS or TACACS+) and is entered during login, Cisco UCS Manager cannot log in the user.

After you create a user account, you cannot change the username. You must delete the user account and create a new one.

**Note**

You can create up to 48 user accounts in a Cisco UCS instance.

Guidelines for Cisco UCS Manager Passwords

For authentication purposes, a password is required for each user account. To prevent users from choosing insecure passwords, each password must be strong. Cisco UCS Manager rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters.

- Must contain at least three of the following:
 - Lower case letters
 - Upper case letters
 - Digits
 - Special characters
- Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: \$ (dollar sign), ? (question mark), and = (equals sign).
- Should not be blank for local user and admin accounts.

If the Cisco UCS instance is configured to use remote authentication with LDAP, RADIUS, or TACACS+, passwords for those remote accounts can be blank. With this configuration, the remote credentials store is used just for authentication, not authorization. The definition of the local user role definition applies to the remotely authenticated user.

User Roles

User roles contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles. For example, if Role1 has storage related privileges, and Role2 has server related privileges, users who are assigned to both Role1 and Role2 have storage and server related privileges.

All roles include read access to all configuration settings in the Cisco UCS instance. The difference between the read-only role and other roles is that a user who is only assigned the read-only role cannot modify the system state. A user assigned another role can modify the system state in that user's assigned area or areas.

The system contains the following default user roles:

| | |
|---------------------------------------|---|
| AAA Administrator | Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system. |
| Administrator | Complete read-and-write access to the entire system. The default admin account is assigned this role by default and it cannot be changed. |
| Network Administrator | Read-and-write access to fabric interconnect infrastructure and network security operations. Read access to the rest of the system. |
| Operations | Read-and-write access to systems logs, including the syslog servers, and faults. Read access to the rest of the system. |
| Read-Only | Read-only access to system configuration with no privileges to modify the system state. |
| Server Equipment Administrator | Read-and-write access to physical server related operations. Read access to the rest of the system. |

| | |
|--------------------------------------|---|
| Server Profile Administrator | Read-and-write access to logical server related operations. Read access to the rest of the system. |
| Server Security Administrator | Read-and-write access to server security related operations. Read access to the rest of the system. |
| Storage Administrator | Read-and-write access to storage operations. Read access to the rest of the system. |

Roles can be created, modified to add new or remove existing privileges, or deleted. When a role is modified, the new privileges are applied to all users assigned to that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Server Administrator and Storage Administrator roles have different set of privileges, but a new Server and Storage Administrator role can be created that combines the privileges of both roles.

If a role is deleted after it has been assigned to users, it is also deleted from those user accounts.

User profiles on AAA servers (RADIUS or TACACS+) should be modified to add the roles corresponding to the privileges granted to that user. The `cisco-av-pair` vendor-specific attribute is used to store the role information. The AAA servers return this attribute with the request and parse it to get the roles. LDAP servers return the roles in the user profile attributes.

Privileges

Privileges give users assigned to user roles access to specific system resources and permission to perform specific tasks. The following table lists each privilege and the user role given that privilege by default.

Table 9: User Privileges

| Privilege | Description | Default Role Assignment |
|------------------|----------------------------|-------------------------|
| aaa | System security and AAA | AAA Administrator |
| admin | System administration | Administrator |
| ext-lan-config | External LAN configuration | Network Administrator |
| ext-lan-policy | External LAN policy | Network Administrator |
| ext-lan-qos | External LAN QoS | Network Administrator |
| ext-lan-security | External LAN security | Network Administrator |
| ext-san-config | External SAN configuration | Storage Administrator |
| ext-san-policy | External SAN policy | Storage Administrator |
| ext-san-qos | External SAN QoS | Storage Administrator |
| ext-san-security | External SAN security | Storage Administrator |
| fault | Alarms and alarm policies | Operations |

| Privilege | Description | Default Role Assignment |
|---------------------------------|---|--------------------------------|
| operations | Logs and Smart Call Home | Operations |
| pod-config | Pod configuration | Network Administrator |
| pod-policy | Pod policy | Network Administrator |
| pod-qos | Pod QoS | Network Administrator |
| pod-security | Pod security | Network Administrator |
| read-only | Read-only access Read-only cannot be selected as a privilege; it is assigned to every user role. | Read-Only |
| server-equipment | Server hardware management | Server Equipment Administrator |
| server-maintenance | Server maintenance | Server Equipment Administrator |
| server-policy | Server policy | Server Equipment Administrator |
| server-security | Server security | Server Security Administrator |
| service-profile-config | Service profile configuration | Server Profile Administrator |
| service-profile-config-policy | Service profile configuration policy | Server Profile Administrator |
| service-profile-ext-access | Service profile end point access | Server Profile Administrator |
| service-profile-network | Service profile network | Network Administrator |
| service-profile-network-policy | Service profile network policy | Network Administrator |
| service-profile-qos | Service profile QoS | Network Administrator |
| service-profile-qos-policy | Service profile QoS policy | Network Administrator |
| service-profile-security | Service profile security | Server Security Administrator |
| service-profile-security-policy | Service profile security policy | Server Security Administrator |
| service-profile-server | Service profile server management | Server Security Administrator |
| service-profile-server-policy | Service profile pool policy | Server Security Administrator |
| service-profile-storage | Service profile storage | Storage Administrator |
| service-profile-storage-policy | Service profile storage policy | Storage Administrator |

User Locales

A user can be assigned one or more locales. Each locale defines one or more organizations (domains) the user is allowed access, and access would be limited to the organizations specified in the locale. One exception to this rule is a locale without any organizations, which gives unrestricted access to system resources in all organizations.

Users with AAA Administrator privileges (AAA Administrator role) can assign organizations to the locale of other users. The assignment of organizations is restricted to only those in the locale of the user assigning the organizations. For example, if a locale contains only the Engineering organization then a user assigned that locale can only assign the Engineering organization to other users.

You can hierarchically manage organizations. A user that is assigned at a top level organization has automatic access to all organizations under it. For example, an Engineering organization can contain a Software Engineering organization and a Hardware Engineering organization. A locale containing only the Software Engineering organization has access to system resources only within that organization; however, a locale that contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

Configuring User Roles

Creating a User Role

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # create role name | Creates the user role and enters security role mode. |
| Step 3 | UCS-A /security/role # add privilege privilege-name | <p>Adds one or more privileges to the role.</p> <p>Note You can specify more than one <i>privilege-name</i> on the same command line to add multiple privileges to the role, or you can add privileges to the same role using multiple add commands.</p> |
| Step 4 | UCS-A /security/role # commit-buffer | Commits the transaction to the system configuration. |

The following example creates the service-profile-security-admin role, adds the service profile security and service profile security policy privileges to the role, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # create role ls-security-admin
UCS-A /security/role* # add privilege service-profile-security service-profile-security-policy
UCS-A /security/role* # commit-buffer
UCS-A /security/role #
```

Adding Privileges to a User Role

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # scope role name | Enters security role mode for the specified role. |
| Step 3 | UCS-A /security/role # add privilege privilege-name | <p>Adds one or more privileges to the existing privileges of the user role.</p> <p>Note You can specify more than one <i>privilege-name</i> on the same command line to add multiple privileges to the role, or you can add privileges to the same role using multiple add privilege commands.</p> |
| Step 4 | UCS-A /security/role # commit-buffer | Commits the transaction to the system configuration. |

The following example adds the server security and server policy privileges to the service-profile-security-admin role and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope role service-profile-security-admin
UCS-A /security/role # add privilege server-security server-policy
UCS-A /security/role* # commit-buffer
UCS-A /security/role #
```

Removing Privileges from a User Role

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # scope role name | Enters security role mode for the specified role. |
| Step 3 | UCS-A /security/role # remove privilege privilege-name | <p>Removes one or more privileges from the existing user role privileges.</p> <p>Note You can specify more than one <i>privilege-name</i> on the same command line to remove multiple privileges from the role, or you can remove privileges from the same role using multiple remove privilege commands.</p> |
| Step 4 | UCS-A /security/role # commit-buffer | Commits the transaction to the system configuration. |

The following example removes the server security and server policy privileges from the service-profile-security-admin role and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope role service-profile-security-admin
UCS-A /security/role # remove privilege server-security server-policy
UCS-A /security/role* # commit-buffer
UCS-A /security/role #
```

Deleting a User Role

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # delete role <i>name</i> | Deletes the user role. |
| Step 3 | UCS-A /security # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the service-profile-security-admin role and commits the transaction:

```
UCS-A# scope security
UCS-A /security # delete role service-profile-security-admin
UCS-A /security* # commit-buffer
UCS-A /security #
```

Configuring Locales

Creating a Locale

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # create locale <i>locale-name</i> | Creates a locale and enters security locale mode. |
| Step 3 | UCS-A /security/locale # create org-ref <i>org-ref-name</i> orgdn <i>orgdn-name</i> | References (binds) an organization to the locale. The <i>org-ref-name</i> argument is the name used to identify the organization reference, and the <i>orgdn-name</i> argument is the distinguished name of the organization being referenced. |
| Step 4 | UCS-A /security/locale # commit-buffer | Commits the transaction to the system configuration. |

The following example creates the western locale, references the finance organization to the locale, names the reference finance-ref, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # create locale western
UCS-A /security/locale* # create org-ref finance-ref orgdn finance
UCS-A /security/locale* # commit-buffer
UCS-A /security/locale #
```

Adding an Organization to a Locale

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A# scope locale <i>locale-name</i> | Enters security locale mode. |
| Step 3 | UCS-A /security/locale # create org-ref <i>org-ref-name</i> orgdn <i>orgdn-name</i> | References (binds) an organization to the locale. The <i>org-ref-name</i> argument is the name used to identify the organization reference, and the <i>orgdn-name</i> argument is the distinguished name of the organization being referenced. |
| Step 4 | UCS-A /security/locale # commit-buffer | Commits the transaction to the system configuration. |

The following example enters the western locale, adds (references) the marketing organization to the locale, names the reference marketing-ref, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope locale western
UCS-A /security/locale* # create org-ref marketing-ref orgdn marketing
UCS-A /security/locale* # commit-buffer
UCS-A /security/locale #
```

Deleting an Organization from a Locale

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # scope locale <i>locale-name</i> | Enters security locale mode. |
| Step 3 | UCS-A /security/locale # delete org-ref <i>org-ref-name</i> | Deletes the organization from the locale. |
| Step 4 | UCS-A /security/locale # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the finance organization from the western locale and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope locale western
UCS-A /security/locale # delete org-ref finance-ref
UCS-A /security/locale* # commit-buffer
UCS-A /security/locale #
```

Deleting a Locale

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # delete locale <i>locale-name</i> | Deletes the locale. |
| Step 3 | UCS-A /security # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the western locale and commits the transaction:

```
UCS-A# scope security
UCS-A /security # delete locale western
UCS-A /security* # commit-buffer
UCS-A /security #
```

Configuring User Accounts

Creating a User Account

At a minimum, we recommend that you create the following users:

- Server administrator account
- Network administrator account
- Storage administrator

Before You Begin

Perform the following tasks, if the system includes any of the following:

- Remote authentication services, ensure the users exist in the remote authentication server with the appropriate roles and privileges.
- Multi-tenancy with organizations, create one or more locales. If you do not have any locales, all users are created in root and are assigned roles and privileges in all organizations.
- SSH authentication, obtain the SSH key.

Procedure

| | Command or Action | Purpose |
|----------------|--|---|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # create local-user <i>local-user-name</i> | Creates a user account for the specified local user and enters security local user mode. |
| Step 3 | UCS-A /security/local-user # set password <i>password</i> | Sets the password for the user account |
| Step 4 | UCS-A /security/local-user # set firstname <i>first-name</i> | (Optional) Specifies the first name of the user. |
| Step 5 | UCS-A /security/local-user # set lastname <i>last-name</i> | (Optional) Specifies the last name of the user. |
| Step 6 | UCS-A /security/local-user # set expiration <i>month day-of-month year</i> | (Optional) Specifies the date that the user account expires. The <i>month</i> argument is the first three letters of the month name. |
| Step 7 | UCS-A /security/local-user # set email <i>email-addr</i> | (Optional) Specifies the user e-mail address. |
| Step 8 | UCS-A /security/local-user # set phone <i>phone-num</i> | (Optional) Specifies the user phone number. |
| Step 9 | UCS-A /security/local-user # set sshkey <i>ssh-key</i> | (Optional) Specifies the SSH key used for passwordless access. |
| Step 10 | UCS-A security/local-user # commit-buffer | Commits the transaction. |

The following example creates the user account named kikipopo, sets the password to foo12345, commits the transaction, and commits the transaction:

```
UCS-A# scope security
UCS-A /security # create local-user kikipopo
UCS-A /security/local-user* # set password
Enter a password:
Confirm the password:
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

The following example creates the user account named lincey, sets an OpenSSH key for passwordless access, and commits the transaction.

```
UCS-A# scope security
UCS-A /security # create local-user lincey
UCS-A /security/local-user* # set sshkey "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30k1CWjnV31gdXMzO0WU15iPw851kdQqap+NFuNmHcb4K
iaQB8X/PDdmtLxQQcawclj+k8f4VcOelBx1sGk51uq51s1ob1VOIEwckEL/h51rdbN1I8y3SS9I/gGiBZ9AR1op9LDpD
m8HPh2LOgyH7Ei1MI8="
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

The following example creates the user account named jforlenz, sets a Secure SSH key for passwordless access, and commits the transaction.

```
UCS-A# scope security
UCS-A /security # create local-user jforlenz
UCS-A /security/local-user* # set sshkey
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
User's SSH key:
> ---- BEGIN SSH2 PUBLIC KEY ----
>AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WU15iPw8
>5lkdQqap+NFuNmHcb4KiaQB8X/PDdmtlxQQcawclj+k8f4VcOelBx1sGk5luq51s1ob1VO
>IEwcKEL/h51rdbN1I8y3SS9I/gGiBZ9ARlop9LDpDm8HPh2LOgyH7Ei1MI8=
> ---- END SSH2 PUBLIC KEY ----
> ENDOFBUF
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

Deleting a User Account

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # delete local-user <i>local-user-name</i> | Deletes the user user account. |
| Step 3 | UCS-A /security # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the foo user account and commits the transaction:

```
UCS-A# scope security
UCS-A /security # delete local-user foo
UCS-A /security* # commit-buffer
UCS-A /security #
```

Assigning a Role to a User Account

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # scope local-user <i>local-user-name</i> | Enters security local user mode for the specified local user account. |
| Step 3 | UCS-A /security/local-user # create role <i>role-name</i> | Assigns the specified role to the user account . Note The create role command can be entered multiple times to assign more than one role to a user account. |
| Step 4 | UCS-A security/local-user # commit-buffer | Commits the transaction. |

The following example assigns the operations role to the kikipopo local user account and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # create role operations
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

Removing a Role from a User Account

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # scope local-user <i>local-user-name</i> | Enters security local user mode for the specified local user account. |
| Step 3 | UCS-A /security/local-user # delete role <i>role-name</i> | Removes the specified role from the user account. Note The delete role command can be entered multiple times to remove more than one role from a user account. |
| Step 4 | UCS-A security/local-user # commit-buffer | Commits the transaction. |

The following example removes the operations role from the kikipopo local user account and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # delete role operations
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

Assigning a Locale to a User Account

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # scope local-user <i>local-user-name</i> | Enters security local user mode for the specified local user account. |
| Step 3 | UCS-A /security/local-user # create locale <i>locale-name</i> | Assigns the specified locale to the user account. Note The create locale command can be entered multiple times to assign more than one locale to a user account. |

| | Command or Action | Purpose |
|---------------|---|--------------------------|
| Step 4 | UCS-A security/local-user # commit-buffer | Commits the transaction. |

The following example assigns the western locale to the kikipopo local user account and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # create locale western
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

Removing a Locale from a User Account

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope security | Enters security mode. |
| Step 2 | UCS-A /security # scope local-user <i>local-user-name</i> | Enters security local user mode for the specified local user account. |
| Step 3 | UCS-A /security/local-user # delete locale <i>locale-name</i> | Removes the specified locale from the user account. Note The delete locale command can be entered multiple times to remove more than one locale from a user account. |
| Step 4 | UCS-A security/local-user # commit-buffer | Commits the transaction. |

The following example removes the western locale from the kikipopo local user account and commits the transaction:

```
UCS-A# scope security
UCS-A /security # scope local-user kikipopo
UCS-A /security/local-user # delete locale western
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```

Monitoring User Sessions

Procedure

| | Command or Action | Purpose |
|---------------|------------------------------|-----------------------|
| Step 1 | UCS-A# scope security | Enters security mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 2 | UCS-A /security # show user-session {local remote} [detail] | Displays session information for all users logged in to the system. |

The following example lists all local users logged in to the system:

```
UCS-A# scope security
UCS-A /security # show user-session local
Session Id      User           Host           Login Time
-----
pts_25_1_31264  steve          192.168.100.111 2009-05-09T14:06:59
ttyS0_1_3532    jeff           console         2009-05-02T15:11:08
web_25277_A     faye           192.168.100.112 2009-05-15T22:11:25
```

The following example displays detailed information on all local users logged in to the system:

```
UCS-A# scope security
UCS-A /security # show user-session local detail
Session Id pts_25_1_31264:
  Fabric Id: A
  Term: pts/25
  User: steve
  Host: 64.101.53.93
  Pid: 31264
  Login Time: 2009-05-09T14:06:59

Session Id ttyS0_1_3532:
  Fabric Id: A
  Term: ttyS0
  User: jeff
  Host: console
  Pid: 3532
  Login Time: 2009-05-02T15:11:08

Session Id web_25277_A:
  Fabric Id: A
  Term: web_25277
  User: faye
  Host: 192.168.100.112
  Pid: 3518
  Login Time: 2009-05-15T22:11:25
```




CHAPTER 10

Managing Firmware

This chapter includes the following sections:

- [Overview of Firmware, page 113](#)
- [Firmware Image Management, page 114](#)
- [Firmware Upgrades, page 115](#)
- [Firmware Downgrades, page 123](#)
- [Completing the Prerequisites for Upgrading the Firmware, page 124](#)
- [Downloading and Managing Images, page 128](#)
- [Directly Upgrading Firmware at Endpoints, page 131](#)
- [Updating Firmware through Service Profiles, page 140](#)
- [Managing the Capability Catalog, page 144](#)

Overview of Firmware

Cisco UCS uses firmware obtained from and certified by Cisco to support the endpoints in a Cisco UCS instance. Each endpoint is a component in the instance that requires firmware to function. A Cisco UCS instance includes the following firmware endpoints that need to be upgraded when you upgrade the firmware:

- Endpoints physically located on servers, such as the BIOS, storage controller (RAID controller), and Cisco Integrated Management Controller (CIMC)
- Endpoints physically located on adapters, including NIC and HBA firmware, and Option ROM (where applicable)
- I/O modules
- Fabric interconnects
- Cisco UCS Manager

**Note**

In Release 1.3(1) the BMC was renamed to CIMC Controller. After you upgrade to this release, Cisco UCS Manager no longer uses the term BMC. Because this document is aimed at Release 1.3(1), the term CIMC is sometimes used rather than BMC.

Cisco maintains a set of best practices for managing firmware images and updates in this document and in the following technical note: [Unified Computing System Firmware Management Best Practices](#).

This document uses the following definitions for managing firmware:

| | |
|-----------------|--|
| Upgrade | Changes the firmware running on an endpoint to another image, such as a release or patch. Upgrade includes both update and activation. |
| Update | Copies the firmware image to the backup partition on an endpoint. |
| Activate | Sets the firmware in the backup partition as the active firmware version on the endpoint. Activation can require or cause the reboot of an endpoint. |

Firmware Image Management

Cisco delivers all firmware updates or packages to Cisco UCS components in images. These images can be the following:

- Component image, which contains the firmware for one component
- Package, which is a collection of component images

Cisco also provides release notes with each image, which you can obtain from the same website from which you obtained the image.

Cisco UCS Manager provides mechanisms to download both component images and packages to the fabric interconnect.

Firmware Image Headers

Every firmware image has a header, which includes the following:

- Checksum
- Version information
- Compatibility information that the system can use to verify the compatibility of component images and any dependencies

Firmware Image Catalog

Cisco UCS Manager provides you with two views of the catalog of firmware images and their contents that have been downloaded to the fabric interconnect:

- Packages** This view provides you with a read-only representation of the packages that have been downloaded onto the fabric interconnect. This view is sorted by image, not by the contents of

the image. For packages, you can use this view to see which component images are (were) in each downloaded package.

Images The images view lists the component images available on the system. You cannot use this view to see packages. The information available about each component image includes the name of the component, the image size, the image version, and the vendor and model of the component.

You can use this view to identify the firmware updates available for each component. You can also use this view to delete obsolete and unneeded images. Cisco UCS Manager deletes a package after all images in the package have been deleted.



Tip Cisco UCS Manager stores the images in bootflash on the fabric interconnect. In a cluster system, space usage in bootflash on both fabric interconnects is the same, because all images are synchronized between them. If Cisco UCS Manager reports that the bootflash is out of space, delete obsolete images to free up space.

Firmware Upgrades

Cisco UCS firmware is upgraded through a combination of the following methods:

- Direct upgrade at the endpoints. For a cluster configuration with two fabric interconnects, a direct upgrade can be minimally disruptive to data traffic. However, it requires that the Cisco UCS instance does not include firmware policies for those endpoints that you upgrade directly. You cannot avoid disruption to traffic in a Cisco UCS instance with only one fabric interconnection.
- Upgrades to server endpoints through service profiles that include a host firmware package, a management firmware package, or both. This method is disruptive to data traffic and should be performed during a maintenance window.



Note Direct upgrade is not available for all endpoints, including the server BIOS, storage controller, HBA firmware, and HBA option ROM. You must upgrade those endpoints through the host firmware package included in the service profile associated with the server.

Guidelines and Cautions for Firmware Upgrades

Before you upgrade the firmware for any endpoint in a Cisco UCS instance, consider the following guidelines and cautions:

Determine Appropriate Type of Firmware Upgrade for Each Endpoint

Some endpoints, such as adapters and the server CIMC, can be upgraded through either a direct firmware upgrade or a firmware package included in a service profile. The configuration of a Cisco UCS instance determines how you upgrade these endpoints. If the service profiles associated with the servers include a host firmware package, upgrade the adapters for those servers through the firmware package. In the same way, if

the service profiles associated with the servers include a management firmware package, upgrade the CIMC for those servers through the firmware package.

Upgrades of a CIMC through a management firmware package or an adapter through a firmware package in the service profile associated with the server take precedence over direct firmware upgrades. You cannot directly upgrade an endpoint if the service profile associated with the server includes a firmware package. To perform a direct upgrade, you must remove the firmware package from the service profile.

No Server or Chassis Maintenance



Caution

Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process has completed. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure may corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Number of Fabric Interconnects

For a cluster configuration with two fabric interconnects, you can take advantage of the failover between the fabric interconnects and perform a direct firmware upgrade of the endpoints without disrupting data traffic. However, you cannot avoid disrupting data traffic for those endpoints which must be upgraded through a host or management firmware package.

For a standalone configuration with a single fabric interconnect, you can minimize the disruption to data traffic when you perform a direct firmware upgrade of the endpoints. However, you must reboot the fabric interconnect to complete the upgrade and, therefore, cannot avoid disrupting traffic.

Do Not Activate All Endpoints Simultaneously in Cisco UCS Manager GUI

If you use Cisco UCS Manager GUI to update the firmware, do not select **ALL** from the **Filter** drop-down list in the **Activate Firmware** dialog box to activate all endpoints simultaneously. Many firmware releases and patches have dependencies that require the endpoints to be activated in a specific order for the firmware update to succeed. This order can change depending upon the contents of the release or patch. Activating all endpoints does not guarantee that the updates occur in the required order and can disrupt communications between the endpoints and the fabric interconnects and Cisco UCS Manager. For information about the dependencies in a specific release or patch, see the release notes provided with that release or patch.

Impact of Activation

During a direct upgrade, you should configure **Set Startup Version Only** for an adapter. With this setting, the activated firmware moves into the pending-next-boot state, and the server is not immediately rebooted. The activated firmware does not become the running version of firmware on the adapter until the server is rebooted. You cannot configure **Set Startup Version Only** for an adapter in the host firmware package.

If a server is not associated with a service profile, the activated firmware moves into the pending-next-boot state. Cisco UCS Manager does not reboot the endpoints or activate the firmware until the server is associated with a service profile. If necessary, you can manually reboot an unassociated server to activate the firmware.

When you configure **Set Startup Version Only** for an I/O module, the I/O module is rebooted when the fabric interconnect in its data path is rebooted. If you do not configure **Set Startup Version Only** for an I/O module, the I/O module reboots and disrupts traffic. In addition, if Cisco UCS Manager detects a protocol and firmware version mismatch between it and the I/O module, Cisco UCS Manager automatically updates

the I/O module with the firmware version that matches its own and then activates the firmware and reboots the I/O module again.

Impact of Upgrade to Release 1.3(1i) or Higher

An upgrade from an earlier Cisco UCS firmware release to release 1.3(1i) or higher has the following impact on the Protect Configuration property of the local disk configuration policy the first time servers are associated with service profiles after the upgrade:

Unassociated Servers After you upgrade the Cisco UCS instance, the initial server association proceeds without configuration errors whether or not the local disk configuration policy matches the server hardware. Even if you enable the Protect Configuration property, Cisco UCS does not protect the user data on the server if there are configuration mismatches between the local disk configuration policy on the previous service profile and the policy in the new service profile.



Note If you enable the Protect Configuration property and the local disk configuration policy encounters mismatches between the previous service profile and the new service profile, all subsequent service profile associations with the server are blocked.

Associated Servers Any servers that are already associated with service profiles do not reboot after the upgrade. Cisco UCS Manager does not report any configuration errors if there is a mismatch between the local disk configuration policy and the server hardware.

When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile.

Cannot Upgrade Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter

The firmware on the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter (N20-AI0002) is burned into the hardware at manufacture. You cannot upgrade the firmware on this adapter.

Firmware Versions

The firmware versions on an endpoint depend upon the type of endpoint. The endpoints physically located on a fabric interconnect have different versions than those physically located on a server or I/O module.

Firmware Versions in CIMC, I/O Modules, and Adapters

Each CIMC, I/O module, and adapter has two slots for firmware in flash. Each slot holds a version of firmware. One slot is active and the other is the backup slot. A component boots from whichever slot is designated as active.

The following firmware version terminology is used in Cisco UCS Manager:

Running Version The running version is the firmware that is active and in use by the endpoint.

Startup Version The startup version is the firmware that will be used when the endpoint next boots up. Cisco UCS Manager uses the activate operation to change the startup version.

Backup Version The backup version is the firmware in the other slot and is not in use by the endpoint. This version can be firmware that you have updated to the endpoint but have not yet activated, or it can be an older firmware version that was replaced by a recent activate. Cisco UCS Manager uses the update operation to replace the image in the backup slot.

If the endpoint cannot boot from the startup version, it boots from the backup version.

Firmware Versions in the Fabric Interconnect and Cisco UCS Manager

You can only activate the fabric interconnect firmware and Cisco UCS Manager on the fabric interconnect. The fabric interconnect and Cisco UCS Manager firmware do not have backup versions, because all the images are stored on the fabric interconnect. As a result, the number of bootable fabric interconnect images is not limited to two, like the server CIMC and adapters. Instead, the number of bootable fabric interconnect images is limited by the available space in the memory of the fabric interconnect and the number of images stored there.

The fabric interconnect and Cisco UCS Manager firmware have running and startup versions of the kernel and system firmware. The kernel and system firmware must run the same versions of firmware.

Direct Firmware Upgrade at Endpoints

If you follow the correct procedure and apply the upgrades in the correct order, a direct firmware upgrade and the activation of the new firmware version on the endpoints is minimally disruptive to traffic in a Cisco UCS instance.

You can directly upgrade the firmware on the following endpoints:

- Adapters
- CIMCs
- I/O modules
- Board controllers
- Cisco UCS Manager
- Fabric interconnects

The adapter and board controller firmware can also be upgraded through the host firmware package in the service profile. If you use a host firmware package to upgrade this firmware, you can reduce the number of times a server needs to be rebooted during the firmware upgrade process.



Note

Upgrades of a CIMC through a management firmware package or an adapter through a firmware package in the service profile associated with the server take precedence over direct firmware upgrades. You cannot directly upgrade an endpoint if the service profile associated with the server includes a firmware package. To perform a direct upgrade, you must remove the firmware package from the service profile.

Stages of a Direct Firmware Upgrade

Cisco UCS Manager separates the direct upgrade process into two stages to ensure that you can push the firmware to an endpoint while the system is running without affecting uptime on the server or other endpoints.

Update

During this stage, the system copies the selected firmware version from the primary fabric interconnect to the backup partition in the endpoint and verifies that the firmware image is not corrupt. The update process always overwrites the firmware in the backup slot.

The update stage applies only to the following endpoints:

- Adapters
- CIMCs
- I/O modules

You can set the update as Startup Version Only to avoid rebooting the endpoint immediately. This allows you to perform the update at any time and then activate and reboot during a maintenance period.



Caution

Do not remove the hardware that contains the endpoint or perform any maintenance on it until the update process has completed. If the hardware is removed or otherwise unavailable due to maintenance, the firmware update fails. This failure may corrupt the backup partition. You cannot update the firmware on an endpoint with a corrupted backup partition.

Activate

During this stage, the system sets the specified image version (normally the backup version) as the startup version and, if you do not specify **Set Startup Version Only**, immediately reboots the endpoint. When the endpoint is rebooted, the backup partition becomes the active partition, and the active partition becomes the backup partition. The firmware in the new active partition becomes the startup version and the running version.

The following endpoints only require activation because the specified firmware image already exists on the endpoint:

- Cisco UCS Manager
- Fabric interconnects
- Board controllers on those servers that support them

When the firmware is activated, the endpoint is rebooted and the new firmware becomes the active kernel version and system version. If the endpoint cannot boot from the startup firmware, it defaults to the backup version and raises a fault.



Caution

When you configure **Set Startup Version Only** for an I/O module, the I/O module is rebooted when the fabric interconnect in its data path is rebooted. If you do not configure **Set Startup Version Only** for an I/O module, the I/O module reboots and disrupts traffic. In addition, if Cisco UCS Manager detects a protocol and firmware version mismatch between it and the I/O module, Cisco UCS Manager automatically updates the I/O module with the firmware version that matches its own and then activates the firmware and reboots the I/O module again.

Recommended Order of Components for Firmware Activation

If you upgrade firmware by individual components in a Cisco UCS instance, we recommend that you activate the updates in the required order for quicker activation and to avoid potential issues with conflicting firmware versions.

Recommended Order when Updating from Cisco UCS, Release 1.0(2) Onwards

- 1 Adapter (interface card)—If you plan to upgrade the adapters directly, perform this step first. However, if you prefer, you can omit this step and upgrade the adapters as part of the last step, in a host firmware package.
- 2 BMC—If you upgrade the adapters in the host firmware package, perform this step first.
- 3 I/O module.
- 4 Cisco UCS Manager.
- 5 Fabric interconnect.
- 6 Host firmware package—Must be the last step in the upgrade process. We recommend that you upgrade the board controller firmware during this step to avoid an additional reboot of the server. You must upgrade the BIOS and storage controller firmware in a host firmware package.

Recommended Order when Updating from Cisco UCS, Release 1.0(1)

- 1 Adapter (interface card)—If you plan to upgrade the adapters directly, perform this step first. However, if you prefer, you can omit this step and upgrade the adapters as part of the last step, in a host firmware package.
- 2 BMC—If you upgrade the adapters in the host firmware package, perform this step first.
- 3 I/O module.
- 4 Fabric interconnect.
- 5 Cisco UCS Manager.
- 6 Host firmware package—Must be the last step in the upgrade process. We recommend that you upgrade the board controller firmware during this step to avoid an additional reboot of the server. You must upgrade the BIOS and storage controller firmware in a host firmware package.

Outage Impacts of Direct Firmware Upgrades

When you perform a direct firmware upgrade on an endpoint, you can disrupt traffic or cause an outage in one or more of the endpoints in the Cisco UCS instance.

Outage Impact of a Fabric Interconnect Firmware Upgrade

When you upgrade the firmware for a fabric interconnect, you cause the following outage impacts and disruptions:

- The fabric interconnect reboots.
- The corresponding I/O modules reboot.

Outage Impact of a Cisco UCS Manager Firmware Upgrade

A firmware upgrade to Cisco UCS Manager causes the following disruptions:

Cisco UCS Manager GUI

- All users logged in to Cisco UCS Manager GUI are logged out and their sessions ended.
- Any unsaved work in progress is lost.

Cisco UCS Manager CLI

All users logged in through telnet are logged out and their sessions ended. Console sessions are not ended.

Outage Impact of an I/O Module Firmware Upgrade

When you upgrade the firmware for an I/O module, you cause the following outage impacts and disruptions:

- For a standalone configuration with a single fabric interconnect, data traffic is disrupted when the I/O module reboots. For a cluster configuration with two fabric interconnects, data traffic fails over to the other I/O module and the fabric interconnect in its data path.
- If you activate the new firmware as the startup version only, the I/O module reboots when the corresponding fabric interconnect is rebooted
- If you activate the new firmware as the running and startup version, the I/O module reboots immediately.
- An I/O module can take up to ten minutes to become available after a firmware upgrade.

Outage Impact of a CIMC Firmware Upgrade

When you upgrade the firmware for a CIMC in a server, you impact only the CIMC and internal processes. You do not interrupt server traffic. This firmware upgrade causes the following outage impacts and disruptions to the CIMC:

- Any activities being performed on the server through the KVM console and vMedia are interrupted.
- Any monitoring or IPMI polling is interrupted.

Outage Impact of an Adapter Firmware Upgrade

If you activate the firmware for an adapter and do not configure the **Set Startup Version Only** option, you cause the following outage impacts and disruptions:

- The server reboots.
- Server traffic is disrupted.

Firmware Upgrades through Service Profiles

You can use service profiles to upgrade the server and adapter firmware, including the BIOS on the server, by defining the following policies and including them in the service profile associated with a server:

- Host Firmware Package policy
- Management Firmware Package policy

**Note**

You cannot upgrade the firmware on an I/O module, fabric interconnect, or Cisco UCS Manager through service profiles. You must upgrade the firmware on those endpoints directly.

Host Firmware Package

This policy enables you to specify a set of firmware versions that make up the host firmware package (also known as the host firmware pack). The host firmware includes the following firmware for server and adapter endpoints:

- **Adapter Firmware Packages**
- **Storage Controller Firmware Packages**
- **Fibre Channel Adapters Firmware Packages**
- **BIOS Firmware Packages**
- **HBA Option ROM Packages**
- **Board Controller Packages**

**Tip**

You can include more than one type of firmware in the same host firmware package. For example, a host firmware package can include both BIOS firmware and storage controller firmware or adapter firmware for two different models of adapters. However, you can only have one firmware version with the same type, vendor, and model number. The system recognizes which firmware version is required for an endpoint and ignores all other firmware versions.

The firmware package is pushed to all servers associated with service profiles that include this policy.

This policy ensures that the host firmware is identical on all servers associated with service profiles which use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained. Also, if you change the firmware version for an endpoint in the firmware package, new versions are applied to all the affected service profiles immediately, which could cause server reboots.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

Prerequisites

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect. If the firmware image is not available when Cisco UCS Manager is associating a server with a service profile, Cisco UCS Manager ignores the firmware upgrade and completes the association.

Management Firmware Package

This policy enables you to specify a set of firmware versions that make up the management firmware package (also known as a management firmware pack). The management firmware package includes the Cisco Integrated Management Controller (CIMC) on the server. You do not need to use this package if you upgrade the CIMC directly.

The firmware package is pushed to all servers associated with service profiles that include this policy. This policy ensures that the CIMC firmware is identical on all servers associated with service profiles which use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Stages of a Firmware Upgrade through Service Profiles

You can use the host and management firmware package policies in service profiles to upgrade server and adapter firmware.



Caution

If you modify a host firmware package by adding an endpoint or changing firmware versions for an existing endpoint, Cisco UCS Manager upgrades the endpoints and reboots all servers associated with that firmware package as soon as the changes are saved, disrupting data traffic to and from the servers.

New Service Profile

For a new service profile, this upgrade takes place over the following stages:

Firmware Package Policy Creation During this stage, you create the host and/or management firmware packages and include them in the appropriate firmware policies.

Service Profile Association During this stage, you include the firmware packages in a service profile, and then associate the service profile with a server. The system pushes the selected firmware versions to the endpoints. For a host firmware package, the server is rebooted to ensure that the endpoints are running the versions specified in the firmware package.

Existing Service Profile

If the service profile is already associated with a server, Cisco UCS Manager upgrades the firmware as soon as you save the changes to the host firmware packages. For a host firmware package, Cisco UCS Manager reboots the server as soon as the change is saved.

Firmware Downgrades

You downgrade firmware in a Cisco UCS instance in the same way that you upgrade firmware. The package or version that you select when you update the firmware determines whether you are performing an upgrade or a downgrade.

Completing the Prerequisites for Upgrading the Firmware

Prerequisites for Upgrading and Downgrading Firmware

All endpoints in a Cisco UCS instance must be fully functional and all processes must be complete before you begin a firmware upgrade or downgrade on those endpoints. You cannot upgrade or downgrade an endpoint that is not in a functional state. For example, the firmware on a server that has not been discovered cannot be upgraded or downgraded. An incomplete process, such as an FSM that has failed after the maximum number of retries, can cause the upgrade or downgrade on an endpoint to fail. If an FSM is in progress, Cisco UCS Manager queues up the update and activation and runs them when the FSM has completed successfully.

Before you upgrade or downgrade firmware in a Cisco UCS instance, complete the following prerequisites:

- Back up the configuration into an All Configuration backup file.
- For a cluster configuration, verify that the high availability status of the fabric interconnects shows that both are up and running.
- For a standalone configuration, verify that the Overall Status of the fabric interconnect is Operable.
- Verify that all servers, I/O modules, and adapters are fully functional. An inoperable server cannot be upgraded.
- Verify that all servers have been discovered. They do not need to be powered on or associated with a service profile.

Creating an All Configuration Backup File

Before You Begin

Obtain the backup server IP address and authentication credentials.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # create backup URL all-configuration enabled } | Creates an enabled All Configuration backup operation that runs as soon as you enter the commit-buffer command. The all-configuration option backs up the server, fabric, and system related configuration. Specify the URL for the backup file using one of the following syntax: <ul style="list-style-type: none"> • ftp://hostname/path • scp://username@hostname/path • sftp://username@hostname/path • tftp://hostname:port-num/path |

| | Command or Action | Purpose |
|---------------|-------------------------------------|--------------------------|
| Step 3 | UCS-A /system# commit-buffer | Commits the transaction. |

The following example uses SCP to create an All Configuration backup file on the host named host35 and commits the transaction:

```
UCS-A# scope system
UCS-A /system* # create backup scp://user@host35/backups/all-config.bak all-configuration
enabled
Password:
UCS-A /system* # commit-buffer
UCS-A /system #
```

Verifying the Operability of a Fabric Interconnect

If your Cisco UCS instance is running in a high availability cluster configuration, you must verify the operability of both fabric interconnects.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope fabric-interconnect {a b} | Enters fabric interconnect mode for the specified fabric interconnect. |
| Step 2 | UCS-A /fabric-interconnect# show | Displays information about the fabric interconnect. Verify that the operability of the fabric interconnects is in the Operable state. If the operability is not in the Operable state, run a show tech-support command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the show tech-support command, see the <i>Cisco UCS Troubleshooting Guide</i> . |

The following example displays that the operability for both fabric interconnects is in the Operable state:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show
Fabric Interconnect:
  ID  OOB IP Addr      OOB Gateway      OOB Netmask      Operability
  --  -
  A   192.168.100.10   192.168.100.20   255.255.255.0    Operable

UCS-A /fabric-interconnect # exit
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # show
Fabric Interconnect:
  ID  OOB IP Addr      OOB Gateway      OOB Netmask      Operability
  --  -
  B   192.168.100.11   192.168.100.20   255.255.255.0    Operable
```

Verifying the High Availability Status and Roles of a Cluster Configuration

The high availability status is the same for both fabric interconnects in a cluster configuration.

Procedure

| | Command or Action | Purpose |
|---------------|----------------------------------|--|
| Step 1 | UCS-A# show cluster state | <p>Displays the operational state and leadership role for both fabric interconnects in a high availability cluster.</p> <p>Verify that both fabric interconnects (A and B) are in the Up state and HA is in the Ready state. If the fabric interconnects are not in the Up state or HA is not in the Ready state, run a show tech-support command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the show tech-support command, see the <i>Cisco UCS Troubleshooting Guide</i>.</p> <p>Also note which fabric interconnect has the primary role and which has the subordinate role; you will need to know this information to upgrade the firmware on the fabric interconnects.</p> |

The following example displays that both fabric interconnects are in the Up state, HA is in the Ready state, fabric interconnect A has the primary role, and fabric interconnect B has the subordinate role:

```
UCS-A# show cluster state
Cluster Id: 0x4432f72a371511de-0xb97c000de1b1ada4

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
```

Verifying the Status of an I/O Module

If your Cisco UCS is running in a high availability cluster configuration, you must verify the status for both I/O modules in all chassis.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope chassis chassis-id | Enters chassis mode for the specified chassis. |
| Step 2 | UCS-A /chassis# scope iom iom-id | Enters chassis I/O module mode for the selected I/O module. |
| Step 3 | UCS-A# show | <p>Shows the status of the specified I/O module on the specified chassis.</p> <p>Verify that the overall status of the I/O module is in the Operable state. If the overall status is not in the Operable state, run a show tech-support command and contact Cisco Technical Support. Do not proceed with the firmware upgrade. For more information about the show tech-support command, see the <i>Cisco UCS Troubleshooting Guide</i>.</p> |

The following example displays that the overall status for both I/O modules on chassis 1 is in the Operable state:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope iom 1
UCS-A /chassis/iom # show
IOM:
  ID          Side Fabric ID Overall Status
  -----
    1 Left    A          Operable

UCS-A /chassis/iom # exit
UCS-A /chassis # scope iom 2
UCS-A /chassis/iom # show
IOM:
  ID          Side Fabric ID Overall Status
  -----
    2 Right   B          Operable
```

Verifying the Status of a Server

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope server <i>chassis-id/server-id</i> | Enters chassis server mode for the specified server in the specified chassis. |
| Step 2 | UCS-A /chassis/server # show status detail | Shows the status detail of the server. Verify that the overall status of the server is Ok, Unavailable, or any value that does not indicate a failure. If the overall status is in a state that indicates a failure, such as Discovery Failed, the endpoints on that server cannot be upgraded. |

The following example displays that the overall status for server 7 on chassis 1 is in the Ok state:

```
UCS-A# scope server 1/7
UCS-A /chassis/server # show status detail
Server 1/7:
  Slot Status: Equipped
  Conn Path: A,B
  Conn Status: A,B
  Managing Instance: B
  Availability: Unavailable
  Admin State: In Service
  Overall Status: Ok
  Oper Qualifier: N/A
  Discovery: Complete
  Current Task:
```

Verifying the Status of an Adapter

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope server <i>chassis-id/server-id</i> | Enters chassis server mode for the specified server in the specified chassis |
| Step 2 | UCS-A /chassis/server # show adapter status | Displays the status of the adapter. Verify that the overall status of the adapter is in the Operable state. If the overall status of the adapter is in any state other than Operable, you cannot upgrade it. However, you can proceed with the upgrade for the other adapters in the Cisco UCS instance. |

The following example displays that the overall status for the adapter in server 7 on chassis 1 is in the Operable state:

```
UCS-A# scope server 1/7
UCS-A /chassis/server # show adapter status
Server 1/1:
  Overall Status
  -----
  Operable
```

Downloading and Managing Images

Obtaining Firmware Packages from Cisco

Procedure

-
- Step 1** In a web browser, navigate to <http://www.cisco.com>.
 - Step 2** Under **Support**, click **Download Software**.
 - Step 3** Click **Unified Computing**.
 - Step 4** Enter your Cisco.com username and password to log in.
 - Step 5** Click **Cisco Unified Computing System**.
If you prefer to download an image for a single component, expand the node for that component and click the link to the appropriate image.
 - Step 6** Click **Unified Computing System (UCS) Complete Software Bundle**.
 - Step 7** Under the **Latest Releases** folder, click the link for the latest release of Cisco UCS. Images for earlier releases are archived under the **All Releases** link.
 - Step 8** Click the Release Notes link to download the latest version of the Release Notes.
 - Step 9** Click one of the following buttons and follow the instructions provided:
 - **Download Now**—Allows you to download the firmware image immediately

- **Add to Cart**—Adds the firmware image to your cart to be downloaded at a later time

Step 10 Follow the prompts to complete your download of the image.

Step 11 Read the release notes before upgrading the Cisco UCS instance.

What to Do Next

Download the firmware image to the fabric interconnect.

Downloading a Firmware Package to the Fabric Interconnect

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope firmware | Enters firmware mode. |
| Step 2 | UCS-A /firmware # download image URL | Downloads the firmware package for Cisco UCS. Using the download path provided by Cisco, specify the URL using one of the following syntax: <ul style="list-style-type: none"> • ftp://server-ip-addr /path • scp://username@server-ip-addr/path • sftp://username@server-ip-addr/path • tftp://server-ip-addr :port-num/path |
| Step 3 | UCS-A /firmware # show download-task | Displays the status for your download task. When your image is completely downloaded, the task state changes from Downloading to Downloaded. The CLI does not automatically refresh, so you may have to enter the show download-task command multiple times until the task state displays Downloaded. |

The following example uses SCP to download the ucs-k9-bundle.1.0.0.988.gbin firmware package.

```
UCS-A# scope firmware
UCS-A /firmware # download image scp://user1@192.168.10.10/images/ucs-k9-bundle.1.0.0.988.gbin
```

What to Do Next

Display the download status to confirm that the firmware package has completely downloaded, and then directly update the firmware at the endpoints.

Displaying the Firmware Package Download Status

After a firmware download operation has been started, you can check the download status to see if the package is still downloading or if it has completely downloaded.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope firmware | Enters firmware mode. |
| Step 2 | UCS-A /firmware # show download-task | Displays the status for your download task. When your image is completely downloaded, the task state changes from Downloading to Downloaded. The CLI does not automatically refresh, so you may have to enter the show download-task command multiple times until the task state displays Downloaded. |

The following example displays the download status for the ucs-k9-bundle.1.0.0.988.gbin firmware package. The **show download-task** command is entered multiple times until the download state indicates that the firmware package has been downloaded:

```
UCS-A# scope firmware
UCS-A /firmware # show download-task

Download task:
File Name Protocol Server      Userid      State
-----
ucs-k9-bundle.1.0.0.988.gbin
      Scp      10.193.32.11  user1      Downloading

UCS-A /firmware # show download-task

Download task:
File Name Protocol Server      Userid      State
-----
ucs-k9-bundle.1.0.0.988.gbin
      Scp      10.193.32.11  user1      Downloading

UCS-A /firmware # show download-task

Download task:
File Name Protocol Server      Userid      State
-----
ucs-k9-bundle.1.0.0.988.gbin
      Scp      10.193.32.11  user1      Downloaded
```

Displaying All Available Software Images on the Fabric Interconnect

This procedure is optional and displays the available software images on the fabric interconnect for all endpoints.. You can also use the **show image** command in each endpoint mode to display the available software images for that endpoint.

Procedure

| | Command or Action | Purpose |
|---------------|-------------------------------------|---|
| Step 1 | UCS-A# scope firmware | Enters firmware mode. |
| Step 2 | UCS-A /firmware # show image | Displays all software images downloaded onto the fabric interconnect. |

| | Command or Action | Purpose |
|--|-------------------|---|
| | | Note You must provide the software version number when directly updating an endpoint. If you intend to directly update firmware at an endpoint, note its version number in the right column. |

The following example displays all available software images on the fabric interconnect:

```
UCS-A# scope firmware
UCS-A /firmware # show image
Name                                                    Type                Version
-----
ucs-2100.1.0.0.988.gbin                                Iom                 1.0(0.988)
ucs-6100-k9-kickstart.4.0.1a.N2.1.0.988.gbin          Switch Kernel
4.0(1a)N2(1.0.988)
ucs-6100-k9-system.4.0.1a.N2.1.0.988.gbin            Switch Software
4.0(1a)N2(1.0.988)
ucs-b200-m1-bios.S5500.86B.01.00.0030-978a.021920.gbin Server Bios
S5500.86B.01.00.0030-978a.021920
ucs-b200-m1-k9-bmc.1.0.0.988.gbin                    Bmc                 1.0(0.988)
ucs-b200-m1-sasctlr.2009.02.09.gbin                  Storage Controller 2009.02.09
ucs-m71kr-e-cna.1.0.0.988.gbin                       Adapter              1.0(0.988)
ucs-m71kr-e-hba.zf280a4.gbin                         Host Hba             zf280a4
ucs-m71kr-e-optionrom.ZN502N5.gbin                   Host Hba Optionrom  ZN502N5
ucs-m71kr-q-cna.1.0.0.988.gbin                       Adapter              1.0(0.988)
ucs-m71kr-q-optionrom.1.69.gbin                       Host Hba Optionrom  1.69
ucs-m81kr-vic.1.0.0.988.gbin                         Adapter              1.0(0.988)
ucs-manager-k9.1.0.0.988.gbin                        System               1.0(0.988)
```

Directly Upgrading Firmware at Endpoints

Updating and Activating the Firmware on an Adapter

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope adapter <i>chassis-id/ blade-id/adapter-id</i> | Enters chassis server adapter mode for the specified adapter. |
| Step 2 | UCS-A /chassis/server/adapter # show image | Displays the available software images for the adapter. |
| Step 3 | UCS-A /chassis/server/adapter # update firmware <i>version-num</i> | Updates the selected firmware version on the adapter. |
| Step 4 | UCS-A /chassis/server/adapter # commit-buffer | (Optional) Commits the transaction. Use this step only if you intend to use the show firmware command in Step 5 to verify that the firmware update completed successfully before activating the firmware in Step 6. You can skip this step and commit the update-firmware and activate-firmware commands in the same transaction; however, |

| | Command or Action | Purpose |
|---------------|---|---|
| | | <p>if the firmware update does not complete successfully, the firmware activation will not start.</p> <p>Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.</p> |
| Step 5 | UCS-A /chassis/server/adapter # show firmware | <p>(Optional)</p> <p>Displays the status of the firmware update.</p> <p>Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the show firmware command multiple times until the task state changes from Updating to Ready. Continue to Step 6 when the update status is Ready.</p> |
| Step 6 | UCS-A /chassis/server/adapter # activate firmware <i>version-num</i> [ignorecompcheck [set-startup-only] set-startup-only] | <p>Activates the selected firmware version on the adapter.</p> <p>Use the set-startup-only keyword if you want to move the activated firmware into the pending-next-boot state and not immediately reboot the server. The activated firmware does not become the running version of firmware on the adapter until the server is rebooted. You cannot use the set-startup-only keyword for an adapter in the host firmware package.</p> <p>Use the ignorecompcheck keyword if you want to ignore the compatibility check and activate the firmware regardless of any possible incompatibilities or currently executing tasks.</p> |
| Step 7 | UCS-A /chassis/server/adapter # commit-buffer | Commits the transaction. |
| Step 8 | UCS-A /chassis/server/adapter # show firmware | <p>(Optional)</p> <p>Displays the status of the firmware activation.</p> <p>Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the show firmware command multiple times until the task state changes from Activating to Ready.</p> |

The following example updates and activates the adapter firmware to version 1.2(1) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

```
UCS-A# scope adapter 1/1/1
UCS-A# /chassis/server/adapter # show image
Name                                     Type                               Version                            State
-----
ucs-m81kr-vic.1.2.1.gbin                Adapter                             1.2(1)                             Active

UCS-A# /chassis/server/adapter # update firmware 1.2(1)
UCS-A# /chassis/server/adapter* # activate firmware 1.2(1) ignorecompcheck set-startup-only
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter #
```

The following example updates the adapter firmware to version 1.2(1), verifies that the firmware update completed successfully before starting the firmware activation, activates the adapter firmware, and verifies that the firmware activation completed successfully:

```
UCS-A# scope adapter 1/1/1
UCS-A# /chassis/server/adapter # show image
Name                                     Type                               Version                            State
-----
ucs-m8lkr-vic.1.2.1.gbin                Adapter                             1.2(1)                             Active

UCS-A# /chassis/server/adapter # update firmware 1.2(1)
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
  Running-Vers: 1.1(1)
  Update-Status: Updating
  Activate-Status: Ready

UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
  Running-Vers: 1.1(1)
  Update-Status: Ready
  Activate-Status: Ready

UCS-A# /chassis/server/adapter # activate firmware 1.2(1) ignorecompcheck
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
  Running-Vers: 1.1(1)
  Update-Status: Ready
  Activate-Status: Activating

UCS-A# /chassis/server/adapter # show firmware
Adapter 1:
  Running-Vers: 1.2(1)
  Update-Status: Ready
  Activate-Status: Ready
```

Updating and Activating the Firmware on a CIMC

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope server <i>chassis-id / blade-id</i> | Enters chassis server mode for the specified server. |
| Step 2 | UCS-A /chassis/server # scope cimc | Enters chassis server CIMC mode. |
| Step 3 | UCS-A /chassis/server/cimc # show image | Displays the available software images for the adapter. |
| Step 4 | UCS-A /chassis/server/cimc # update firmware <i>version-num</i> | Updates the selected firmware version on the CIMC in the server. |
| Step 5 | UCS-A /chassis/cimc # commit-buffer | (Optional) Commits the transaction. Use this step only if you intend to use the show firmware command in Step 6 to verify that the firmware update completed |

| | Command or Action | Purpose |
|---------------|---|---|
| | | successfully before activating the firmware in Step 7. You can skip this step and commit the update-firmware and activate-firmware commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation will not start. Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it. |
| Step 6 | UCS-A /chassis/cimc # show firmware | (Optional) Displays the status of the firmware update. Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the show firmware command multiple times until the task state changes from Updating to Ready. Continue to Step 7 when the update status is Ready. |
| Step 7 | UCS-A /chassis/server/cimc # activate firmware version-num [ignorecompcheck] | Activates the selected firmware version on the CIMC in the server. Use the ignorecompcheck keyword if you want to ignore the compatibility check and activate the firmware regardless of any possible incompatibilities or currently executing tasks. |
| Step 8 | UCS-A /chassis/server/cimc # commit-buffer | Commits the transaction. |
| Step 9 | UCS-A /chassis/cimc # show firmware | (Optional) Displays the status of the firmware activation. Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the show firmware command multiple times until the task state changes from Activating to Ready. |

The following example updates and activates the CIMC firmware to version 1.2(1) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope cimc
UCS-A# /chassis/server/cimc # show image
-----
Name                                     Type                               Version                            State
-----
ucs-b200-m1-k9-cimc.1.2.1.gbin          Bmc                                1.2 (1)
Active

UCS-A# /chassis/server/cimc # update firmware 1.2(1)
UCS-A# /chassis/server/cimc* # activate firmware 1.2(1) ignorecompcheck set-startup-only
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc #
```

The following example updates the CIMC firmware to version 1.2(1), verifies that the firmware update completed successfully before starting the firmware activation, activates the CIMC firmware, and verifies that the firmware activation completed successfully:

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope cimc
UCS-A# /chassis/server/cimc # show image
-----
Name                                                    Type           Version        State
-----
ucs-b200-m1-k9-cimc.1.2.1.gbin                         Bmc            1.2(1)
Active

UCS-A# /chassis/server/cimc # update firmware 1.2(1)
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc # show firmware
Running-Vers      Update-Status    Activate-Status
-----
1.1(1)            Updating         Ready

UCS-A# /chassis/server/cimc # show firmware
Running-Vers      Update-Status    Activate-Status
-----
1.1(1)            Ready           Ready

UCS-A# /chassis/server/cimc # activate firmware 1.2(1) ignorecompcheck
UCS-A# /chassis/server/cimc* # commit-buffer
UCS-A# /chassis/server/cimc # show firmware
Running-Vers      Update-Status    Activate-Status
-----
1.1(1)            Ready           Activating

UCS-A# /chassis/server/cimc # show firmware
Running-Vers      Update-Status    Activate-Status
-----
1.2(1)            Ready           Ready
```

Updating an Activating the Firmware on an I/O Module

If your system is running in a high availability cluster configuration, you must update and activate both I/O modules.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope chassis <i>chassis-id</i> | Enters chassis mode for the specified chassis. |
| Step 2 | UCS-A /chassis # scope iom <i>iom-id</i> | Enters chassis I/O module mode for the selected I/O module. |
| Step 3 | UCS-A /chassis/iom # show image | Displays the available software images for the I/O module. |
| Step 4 | UCS-A /chassis/iom # update firmware <i>version-num</i> | Updates the selected firmware version on the I/O module. |
| Step 5 | UCS-A /chassis/iom # commit-buffer | (Optional) Commits the transaction. |

| | Command or Action | Purpose |
|---------------|---|---|
| | | <p>Use this step only if you intend to use the show firmware command in Step 6 to verify that the firmware update completed successfully before activating the firmware in Step 7. You can skip this step and commit the update-firmware and activate-firmware commands in the same transaction; however, if the firmware update does not complete successfully, the firmware activation will not start.</p> <p>Cisco UCS Manager copies the selected firmware image to the backup memory partition and verifies that image is not corrupt. The image remains as the backup version until you explicitly activate it.</p> |
| Step 6 | UCS-A /chassis/iom # show firmware | <p>(Optional) Displays the status of the firmware update.</p> <p>Use this step only if you want to verify that the firmware update completed successfully. The firmware update is complete when the update status is Ready. The CLI does not automatically refresh, so you may have to enter the show firmware command multiple times until the task state changes from Updating to Ready. Continue to Step 7 when the update status is Ready.</p> |
| Step 7 | UCS-A /chassis/iom # activate firmware version-num [ignorecompcheck] [set-startup-only] set-startup-only | <p>Activates the selected firmware version on the I/O module.</p> <p>Use the set-startup-only keyword if you want to reboot the I/O module only when the fabric interconnect in its data path reboots. If you do not use the set-startup-only keyword, the I/O module reboots and disrupts traffic. In addition, if Cisco UCS Manager detects a protocol and firmware version mismatch between it and the I/O module, it updates the I/O module with the firmware version that matches its own and then activates the firmware and reboots the I/O module again.</p> <p>Use the ignorecompcheck keyword if you want to ignore the compatibility check and activate the firmware regardless of any possible incompatibilities or currently executing tasks.</p> |
| Step 8 | UCS-A /chassis/iom # commit-buffer | Commits the transaction. |
| Step 9 | UCS-A /chassis/iom # show firmware | <p>(Optional) Displays the status of the firmware activation.</p> <p>Use this step only if you want to verify that the firmware activation completed successfully. The CLI does not automatically refresh, so you may have to enter the show firmware command multiple times until the task state changes from Activating to Ready.</p> |

The following example updates and activates the I/O module firmware to version 1.2(1) in the same transaction, without verifying that the firmware update and firmware activation completed successfully:

```
UCS-A# scope chassis 1
UCS-A# /chassis # scope iom 1
UCS-A# /chassis/iom # show image
```

| Name | Type | Version | State |
|------|------|---------|-------|
|------|------|---------|-------|

```

-----
ucs-2100.1.2.1.gbin                                Iom                                1.2(1)                                Active
UCS-A# /chassis/iom # update firmware 1.2(1)
UCS-A# /chassis/iom* # activate firmware 1.2(1) ignorecompcheck set-startup-only
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom #

```

The following example updates the I/O module firmware to version 1.2(1), verifies that the firmware update completed successfully before starting the firmware activation, activates the I/O module firmware, and verifies that the firmware activation completed successfully:

```

UCS-A# scope chassis 1
UCS-A# /chassis # scope iom 1
UCS-A# /chassis/iom # show image
Name                                         Type                                Version                                State
-----
ucs-2100.1.2.1.gbin                        Iom                                1.2(1)                                Active

UCS-A# /chassis/iom # update firmware 1.2(1)
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers      Update-Status      Activate-Status
-----
      1 A          1.1(1)          Updating          Ready

UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers      Update-Status      Activate-Status
-----
      1 A          1.1(1)          Ready            Ready

UCS-A# /chassis/iom # activate firmware 1.2(1) ignorecompcheck
UCS-A# /chassis/iom* # commit-buffer
UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers      Update-Status      Activate-Status
-----
      1 A          1.1(1)          Ready            Activating

UCS-A# /chassis/iom # show firmware
IOM      Fabric ID Running-Vers      Update-Status      Activate-Status
-----
      1 A          1.2(1)          Ready            Ready

```

Activating the Board Controller Firmware on a Server

Only certain servers, such as the Cisco UCS B440 High Performance blade server, have board controller firmware. The board controller firmware controls the algorithms for functions such as lighting the front panel LEDs on the server.



Note

This activation procedure causes the server to reboot immediately. To reduce the number of times a server needs to be rebooted during the upgrade process, we recommend that you upgrade the board controller firmware through the host firmware package in the service profile.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope server <i>chassis-id/server-id</i> | Enters chassis server mode for the specified server. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 2 | UCS-A /chassis/server # scope boardcontroller | Enters board controller mode for the server. |
| Step 3 | UCS-A /chassis/server/boardcontroller # show image | (Optional) Displays the available software images for the board controller. |
| Step 4 | UCS-A /chassis/server/boardcontroller # show firmware | (Optional) Displays the current running software image for the board controller. |
| Step 5 | UCS-A /chassis/server/boardcontroller # activate firmware <i>version-num</i> [ignorecompcheck] | Activates the selected firmware version on the board controller in the server. Use the ignorecompcheck keyword if you want to ignore the compatibility check and activate the firmware regardless of any possible incompatibilities or currently executing tasks. |
| Step 6 | UCS-A /chassis/server/boardcontroller # commit-buffer | Commits the transaction to the system configuration. |

Cisco UCS Manager disconnects all active sessions, logs out all users, and then activates the software. When the upgrade is complete, you are prompted to log back in.

The following example activates the board controller firmware:

```
UCS-A# scope server 1/1
UCS-A# /chassis/server # scope boardcontroller
UCS-A# /chassis/server/boardcontroller # show image
Name                                     Type           Version        State
-----
ucs-b440-m1-pld.B440100C-B4402006.bin  Board Controller B440100C-B4402006 Active

UCS-A# /chassis/server/boardcontroller # show firmware
BoardController:
  Running-Vers: B440100C-B4402006
  Activate-Status: Ready

UCS-A# /chassis/server/boardcontroller # activate firmware B440100C-B4402006
ignorecompcheck
UCS-A# /chassis/server/boardcontroller* # commit-buffer
```

Activating the Cisco UCS Manager Software

Procedure

| | Command or Action | Purpose |
|---------------|-----------------------------------|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # show image | Displays the available software images for Cisco UCS Manager (system). |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 3 | UCS-A /system # activate firmware <i>version-num</i> [ignorecompcheck] | Activates the selected firmware version on the system. Use the ignorecompcheck keyword if you want to ignore the compatibility check and activate the firmware regardless of any possible incompatibilities or currently executing tasks. Note Activating Cisco UCS Manager does not require rebooting the fabric interconnect; however, management services will briefly go down and all VSH shells will be terminated as part of the activation. |
| Step 4 | UCS-A /system # commit-buffer | Commits the transaction. Cisco UCS Manager makes the selected version the startup version and schedules the activation to occur when the fabric interconnects are upgraded. |

The following example upgrades Cisco UCS Manager to version 1.2(1) and commits the transaction:

```
UCS-A# scope system
UCS-A# /system # show image
Name                                     Type                Version             State
-----
ucs-manager-k9.1.2.1.gbin               System               1.2(1)             Active

UCS-A# /system # activate firmware 1.2(1)
UCS-A# /system* # commit-buffer
UCS-A# /system #
```

Activating the Firmware on a Fabric Interconnect

When updating the firmware on two fabric interconnects in a high availability cluster configuration, you must activate the subordinate fabric interconnect before activating the primary fabric interconnect. For more information about determining the role for each fabric interconnect, see [Verifying the High Availability Status and Roles of a Cluster Configuration](#), page 125.



Tip

If you ever need to recover the password to the admin account that was created when you configured the fabric interconnects for the Cisco UCS instance, you must know the running kernel version and the running system version. If you do not plan to create additional accounts, we recommend that you save the path to these firmware versions in a text file so that you can access them if required.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope fabric-interconnect {a b} | Enters fabric interconnect mode for the specified fabric interconnect. |
| Step 2 | UCS-A /fabric-interconnect # show image | Displays the available software images for the fabric interconnect. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 3 | UCS-A /fabric-interconnect # activate firmware { kernel-version <i>kernel-ver-num</i> system-version <i>system-ver-num</i> } | Activates the selected firmware version on the fabric interconnect. |
| Step 4 | UCS-A /fabric-interconnect # commit-buffer | Commits the transaction. Cisco UCS Manager updates and activates the firmware, and then reboots the fabric interconnect and any I/O module in the data path to that fabric interconnect, disrupting data traffic to and from that fabric interconnect. |

The following example upgrades the fabric interconnect to version 4.0(1a)N2(1.2.1) and commits the transaction:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # show image
Name                                     Type                               Version                               State
-----
ucs-6100-k9-kickstart.4.0.1a.N2.1.2.1.gbin  Fabric Interconnect  4.0(1a)N2(1.2.1)  Active
ucs-6100-k9-system.4.0.1a.N2.1.2.1.gbin    Fabric Interconnect  4.0(1a)N2(1.2.1)  Active

UCS-A /fabric-interconnect # activate firmware kernel-version 4.0(1a)N2(1.2.1) system-version
4.0(1a)N2(1.2.1)
UCS-A /fabric-interconnect* # commit-buffer
UCS-A /fabric-interconnect #
```

Updating Firmware through Service Profiles

Host Firmware Package

This policy enables you to specify a set of firmware versions that make up the host firmware package (also known as the host firmware pack). The host firmware includes the following firmware for server and adapter endpoints:

- **Adapter Firmware Packages**
- **Storage Controller Firmware Packages**
- **Fibre Channel Adapters Firmware Packages**
- **BIOS Firmware Packages**
- **HBA Option ROM Packages**
- **Board Controller Packages**

**Tip**

You can include more than one type of firmware in the same host firmware package. For example, a host firmware package can include both BIOS firmware and storage controller firmware or adapter firmware for two different models of adapters. However, you can only have one firmware version with the same type, vendor, and model number. The system recognizes which firmware version is required for an endpoint and ignores all other firmware versions.

The firmware package is pushed to all servers associated with service profiles that include this policy.

This policy ensures that the host firmware is identical on all servers associated with service profiles which use the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained. Also, if you change the firmware version for an endpoint in the firmware package, new versions are applied to all the affected service profiles immediately, which could cause server reboots.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

Prerequisites

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect. If the firmware image is not available when Cisco UCS Manager is associating a server with a service profile, Cisco UCS Manager ignores the firmware upgrade and completes the association.

Creating and Updating a Host Firmware Package

**Caution**

If the policy is included in one or more service profiles associated with a server, Cisco UCS Manager updates and activates the firmware in the server and adapter with the new versions and reboots the server as soon as you save the host firmware package policy.

Before You Begin

Ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A org/ # create fw-host-pack <i>pack-name</i> | Creates a host firmware package with the specified package name and enters organization firmware host package mode. |
| Step 3 | UCS-A /org/fw-host-pack # set descr <i>description</i> | (Optional) Provides a description for the host firmware package. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 4 | UCS-A org/fw-host-pack # create pack-image <i>hw-vendor-name</i> <i>hw-model</i> { adapter host-hba host-hba-combined host-hba-optionrom host-nic server-bios storage-controller unspecified } <i>version-num</i> | Creates a package image for the host firmware package and enters organization firmware host package image mode. The <i>hw-vendor-name</i> and <i>hw-model</i> values are labels that help you easily identify the package image when you enter the show image detail command. The <i>version-num</i> value specifies the version number of the firmware being used for the package image. The firmware version must match the model numbers (PID) on the servers that are associated with this firmware pack. If you select a firmware version with the wrong model number, Cisco UCS Manager cannot install the firmware update. |
| Step 5 | UCS-A org/fw-host-pack/pack-image # set version <i>version-num</i> | (Optional) Specifies the package image version number. Changing this number triggers firmware updates on all components using the firmware through a service profile. Use this step only when updating a host firmware package, not when creating a package. Note The host firmware package can contain multiple package images. Repeat Steps Step 4, page 408 and Step 5, page 408 to create additional package images for other components. |
| Step 6 | UCS-A org/fw-host-pack/pack-image # commit-buffer | Commits the transaction. Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware. |

The following example creates the app1 host firmware package, creates a storage controller package image with version 2009.02.09 firmware, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create fw-host-pack app1
UCS-A /org/fw-host-pack* # set descr "This is a host firmware package example."
UCS-A /org/fw-host-pack* # create pack-image Cisco UCS storage-controller 2009.02.09
UCS-A /org/fw-host-pack/pack-image* # commit-buffer
UCS-A /org/fw-host-pack/pack-image #
```

What to Do Next

Include the policy in a service profile and/or template.

Management Firmware Package

This policy enables you to specify a set of firmware versions that make up the management firmware package (also known as a management firmware pack). The management firmware package includes the Cisco Integrated Management Controller (CIMC) on the server. You do not need to use this package if you upgrade the CIMC directly.

The firmware package is pushed to all servers associated with service profiles that include this policy. This policy ensures that the CIMC firmware is identical on all servers associated with service profiles which use

the same policy. Therefore, if you move the service profile from one server to another, the firmware versions are maintained.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect.

This policy is not dependent upon any other policies. However, you must ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Creating and Updating a Management Firmware Package



Caution

If the policy is included in a one or more service profiles associated with a server, as soon as you save the management firmware package policy, Cisco UCS Manager updates and activates the CIMC firmware in the server with the new version.

Before You Begin

Ensure that the appropriate firmware has been downloaded to the fabric interconnect.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A org/ # create fw-mgmt-pack <i>pack-name</i> | Creates a management firmware package with the specified package name and enters organization firmware management package mode. |
| Step 3 | UCS-A /org/fw-mgmt-pack # set descr <i>description</i> | (Optional) Provides a description for the management firmware package. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A org/fw-mgmt-pack # create pack-image <i>hw-vendor-name hw-model bmc version-num</i> | Creates a package image for the management firmware package and enters organization firmware management package image mode. The <i>hw-vendor-name</i> and <i>hw-model</i> values are labels that help you easily identify the package image when you enter the show image detail command. The <i>version-num</i> value specifies the version number of the firmware being used for the package image. The firmware version must match the model numbers (PID) on the servers that are associated with this firmware pack. If you select a firmware version with the wrong model number, Cisco UCS Manager cannot install the firmware update. |
| Step 5 | UCS-A org/fw-mgmt-pack/pack-image # set version <i>version-num</i> | (Optional) Specifies the package image version number. Changing this number triggers firmware updates on all components using the firmware |

| | Command or Action | Purpose |
|---------------|--|--|
| | | through a service profile. Use this step only when updating a firmware package, not when creating a package. |
| Step 6 | UCS-A org/fw-mgmt-pack/pack-image # commit-buffer | Commits the transaction. Cisco UCS Manager verifies the model numbers and vendor against all servers associated with service profiles that include this policy. If the model numbers and vendor match a firmware version in the policy, Cisco UCS Manager updates the firmware. |

The following example creates the cim1 host firmware package, creates a CIMC package image with version 1.0(0.988) firmware, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create fw-mgmt-pack cim1
UCS-A /org/fw-mgmt-pack* # set descr "This is a management firmware package example."
UCS-A /org/fw-mgmt-pack* # create pack-image Cisco UCS cimc 1.0(0.988)
UCS-A /org/fw-mgmt-pack/pack-image* # commit-buffer
UCS-A /org/fw-mgmt-pack/pack-image #
```

What to Do Next

Include the policy in a service profile and/or template.

Managing the Capability Catalog

Capability Catalog

The capability catalog is a set of tunable parameters, strings, and rules. Cisco UCS Manager uses the catalog to update the display and configurability of components such as newly qualified DIMMs and disk drives for servers.

The catalog is divided by hardware components, such as the chassis, CPU, local disk, and I/O module. You can use the catalog to view the list of providers available for that component. There is one provider per hardware component. Each provider is identified by the vendor, model (PID), and revision. For each provider, you can also view details of the equipment manufacture and the form factor.

Contents of the Capability Catalog

The contents of the capability catalog include the following:

Implementation-Specific Tunable Parameters

- Power and thermal constraints
- Slot ranges and numbering
- Adaptor capacities

Hardware-Specific Rules

- Firmware compatibility for components such as the BIOS, CIMC, RAID controller, and adapters
- Diagnostics

- Hardware-specific reboot

User Display Strings

- Part numbers, such as the CPN, PID/VID
- Component descriptions
- Physical layout/dimensions
- OEM information

Updates to the Capability Catalog

Each Cisco UCS Manager release contains a baseline catalog. When appropriate, Cisco releases an update to the capability catalog and makes it available on the same site where you download firmware images. The catalog update is compatible with Cisco UCS, Release 1.3(1) and above.

As soon as you download a capability catalog update, Cisco UCS Manager immediately updates to the new baseline catalog. You do not have to perform any further tasks. Updates to the capability catalog do not require you to reboot any component in the Cisco UCS instance, or reinstall Cisco UCS Manager.

Obtaining Capability Catalog Updates from Cisco

Procedure

- Step 1** In a web browser, navigate to <http://www.cisco.com>.
 - Step 2** Under **Support**, click **Download Software**.
 - Step 3** Click **Unified Computing**.
 - Step 4** Enter your Cisco.com username and password to log in.
 - Step 5** Click **Cisco Unified Computing System**.
 - Step 6** Click **Unified Computing System (UCS) Manager Capability Catalog**.
 - Step 7** Under the **Latest Releases** folder, click the link for the latest release of the capability catalog. Images for earlier releases are archived under the **All Releases** link.
 - Step 8** Click one of the following buttons and follow the instructions provided:
 - **Download Now**—Allows you to download the catalog update immediately
 - **Add to Cart**—Adds the catalog update to your cart to be downloaded at a later time
 - Step 9** Follow the prompts to complete your download of the catalog update.
-

What to Do Next

Update the capability catalog.

Updating the Capability Catalog

You cannot perform a partial update to the capability catalog. When you update the capability catalog, all components included in the catalog image are updated.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope system | Enters system command mode. |
| Step 2 | UCS-A /system # scope capability | Enters capability command mode. |
| Step 3 | UCS-A /system/capability # update catalog URL | Imports and applies the specified capability catalog file. Specify the URL for the operation using one of the following syntax: <ul style="list-style-type: none"> • ftp://hostname/path • scp://username@hostname/path • sftp://username@hostname/path • tftp://hostname:port-num/path When a user name is specified, you are prompted for a password. |
| Step 4 | UCS-A /system/capability # show version | (Optional) Displays the catalog update version. |
| Step 5 | UCS-A /system/capability # show cat-updater [filename] | (Optional) Displays the update history for a capability catalog file, if specified, or for all capability catalog file update operations. |

Cisco UCS Manager downloads the image and immediately updates the capability catalog. You do not need to reboot any hardware components or perform any other tasks for the update to take effect.

The following example uses SCP to import a capability catalog file:

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # update catalog
scp://user1@192.0.2.111/catalogs/ucs-catalog.1.0.0.4.bin
Password:
UCS-A /system/capability # show version
Catalog:
  Update Version: 1.0(0.4)

UCS-A /system/capability # show cat-updater

Catalog Updater:
  File Name Protocol Server          Userid      Status
  -----
  ucs-catalog.1.0.0.4.bin
    Scp          192.0.2.111    user1      Success

UCS-A /system/capability #
```

Restarting a Capability Catalog Update

You can restart a failed capability catalog file update, modifying the update parameters if necessary.

Procedure

| | Command or Action | Purpose |
|----------------|--|---|
| Step 1 | UCS-A# scope system | Enters system command mode. |
| Step 2 | UCS-A /system # scope capability | Enters capability command mode. |
| Step 3 | UCS-A /system/capability # show cat-updater [filename] | (Optional) Displays the update history for capability catalog file update operations. |
| Step 4 | UCS-A /system/capability # scope cat-updater filename | Enters the command mode for the capability catalog file update operation. |
| Step 5 | UCS-A /system/capability/cat-updater # set userid username | (Optional) Specifies the user name for the remote server. |
| Step 6 | UCS-A /system/capability/cat-updater # set password password | (Optional) Specifies the password for the remote server user name. If no password is configured, you are prompted for a password when you start the update. |
| Step 7 | UCS-A /system/capability/cat-updater # set protocol {ftp scp sftp tftp} | (Optional) Specifies the file transfer protocol for the remote server. Note TFTP has a file size limitation of 32 MB. Because catalog images can be much larger than that, we recommend that you do not use TFTP for catalog image downloads. |
| Step 8 | UCS-A /system/capability/cat-updater # set server {hostname ip-address} | (Optional) Specifies the host name or IP address of the remote server. |
| Step 9 | UCS-A /system/capability/cat-updater # set path pathname/filename | (Optional) Specifies the path and file name of the capability catalog file on the remote server. |
| Step 10 | UCS-A /system/capability/cat-updater # restart | Restarts the capability catalog file update operation. |

The following example changes the server IP address and restarts the capability catalog file update operation:

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # show cat-updater

Catalog Updater:
  File Name Protocol Server          Userid          Status
  -----
  ucs-catalog.1.0.0.4.bin
    Scp          192.0.2.111    user1          Failed

UCS-A /system/capability # scope cat-updater ucs-catalog.1.0.0.4.bin
UCS-A /system/capability/cat-updater # set server 192.0.2.112
```

```
UCS-A /system/capability/cat-updater # restart
UCS-A /system/capability/cat-updater #
```

Viewing a Capability Catalog Provider

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope system | Enters system command mode. |
| Step 2 | UCS-A /system # scope capability | Enters capability command mode. |
| Step 3 | UCS-A /system/capability # show { chassis cpu disk fan fru iom memory psu server } [<i>vendor model</i> <i>revision</i>] [detail expand] | Displays vendor, model, and revision information for all components in the specified component category. To view manufacturing and form factor details for a specific component, specify the <i>vendor</i> , <i>model</i> , and <i>revision</i> with the expand keyword. If any of these fields contains spaces, you must enclose the field with quotation marks. |



Note

If the server contains one or more SATA devices, such as a hard disk drive or solid state drive, the **show disk** command displays ATA in the Vendor field. Use the **expand** keyword to display additional vendor information.

The following example lists the installed fans and displays detailed information from the capability catalog about a specific fan:

```
UCS-A# scope system
UCS-A /system # scope capability
UCS-A /system/capability # show fan
```

```
Fan Module:
  Vendor                Model                Revision
  -----
  Cisco Systems, Inc.   N10-FAN1             0
  Cisco Systems, Inc.   N10-FAN2             0
  Cisco Systems, Inc.   N20-FAN5             0
```

```
UCS-A /system/capability # show fan "Cisco Systems, Inc." N10-FAN1 0 expand
```

```
Fan Module:
  Vendor: Cisco Systems, Inc.
  Model: N10-FAN1
  Revision: 0

Equipment Manufacturing:
  Name: Fan Module for UCS 6140 Fabric Interconnect
  PID: N10-FAN1
  VID: NA
  Caption: Fan Module for UCS 6140 Fabric Interconnect
  Part Number: N10-FAN1
  SKU: N10-FAN1
  CLEI:
  Equipment Type:

Form Factor:
  Depth (C): 6.700000
```

```
Height (C): 1.600000  
Width (C): 4.900000  
Weight (C): 1.500000
```

```
UCS-A /system/capability #
```




CHAPTER 11

Configuring DNS Servers

This chapter includes the following sections:

- [DNS Servers in Cisco UCS, page 151](#)
- [Configuring a DNS Server, page 151](#)
- [Deleting a DNS Server, page 152](#)

DNS Servers in Cisco UCS

You need to specify an external DNS server for each Cisco UCS instance to use if the system requires name resolution of hostnames. For example, you cannot use a name such as `www.cisco.com` when you are configuring a setting on a fabric interconnect if you do not configure a DNS server. You would need to use the IP address of the server.

Configuring a DNS Server

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope services | Enters system services mode. |
| Step 3 | UCS-A /system/services # create dns <i>ip-addr</i> | Configures the system to use the DNS server with the specified IP address. |
| Step 4 | UCS-A /system/services # commit-buffer | Commits the transaction to the system configuration. |

The following example configures a DNS server with the IP address 192.168.200.105 and commits the transaction:

```
UCS-A# scope system  
UCS-A /system # scope services
```

```
UCS-A /system/services # create dns 192.168.200.105
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

Deleting a DNS Server

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope services | Enters system services mode. |
| Step 3 | UCS-A /system/services # delete dns <i>ip-addr</i> | Deletes the NTP server with the specified IP address. |
| Step 4 | UCS-A /system/services # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the DNS server with the IP address 192.168.200.105 and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # delete dns 192.168.200.105
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```



CHAPTER 12

Configuring System-Related Policies

This chapter includes the following sections:

- [Configuring the Chassis Discovery Policy, page 153](#)
- [Configuring the Power Policy, page 155](#)
- [Configuring the Aging Time for the MAC Address Table, page 156](#)

Configuring the Chassis Discovery Policy

Chassis Discovery Policy

The chassis discovery policy determines how the system reacts when you add a new chassis. Cisco UCS Manager uses the settings in the chassis discovery policy to determine the minimum threshold for the number of links between the chassis and the fabric interconnect. However, the configuration in the chassis discovery policy does not prevent you from connecting multiple chassis to the fabric interconnects in a Cisco UCS instance and wiring those chassis with a different number of links.

If you have a Cisco UCS instance that has some chassis wired with 1 link, some with 2 links, and some with 4 links, we recommend that you configure the chassis discovery policy for the minimum number links in the instance so that Cisco UCS Manager can discover all chassis. After the initial discovery, you must reacknowledge the chassis that are wired for a greater number of links and Cisco UCS Manager configures the chassis to use all available links.

Cisco UCS Manager cannot discover any chassis that is wired for fewer links than are configured in the chassis discovery policy. For example, if the chassis discovery policy is configured for 4 links, Cisco UCS Manager cannot discover any chassis that is wired for 1 link or 2 links. Reacknowledgement of the chassis does not resolve this issue.

The following table provides an overview of how the chassis discovery policy works in a multi-chassis Cisco UCS instance:

Table 10: Chassis Discovery Policy and Chassis Links

| Number of Links Wired for the Chassis | 1-Link Chassis Discovery Policy | 2-Link Chassis Discovery Policy | 4-Link Chassis Discovery Policy |
|---|--|---|--|
| 1 link between IOM and fabric interconnects | Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 1 link. | Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS instance. | Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS instance. |
| 2 links between IOM and fabric interconnects | Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 1 link. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links. | Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 2 link. | Chassis cannot be discovered by Cisco UCS Manager and is not added to the Cisco UCS instance. |
| 4 links between IOM and fabric interconnects | Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 1 link. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links. | Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 2 links. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links. | Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS instance as a chassis wired with 4 link. |

Configuring the Chassis Discovery Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org / | Enters the root organization mode. Note The chassis discovery policy can be accessed only from the root organization. |
| Step 2 | UCS-A /org # scope chassis-disc-policy | Enters organization chassis discovery policy mode. |
| Step 3 | UCS-A /org/chassis-disc-policy # set action {1-link 2-link 4-link} | Specifies the number of links to the fabric interconnect that the chassis must have before it can be discovered. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 4 | UCS-A /org/chassis-disc-policy # set descr <i>description</i> | (Optional) Provides a description for the chassis discovery policy. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 5 | UCS-A /org/chassis-disc-policy # set qualifier <i>qualifier</i> | (Optional) Uses the specified server pool policy qualifications to associate this policy with a server pool. |
| Step 6 | UCS-A /org/chassis-disc-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example scopes to the default chassis discovery policy, sets it to discover chassis with four links to a fabric interconnect, provides a description for the policy, specifies the server pool policy qualifications that will be used to qualify the chassis, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope chassis-disc-policy
UCS-A /org/chassis-disc-policy* # set action 4-link
UCS-A /org/chassis-disc-policy* # set descr "This is an example chassis discovery policy."
UCS-A /org/chassis-disc-policy* # set qualifier ExampleQual
UCS-A /org/chassis-disc-policy* # commit-buffer
UCS-A /org/chassis-disc-policy #
```

Configuring the Power Policy

Power Policy

The power policy is a global policy that specifies the redundancy for power supplies in all chassis in the Cisco UCS instance. This policy is also known as the PSU policy.

For more information about power supply redundancy, see *Cisco UCS 5108 Server Chassis Hardware Installation Guide*.

Configuring the Power Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope psu-policy | Enters PSU policy mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 3 | UCS-A /org/psu-policy # set redundancy { grid n-plus-1 non-redund } | <p>Specifies one of the following redundancy types:</p> <ul style="list-style-type: none"> • grid—Provides power redundancy when two power sources are used to power the chassis. If one power source fails, the surviving power supplies on the other power circuit continue to provide power to the chassis. • n-plus-1—Balances the power load for the chassis across the number of power supplies needed to satisfy non-redundancy plus one additional power supply for redundancy. If any additional power supplies are installed, they are recognized and powered off. • non-redund—Balances the power load for the chassis evenly across all installed power supplies. <p>For more information about power redundancy, see the <i>Cisco UCS 5108 Server Chassis Installation Guide</i>.</p> |
| Step 4 | UCS-A /org/psu-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example configures the power policy to use grid redundancy and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope psu-policy
UCS-A /org/psu-policy # set redundancy grid
UCS-A /org/psu-policy* # commit-buffer
UCS-A /org/psu-policy #
```

Configuring the Aging Time for the MAC Address Table

Aging Time for the MAC Address Table

To efficiently switch packets between ports, the fabric interconnect maintains a MAC address table. It dynamically builds the MAC address table by using the MAC source address from the packets received and the associated port on which the packets were learned. The fabric interconnect uses an aging mechanism, defined by a configurable aging timer, to determine how long an entry remains in the MAC address table. If an address remains inactive for a specified number of seconds, it is removed from the MAC address table.

You can configure the amount of time (age) that a MAC address entry (MAC address and associated port) remains in the MAC address table.

Configuring the Aging Time for the MAC Address Table

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # set mac-aging {seconds mode-default never} | Specifies the aging time for the MAC address table. Use the mode-default keyword to set the aging time to a default value dependent on the configured Ethernet switching mode. For end-host mode, the default aging time is 14500 seconds; for switch mode, the default aging time is 300 seconds. Use the never keyword to never remove MAC addresses from the table regardless of how long they have been idle. |
| Step 3 | UCS-A /eth-uplink # commit-buffer | Commits the transaction to the system configuration. |

The following example sets the aging time for the MAC address table to 10,000 seconds and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # set mac-aging 10000
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink #
```




CHAPTER 13

Managing Port Licenses

This chapter includes the following sections:

- [Port Licenses, page 159](#)
- [Obtaining the Host ID for a Fabric Interconnect, page 159](#)
- [Obtaining a Port License, page 160](#)
- [Installing a Port License on a Fabric Interconnect, page 161](#)
- [Viewing the Port Licenses Installed on a Fabric Interconnect, page 162](#)
- [Viewing Port License Usage for a Fabric Interconnect, page 162](#)
- [Uninstalling a Port License from a Fabric Interconnect, page 163](#)

Port Licenses

Port licenses for each Cisco UCS fabric interconnect are factory installed and shipped with the hardware. At a minimum, each fabric interconnect ships with the following licenses pre-installed:

- Cisco UCS 6120XP fabric interconnect—pre-installed licenses for the first eight Ethernet ports and any Fibre Channel ports on expansion modules
- Cisco UCS 6140XP fabric interconnect—pre-installed licenses for the first sixteen Ethernet ports and any Fibre Channel ports on expansion modules

If you want to use additional fixed ports, you must purchase and install licenses for those ports.

At this time, you can only install port licenses through Cisco UCS Manager CLI.

Obtaining the Host ID for a Fabric Interconnect

The host ID is also known as the serial number. You can also view the serial number in the Cisco UCS Manager GUI on the **General** tab for the fabric interconnect.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# connect local-mgmt | Enters local management mode. |
| Step 2 | UCS-A(local-mgmt)# show license host-id | Obtains the host ID or serial number for the fabric interconnect. Tip Use the entire host ID that displays after the equal (=) sign. |

The following example obtains the host ID for a fabric interconnect:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# show license host-id
License hostid: VDH=FLC12121212
```

What to Do Next

Obtain the port license from Cisco.

Obtaining a Port License

**Note**

This process may change after the release of this document. If one or more of these steps no longer applies, contact your Cisco representative for information on how to obtain a license file.

Before You Begin

Obtain the following:

- Host ID or serial number for the fabric interconnect
- Claim certificate or other proof of purchase document for the fabric interconnect or expansion module

Procedure

-
- Step 1** Obtain the product authorization key (PAK) from the claim certificate or other proof of purchase document.
- Step 2** Locate the website URL in the claim certificate or proof of purchase document.
- Step 3** Access the website URL for the fabric interconnect and enter the serial number and the PAK. Cisco sends you the license file by email. The license file is digitally signed to authorize use on only the requested fabric interconnect. The requested features are also enabled once Cisco UCS Manager accesses the license file.
-

What to Do Next

Install the port license on the fabric interconnect.

Installing a Port License on a Fabric Interconnect

You must use Cisco UCS Manager CLI to install a port license.

Before You Begin

Obtain the port license from Cisco.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# connect local-mgmt | Enters local management mode. |
| Step 2 | UCS-A(local-mgmt)# copy <i>from-filesystem:[from-path]/license_filename</i> Workspace:license_filename | Copies the port license from its source location to its destination location. For the <i>from-filesystem:</i> argument, use one of the following syntax: <ul style="list-style-type: none"> • ftp://server-ip-addr • scp://username@server-ip-addr • sftp://username@server-ip-addr • tftp://server-ip-addr :port-num |
| Step 3 | UCS-A(local-mgmt)# install-license workspace:license_filename | Installs the port license. |

The following example uses FTP to copy a port license to the workspace and then installs that port license:

```
UCS-A # connect local-mgmt
Cisco UCS 6100 Series Fabric Interconnect

TAC support: http://www.cisco.com/tac

Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software may be covered under the GNU Public
License or the GNU Lesser General Public License. A copy of
each such license is available at
http://www.gnu.org/licenses/gpl.html and
http://www.gnu.org/licenses/lgpl.html

UCS-A(local-mgmt) # copy ftp://192.168.10.10/license/port9.lic workspace:/port9.lic
UCS-A(local-mgmt) # install-license workspace:port9.lic
```

Viewing the Port Licenses Installed on a Fabric Interconnect

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# connect local-mgmt | Enters local management mode. |
| Step 2 | UCS-A(local-mgmt)# show license [brief file [license_filename]] | Displays the port licenses installed on the fabric interconnect with the level of detail specified in the command. |

The following example displays full details of the port licenses installed on a fabric interconnect:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# show license file

enter.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT ENTERPRISE_PKG cisco 1.0 permanent uncounted \
  VENDOR_STRING=<LIC_SOURCE>UCS_SWIFT</LIC_SOURCE><SKU>ENTERPRISE_PKG=</SKU> \
  HOSTID=VDH=FLC12360025 \
  NOTICE="<LicFileID>20090519230254773</LicFileID><LicLineID>1</LicLineID> \
  <PAK></PAK>" SIGN=134D2848E9B0

port1.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT ETH_PORT_ACTIVATION_PKG cisco 1.0 permanent 1 \
  VENDOR_STRING=<LIC_SOURCE>UCS_SWIFT</LIC_SOURCE><SKU>N10-L001=</SKU> \
  HOSTID=VDH=FLC12360025 \
  NOTICE="<LicFileID>20090519200954833</LicFileID><LicLineID>1</LicLineID> \
  <PAK></PAK>" SIGN=C01FAE4E87FA

port2.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT ETH_PORT_ACTIVATION_PKG cisco 1.0 permanent 8 \
  VENDOR_STRING=<LIC_SOURCE>UCS_SWIFT</LIC_SOURCE><SKU>ETH_PORT_ACTIVATION_PKG=</SKU> \
  \
  HOSTID=VDH=FLC12360025 \
  NOTICE="<LicFileID>20090519231228131</LicFileID><LicLineID>1</LicLineID> \
  <PAK></PAK>" SIGN=DF6A586C43C6
UCS-A(local-mgmt)#
```

Viewing Port License Usage for a Fabric Interconnect

Procedure

| | Command or Action | Purpose |
|---------------|----------------------------------|-------------------------------|
| Step 1 | UCS-A# connect local-mgmt | Enters local management mode. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 2 | UCS-A(local-mgmt)# show license usage | Displays the license usage table for all license files installed on the fabric interconnect. |

The following example displays full details of the licenses installed on a fabric interconnect:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# show license usage
Feature                               Ins  Lic  Status Expiry Date Comments
                                Count
-----
FM_SERVER_PKG                         No   -   Unused
ENTERPRISE_PKG                        No   -   Unused
FC_FEATURES_PKG                       No   -   Unused      Grace expired
ETH_PORT_ACTIVATION_PKG               No   8   Unused      Never
ETH_MODULE_ACTIVATION_PKG              No   0   Unused
-----
UCS-A(local-mgmt)#
```

Uninstalling a Port License from a Fabric Interconnect

You can only uninstall a permanent license that is not in use. If you try to delete a permanent license that is being used, Cisco UCS Manager rejects the request with an error message.

If you attempt to use a port that does not have an installed license, Cisco UCS initiates a grace period. The grace period is measured from the first use of the feature without a license and is reset when a valid license file is installed. After the grace period expires, the ports are not functional. Contact your Cisco representative for information about the length of the grace period for your fabric interconnect.



Note

Permanent licenses cannot be uninstalled if they are in use.

Before You Begin

- Back up the Cisco UCS Manager configuration
- Disable the port associated with the port license you want to uninstall

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# connect local-mgmt | Enters local management mode. |
| Step 2 | UCS-A(local-mgmt)# clear license <i>license_filename</i> | Uninstalls the port license that you specify by name. |

The following example shows the uninstallation of port9.lic:

```
UCS-A # connect local-mgmt
Cisco UCS 6100 Series Fabric Interconnect

TAC support: http://www.cisco.com/tac
```

Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained herein are owned by other third parties and are used and distributed under license. Some parts of this software may be covered under the GNU Public License or the GNU Lesser General Public License. A copy of each such license is available at <http://www.gnu.org/licenses/gpl.html> and <http://www.gnu.org/licenses/lgpl.html>

```
UCS-A(local-mgmt)# clear license port9.lic
Clearing license port9.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT ETH_PORT_ACTIVATION_PKG cisco 1.0 permanent 1 \
  VENDOR_STRING=<LIC_SOURCE>UCS_SWIFT</LIC_SOURCE><SKU>N10-L001=</SKU> \
  HOSTID=VDH=FLC12360025 \
  NOTICE="<LicFileID>20090519200954833</LicFileID><LicLineID>1</LicLineID> \
  <PAK></PAK>" SIGN=C01FAE4E87FA

Clearing license .....done
UCS-A(local-mgmt)#
```

What to Do Next

For a cluster configuration, uninstall the port license for the same port on the other fabric interconnect.



PART **III**

Network Configuration

- [Configuring Named VLANs, page 167](#)
- [Configuring LAN Pin Groups, page 171](#)
- [Configuring MAC Pools, page 173](#)
- [Configuring Quality of Service, page 175](#)
- [Configuring Network-Related Policies, page 183](#)



CHAPTER 14

Configuring Named VLANs

This chapter includes the following sections:

- [Named VLANs, page 167](#)
- [Creating a Named VLAN Accessible to Both Fabric Interconnects, page 167](#)
- [Creating a Named VLAN Accessible to One Fabric Interconnect, page 168](#)
- [Deleting a Named VLAN, page 169](#)

Named VLANs

A named VLAN creates a connection to a specific external LAN. The VLAN isolates traffic to that external LAN, including broadcast traffic.

The name that you assign to a VLAN ID adds a layer of abstraction that allows you to globally update all servers associated with service profiles that use the named VLAN. You do not need to reconfigure the servers individually to maintain communication with the external LAN.

You can create more than one named VLAN with the same VLAN ID. For example, if servers that host business services for HR and Finance need to access the same external LAN, you can create VLANs named HR and Finance with the same VLAN ID. Then, if the network is reconfigured and Finance is assigned to a different LAN, you only have to change the VLAN ID for the named VLAN for Finance.

In a cluster configuration, you can configure a named VLAN to be accessible only to one fabric interconnect or to both fabric interconnects.

Creating a Named VLAN Accessible to Both Fabric Interconnects



Important

You cannot create VLANs with IDs from 3968 to 4047. This range of VLAN IDs is reserved. The VLAN name is case sensitive.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # create vlan <i>vlan-name vlan-id</i> | Creates a named VLAN, specifies the VLAN name and VLAN ID, and enters Ethernet uplink VLAN mode. |
| Step 3 | UCS-A /eth-uplink/vlan # set default-net | (Optional) Sets the VLAN as the default VLAN. Note Only one VLAN can exist as the default VLAN. If multiple VLANs are set as the default, the most recently set VLAN is the default. |
| Step 4 | UCS-A /eth-uplink/vlan # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a named VLAN for both fabric interconnects, names the VLAN accounting, assigns the VLAN ID 2112, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create vlan accounting 2112
UCS-A /eth-uplink/vlan* # commit-buffer
UCS-A /eth-uplink/vlan #
```

Creating a Named VLAN Accessible to One Fabric Interconnect



Important You cannot create VLANs with IDs from 3968 to 4047. This range of VLAN IDs is reserved. The VLAN name is case sensitive.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # scope fabric {a b} | Enters Ethernet uplink fabric interconnect mode for the specified fabric interconnect (A or B). |
| Step 3 | UCS-A /eth-uplink/fabric # create vlan <i>vlan-name vlan-id</i> | Creates a named VLAN, specifies the VLAN name and VLAN ID, and enters Ethernet uplink fabric interconnect VLAN mode. |
| Step 4 | UCS-A /eth-uplink/fabric/vlan # set default-net | (Optional) Sets the VLAN as the native VLAN. |

| | Command or Action | Purpose |
|---------------|---|---|
| | | Note Only one VLAN can exist as the native VLAN. If you set multiple VLANs as the native VLAN, the last one to be set becomes the native VLAN. |
| Step 5 | UCS-A /eth-uplink/fabric/vlan # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a named VLAN for fabric interconnect A, names the VLAN finance, assigns the VLAN ID 3955, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # create vlan finance 3955
UCS-A /eth-uplink/fabric/vlan* # commit-buffer
UCS-A /eth-uplink/fabric/vlan #
```

Deleting a Named VLAN

If Cisco UCS Manager includes a named VLAN with the same VLAN ID as the one you delete, the VLAN is not removed from the fabric interconnect configuration until all named VLANs with that ID are deleted.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # scope fabric {a b} | (Optional) Enters Ethernet uplink fabric mode. Use this command when you want to delete a named VLAN only from the specified fabric (a or b). |
| Step 3 | UCS-A /eth-uplink # delete vlan vlan-name | Deletes the specified named VLAN. |
| Step 4 | UCS-A /eth-uplink # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes a named VLAN accessible to both fabric interconnects and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # delete vlan accounting
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink #
```

The following example deletes a named VLAN accessible to one fabric interconnect and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric a
UCS-A /eth-uplink/fabric # delete vlan finance
UCS-A /eth-uplink/fabric* # commit-buffer
UCS-A /eth-uplink/fabric #
```




CHAPTER 15

Configuring LAN Pin Groups

This chapter includes the following sections:

- [LAN Pin Groups, page 171](#)
- [Configuring a LAN Pin Group, page 171](#)

LAN Pin Groups

Cisco UCS uses LAN pin groups to pin Ethernet traffic from a vNIC on a server to an uplink Ethernet port or port channel on the fabric interconnect. You can use this pinning to manage the distribution of traffic from the servers.

To configure pinning for a server, you must include the LAN pin group in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server. All traffic from the vNIC travels through the I/O module to the specified uplink Ethernet port.



Note

If you do not assign a pin group to a server interface through a vNIC policy, Cisco UCS Manager chooses an uplink Ethernet port or port channel for traffic from that server interface dynamically. This choice is not permanent. A different uplink Ethernet port or port channel may be used for traffic from that server interface after an interface flap or a server reboot.

Configuring a LAN Pin Group

In a system with two fabric interconnects, you can associate the pin group with only one fabric interconnect or with both fabric interconnects.

Before You Begin

Configure the ports and port channels with which you want to configure the pin group. You can only include ports and port channels configured as uplink ports in a LAN pin group.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # create pin-group <i>pin-group-name</i> | Creates an Ethernet (LAN) pin group with the specified name, and enters Ethernet uplink pin group mode. |
| Step 3 | UCS-A /eth-uplink/pin-group # set descr <i>description</i> | (Optional) Provides a description for the pin group. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /eth-uplink/pin-group # set target { a b dual } { port slot-num / <i>port-num</i> port-channel <i>port-num</i> } | (Optional) Sets the Ethernet pin target to the specified fabric and port, or fabric and port channel. |
| Step 5 | UCS-A /eth-uplink/pin-group # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a LAN pin group named pingroup54 on fabric A, provides a description for the pin group, sets the pin group target to port channel 28, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # create pin-group pingroup54
UCS-A /eth-uplink/pin-group* # set descr "This is my pin group #54"
UCS-A /eth-uplink/pin-group* # set target a port-channel 28
UCS-A /eth-uplink/pin-group* # commit-buffer
UCS-A /eth-uplink/pin-group #
```

What to Do Next

Include the pin group in a vNIC template.



CHAPTER 16

Configuring MAC Pools

This chapter includes the following sections:

- [MAC Pools, page 173](#)
- [Configuring a MAC Pool, page 173](#)

MAC Pools

A MAC pool is a collection of network identities, or MAC addresses, that are unique in their layer 2 environment and are available to be assigned to vNICs on a server. If you use MAC pools in service profiles, you do not have to manually configure the MAC addresses to be used by the server associated with the service profile.

In a system that implements multi-tenancy, you can use the organizational hierarchy to ensure that MAC pools can only be used by specific applications or business services. Cisco UCS Manager uses the name resolution policy to assign MAC addresses from the pool.

To assign a MAC address to a server, you must include the MAC pool in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server.

You can specify your own MAC addresses or use a group of MAC addresses provided by Cisco.

Configuring a MAC Pool

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create mac-pool <i>mac-pool-name</i> | Creates a MAC pool with the specified name, and enters organization MAC pool mode. |
| Step 3 | UCS-A /org/mac-pool # set descr <i>description</i> | (Optional) Provides a description for the MAC pool. |

| | Command or Action | Purpose |
|---------------|---|---|
| | | Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /org/mac-pool # create block <i>first-mac-addr</i> <i>last-mac-addr</i> | Creates a block (range) of MAC addresses, and enters organization MAC pool block mode. You must specify the first and last MAC addresses in the address range using the form <i>nn : nn : nn : nn : nn</i> , with the addresses separated by a space. Note A MAC pool can contain more than one MAC address block. To create multiple MAC address blocks, you must enter multiple create block commands from organization MAC pool mode. |
| Step 5 | UCS-A /org/mac-pool # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a MAC pool named pool37, provides a description for the pool, defines a MAC address block by specifying the first and last MAC addresses in the block, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create mac-pool pool37
UCS-A /org/mac-pool* # set descr "This is my MAC pool"
UCS-A /org/mac-pool* # create block 00:A0:D7:42:00:01 00:A0:D7:42:01:00
UCS-A /org/mac-pool/block* # commit-buffer
UCS-A /org/mac-pool/block #
```

What to Do Next

Include the MAC pool in a vNIC template.



CHAPTER 17

Configuring Quality of Service

This chapter includes the following sections:

- [Quality of Service, page 175](#)
- [Configuring System Classes, page 175](#)
- [Configuring Quality of Service Policies, page 178](#)
- [Configuring Flow Control Policies, page 180](#)

Quality of Service

Cisco UCS provides the following methods to implement quality of service:

- System classes that specify the global configuration for certain types of traffic across the entire system
- QoS policies that assign system classes for individual vNICs
- Flow control policies that determine how uplink Ethernet ports handle pause frames

Configuring System Classes

System Classes

Cisco UCS uses Data Center Ethernet (DCE) to handle all traffic inside a Cisco UCS instance. This industry standard enhancement to Ethernet divides the bandwidth of the Ethernet pipe into eight virtual lanes. Two virtual lanes are reserved for internal system and management traffic. You can configure quality of service for the other six virtual lanes. System classes determine how the DCE bandwidth in these six virtual lanes is allocated across the entire Cisco UCS instance.

Each system class reserves a specific segment of the bandwidth for a specific type of traffic. This provides a level of traffic management, even in an oversubscribed system. For example, you can configure the Fibre Channel Priority system class to determine the percentage of DCE bandwidth allocated to FCoE traffic.

The following table describes the system classes that you can configure:

Table 11: System Classes

| System Class | Description |
|--------------------------------------|--|
| Platinum Gold Silver Bronze | A configurable set of system classes that you can include in the QoS policy for a service profile. Each system class manages one lane of traffic. All properties of these system classes are available for you to assign custom settings and policies. |
| Best Effort | A system class that sets the quality of service for the lane reserved for Basic Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a drop policy that allows it to drop data packets if required. You cannot disable this system class. |
| Fibre Channel | A system class that sets the quality of service for the lane reserved for Fibre Channel over Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a no-drop policy that ensures it never drops data packets. You cannot disable this system class. |

Configuring a System Class

The type of adapter in a server may limit the maximum MTU supported. For example, network MTU above the maximums may cause the packet to be dropped for the following adapters:

- The Cisco UCS CNA M71KR adapter, which supports a maximum MTU of 9216.
- The Cisco UCS 82598KR-CI adapter, which supports a maximum MTU of 14000.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope eth-server | Enters Ethernet server mode. |
| Step 2 | UCS-A /eth-server # scope qos | Enters Ethernet server QoS mode. |
| Step 3 | UCS-A /eth-server/qos # scope eth-classified {bronze gold platinum silver} | Enters Ethernet server QoS Ethernet classified mode for the specified system class. |
| Step 4 | UCS-A /eth-server/qos/eth-classified # enable | Enables the specified system class. |
| Step 5 | UCS-A /eth-server/qos/eth-classified # set cos cos-value | Specifies the class of service for the specified system class. Valid class of service values are 0 to 6; higher values indicate more important traffic. |

| | Command or Action | Purpose |
|----------------|--|---|
| Step 6 | UCS-A /eth-server/qos/eth-classified # set drop {drop no-drop} | Specifies whether the channel can drop packets or not. Note Only one system class can use the no-drop option. |
| Step 7 | UCS-A /eth-server/qos/eth-classified # set mtu {mtu-value fc normal} | Specifies the maximum transmission unit (MTU) for the specified system class. Valid MTU values are 1538 to 9216. |
| Step 8 | UCS-A /eth-server/qos/eth-classified # set multicast-optimize {no yes} | Specifies whether the class is optimized to for sending multicast packets. |
| Step 9 | UCS-A /eth-server/qos/eth-classified # set weight {weight-value best-effort none} | Specifies the relative weight for the specified system class. Valid weight values are 0 to 10. |
| Step 10 | UCS-A /eth-server/qos/eth-classified # commit-buffer | Commits the transaction to the system configuration. |

The following example enables the platinum system class, allows the channel to drop packets, sets the class of service to 6, sets the MTU to normal, optimizes the class for sending multicast packets, sets the relative weight to 5, and commits the transaction:

```
UCS-A# scope eth-server
UCS-A /eth-server # scope qos
UCS-A /eth-server/qos # scope eth-classified platinum
UCS-A /eth-server/qos/eth-classified # enable
UCS-A /eth-server/qos/eth-classified* # set drop drop
UCS-A /eth-server/qos/eth-classified* # set cos 6
UCS-A /eth-server/qos/eth-classified* # set mtu normal
UCS-A /eth-server/qos/eth-classified* # set multicast-optimize yes
UCS-A /eth-server/qos/eth-classified* # set weight 5
UCS-A /eth-server/qos/eth-classified* # commit-buffer
UCS-A /eth-server/qos/eth-classified #
```

Disabling a System Class

If you disable a system class that is used in a QoS policy, Cisco UCS Manager uses the system class configured with CoS 0 for traffic on servers that are configured with the QoS policy. If no system class is configured as CoS 0, the Best Effort system class is used. You cannot disable the Best Effort or Fibre Channel system classes.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope eth-server | Enters Ethernet server mode. |
| Step 2 | UCS-A /eth-server # scope qos | Enters Ethernet server QoS mode. |
| Step 3 | UCS-A /eth-server/qos # scope eth-classified {bronze gold platinum silver} | Enters Ethernet server QoS Ethernet classified mode for the specified system class. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 4 | UCS-A /eth-server/qos/eth-classified # disable | Disables the specified system class. |
| Step 5 | UCS-A /eth-server/qos/eth-classified # commit-buffer | Commits the transaction to the system configuration. |

The following example disables the platinum system class and commits the transaction:

```
UCS-A# scope eth-server
UCS-A /eth-server # scope qos
UCS-A /eth-server/qos # scope eth-classified platinum
UCS-A /eth-server/qos/eth-classified # disable
UCS-A /eth-server/qos/eth-classified* # commit-buffer
UCS-A /eth-server/qos/eth-classified #
```

Configuring Quality of Service Policies

Quality of Service Policy

A quality of service (QoS) policy assigns a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic. For certain adapters you can also specify additional controls on the outgoing traffic, such as burst and rate.

You must include a QoS policy in a vNIC policy or vHBA policy and then include that policy in a service profile to configure the vNIC or vHBA.

Configuring a QoS Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | Switch-A# scope org <i>org-name</i> | Enters org mode for the specified organization. To enter the default org mode, type / as the <i>org-name</i> . |
| Step 2 | Switch-A /org # create qos-policy <i>policy-name</i> | Creates the specified QoS policy, and enters org QoS policy mode. |
| Step 3 | Switch-A /org/qos-policy # create egress-policy | Creates the egress policy (for both vNICs and vHBAs) to be used by the QoS policy, and enters org QoS policy egress policy mode. |
| Step 4 | Switch-A /org/qos-policy/egress-policy # set host-cos-control { full none } | (Optional) Specifies whether the host or Cisco UCS Manager controls the class of service (CoS). Use the full keyword to have the host control the CoS. If the packet has a valid CoS value, the host uses that value. Otherwise, it uses the CoS value associated with the specified class priority. Use the none keyword to have Cisco UCS Manager use the CoS value associated with the specified priority. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 5 | Switch-A /org/qos-policy/egress-policy # set prio <i>sys-class-name</i> | Specifies the system class to be used for the egress policy. The <i>sys-class-name</i> argument can be one of the following class keywords: <ul style="list-style-type: none"> • best-effort—Do not use this priority. It is reserved for the Basic Ethernet traffic lane. If you assign this priority to a QoS policy and configure another system class as CoS 0, Cisco UCS Manager does not default to this system class. It defaults to the priority with CoS 0 for that traffic. • bronze—Use this priority for QoS policies that control vNIC traffic only. • fc—Use this priority for QoS policies that control vHBA traffic only. • gold—Use this priority for QoS policies that control vNIC traffic only. • platinum—Use this priority for QoS policies that control vNIC traffic only. • silver—Use this priority for QoS policies that control vNIC traffic only. |
| Step 6 | Switch-A /org/qos-policy/egress-policy # set rate { line-rate <i>Kbps</i> } burst <i>bytes</i> | Specifies the rate limit for egress traffic by defining the average traffic rate and burst size. The line-rate keyword sets the rate limit to the physical line rate. |
| Step 7 | Switch-A /org/qos-policy/egress-policy # committ-buffer | Commits the transaction to the system configuration. |

The following example creates a QoS policy for vNIC traffic, assigns the platinum system class and sets the rate limit (traffic rate and burst size) for the egress policy, and commits the transaction:

```
Switch-A# scope org /
Switch-A /org # create qos-policy VnicPolicy34
Switch-A /org/qos-policy* # create egress-policy
Switch-A /org/qos-policy/egress-policy* # set prio platinum
Switch-A /org/qos-policy/egress-policy* # set rate 5000000 burst 65000
Switch-A /org/qos-policy/egress-policy* # committ-buffer
Switch-A /org/qos-policy/egress-policy #
```

The following example creates a QoS policy for vHBA traffic, assigns the fc (Fibre Channel) system class and sets the rate limit (traffic rate and burst size) for the egress policy, and commits the transaction:

```
Switch-A# scope org /
Switch-A /org # create qos-policy VhbaPolicy12
Switch-A /org/qos-policy* # create egress-policy
Switch-A /org/qos-policy/egress-policy* # set prio fc
Switch-A /org/qos-policy/egress-policy* # set rate 5000000 burst 65000
Switch-A /org/qos-policy/egress-policy* # committ-buffer
Switch-A /org/qos-policy/egress-policy #
```

What to Do Next

Include the QoS policy in a vNIC or vHBA template.

Deleting a QoS Policy

If you delete a QoS policy that is in use or you disable a system class that is used in a QoS policy, any vNIC or vHBA that uses that QoS policy is assigned to the Best Effort system class or to the system class with a CoS of 0. In a system that implements multi-tenancy, Cisco UCS Manager first attempts to find a matching QoS policy in the organization hierarchy.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete qos-policy <i>policy-name</i> | Deletes the specified QoS policy. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following deletes the QoS policy named QoSPolicy34 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete qos-policy QoSPolicy34
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Flow Control Policies**Flow Control Policy**

Flow control policies determine whether the uplink Ethernet ports in a Cisco UCS instance send and receive IEEE 802.3x pause frames when the receive buffer for a port fills. These pause frames request that the transmitting port stop sending data for a few milliseconds until the buffer clears.

For flow control to work between a LAN port and an uplink Ethernet port, you must enable the corresponding receive and send flow control parameters for both ports. For Cisco UCS, the flow control policies configure these parameters.

When you enable the send function, the uplink Ethernet port sends a pause request to the network port if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels. If you enable the receive function, the uplink Ethernet port honors all pause requests from the network port. All traffic is halted on that uplink port until the network port cancels the pause request.

Because you assign the flow control policy to the port, changes to the policy have an immediate effect on how the port reacts to a pause frame or a full receive buffer.

Configuring a Flow Control Policy

Before You Begin

Configure the network port with the corresponding setting for the flow control that you need. For example, if you enable the send setting for flow-control pause frames in the policy, make sure that the receive parameter in the network port is set to on or desired. If you want the Cisco UCS port to receive flow-control frames, make sure that the network port has a send parameter set to on or desired. If you do not want to use flow control, you can set the send and receive parameters on the network port to off.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # scope flow-control | Enters Ethernet uplink flow control mode. |
| Step 3 | UCS-A /eth-uplink/flow-control # create policy <i>policy-name</i> | Creates the specified flow control policy. |
| Step 4 | UCS-A /eth-uplink/flow-control/policy # set prio <i>prio-option</i> | Specifies one of the following flow control priority options: <ul style="list-style-type: none"> • auto—The Cisco UCS system and the network negotiate whether PPP will be used on this fabric interconnect. • on—PPP is enabled on this fabric interconnect. |
| Step 5 | UCS-A /eth-uplink/flow-control/policy # set receive <i>receive-option</i> | Specifies one of the following flow control receive options: <ul style="list-style-type: none"> • off—Pause requests from the network are ignored and traffic flow continues as normal. • on—Pause requests are honored and all traffic is halted on that uplink port until the network cancels the pause request. |
| Step 6 | UCS-A /eth-uplink/flow-control/policy # set send <i>send-option</i> | Specifies one of the following flow control send options: <ul style="list-style-type: none"> • off—Traffic on the port flows normally regardless of the packet load. • on—The Cisco UCS system sends a pause request to the network if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels. |
| Step 7 | UCS-A /org/qos-policy/vnic-egress-policy # commit-buffer | Commits the transaction to the system configuration. |

The following configures a flow control policy and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope flow-control
UCS-A /eth-uplink/flow-control # create policy FlowControlPolicy23
UCS-A /eth-uplink/flow-control/policy* # set prio auto
UCS-A /eth-uplink/flow-control/policy* # set receive on
UCS-A /eth-uplink/flow-control/policy* # set send on
UCS-A /eth-uplink/flow-control/policy* # commit-buffer
UCS-A /eth-uplink/flow-control/policy #
```

What to Do Next

Associate the flow control policy with an uplink Ethernet port or port channel.

Deleting a Flow Control Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # scope flow-control | Enters Ethernet uplink flow control mode. |
| Step 3 | UCS-A /eth-uplink/flow-control # delete policy <i>policy-name</i> | Deletes the specified flow control policy. |
| Step 4 | UCS-A /eth-uplink/flow-control # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the flow control policy named FlowControlPolicy23 and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope flow-control
UCS-A /eth-uplink/flow-control # delete policy FlowControlPolicy23
UCS-A /eth-uplink/flow-control* # commit-buffer
UCS-A /eth-uplink/flow-control #
```



CHAPTER 18

Configuring Network-Related Policies

This chapter includes the following sections:

- [Configuring vNIC Templates, page 183](#)
- [Configuring Ethernet Adapter Policies, page 185](#)
- [Configuring Network Control Policies, page 188](#)

Configuring vNIC Templates

vNIC Template

This policy defines how a vNIC on a server connects to the LAN. This policy is also referred to as a vNIC LAN connectivity policy.

You need to include this policy in a service profile for it to take effect.

Configuring a vNIC Template

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create vnic-templ <i>vnic-templ-name</i> [eth-if <i>vlan-name</i>] [fabric { <i>a</i> <i>b</i> }] [target [<i>adapter</i> <i>vm</i>]] | Creates a vNIC template and enters organization vNIC template mode. |
| Step 3 | UCS-A /org/vnic-templ # set descr <i>description</i> | (Optional) Provides a description for the vNIC template. |

| | Command or Action | Purpose |
|----------------|--|--|
| Step 4 | UCS-A /org/vnic-templ # set fabric {a b} | (Optional) Specifies the fabric to use for the vNIC. If you did not specify the fabric when creating the vNIC template in Step 2, you have the option to specify it with this command. |
| Step 5 | UCS-A /org/vnic-templ # set mac-pool <i>mac-pool-name</i> | Specifies the MAC pool to use for the vNIC. |
| Step 6 | UCS-A /org/vnic-templ # set mtu <i>mtu-value</i> | Specifies the maximum transmission unit, or packet size, that the vNIC accepts. |
| Step 7 | UCS-A /org/vnic-templ # set nw-control-policy <i>policy-name</i> | Specifies the network control policy to use for the vNIC. |
| Step 8 | UCS-A /org/vnic-templ # set pin-group <i>group-name</i> | Specifies the LAN pin group to use for the vNIC. |
| Step 9 | UCS-A /org/vnic-templ # set qos-policy <i>policy-name</i> | Specifies the QoS policy to use for the vNIC. |
| Step 10 | UCS-A /org/vnic-templ # set stats-policy <i>policy-name</i> | Specifies the server and server component statistics threshold policy to use for the vNIC. |
| Step 11 | UCS-A /org/vnic-templ # set type { initial-template updating-template } | Specifies the vNIC template update type. If you do not want vNIC instances created from this template to be automatically updated when the template is updated, use the initial-template keyword; otherwise, use the updating-template keyword to ensure that all vNIC instance are updated when the vNIC template is updated. |
| Step 12 | UCS-A /org/vnic-templ # commit-buffer | Commits the transaction to the system configuration. |

The following example configures a vNIC template and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create vnic template VnicTempFoo
UCS-A /org/vnic-templ* # set descr "This is a vNIC template example."
UCS-A /org/vnic-templ* # set fabric a
UCS-A /org/vnic-templ* # set mac-pool pool137
UCS-A /org/vnic-templ* # set mtu 8900
UCS-A /org/vnic-templ* # set nw-control-policy ncp5
UCS-A /org/vnic-templ* # set pin-group PinGroup54
UCS-A /org/vnic-templ* # set qos-policy QosPol5
UCS-A /org/vnic-templ* # set stats-policy ServStatsPolicy
UCS-A /org/vnic-templ* # set type updating-template
UCS-A /org/vnic-templ* # commit-buffer
UCS-A /org/vnic-templ #
```

Deleting a vNIC Template

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete vnic-templ <i>vnic-templ-name</i> | Deletes the specified vNIC template. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the vNIC template named VnicTempFoo and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete vnic template VnicTempFoo
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Ethernet Adapter Policies

Ethernet and Fibre Channel Adapter Policies

These policies govern the host-side behavior of the adapter, including how the adapter handles traffic. For example, you can use these policies to change default settings for the following:

- Queues
- Interrupt handling
- Performance enhancement
- RSS hash
- Failover in an cluster configuration with two fabric interconnects

**Note**

For Fibre Channel adapter policies, the values displayed by Cisco UCS Manager may not match those displayed by applications such as QLogic SANsurfer. For example, the following values may result in an apparent mismatch between SANsurfer and Cisco UCS Manager:

- Max LUNs Per Target—SANsurfer has a maximum of 256 LUNs and does not display more than that number. Cisco UCS Manager supports a higher maximum number of LUNs.
- Link Down Timeout—In SANsurfer, you configure the timeout threshold for link down in seconds. In Cisco UCS Manager, you configure this value in milliseconds. Therefore, a value of 5500 ms in Cisco UCS Manager displays as 5s in SANsurfer.
- Max Data Field Size—SANsurfer has allowed values of 512, 1024, and 2048. Cisco UCS Manager allows you to set values of any size. Therefore, a value of 900 in Cisco UCS Manager displays as 512 in SANsurfer.

Operating System Specific Adapter Policies

By default, Cisco UCS provides a set of Ethernet adapter policies and Fibre Channel adapter policies. These policies include the recommended settings for each supported server operating system. Operating systems are sensitive to the settings in these policies. Storage vendors typically require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.

**Important**

We recommend that you use the values in these policies for the applicable operating system. Do not modify any of the values in the default policies unless directed to do so by Cisco Technical Support.

However, if you are creating an Ethernet adapter policy for a Windows OS (instead of using the default Windows adapter policy), you must use the following formulas to calculate values that work with Windows:

$$\text{Completion Queues} = \text{Transmit Queues} + \text{Receive Queues}$$

$$\text{Interrupt Count} = (\text{Completion Queues} + 2) \text{ rounded up to nearest power of } 2$$

For example, if Transmit Queues = 1 and Receive Queues = 8 then:

$$\text{Completion Queues} = 1 + 8 = 9$$

$$\text{Interrupt Count} = (9 + 2) \text{ rounded up to the nearest power of } 2 = 16$$

Configuring an Ethernet Adapter Policy

Procedure

| | Command or Action | Purpose |
|---------------|----------------------------------|---|
| Step 1 | UCS-A# scope org org-name | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |

| | Command or Action | Purpose |
|----------------|---|--|
| Step 2 | UCS-A /org # create eth-policy <i>policy-name</i> | Creates the specified Ethernet adapter policy and enters organization Ethernet policy mode. |
| Step 3 | UCS-A /org/eth-policy # set comp-queue count <i>count</i> | (Optional) Configures the Ethernet completion queue. |
| Step 4 | UCS-A /org/eth-policy # set descr <i>description</i> | (Optional) Provides a description for the policy. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 5 | UCS-A /org/eth-policy # set failover timeout <i>timeout-sec</i> | (Optional) Configures the Ethernet failover. |
| Step 6 | UCS-A /org/eth-policy # set interrupt { coalescing-time <i>sec</i> coalescing-type { idle min } count <i>count</i> mode { intx msi msi-x }} | (Optional) Configures the Ethernet interrupt. |
| Step 7 | UCS-A /org/eth-policy # set offload { large-receive tcp-rx-checksum tcp-segment tcp-tx-checksum } { disabled enabled } | (Optional) Configures the Ethernet offload. |
| Step 8 | UCS-A /org/eth-policy # set recv-queue { count <i>count</i> ring-size <i>size-num</i> } | (Optional) Configures the Ethernet receive queue. |
| Step 9 | UCS-A /org/eth-policy # set rss receivesidescaling { disabled enabled } | (Optional) Configures the RSS. |
| Step 10 | UCS-A /org/eth-policy # set trans-queue { count <i>count</i> ring-size <i>size-num</i> } | (Optional) Configures the Ethernet transmit queue. |
| Step 11 | UCS-A /org/eth-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example configures an Ethernet adapter policy, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create eth-policy EthPolicy19
UCS-A /org/eth-policy* # set comp-queue count 16
UCS-A /org/eth-policy* # set descr "This is an Ethernet adapter policy example."
UCS-A /org/eth-policy* # set failover timeout 300
UCS-A /org/eth-policy* # set interrupt count 64
UCS-A /org/eth-policy* # set offload large-receive disabled
UCS-A /org/eth-policy* # set recv-queue count 32
UCS-A /org/eth-policy* # set rss receivesidescaling enabled
UCS-A /org/eth-policy* # set trans-queue
UCS-A /org/eth-policy* # commit-buffer
UCS-A /org/eth-policy #
```

Deleting an Ethernet Adapter Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete eth-policy <i>policy-name</i> | Deletes the specified Ethernet adapter policy. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the Ethernet adapter policy named EthPolicy19 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete eth-policy EthPolicy19
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Network Control Policies

Network Control Policy

This policy configures the network control settings for the Cisco UCS instance, including the following:

- Whether the Cisco Discovery Protocol (CDP) is enabled or disabled
- How the VIF behaves if no uplink port is available in end-host mode
- Whether the server can use different MAC addresses when sending packets to the fabric interconnect

The network control policy also determines the action that Cisco UCS Manager takes on the remote Ethernet port or the vEthernet interface when the associated border port fails. By default, the **Action on Uplink Fail** property in the network control policy is configured with a value of link-down. This default behavior directs Cisco UCS Manager to bring the remote Ethernet or vEthernet port down if the border port fails.



Note

The default behaviour of the **Action on Uplink Fail** property is optimal for most Cisco UCS that support link failover at the adapter level or only carry Ethernet traffic. However, for those converged network adapters that support both Ethernet and Fibre Channel traffic, such as the Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, the default behavior can affect and interrupt Fibre Channel traffic as well. Therefore, if the server includes one of those converged network adapters and the the adapter is expected to handle both Ethernet and Fibre Channel traffic, we recommend that you configure the **Action on Uplink Fail** property with a value of warning. Please note that this configuration may result in an Ethernet teaming driver not being able to detect a link failure when the border port goes down.

Configuring a Network Control Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org / | Enters the root organization mode. |
| Step 2 | UCS-A /org# create nwctrl-policy <i>policy-name</i> | Creates the specified network control policy, and enters organization network control policy mode. |
| Step 3 | UCS-A /org/nwctrl-policy # { disable enable } cdp | Disables or enables Cisco Discovery Protocol (CDP). |
| Step 4 | UCS-A /org/nwctrl-policy # set uplink-fail-action { link-down warning } | Specifies the action to be taken when no uplink port is available in end-host mode. Use the link-down keyword to change the operational state of a vNIC to down when uplink connectivity is lost on the fabric interconnect, and facilitate fabric failover for vNICs. Use the warning keyword to maintain server-to-server connectivity even when no uplink port is available, and disable fabric failover when uplink connectivity is lost on the fabric interconnect. The default uplink failure action is link-down. |
| Step 5 | UCS-A /org/nwctrl-policy # { create mac-security } | Enters organization network control policy MAC security mode |
| Step 6 | UCS-A /org/nwctrl-policy/mac-security # { set forged-transmit { allow deny } | Allows or denies the forging of MAC addresses when sending traffic. MAC security is disabled when forged MAC addresses are allowed, and MAC security is enabled when forged MAC addresses are denied. By default, forged MAC addresses are allowed (MAC security is disabled). |
| Step 7 | UCS-A /org/nwctrl-policy/mac-security # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a network control policy named ncp5, enables CDP, sets the uplink fail action to link-down, denies forged MAC addresses (enables MAC security), and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create nwctrl-policy ncp5
UCS-A /org/nwctrl-policy* # enable cdp
UCS-A /org/nwctrl-policy* # set uplink-fail-action link-down
UCS-A /org/nwctrl-policy* # create mac-security
UCS-A /org/nwctrl-policy/mac-security* # set forged-transmit deny
UCS-A /org/nwctrl-policy/mac-security* # commit-buffer
UCS-A /org/nwctrl-policy/mac-security #
```

Deleting a Network Control Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope org / | Enters the root organization mode. |
| Step 2 | UCS-A /org # delete nwctrl-policy <i>policy-name</i> | Deletes the specified network control policy. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the network control policy named ncp5 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete nwctrl-policy ncp5
UCS-A /org* # commit-buffer
UCS-A /org #
```



PART **IV**

Storage Configuration

- [Configuring Named VSANs, page 193](#)
- [Configuring SAN Pin Groups, page 197](#)
- [Configuring WWN Pools, page 199](#)
- [Configuring Storage-Related Policies, page 203](#)



CHAPTER 19

Configuring Named VSANs

This chapter includes the following sections:

- [Named VSANs, page 193](#)
- [Creating a Named VSAN Accessible to Both Fabric Interconnects, page 194](#)
- [Creating a Named VSAN Accessible to One Fabric Interconnect, page 194](#)
- [Deleting a Named VSAN, page 195](#)

Named VSANs

A named VSAN creates a connection to a specific external SAN. The VSAN isolates traffic to that external SAN, including broadcast traffic. The traffic on one named VSAN knows that the traffic on another named VSAN exists, but cannot read or access that traffic.

Like a named VLAN, the name that you assign to a VSAN ID adds a layer of abstraction that allows you to globally update all servers associated with service profiles that use the named VSAN. You do not need to reconfigure the servers individually to maintain communication with the external SAN. You can create more than one named VSAN with the same VSAN ID.

Named VSANs in Cluster Configurations

In a cluster configuration, a named VSAN can be configured to be accessible only to the FC uplinks on one fabric interconnect or to the FC Uplinks on both fabric interconnects.

Named VSANs and the FCoE VLAN ID

You must configure each named VSAN with an FCoE VLAN ID. This property determines which VLAN is used for transporting the VSAN and its Fibre Channel packets.

For FIP capable, converged network adapters, such as the Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, the named VSAN must be configured with a named VLAN that is not the native VLAN for the FCoE VLAN ID. This configuration ensures that FCoE traffic can pass through these adapters.

In the following sample configuration, a service profile with a vNIC and vHBA mapped to fabric A is associated with a server that has FIP capable, converged network adapters:

- The vNIC is configured to use VLAN 10.

- VLAN 10 is also designated as the native VLAN for the vNIC.
- The vHBA is configured to use VSAN 2.
- Therefore, VSAN 2 cannot be configured with VLAN 10 as the FCoE VLAN ID. VSAN 2 can be mapped to any other VLAN configured on fabric A.

Creating a Named VSAN Accessible to Both Fabric Interconnects

You can create a named VSAN with IDs from 1 to 4093.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope fc-uplink | Enters Fibre Channel uplink mode. |
| Step 2 | UCS-A /fc-uplink # create vsan <i>vsan-name vsan-id fcoe-id</i> | Creates the specified named VSAN, specifies the VSAN name, VSAN ID and FCoE VLAN ID, and enters Fibre Channel uplink VSAN mode. |
| Step 3 | UCS-A /fc-uplink/vsan # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a named VSAN for both fabric interconnects, names the VSAN accounting, assigns the VSAN ID 2112, assigns the FCoE VLAN ID 4021, and commits the transaction:

```
UCS-A# scope fc-uplink
UCS-A /eth-uplink* # create vsan accounting 2112 4021
UCS-A /eth-uplink/vsan* # commit-buffer
UCS-A /eth-uplink/vsan #
```

Creating a Named VSAN Accessible to One Fabric Interconnect

You can create a named VSAN with IDs from 1 to 4093.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope fc-uplink | Enters Fibre Channel uplink mode. |
| Step 2 | UCS-A /fc-uplink # scope fabric {a b} | Enters Fibre Channel uplink fabric interconnect mode for the specified fabric interconnect (A or B). |
| Step 3 | UCS-A /fc-uplink/fabric # create vsan <i>vsan-name vsan-id fcoe-id</i> | Creates the specified named VSAN, specifies the VSAN name, VSAN ID, and FCoE VLAN ID, and enters Fibre Channel uplink VSAN mode. |
| Step 4 | UCS-A /fc-uplink/fabric/vsan # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a named VSAN for fabric interconnect A, names the VSAN finance, assigns the VSAN ID 3955, assigns the FCoE VLAN ID 2221, and commits the transaction:

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create vsan finance 3955 2221
UCS-A /fc-uplink/fabric/vsan* # commit-buffer
UCS-A /fc-uplink/fabric/vsan #
```

Deleting a Named VSAN

If Cisco UCS Manager includes a named VSAN with the same VSAN ID as the one you delete, the VSAN is not removed from the fabric interconnect configuration until all named VSANs with that ID are deleted.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /fc-uplink # delete vsan <i>vsan-name</i> | Deletes the specified named VSAN. |
| Step 3 | UCS-A /fc-uplink # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes a named VSAN and commits the transaction:

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # delete vsan finance
UCS-A /fc-uplink* # commit-buffer
UCS-A /fc-uplink #
```




CHAPTER 20

Configuring SAN Pin Groups

This chapter includes the following sections:

- [SAN Pin Groups, page 197](#)
- [Configuring a SAN Pin Group, page 197](#)

SAN Pin Groups

Cisco UCS uses SAN pin groups to pin Fibre Channel traffic from a vHBA on a server to an uplink Fibre Channel port on the fabric interconnect. You can use this pinning to manage the distribution of traffic from the servers.

To configure pinning for a server, you must include the SAN pin group in a vHBA policy. The vHBA policy is then included in the service profile assigned to that server. All traffic from the vHBA will travel through the I/O module to the specified uplink Fibre Channel port.

You can assign the same pin group to multiple vHBA policies. As a result, you do not need to manually pin the traffic for each vHBA.



Important

Changing the target interface for an existing SAN pin group disrupts traffic for all vHBAs which use that pin group. The fabric interconnect performs a log in and log out for the Fibre Channel protocols to re-pin the traffic.

Configuring a SAN Pin Group

In a system with two fabric interconnects, you can associate the pin group with only one fabric interconnect or with both fabric interconnects.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope fc-uplink | Enters Fibre Channel uplink mode. |
| Step 2 | UCS-A /fc-uplink # create pin-group <i>pin-group-name</i> | Creates a Fibre Channel (SAN) pin group with the specified name, and enters Fibre Channel uplink pin group mode. |
| Step 3 | UCS-A /fc-uplink/pin-group # set descr <i>description</i> | (Optional) Provides a description for the pin group. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /fc-uplink/pin-group # set target {a b dual} port <i>slot-num / port-num</i> | (Optional) Sets the Fibre Channel pin target to the specified fabric and port. |

The following example creates a SAN pin group named fcpingroup12, provides a description for the pin group, sets the pin group target to slot 2, port 1, and commits the transaction:

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # create pin-group fcpingroup12
UCS-A /fc-uplink/pin-group* # set descr "This is my pin group #12"
UCS-A /fc-uplink/pin-group* # set target a port 2/1
```

What to Do Next

Include the pin group in a vHBA template.



CHAPTER 21

Configuring WWN Pools

This chapter includes the following sections:

- [WWN Pools, page 199](#)
- [Configuring a WWN Pool, page 200](#)

WWN Pools

A WWN pool is a collection of WWNs for use by the Fibre Channel vHBAs in a Cisco UCS instance. You create separate pools for the following:

- WW node names assigned to the server
- WW port names assigned to the vHBA



Important

A WWN pool can include only WWNNs or WWPNS in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNS in the SAN fabric, we recommend that you use the following WWN prefix for all blocks in a pool:
20:00:00:25:B5:XX:XX:XX

If you use WWN pools in service profiles, you do not have to manually configure the WWNs that will be used by the server associated with the service profile. In a system that implements multi-tenancy, you can use a WWN pool to control the WWNs used by each organization.

You assign WWNs to pools in blocks. For each block or individual WWN, you can assign a boot target.

WWNN Pools

A WWNN pool is a WWN pool that contains only WW node names. If you include a pool of WWNNs in a service profile, the associated server is assigned a WWNN from that pool.

WWPN Pools

A WWPNS pool is a WWN pool that contains only WW port names. If you include a pool of WWPNS in a service profile, the port on each vHBA of the associated server is assigned a WWPNS from that pool.

Configuring a WWN Pool



Important

A WWN pool can include only WWNNs or WWPNS in the ranges from 20:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNS in the SAN fabric, we recommend that you use the following WWN prefix for all blocks in a pool:
20:00:00:25:B5:XX:XX:XX

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> |
| Step 2 | UCS-A /org # create wwn-pool <i>wwn-pool-name</i> { node-wwn-assignment port-wwn-assignment } | Creates a WWN pool with the specified name and purpose, and enters organization WWN pool mode. The purpose of the WWN pool can be one of the following: <ul style="list-style-type: none"> • To assign world wide node names (WWNNs) and world wide port names (WWPNS) • To assign only WWNNs • To assign only WWPNS |
| Step 3 | UCS-A /org/wwn-pool # set descr <i>description</i> | (Optional) Provides a description for the WWN pool. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /org/wwn-pool # create block <i>first-wwn last-wwn</i> | (Optional) Creates a block (range) of WWNs, and enters organization WWN pool block mode. You must specify the first and last WWN in the block using the form <i>nn : nn : nn : nn : nn : nn : nn</i> , with the WWNs separated by a space. Note A WWN pool can contain more than one WWN block. To create multiple WWN blocks, you must enter multiple create block commands from organization WWN pool mode. |
| Step 5 | UCS-A /org/wwn-pool # create initiator <i>wwn wwn</i> | (Optional) Creates a single initiator, and enters organization WWN pool initiator mode. You must specify the initiator using the form <i>nn : nn : nn : nn : nn : nn : nn</i> . |

| | Command or Action | Purpose |
|---------------|---|--|
| | | Note A WWN pool can contain more than one initiator. To create multiple initiators, you must enter multiple create initiator commands from organization WWN pool mode. |
| Step 6 | UCS-A /org/wwn-pool/block commit-buffer | Commits the transaction to the system configuration. |

The following example creates a WWN pool named sanpool, provides a description for the pool, specifies a block of WWNs and an initiator to be used for the pool, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create wwn-pool sanpool node-wwn-assignment
UCS-A /org/wwn-pool* # set descr "This is my WWNN pool"
UCS-A /org/wwn-pool* # create block 23:00:00:05:AD:1E:00:01 23:00:00:05:AD:1E:01:00
UCS-A /org/wwn-pool/block* # exit
UCS-A /org/wwn-pool* # create initiator 23:00:00:05:AD:1E:02:00
UCS-A /org/wwn-pool/initiator* # commit-buffer
UCS-A /org/wwn-pool/initiator #
```

What to Do Next

Include the WWPN pool in a vHBA template.



CHAPTER 22

Configuring Storage-Related Policies

This chapter includes the following sections:

- [Configuring vHBA Templates, page 203](#)
- [Configuring Fibre Channel Adapter Policies, page 205](#)

Configuring vHBA Templates

vHBA Template

This template is a policy that defines how a vHBA on a server connects to the SAN. It is also referred to as a vHBA SAN connectivity template.

You need to include this policy in a service profile for it to take effect.

Configuring a vHBA Template

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create vhba-templ <i>vhba-templ-name</i> [fabric { a b }] [fc-if <i>vsan-name</i>] | Creates a vHBA template and enters organization vHBA template mode. |
| Step 3 | UCS-A /org/vhba-templ # set descr <i>description</i> | (Optional) Provides a description for the vHBA template. |
| Step 4 | UCS-A /org/vhba-templ # set fabric { a b } | (Optional) Specifies the fabric to use for the vHBA. If you did not specify the fabric when creating the vHBA template in |

| | Command or Action | Purpose |
|----------------|--|--|
| | | Step 2, then you have the option to specify it with this command. |
| Step 5 | UCS-A /org/vhba-templ # set fc-if <i>vsan-name</i> | (Optional) Specifies the Fibre Channel interface (named VSAN) to use for the vHBA template. If you did not specify the Fibre Channel interface when creating the vHBA template in Step 2, you have the option to specify it with this command. |
| Step 6 | UCS-A /org/vhba-templ # set max-field-size <i>size-num</i> | Specifies the maximum size of the Fibre Channel frame payload (in bytes) that the vHBA supports. |
| Step 7 | UCS-A /org/vhba-templ # set pin-group <i>group-name</i> | Specifies the pin group to use for the vHBA template. |
| Step 8 | UCS-A /org/vhba-templ # set qos-policy <i>mac-pool-name</i> | Specifies the QoS policy to use for the vHBA template. |
| Step 9 | UCS-A /org/vhba-templ # set stats-policy <i>policy-name</i> | Specifies the server and server component statistics threshold policy to use for the vHBA template. |
| Step 10 | UCS-A /org/vhba-templ # set type { initial-template updating-template } | Specifies the vHBA template update type. If you do not want vHBA instances created from this template to be automatically updated when the template is updated, use the initial-template keyword; otherwise, use the updating-template keyword to ensure that all vHBA instance are updated when the vHBA template is updated. |
| Step 11 | UCS-A /org/vhba-templ # set wwpn-pool <i>pool-name</i> | Specifies the WWPN pool to use for the vHBA template. |
| Step 12 | UCS-A /org/vhba-templ # commit-buffer | Commits the transaction to the system configuration. |

The following example configures a vHBA template and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create vhba template VhbaTempFoo
UCS-A /org/vhba-templ* # set descr "This is a vHBA template example."
UCS-A /org/vhba-templ* # set fabric a
UCS-A /org/vhba-templ* # set fc-if accounting
UCS-A /org/vhba-templ* # set max-field-size 2112
UCS-A /org/vhba-templ* # set pin-group FcPinGroup12
UCS-A /org/vhba-templ* # set qos-policy policy34foo
UCS-A /org/vhba-templ* # set stats-policy ServStatsPolicy
UCS-A /org/vhba-templ* # set type updating-template
UCS-A /org/vhba-templ* # set wwpn-pool SanPool7
UCS-A /org/vhba-templ* # commit-buffer
UCS-A /org/vhba-templ #
```

Deleting a vHBA Template

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete vhma-templ <i>vhba-templ-name</i> | Deletes the specified vHBA template. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the vHBA template named VhbaTempFoo and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete vhma template VhbaTempFoo
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Fibre Channel Adapter Policies

Ethernet and Fibre Channel Adapter Policies

These policies govern the host-side behavior of the adapter, including how the adapter handles traffic. For example, you can use these policies to change default settings for the following:

- Queues
- Interrupt handling
- Performance enhancement
- RSS hash
- Failover in an cluster configuration with two fabric interconnects

**Note**

For Fibre Channel adapter policies, the values displayed by Cisco UCS Manager may not match those displayed by applications such as QLogic SANsurfer. For example, the following values may result in an apparent mismatch between SANsurfer and Cisco UCS Manager:

- Max LUNs Per Target—SANsurfer has a maximum of 256 LUNs and does not display more than that number. Cisco UCS Manager supports a higher maximum number of LUNs.
- Link Down Timeout—In SANsurfer, you configure the timeout threshold for link down in seconds. In Cisco UCS Manager, you configure this value in milliseconds. Therefore, a value of 5500 ms in Cisco UCS Manager displays as 5s in SANsurfer.
- Max Data Field Size—SANsurfer has allowed values of 512, 1024, and 2048. Cisco UCS Manager allows you to set values of any size. Therefore, a value of 900 in Cisco UCS Manager displays as 512 in SANsurfer.

Operating System Specific Adapter Policies

By default, Cisco UCS provides a set of Ethernet adapter policies and Fibre Channel adapter policies. These policies include the recommended settings for each supported server operating system. Operating systems are sensitive to the settings in these policies. Storage vendors typically require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.

**Important**

We recommend that you use the values in these policies for the applicable operating system. Do not modify any of the values in the default policies unless directed to do so by Cisco Technical Support.

However, if you are creating an Ethernet adapter policy for a Windows OS (instead of using the default Windows adapter policy), you must use the following formulas to calculate values that work with Windows:

$$\text{Completion Queues} = \text{Transmit Queues} + \text{Receive Queues}$$

$$\text{Interrupt Count} = (\text{Completion Queues} + 2) \text{ rounded up to nearest power of } 2$$

For example, if Transmit Queues = 1 and Receive Queues = 8 then:

$$\text{Completion Queues} = 1 + 8 = 9$$

$$\text{Interrupt Count} = (9 + 2) \text{ rounded up to the nearest power of } 2 = 16$$
Configuring a Fibre Channel Adapter Policy**Procedure**

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |

| | Command or Action | Purpose |
|----------------|---|--|
| Step 2 | UCS-A /org # create fc-policy <i>policy-name</i> | Creates the specified Fibre Channel adapter policy and enters organization Fibre Channel policy mode. |
| Step 3 | UCS-A /org/fc-policy # set descr <i>description</i> | (Optional) Provides a description for the policy. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /org/fc-policy # set error-recovery { fc-error-recovery { disabled enabled } link-down-timeout <i>timeout-msec</i> port-down-io-retry-count <i>retry-count</i> port-down-timeout <i>timeout-msec</i> } | (Optional) Configures the Fibre Channel error recovery. |
| Step 5 | UCS-A /org/fc-policy # set interrupt mode { intx msi msi-x } | (Optional) Configures the driver interrupt mode. |
| Step 6 | UCS-A /org/fc-policy # set port { io-throttle-count <i>throttle-count</i> max-luns <i>max-num</i> } | (Optional) Configures the Fibre Channel port. |
| Step 7 | UCS-A /org/fc-policy # set port-f-logi { retries <i>retry-count</i> timeout <i>timeout-msec</i> } | (Optional) Configures the Fibre Channel port fabric login (FLOGI). |
| Step 8 | UCS-A /org/fc-policy # set port-p-logi { retries <i>retry-count</i> timeout <i>timeout-msec</i> } | (Optional) Configures the Fibre Channel port-to-port login (PLOGI). |
| Step 9 | UCS-A /org/fc-policy # set recv-queue { count <i>count</i> ring-size <i>size-num</i> } | (Optional) Configures the Fibre Channel receive queue. |
| Step 10 | UCS-A /org/fc-policy # set scsi-io { count <i>count</i> ring-size <i>size-num</i> } | (Optional) Configures the Fibre Channel SCSI I/O. |
| Step 11 | UCS-A /org/fc-policy # set trans-queue ring-size <i>size-num</i> } | (Optional) Configures the Fibre Channel transmit queue. |
| Step 12 | UCS-A /org/fc-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example configures a Fibre Channel adapter policy and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create fc-policy FcPolicy42
UCS-A /org/fc-policy* # set descr "This is a Fibre Channel adapter policy example."
UCS-A /org/fc-policy* # set error-recovery error-detect-timeout 2500
UCS-A /org/fc-policy* # set port max-luns 4
UCS-A /org/fc-policy* # set port-f-logi retries 250
```

```

UCS-A /org/fc-policy* # set port-p-logi timeout 5000
UCS-A /org/fc-policy* # set recv-queue count 1
UCS-A /org/fc-policy* # set scsi-io ring-size 256
UCS-A /org/fc-policy* # set trans-queue ring-size 256
UCS-A /org/fc-policy* # commit-buffer
UCS-A /org/fc-policy #

```

Deleting a Fibre Channel Adapter Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org org-name | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete fc-policy policy-name | Deletes the specified Fibre Channel adapter policy. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the Fibre Channel adapter policy named FcPolicy42 and commits the transaction:

```

UCS-A# scope org /
UCS-A /org # delete fc-policy FcPolicy42
UCS-A /org* # commit-buffer
UCS-A /org #

```



PART **V**

Server Configuration

- [Configuring Server-Related Pools, page 211](#)
- [Configuring Server-Related Policies, page 217](#)
- [Configuring Service Profiles, page 271](#)
- [Configuring Server Power Usage, page 293](#)



CHAPTER 23

Configuring Server-Related Pools

This chapter includes the following sections:

- [Server Pool Configuration, page 211](#)
- [UUID Suffix Pool Configuration, page 212](#)
- [Management IP Pool Configuration, page 214](#)

Server Pool Configuration

Server Pools

A server pool contains a set of servers. These servers typically share the same characteristics. Those characteristics can be their location in the chassis, or an attribute such as server type, amount of memory, local storage, type of CPU, or local drive configuration. You can manually assign a server to a server pool, or use server pool policies and server pool policy qualifications to automate the assignment.

If your system implements multi-tenancy through organizations, you can designate one or more server pools to be used by a specific organization. For example, a pool that includes all servers with two CPUs could be assigned to the Marketing organization, while all servers with 64 GB memory could be assigned to the Finance organization.

A server pool can include servers from any chassis in the system. A given server can belong to multiple server pools.

Configuring a Server Pool

Procedure

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | UCS-A# <code>scope org org-name</code> | Enters organization mode for the specified organization. To enter the root organization mode, type <code>/</code> as the <code>org-name</code> . |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 2 | UCS-A /org # create server-pool <i>server-pool-name</i> | Creates a server pool with the specified name, and enters organization server pool mode. |
| Step 3 | UCS-A /org/server-pool # create server <i>chassis-num / slot-num</i> | Creates a server for the server pool. Note A server pool can contain more than one server. To create multiple servers for the pool, you must enter multiple create server commands from organization server pool mode. |
| Step 4 | UCS-A /org/server-pool # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a server pool named ServPool2, creates two servers for the server pool, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create server-pool ServPool2
UCS-A /org/server-pool* # create server 1/1
UCS-A /org/server-pool* # create server 1/4
UCS-A /org/server-pool* # commit-buffer
UCS-A /org/server-pool #
```

Deleting a Server Pool

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete server-pool <i>server-pool-name</i> | Deletes the specified server pool. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the server pool named ServPool2 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete server-pool ServPool2
UCS-A /org* # commit-buffer
UCS-A /org #
```

UUID Suffix Pool Configuration

UUID Suffix Pools

A UUID suffix pool is a collection of SMBIOS UUIDs that are available to be assigned to servers. The first number of digits that constitute the prefix of the UUID are fixed. The remaining digits, the UUID suffix, are

variable. A UUID suffix pool ensures that these variable values are unique for each server associated with a service profile which uses that particular pool to avoid conflicts.

If you use UUID suffix pools in service profiles, you do not have to manually configure the UUID of the server associated with the service profile.

Configuring a UUID Suffix Pool

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create uuid-suffix-pool <i>pool-name</i> | Creates a UUID suffix pool with the specified pool name and enters organization UUID suffix pool mode. |
| Step 3 | UCS-A /org/uuid-suffix-pool # set descr <i>description</i> | (Optional) Provides a description for the UUID suffix pool. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /org/uuid-suffix-pool # create block <i>first-uuid last-uuid</i> | Creates a block (range) of UUID suffixes, and enters organization UUID suffix pool block mode. You must specify the first and last UUID suffixes in the block using the form <i>nnnn-nnnnnnnnnnnnn</i> , with the UUID suffixes separated by a space. Note A UUID suffix pool can contain more than one UUID suffix block. To create multiple blocks, you must enter multiple create block commands from organization UUID suffix pool mode. |
| Step 5 | UCS-A /org/uuid-suffix-pool/block # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a UUID suffix pool named pool4, provides a description for the pool, specifies a block of UUID suffixes to be used for the pool, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create uuid-suffix-pool pool4
UCS-A /org/uuid-suffix-pool* # set descr "This is UUID suffix pool 4"
UCS-A /org/uuid-suffix-pool* # create block 1000-000000000001 1000-000000000010
UCS-A /org/uuid-suffix-pool/block* # commit-buffer
UCS-A /org/uuid-suffix-pool/block #
```

What to Do Next

Include the UUID suffix pool in a service profile and/or template.

Deleting a UUID Suffix Pool

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete uuid-suffix-pool <i>pool-name</i> | Deletes the specified UUID suffix pool. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the UUID suffix pool named pool4 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete uuid-suffix-pool pool4
UCS-A /org* # commit-buffer
```

Management IP Pool Configuration

Management IP Pool

The management IP pool is a collection of external IP addresses. Cisco UCS Manager reserves each block of IP addresses in the management IP pool for external access that terminates in the Cisco Integrated Management Controller (CIMC) on a server.

Cisco UCS Manager uses the IP addresses in a management IP pool for external access to a server through the following:

- KVM console
- Serial over LAN
- IPMI

Configuring an IP Address Block for the Management IP Pool

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org / | Enters root organization mode. |
| Step 2 | UCS-A /org # scope ip-pool ext-mgmt | Enters organization IP pool mode. Note You cannot create (or delete) a management IP pool. You can only enter (scope to) the existing default pool. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 3 | UCS-A /org/ip-pool # set descr <i>description</i> | (Optional) Provides a description for the management IP pool. This description applies to all address blocks in the management IP pool. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /org/ip-pool # create block <i>first-ip-addr last-ip-addr gateway-ip-addr subnet-mask</i> | Creates a block (range) of IP addresses, and enters organization IP pool block mode. You must specify the first and last IP addresses in the address range, the gateway IP address, and subnet mask. Note A IP pool can contain more than one IP address block. To create multiple IP address blocks, you must enter multiple create block commands from organization IP pool mode. |
| Step 5 | UCS-A /org/ip-pool/block # commit-buffer | Commits the transaction to the system configuration. |

The following example configures an IP address block for the management IP pool and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope ip-pool ext-mgmt
UCS-A /org/ip-pool* # set descr "This is a management IP pool example."
UCS-A /org/ip-pool* # create block 192.168.100.1 192.168.100.200 192.168.100.10 255.255.255.0
UCS-A /org/ip-pool/block* # commit-buffer
UCS-A /org/ip-pool/block #
```

Deleting an IP Address Block from the Management IP Pool

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope ip-pool ext-mgmt | Enters the management IP pool. |
| Step 3 | UCS-A /org/ip-pool # delete block <i>first-ip-addr last-ip-addr</i> | Deletes the specified block (range) of IP addresses. |
| Step 4 | UCS-A /org/ip-pool # commit-buffer | Commits the transaction to the system configuration. |

The following example configures an IP address block for the management IP pool and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope ip-pool ext-mgmt
UCS-A /org/ip-pool # delete block 192.168.100.1 192.168.100.200
UCS-A /org/ip-pool* # commit-buffer
UCS-A /org/ip-pool #
```



CHAPTER 24

Configuring Server-Related Policies

This chapter includes the following sections:

- [Configuring BIOS Settings, page 217](#)
- [Configuring Boot Policies, page 233](#)
- [Configuring IPMI Access Profiles, page 240](#)
- [Configuring Local Disk Configuration Policies, page 243](#)
- [Configuring Scrub Policies, page 247](#)
- [Configuring Serial over LAN Policies, page 248](#)
- [Configuring Server Autoconfiguration Policies, page 251](#)
- [Configuring Server Discovery Policies, page 252](#)
- [Configuring Server Inheritance Policies, page 254](#)
- [Configuring Server Pool Policies, page 256](#)
- [Configuring Server Pool Policy Qualifications, page 257](#)
- [Configuring vNIC/vHBA Placement Profiles, page 268](#)

Configuring BIOS Settings

Server BIOS Settings

Cisco UCS provides two methods for making global modifications to the BIOS settings on servers in an instance. You can create one or more BIOS policies that include a specific grouping of BIOS settings that match the needs of a server or set of servers, or you can use the default BIOS settings for a specific server platform.

Both the BIOS policy and the default BIOS settings for a server platform enable you to fine tune the BIOS settings for options such as the following:

Main Server Settings

- Quiet boot

- Resume on AC power loss
- Front panel lockout

Processor Settings

- Intel TurboBoost Technology
- Enhanced Intel SpeedStep
- Intel Hyperthreading Technology
- Intel Virtualization Technology
- Processor C3 report
- Processor C6 report

Intel-Directed I/O

- Intel VT for directed I/O
- Interrupt remap
- Coherency support
- ATS Support
- Pass Through DMA

RAS Memory

- Memory RAS configuration
- NUMA Optimized
- Mirroring mode
- LV DDR mode

Depending upon the needs of the data center, you can combine both of these options in a Cisco UCS instance, or you can use only one of them. You can also use Cisco UCS Manager to view the actual BIOS settings on a server and determine whether they are meeting current needs.



Note

Cisco UCS Manager pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the CIMC buffer. These changes remain in the buffer until the server is rebooted.

If you change a BIOS policy, you must reboot any servers associated with service profiles that include the policy for the changes to take effect.

If you change the default BIOS settings, those changes are applied to servers upon association with service profiles that do not include a BIOS policy or when the server is rebooted. Changes to the default BIOS settings do not affect servers that are already associated with service profiles.

BIOS Policy

The BIOS policy is a policy that automates the configuration of BIOS settings for a server or group of servers. You can create global BIOS policies available to all servers in the root organization, or you can create BIOS policies in sub-organizations that are only available to that hierarchy.

To use a BIOS policy, do the following:

- Create the BIOS policy in Cisco UCS Manager
- Assign the BIOS policy to one or more service profiles
- Associate the service profile with a server

During service profile association, Cisco UCS Manager modifies the BIOS settings on the server to match the configuration in the BIOS policy. If you do not create and assign a BIOS policy to a service profile, the server uses the default BIOS settings for that server platform.

Default BIOS Settings

Default BIOS settings are applicable to all servers of a specific type that do not have a BIOS policy included in their service profiles. These settings are available only in the root organization and are global. Only one set of BIOS settings can exist for each server platform supported by Cisco UCS.

Cisco UCS Manager applies these server platform-specific BIOS settings as follows:

- The service profile associated with a server does not include a BIOS policy
- The BIOS policy is configured with the platform-default option for a specific setting

You can modify the default BIOS settings provided by Cisco UCS Manager. However, any changes to the default BIOS settings apply to all servers of that particular type or platform. If you want to modify the BIOS settings for only certain servers, we recommend that you use a BIOS policy.

Creating a BIOS Policy

If you change a BIOS policy, you must reboot any servers associated with service profiles that include the policy for the changes to take effect.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters org mode for the specified organization. To enter the default org mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org# create bios-policy <i>policy-name</i> | Creates a BIOS policy with the specified policy name, and enters org BIOS policy mode. |
| Step 3 | UCS-A /org/bios-policy# set quiet-boot-config quiet-boot { disabled enabled platform-default } | (Optional) Determines what the BIOS displays during Power On Self-Test (POST). This can be one of the following: <ul style="list-style-type: none"> • disabled—The BIOS displays the logo screen. • enabled—The BIOS does not display any messages during boot. |

| | Command or Action | Purpose |
|---------------|---|---|
| | | <ul style="list-style-type: none"> • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 4 | <pre>UCS-A /org/bios-policy # set resume-ac-on-power-loss-config resume-action {stay-off last-state reset platform-default}</pre> | <p>(Optional) Determines how the server behaves when power is restored after an unexpected power loss. This can be one of the following:</p> <ul style="list-style-type: none"> • stay-off—The server remains off until manually powered on. • last-state—The server is powered on and the system attempts to restore its last state. • reset—The server is powered on and automatically reset. • platform-default—The server uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 5 | <pre>UCS-A /org/bios-policy # set front-panel-lockout-config front-panel-lockout {disabled enabled platform-default}</pre> | <p>(Optional) Specifies whether the power and reset buttons on the front panel are ignored by the server. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The power and reset buttons on the front panel are active and can be used to affect the server. • enabled—The power and reset buttons are locked out. The server can only be reset or powered on or off from the CIMC GUI. • platform-default—The server uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 6 | <pre>UCS-A /org/bios-policy # set intel-turbo-boost-config turbo-boost {disabled enabled platform-default}</pre> | <p>(Optional) Specifies whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor never increases its frequency automatically. • enabled—The processor utilizes Turbo Boost Technology if required. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 7 | <pre>UCS-A /org/bios-policy # set enhanced-intel-speedstep-config</pre> | <p>(Optional) Specifies whether the processor uses Enhanced Intel SpeedStep Technology that allows the system to dynamically</p> |

| | Command or Action | Purpose |
|----------------|--|---|
| | <code>speed-step {disabled enabled platform-default}</code> | <p>adjust processor voltage and core frequency, which can result in decreased average power consumption and decreased average heat production. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor never dynamically adjusts its voltage or frequency. • enabled—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. Contact your operating system vendor to make sure the operating system supports this feature. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 8 | UCS-A /org/bios-policy # <code>set hyper-threading-config hyper-threading {disabled enabled platform-default}</code> | <p>(Optional) Specifies whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not permit hyperthreading. • enabled—The processor allows for the parallel execution of multiple threads. Contact your operating system vendor to make sure the operating system supports this feature. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 9 | UCS-A /org/bios-policy # <code>set intel-vt-config vt {disabled enabled platform-default}</code> | <p>(Optional) Specifies whether the processor uses Intel Virtualization Technology, which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not permit virtualization. • enabled—The processor allows multiple operating systems in independent partitions. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>Note If you change this option, you must power cycle the server before the setting takes effect.</p> |
| Step 10 | UCS-A /org/bios-policy # <code>set processor-c3-report-config processor-c3-report {acpi-c2 </code> | <p>(Optional) Determines whether the processor sends the C3 report to the operating system. This can be one of the following:</p> |

| | Command or Action | Purpose |
|----------------|--|--|
| | acpi-c2 disabled platform-default } | <ul style="list-style-type: none"> • acpi-c2—The processor sends the C3 report using the ACPI C2 format. • acpi-c3—The processor sends the C3 report using the ACPI C3 format. • disabled—The processor does not send the C3 report. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 11 | UCS-A /org/bios-policy # set processor-c6-report-config processor-report { disabled enabled platform-default } | <p>(Optional) Determines whether the processor sends the C6 report to the operating system. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not send the C6 report. • enabled—The processor sends the C6 report. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 12 | UCS-A /org/bios-policy # set intel-vt-directed-io-config vtd { disabled enabled platform-default } | <p>(Optional) Specifies whether the processor uses Intel Virtualization Technology for Directed I/O. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not use virtualization technology. • enabled—The processor uses virtualization technology. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 13 | UCS-A /org/bios-policy # set intel-vt-directed-io-config interrupt-remapping { disabled enabled platform-default } | <p>(Optional) Specifies whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not support remapping. • enabled—The processor uses VT-d Interrupt Remapping as required. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 14 | UCS-A /org/bios-policy # set intel-vt-directed-io-config coherency-support { disabled enabled platform-default } | <p>(Optional) Specifies whether the processor supports Intel VT-d Coherency. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not support coherency. • enabled—The processor uses VT-d Coherency as required. |

| | Command or Action | Purpose |
|----------------|---|--|
| | | <ul style="list-style-type: none"> • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 15 | UCS-A /org/bios-policy # set intel-vt-directed-io-config ats-support {disabled enabled platform-default} | <p>(Optional) Specifies whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not support ATS. • enabled—The processor uses VT-d ATS as required. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 16 | UCS-A /org/bios-policy # set intel-vt-directed-io-config passthrough-dma {disabled enabled platform-default} | <p>(Optional) Specifies whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not support pass-through DMA. • enabled—The processor uses VT-d Pass-through DMA as required. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 17 | UCS-A /org/bios-policy # set memory-ras-config ras-config {lockstep maximum performance mirroring platform-default} | <p>(Optional) Specifies the memory reliability, availability and serviceability (RAS) configuration. This can be one of the following:</p> <ul style="list-style-type: none"> • lockstep—If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. Lockstep is enabled by default for B400 servers. • maximum performance—System performance is optimized. • mirroring—System reliability is optimized by using half the system memory as backup. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 18 | UCS-A /org/bios-policy # set numa-config numa-optimization | <p>(Optional) Specifies whether the BIOS supports NUMA. This can be one of the following:</p> |

| | Command or Action | Purpose |
|----------------|--|--|
| | <code>{disabled enabled platform-default}</code> | <ul style="list-style-type: none"> • disabled—The BIOS does not support NUMA. • enabled—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 19 | <code>UCS-A /org/bios-policy # set memory-mirroring-mode mirroring-mode {intersocket intrasocket platform-default}</code> | <p>(Optional) Specifies memory mirroring, which enhances system reliability by keeping two identical data images in memory. This can be one of the following:</p> <ul style="list-style-type: none"> • intersocket—Memory is mirrored between two Integrated Memory Controllers (IMCs) across CPU sockets. • intrasocket—One IMC is mirrored with another IMC in the same socket. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 20 | <code>UCS-A /org/bios-policy # set lv-dimm-support-config lv-ddr-mode {performance-mode power-saving-mode platform-default}</code> | <p>(Optional) Specifies whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following:</p> <ul style="list-style-type: none"> • performance-mode—The system prioritizes high frequency operations over low voltage operations. • power-saving-mode—The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 21 | <code>UCS-A /org/bios-policy # set console-redirect-config console-redirect {disabled platform-default serial-port-a serial-port-b}</code> | <p>(Optional) Specifies whether a serial port can be used for server management tasks. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—Serial ports cannot be used for management tasks. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • serial-port-a—Serial port A is configured for management tasks. |

| | Command or Action | Purpose |
|----------------|---|---|
| | | <ul style="list-style-type: none"> • serial-port-b—Serial port B is configured for management tasks. |
| Step 22 | UCS-A /org/bios-policy # set console-redir-config baud-rate {115200 57600 38400 19200 9600} | (Optional) If a serial port can be used for management tasks, set the serial port transmission speed so that it matches the rate of the remote terminal application. This can be one of the following: <ul style="list-style-type: none"> • 115200 • 57600 • 38400 • 19200 • 9600 • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 23 | UCS-A /org/bios-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a BIOS policy under the root organization and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create bios-policy biosPolicy3
UCS-A /org/bios-policy* # set numa-config numa-optimization enabled
UCS-A /org/bios-policy* # commit-buffer
UCS-A /org/bios-policy #
```

Modifying BIOS Defaults

If you change the default BIOS settings, those changes are applied to servers upon association with service profiles that do not include a BIOS policy or when the server is rebooted. Changes to the default BIOS settings do not affect servers that are already associated with service profiles.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope server-defaults | Enters server defaults mode. |
| Step 3 | UCS-A /system/server-defaults # show platform | (Optional) Displays platform descriptions for all servers. |
| Step 4 | UCS-A /system/server-defaults # scope platform platform-description | Enters server defaults mode for the server specified. For the <i>platform-description</i> argument, enter the entire server description as displayed by the show platform command. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 5 | UCS-A /system/server-defaults/platform # scope bios-settings | Enters server defaults BIOS settings mode for the server. |
| Step 6 | UCS-A /system/server-defaults/platform/bios-settings # set quiet-boot-config quiet-boot { disabled enabled platform-default } | (Optional) Determines what the BIOS displays during Power On Self-Test (POST). This can be one of the following: <ul style="list-style-type: none"> • disabled—The BIOS displays the logo screen. • enabled—The BIOS does not display any messages during boot. • platform-default—The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 7 | UCS-A /system/server-defaults/platform/bios-settings # set resume-ac-on-power-loss-config resume-action { stay-off last-state reset platform-default } | (Optional) Determines how the server behaves when power is restored after an unexpected power loss. This can be one of the following: <ul style="list-style-type: none"> • stay-off—The server remains off until manually powered on. • last-state—The server is powered on and the system attempts to restore its last state. • reset—The server is powered on and automatically reset. • platform-default—The server uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 8 | UCS-A /system/server-defaults/platform/bios-settings # set front-panel-lockout-config front-panel-lockout { disabled enabled platform-default } | (Optional) Specifies whether the power and reset buttons on the front panel are ignored by the server. This can be one of the following: <ul style="list-style-type: none"> • disabled—The power and reset buttons on the front panel are active and can be used to affect the server. • enabled—The power and reset buttons are locked out. The server can only be reset or powered on or off from the CIMC GUI. • platform-default—The server uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 9 | UCS-A /system/server-defaults/platform/bios-settings | (Optional) Specifies whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running |

| | Command or Action | Purpose |
|----------------|--|---|
| | <code># set intel-turbo-boost-config turbo-boost {disabled enabled platform-default}</code> | <p>below power, temperature, or voltage specifications. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor never increases its frequency automatically. • enabled—The processor utilizes Turbo Boost Technology if required. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 10 | UCS-A /system/server-defaults/platform/bios-settings <code># set enhanced-intel-speedstep-config speed-step {disabled enabled platform-default}</code> | <p>(Optional) Specifies whether the processor uses Enhanced Intel SpeedStep Technology that allows the system to dynamically adjust processor voltage and core frequency, which can result in decreased average power consumption and decreased average heat production. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor never dynamically adjusts its voltage or frequency. • enabled—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. Contact your operating system vendor to make sure the operating system supports this feature. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 11 | UCS-A /system/server-defaults/platform/bios-settings <code># set hyper-threading-config hyper-threading {disabled enabled platform-default}</code> | <p>(Optional) Specifies whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not permit hyperthreading. • enabled—The processor allows for the parallel execution of multiple threads. Contact your operating system vendor to make sure the operating system supports this feature. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |

| | Command or Action | Purpose |
|----------------|--|---|
| Step 12 | UCS-A /system/server-defaults/platform/bios-settings # set intel-vt-config vt { disabled enabled platform-default } | <p>(Optional) Specifies whether the processor uses Intel Virtualization Technology, which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not permit virtualization. • enabled—The processor allows multiple operating systems in independent partitions. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. <p>Note If you change this option, you must power cycle the server before the setting takes effect.</p> |
| Step 13 | UCS-A /system/server-defaults/platform/bios-settings # set processor-c3-report-config processor-c3-report { acpi-c2 acpi-c2 disabled platform-default } | <p>(Optional) Determines whether the processor sends the C3 report to the operating system. This can be one of the following:</p> <ul style="list-style-type: none"> • acpi-c2—The processor sends the C3 report using the ACPI C2 format. • acpi-c3—The processor sends the C3 report using the ACPI C3 format. • disabled—The processor does not send the C3 report. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 14 | UCS-A /system/server-defaults/platform/bios-settings # set processor-c6-report-config processor-report { disabled enabled platform-default } | <p>(Optional) Determines whether the processor sends the C6 report to the operating system. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—The processor does not send the C6 report. • enabled—The processor sends the C6 report. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 15 | UCS-A /system/server-defaults/platform/bios-settings # set intel-vt-directed-io-config vtd { disabled enabled platform-default } | <p>(Optional) Specifies whether the processor uses Intel Virtualization Technology for Directed I/O. This can be one of the following:</p> |

| | Command or Action | Purpose |
|----------------|---|--|
| | | <ul style="list-style-type: none"> • disabled—The processor does not use virtualization technology. • enabled—The processor uses virtualization technology. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 16 | UCS-A /system/server-defaults/platform/bios-settings # set intel-vt-directed-io-config interrupt-remapping {disabled enabled platform-default} | (Optional) Specifies whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following: <ul style="list-style-type: none"> • disabled—The processor does not support remapping. • enabled—The processor uses VT-d Interrupt Remapping as required. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 17 | UCS-A /system/server-defaults/platform/bios-settings # set intel-vt-directed-io-config coherency-support {disabled enabled platform-default} | (Optional) Specifies whether the processor supports Intel VT-d Coherency. This can be one of the following: <ul style="list-style-type: none"> • disabled—The processor does not support coherency. • enabled—The processor uses VT-d Coherency as required. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 18 | UCS-A /system/server-defaults/platform/bios-settings # set intel-vt-directed-io-config ats-support {disabled enabled platform-default} | (Optional) Specifies whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: <ul style="list-style-type: none"> • disabled—The processor does not support ATS. • enabled—The processor uses VT-d ATS as required. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |

| | Command or Action | Purpose |
|----------------|---|---|
| Step 19 | UCS-A /system/server-defaults/platform/bios-settings # set intel-vt-directed-io-config passthrough-dma {disabled enabled platform-default } | (Optional) Specifies whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following: <ul style="list-style-type: none"> • disabled—The processor does not support pass-through DMA. • enabled—The processor uses VT-d Pass-through DMA as required. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 20 | UCS-A /system/server-defaults/platform/bios-settings # set memory-ras-config ras-config {lockstep maximum performance mirroring platform-default } | (Optional) Specifies the memory reliability, availability and serviceability (RAS) configuration. This can be one of the following: <ul style="list-style-type: none"> • lockstep—If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. Lockstep is enabled by default for B400 servers. • maximum performance—System performance is optimized. • mirroring—System reliability is optimized by using half the system memory as backup. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 21 | UCS-A /system/server-defaults/platform/bios-settings # set numa-config numa-optimization {disabled enabled platform-default } | (Optional) Specifies whether the BIOS supports NUMA. This can be one of the following: <ul style="list-style-type: none"> • disabled—The BIOS does not support NUMA. • enabled—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 22 | UCS-A /system/server-defaults/platform/bios-settings | (Optional) Specifies memory mirroring, which enhances system reliability by keeping two identical |

| | Command or Action | Purpose |
|----------------|--|--|
| | <pre># set memory-mirroring-mode mirroring-mode {intersocket intrasocket platform-default}</pre> | <p>data images in memory. This can be one of the following:</p> <ul style="list-style-type: none"> • intersocket—Memory is mirrored between two Integrated Memory Controllers (IMCs) across CPU sockets. • intrasocket—One IMC is mirrored with another IMC in the same socket. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 23 | <pre>UCS-A /system/server-defaults/platform/bios-settings # set lv-dimm-support-config lv-ddr-mode {performance-mode power-saving-mode platform-default}</pre> | <p>(Optional) Specifies whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following:</p> <ul style="list-style-type: none"> • performance-mode—The system prioritizes high frequency operations over low voltage operations. • power-saving-mode—The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 24 | <pre>UCS-A /system/server-defaults/platform/bios-settings # set console-redirect-config console-redirect {disabled platform-default serial-port-a serial-port-b}</pre> | <p>(Optional) Specifies whether a serial port can be used for server management tasks. This can be one of the following:</p> <ul style="list-style-type: none"> • disabled—Serial ports cannot be used for management tasks. • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • serial-port-a—Serial port A is configured for management tasks. • serial-port-b—Serial port B is configured for management tasks. |
| Step 25 | <pre>UCS-A /system/server-defaults/platform/bios-settings</pre> | <p>(Optional) If a serial port can be used for management tasks, set the serial port transmission speed so that it</p> |

| | Command or Action | Purpose |
|----------------|---|--|
| | <code># set console-redir-config baud-rate {115200 57600 38400 19200 9600}</code> | <p>matches the rate of the remote terminal application. This can be one of the following:</p> <ul style="list-style-type: none"> • 115200 • 57600 • 38400 • 19200 • 9600 • platform-default—The processor uses the value for this attribute contained in the BIOS defaults for the server type and vendor. |
| Step 26 | <pre>UCS-A /system/server-defaults/platform/bios-settings # commit-buffer</pre> | Commits the transaction to the system configuration. |

The following example shows how to change the NUMA default BIOS setting for a platform and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope server-defaults
UCS-A /system/server-defaults # show platform

Platform:
  Product Name Vendor      Model      Revision
  -----
Cisco B200-M1
                Cisco Systems, Inc.
                N20-B6620-1
                0

UCS-A /system/server-defaults # scope platform 'Cisco Systems Inc' N20-B6620-1 0
UCS-A /system/server-defaults/platform # scope bios-settings
UCS-A /system/server-defaults/platform/bios-settings # set numa-config numa-optimization
disabled
UCS-A /system/server-defaults/platform/bios-settings* # commit-buffer
UCS-A /system/server-defaults/platform/bios-settings #
```

Viewing the Actual BIOS Settings for a Server

Follow this procedure to see the actual BIOS settings on a server.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | <code>UCS-A# scope server chassis-id / server-id</code> | Enters chassis server mode for the specified server. |
| Step 2 | <code>UCS-A /chassis/server # scope bios</code> | Enters BIOS mode for the specified server. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 3 | UCS-A /chassis/server/bios # scope bios-settings | Enters BIOS settings mode for the specified server. |
| Step 4 | UCS-A /chassis/server/bios/bios-settings # show setting | Displays the BIOS setting. Enter show ? to display a list of allowed values for <i>setting</i> . |

The following example displays a BIOS setting for blade 3 in chassis 1:

```
UCS-A# scope server 1/3
UCS-A /chassis/server # scope bios
UCS-A /chassis/server/bios # scope bios-settings
UCS-A /chassis/server/bios/bios-settings # show intel-vt-config

Intel Vt Config:
  Vt
  --
  Enabled

UCS-A /chassis/server/bios/bios-settings #
```

Configuring Boot Policies

Boot Policy

The boot policy determines the following:

- Configuration of the boot device
- Location from which the server boots
- Order in which boot devices are invoked

For example, you can choose to have associated servers boot from a local device, such as a local disk or CD-ROM (VMedia), or you can select a SAN boot or a LAN (PXE) boot.

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect. If you do not include a boot policy in a service profile, the server uses the default settings in the BIOS to determine the boot order.



Important

Changes to a boot policy may be propagated to all servers created with an updating service profile template that includes that boot policy. Reassociation of the service profile with the server to rewrite the boot order information in the BIOS is auto-triggered.

Guidelines

When you create a boot policy, you can add one or more of the following to the boot policy and specify their boot order:

| Boot type | Description |
|--------------------|---|
| SAN boot | Boots from an operating system image on the SAN. You can specify a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary. We recommend that you use a SAN boot, because it offers the most service profile mobility within the system. If you boot from the SAN when you move a service profile from one server to another, the new server boots from the exact same operating system image. Therefore, the new server appears to be the exact same server to the network. |
| LAN boot | Boots from a centralized provisioning server. It is frequently used to install operating systems on a server from that server. |
| Local disk boot | If the server has a local drive, boots from that drive. Note Cisco UCS Manager does not differentiate between the types of local drives. If an operating system has been installed on more than one local drive or on an internal USB drive (eUSB), you cannot specify which of these local drives the server should use as the boot drive. |
| Virtual media boot | Mimics the insertion of a physical CD-ROM disk (read-only) or floppy disk (read-write) into a server. It is typically used to manually install operating systems on a server. |

**Note**

The default boot order is as follows:

- 1 Local disk boot
 - 2 LAN boot
 - 3 Virtual media read-only boot
 - 4 Virtual media read-write boot
-

Configuring a Boot Policy

You can also create a local boot policy that is restricted to a service profile or service profile template. However, we recommend that you create a global boot policy that can be included in multiple service profiles or service profile templates.

Before You Begin

If you are creating a boot policy that boots the server from a SAN LUN and you require reliable SAN boot operations, you must first remove all local disks from servers associated with a service profile that includes the boot policy.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org# create boot-policy <i>policy-name</i> [purpose { operational utility }] | Creates a boot policy with the specified policy name, and enters organization boot policy mode. When you create the boot policy, specify the operational option. This ensures that the server boots from the operating system installed on the server. The utility options is reserved and should only be used if instructed to do so by a Cisco representative. |
| Step 3 | UCS-A /org/boot-policy # set descr <i>description</i> | (Optional) Provides a description for the boot policy. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks do not appear in the description field of any show command output. |
| Step 4 | UCS-A /org/boot-policy # set reboot-on-update { no yes } | Specifies whether the servers using this boot policy are automatically rebooted after you make changes to the boot order. |
| Step 5 | UCS-A /org/boot-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a boot policy named boot-policy-LAN, provides a description for the boot policy, specifies that servers using this policy will not be automatically rebooted when the boot order is changed, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create boot-policy boot-policy-LAN purpose operational
UCS-A /org/boot-policy* # set descr "Boot policy that boots from the LAN."
UCS-A /org/boot-policy* # set reboot-on-update no
UCS-A /org/boot-policy* # commit-buffer
UCS-A /org/boot-policy #
```

What to Do Next

Configure one or more of the following boot options for the boot policy and set their boot order:

- **LAN Boot**—Boots from a centralized provisioning server. It is frequently used to install operating systems on a server from that server.

If you choose the LAN Boot option, continue to [Configuring a LAN Boot for a Boot Policy](#), page 236.

- **Storage Boot**— Boots from an operating system image on the SAN. You can specify a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary.

We recommend that you use a SAN boot, because it offers the most service profile mobility within the system. If you boot from the SAN, when you move a service profile from one server to another, the new

server boots from exactly the same operating system image. Therefore, the new server appears to be exactly the same server to the network.

If you choose the Storage Boot option, continue to [Configuring a Storage Boot for a Boot Policy](#), page 237.

- **Virtual Media Boot**—Mimics the insertion of a physical CD into a server. It is typically used to manually install operating systems on a server.

If you choose the Virtual Media boot option, continue to [Configuring a Virtual Media Boot for a Boot Policy](#), page 238.



Tip

We recommend that the boot order in a boot policy include either a local disk or a SAN LUN, but not both, to avoid the possibility of the server booting from the wrong storage type. If you configure a local disk and a SAN LUN for the boot order storage type and the operating system or logical volume manager (LVM) is configured incorrectly, the server may boot from the local disk rather than the SAN LUN.

For example, on a server with Red Hat Linux installed, where the LVM is configured with default LV names and the boot order is configured with a SAN LUN and a local disk, Linux reports that there are two LVs with the same name and boots from the LV with the lowest SCSI ID, which could be the local disk.

Include the boot policy in a service profile and/or template.

Configuring a LAN Boot for a Boot Policy

Before You Begin

Create a boot policy to contain the LAN boot configuration.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope boot-policy <i>policy-name</i> | Enters organization boot policy mode for the specified boot policy. |
| Step 3 | UCS-A /org/boot-policy # create lan | Creates a LAN boot for the boot policy and enters organization boot policy LAN mode. |
| Step 4 | UCS-A /org/boot-policy/lan # set order {1 2 3 4} | Specifies the boot order for the LAN boot. |
| Step 5 | UCS-A /org/boot-policy/lan # create path {primary secondary} | Creates a primary or secondary LAN boot path and enters organization boot policy LAN path mode. |
| Step 6 | UCS-A /org/boot-policy/lan/path # set vnic <i>vnic-name</i> | Specifies the vNIC to use for the LAN path to the boot image. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 7 | UCS-A /org/boot-policy/lan/path # commit-buffer | Commits the transaction to the system configuration. |

The following example enters the boot policy named lab2-boot-policy, creates a LAN boot for the policy, sets the boot order to 2, creates primary and secondary paths using the vNICs named vNIC1 and vNIC2, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope boot-policy lab2-boot-policy
UCS-A /org/boot-policy* # create lan
UCS-A /org/boot-policy/lan* # set order 2
UCS-A /org/boot-policy/lan* # create path primary
UCS-A /org/boot-policy/lan/path* # set vnic vNIC1
UCS-A /org/boot-policy/lan/path* # exit
UCS-A /org/boot-policy/lan* # create path secondary
UCS-A /org/boot-policy/lan/path* # set vnic vNIC2
UCS-A /org/boot-policy/lan/path* # commit-buffer
UCS-A /org/boot-policy/lan/path #
```

What to Do Next

Include the boot policy in a service profile and/or template.

Configuring a Storage Boot for a Boot Policy

Before You Begin

Create a boot policy to contain the storage boot configuration.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope boot-policy <i>policy-name</i> | Enters organization boot policy mode for the specified boot policy. |
| Step 3 | UCS-A /org/boot-policy # create storage | Creates a storage boot for the boot policy and enters organization boot policy storage mode. |
| Step 4 | UCS-A /org/boot-policy/storage # set order {1 2 3 4} | Sets the boot order for the storage boot. |
| Step 5 | UCS-A /org/boot-policy/storage # create {local san-image {primary secondary}} | Creates a local or SAN image storage location, and if the san-image option is specified, enters organization boot policy storage SAN image mode. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 6 | UCS-A /org/boot-policy/storage/san-image # set vhma vhma-name | Specifies the vHBA to be used for the storage boot. |
| Step 7 | UCS-A /org/boot-policy/storage/san-image # create path {primary secondary} | Creates a primary or secondary storage boot path and enters organization boot policy SAN path mode. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order. |
| Step 8 | UCS-A /org/boot-policy/storage/san-image/path # set {lun lun-id wwn wwn-num} | Specifies the LUN or WWN to be used for the storage path to the boot image. |
| Step 9 | UCS-A /org/boot-policy/storage/san-image/path # commit-buffer | Commits the transaction to the system configuration. |

The following example enters the boot policy named lab1-boot-policy, creates a storage boot for the policy, sets the boot order to 1, creates a primary SAN image, uses a vHBA named vHBA2, creates primary path using LUN 967295200, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope boot-policy lab1-boot-policy
UCS-A /org/boot-policy* # create storage
UCS-A /org/boot-policy/storage* # set order 1
UCS-A /org/boot-policy/storage* # create san-image primary
UCS-A /org/boot-policy/storage* # set vhma vHBA2
UCS-A /org/boot-policy/storage/san-image* # create path primary
UCS-A /org/boot-policy/storage/san-image/path* # set lun 967295200
UCS-A /org/boot-policy/storage/san-image/path* # commit-buffer
UCS-A /org/boot-policy/storage/san-image/path #
```

What to Do Next

Include the boot policy in a service profile and/or template.

Configuring a Virtual Media Boot for a Boot Policy

Before You Begin

Create a boot policy to contain the virtual media boot configuration.

Procedure

| | Command or Action | Purpose |
|---------------|----------------------------------|---|
| Step 1 | UCS-A# scope org org-name | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 2 | UCS-A /org # scope boot-policy <i>policy-name</i> | Enters organization boot policy mode for the specified boot policy. |
| Step 3 | UCS-A /org/boot-policy # create virtual-media { read-only read-write } | Creates a virtual media boot for the boot policy, specifies whether the virtual media is has read-only or read-write privileges, and enters organization boot policy virtual media mode. |
| Step 4 | UCS-A /org/boot-policy/virtual-media # set order { 1 2 3 4 } | Sets the boot order for the virtual-media boot. |
| Step 5 | UCS-A /org/boot-policy/virtual-media # commit-buffer | Commits the transaction to the system configuration. |

The following example enters the boot policy named lab3-boot-policy, creates a virtual media boot with read-only privileges for the policy, sets the boot order to 3, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope boot-policy lab3-boot-policy
UCS-A /org/boot-policy* # create virtual-media read-only
UCS-A /org/boot-policy/virtual-media* # set order 3
UCS-A /org/boot-policy/virtual-media* # commit-buffer
```

What to Do Next

Include the boot policy in a service profile and/or template.

Viewing a Boot Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # show boot-policy <i>policy-name</i> | Displays the boot definition (set by the create boot-definition command). If the boot-definition is not set, and if a policy is set (using the set boot-policy command), then the policy will be displayed. |

The following example shows how to display boot policy information for a boot policy called boot-policy-LAN:

```
UCS-A# scope org /
UCS-A /org # show boot-policy boot-policy-LAN
```

```
Boot Policy:
Full Name: org-root/boot-policy-LAN
Name: boot-policy-LAN
Purpose: Operational
Reboot on Update: Yes
Description:
Enforce vNIC Name: No
```

Deleting a Boot Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete boot-policy <i>policy-name</i> | Deletes the specified boot policy. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the boot policy named boot-policy-LAN and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete boot-policy boot-policy-LAN
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring IPMI Access Profiles

IPMI Access Profile

This policy allows you to determine whether IPMI commands can be sent directly to the server, using the IP address. For example, you can send commands to retrieve sensor data from the CIMC. This policy defines the IPMI access, including a username and password that can be authenticated locally on the server, and whether the access is read-only or read-write.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Configuring an IPMI Access Profile

Before You Begin

Obtain the following:

- Username with appropriate permissions that can be authenticated by the operating system of the server
- Password for the username
- Permissions associated with the username

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create ipmi-access-profile <i>profile-name</i> | Creates the specified IPMI access profile and enters organization IPMI access profile mode. |
| Step 3 | UCS-A /org/ipmi-access-profile # create epuser <i>epuser-name</i> | Creates the specified endpoint user and enters organization IPMI access profile endpoint user mode. Note More than one endpoint user can be created within an IPMI access profile, with each endpoint user having its own password and privileges. |
| Step 4 | UCS-A /org/ipmi-access-profile/epuser # set password | Sets the password for the endpoint user. After entering the set password command, you are prompted to enter and confirm the password. For security purposes, the password that you type does not appear in the CLI. |
| Step 5 | UCS-A /org/ipmi-access-profile/epuser # set privilege {admin readonly} | Specifies whether the endpoint user has administrative or read-only privileges. |
| Step 6 | UCS-A /org/ipmi-access-profile/epuser # commit-buffer | Commits the transaction to the system configuration. |

The following example creates an IPMI access profile named ReadOnly, creates an endpoint user named bob, sets the password and the privileges for bob, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create ipmi-access-profile ReadOnly
UCS-A /org/ipmi-access-profile* # create epuser bob
UCS-A /org/ipmi-access-profile/epuser* # set password
Enter a password:
Confirm the password:
UCS-A /org/ipmi-access-profile/epuser* # set privilege readonly
UCS-A /org/ipmi-access-profile/epuser* # commit-buffer
UCS-A /org/ipmi-access-profile/epuser #
```

What to Do Next

Include the IPMI profile in a service profile and/or template.

Deleting an IPMI Access Profile

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete ipmi-access-profile <i>profile-name</i> | Deletes the specified IPMI access profile. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the IPMI access profile named ReadOnly and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete ipmi-access-profile ReadOnly
UCS-A /org* # commit-buffer
UCS-A /org #
```

Adding an Endpoint User to an IPMI Access Profile

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope ipmi-access-profile <i>profile-name</i> | Enters organization IPMI access profile mode for the specified IPMI access profile. |
| Step 3 | UCS-A /org/ipmi-access-profile # create epuser <i>epuser-name</i> | Creates the specified endpoint user and enters organization IPMI access profile endpoint user mode. Note More than one endpoint user can be created within an IPMI access profile, with each endpoint user having its own password and privileges. |
| Step 4 | UCS-A /org/ipmi-access-profile/epuser # set password | Sets the password for the endpoint user. After entering the set password command, you are prompted to enter and confirm the password. For security purposes, the password that you type does not appear in the CLI. |
| Step 5 | UCS-A /org/ipmi-access-profile/epuser # set privilege { admin readonly } | Specifies whether the endpoint user has administrative or read-only privileges. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 6 | UCS-A /org/ipmi-access-profile/epuser # commit-buffer | Commits the transaction to the system configuration. |

The following example adds an endpoint user named alice to the IPMI access profile named ReadOnly and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope ipmi-access-profile ReadOnly
UCS-A /org/ipmi-access-profile* # create epuser alice
UCS-A /org/ipmi-access-profile/epuser* # set password
Enter a password:
Confirm the password:
UCS-A /org/ipmi-access-profile/epuser* # set privilege readonly
UCS-A /org/ipmi-access-profile/epuser* # commit-buffer
UCS-A /org/ipmi-access-profile/epuser #
```

Deleting an Endpoint User from an IPMI Access Profile

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org org-name | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope ipmi-access-profile profile-name | Enters organization IPMI access profile mode for the specified IPMI access profile. |
| Step 3 | UCS-A /org/ipmi-access-profile # delete epuser epuser-name | Deletes the specified endpoint user from the IPMI access profile. |
| Step 4 | UCS-A /org/ipmi-access-profile # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the endpoint user named alice from the IPMI access profile named ReadOnly and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope ipmi-access-profile ReadOnly
UCS-A /org/ipmi-access-profile # delete epuser alice
UCS-A /org/ipmi-access-profile* # commit-buffer
UCS-A /org/ipmi-access-profile #
```

Configuring Local Disk Configuration Policies

Local Disk Configuration Policy

This policy configures any optional SAS local drives that have been installed on a server through the onboard RAID controller of the local drive. This policy enables you to set a local disk mode for all servers that are associated with a service profile that includes the local disk configuration policy.

The local disk modes include the following:

- **Any Configuration**—For a server configuration that carries forward the local disk configuration without any changes.
- **No Local Storage**—For a diskless server or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk.
- **No RAID**—For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.
- **RAID 1 Mirrored**—Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives.
- **RAID10 Mirrored and Striped**— RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.
- **RAID 0 Stripes**—Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails.
- **RAID 6 Stripes Dual Parity**—Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.
- **RAID 5 Striped Parity**—Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.

You must include this policy in a service profile, and that service profile must be associated with a server for the policy to take effect.

Guidelines and Considerations for a Local Disk Configuration Policy

Before you create a local disk configuration policy, consider the following guidelines:

No Mixed HDDs and SSDs

Do not include HDDs and SSDs in a single RAID configuration or in a single blade server.

Impact of Upgrade to Release 1.3(1i) or Higher

An upgrade from an earlier Cisco UCS firmware release to release 1.3(1i) or higher has the following impact on the Protect Configuration property of the local disk configuration policy the first time servers are associated with service profiles after the upgrade:

- Unassociated Servers** After you upgrade the Cisco UCS instance, the initial server association proceeds without configuration errors whether or not the local disk configuration policy matches the server hardware. Even if you enable the Protect Configuration property, Cisco UCS does not protect the user data on the server if there are configuration mismatches between the local disk configuration policy on the previous service profile and the policy in the new service profile.



Note If you enable the Protect Configuration property and the local disk configuration policy encounters mismatches between the previous service profile and the new service profile, all subsequent service profile associations with the server are blocked.

Associated Servers Any servers that are already associated with service profiles do not reboot after the upgrade. Cisco UCS Manager does not report any configuration errors if there is a mismatch between the local disk configuration policy and the server hardware.

When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile.

Creating a Local Disk Configuration Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create local-disk-config-policy <i>policy-name</i> | Creates a local disk configuration policy and enters local disk configuration policy mode. |
| Step 3 | UCS-A /org/local-disk-config-policy # set descr <i>description</i> | (Optional) Provides a description for the local disk configuration policy. |
| Step 4 | UCS-A /org/local-disk-config-policy # set mode { any-configuration no-local-storage no-raid raid-0-striped raid-1-mirrored raid-5-striped-parity raid-6-striped-dual-parity raid-10-mirrored-and-striped } | Specifies the mode for the local disk configuration policy. |
| Step 5 | UCS-A /org/local-disk-config-policy # set protect { yes no } | Specifies whether the local disk will be protected or not. |
| Step 6 | UCS-A /org/local-disk-config-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example configures a local disk configuration policy and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create local-disk-config-policy DiskPolicy7
UCS-A /org/local-disk-config-policy* # set mode raid-1-mirrored
UCS-A /org/local-disk-config-policy* # set protect yes
UCS-A /org/local-disk-config-policy* # commit-buffer
UCS-A /org/local-disk-config-policy #
```

Viewing a Local Disk Configuration Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # show local-disk-config-policy <i>policy-name</i> | Displays the local disk policy. If you have not configured a local disk policy, the local disk configuration (created by the create local-disk-config command) displays. Displays the local disk definition (set by the create local-disk-config command). If the serial over LAN definition is not set, and if a policy is set (using the set local-disk-config-policy command), then the policy will be displayed. |

The following example shows how to display local disk policy information for a local disk configuration policy called DiskPolicy7:

```
UCS-A# scope org /
UCS-A /org # show local-disk-config-policy DiskPolicy7

Local Disk Config Policy:
Name: DiskPolicy7
Mode: Raid 1 Mirrored
Description:
Protect Configuration: Yes
```

Deleting a Local Disk Configuration Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete local-disk-config-policy <i>policy-name</i> | Deletes the specified local disk configuration policy. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the local disk configuration policy named DiskPolicy7 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete local-disk-config-policy DiskPolicy7
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Scrub Policies

Scrub Policy

This policy determines what happens to local data and to the BIOS settings on a server during the discovery process and when the server is disassociated from a service profile. Depending upon how you configure a scrub policy, the following can occur at those times:

- Disk Scrub** One of the following occurs to the data on any local drives on disassociation:
- If enabled, destroys all data on any local drives
 - If disabled, preserves all data on any local drives, including local storage configuration
- BIOS Settings Scrub** One of the following occurs to the BIOS settings when a service profile containing the scrub policy is disassociated from a server:
- If enabled, erases all BIOS settings for the server and resets them to the BIOS defaults for that server type and vendor
 - If disabled, preserves the existing BIOS settings on the server

Creating a Scrub Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create scrub-policy <i>policy-name</i> | Creates a scrub policy with the specified policy name, and enters organization scrub policy mode. |
| Step 3 | UCS-A /org/scrub-policy # set descr <i>description</i> | (Optional) Provides a description for the scrub policy. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /org/scrub-policy # set disk-scrub {no yes} | Disables or enables disk scrubbing on servers using this scrub policy as follows: <ul style="list-style-type: none"> • If enabled, destroys all data on any local drives • If disabled, preserves all data on any local drives, including local storage configuration |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 5 | UCS-A /org/scrub-policy # set bios-settings-scrub {no yes} | Disables or enables BIOS settings scrubbing on servers using this scrub policy as follows: <ul style="list-style-type: none"> • If enabled, erases all BIOS settings for the server and resets them to the BIOS defaults for that server type and vendor • If disabled, preserves the existing BIOS settings on the server |
| Step 6 | UCS-A /org/scrub-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a scrub policy named ScrubPolicy2, enables disk scrubbing on servers using the scrub policy, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create scrub-policy ScrubPolicy2
UCS-A /org/scrub-policy* # set descr "Scrub disk but not BIOS."
UCS-A /org/scrub-policy* # set disk-scrub yes
UCS-A /org/scrub-policy* # set bios-settings-scrub no
UCS-A /org/scrub-policy* # commit-buffer
UCS-A /org/scrub-policy #
```

Deleting a Scrub Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete scrub-policy <i>policy-name</i> | Deletes the specified scrub policy. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the scrub policy named ScrubPolicy2 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete scrub-policy ScrubPolicy2
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Serial over LAN Policies

Serial over LAN Policy

This policy sets the configuration for the serial over LAN connection for all servers associated with service profiles that use the policy. By default, the serial over LAN connection is disabled.

If you implement a serial over LAN policy, we recommend that you also create an IPMI profile.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Configuring a Serial over LAN Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create sol-policy <i>policy-name</i> | Creates a serial over LAN policy and enters organization serial over LAN policy mode. |
| Step 3 | UCS-A /org/sol-policy # set descr <i>description</i> | (Optional) Provides a description for the policy. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /org/sol-policy # set speed {115200 19200 38400 57600 9600} | Specifies the serial baud rate. |
| Step 5 | UCS-A /org/sol-policy # { disable enable } | Disables or enables the serial over LAN policy. By default, the serial over LAN policy is disabled; you must enable it before it can be applied. |
| Step 6 | UCS-A /org/sol-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a serial over LAN policy named Sol9600, provides a description for the policy, sets the speed to 9,600 baud, enables the policy, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create sol-policy Sol9600
UCS-A /org/sol-policy* # set descr "Sets serial over LAN policy to 9600 baud."
UCS-A /org/sol-policy* # set speed 9600
UCS-A /org/sol-policy* # enable
UCS-A /org/sol-policy* # commit-buffer
UCS-A /org/sol-policy #
```

Viewing a Serial over LAN Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # show sol-policy <i>policy-name</i> | Displays the serial over LAN definition (set by the create sol-config command). If the serial over LAN definition is not set, and if a policy is set (using the set sol-policy command), then the policy will be displayed. |

The following example shows how to display serial over LAN information for a serial over LAN policy called Sol9600:

```
UCS-A# scope org /
UCS-A /org # show sol-policy Sol9600

SOL Policy:
Full Name: Sol9600
SOL State: Enable
Speed: 9600
Description:
```

Deleting a Serial over LAN Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete sol-policy <i>policy-name</i> | Deletes the specified serial over LAN policy. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the serial over LAN policy named Sol9600 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # delete sol-policy Sol9600
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Server Autoconfiguration Policies

Server Autoconfiguration Policy

Cisco UCS Manager uses this policy to determine how to configure a new server. If you create a server autoconfiguration policy, the following occurs when a new server starts:

- 1 The qualification in the server autoconfiguration policy is executed against the server.
- 2 If the server meets the required qualifications, the server is associated with a service profile created from the service profile template configured in the server autoconfiguration policy. The name of that service profile is based on the name given to the server by Cisco UCS Manager.
- 3 The service profile is assigned to the organization configured in the server autoconfiguration policy.

Configuring a Server Autoconfiguration Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create server-autoconfig-policy <i>policy-name</i> | Creates a server autoconfiguration policy with the specified policy name, and enters organization server autoconfiguration policy mode. |
| Step 3 | UCS-A /org/server-autoconfig-policy # set descr <i>description</i> | (Optional) Provides a description for the policy. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /org/server-autoconfig-policy # set destination org <i>org-name</i> | (Optional) Specifies the organization for which the server is to be used. |
| Step 5 | UCS-A /org/server-autoconfig-policy # set qualifier <i>server-qual-name</i> | (Optional) Specifies server pool policy qualification to use for qualifying the server. |
| Step 6 | UCS-A /org/server-autoconfig-policy # set template <i>profile-name</i> | (Optional) Specifies a service profile template to use for creating a service profile instance for the server. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 7 | UCS-A /org/server-autoconfig-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a server autoconfiguration policy named AutoConfigFinance, provides a description for the policy, specifies finance as the destination organization, ServPoolQual22 as the server pool policy qualification, and ServTemp2 as the service profile template, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create server-autoconfig-policy AutoConfigFinance
UCS-A /org/server-autoconfig-policy* # set descr "Server Autoconfiguration Policy for Finance"
UCS-A /org/server-autoconfig-policy* # set destination org finance
UCS-A /org/server-autoconfig-policy* # set qualifier ServPoolQual22
UCS-A /org/server-autoconfig-policy* # set template ServTemp2
UCS-A /org/server-autoconfig-policy* # commit-buffer
UCS-A /org/server-autoconfig-policy #
```

Deleting a Server Autoconfiguration Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org org-name | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete server-autoconfig-policy policy-name | Deletes the specified server autoconfiguration policy. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the server autoconfiguration policy named AutoConfigFinance and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # delete server-autoconfig-policy AutoConfigFinance
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Server Discovery Policies

Server Discovery Policy

This discovery policy determines how the system reacts when you add a new server. If you create a server discovery policy, you can control whether the system conducts a deep discovery when a server is added to a chassis, or whether a user must first acknowledge the new server. By default, the system conducts a full discovery.

If you create a server discovery policy, the following occurs when a new server starts:

- 1 The qualification in the server discovery policy is executed against the server.

- 2 If the server meets the required qualifications, Cisco UCS Manager applies the following to the server:
 - Depending upon the option selected for the action, either discovers the new server immediately or waits for a user to acknowledge the new server
 - Applies the scrub policy to the server

Configuring a Server Discovery Policy

Before You Begin

If you plan to associate this policy with a server pool, create server pool policy qualifications.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org / | Enters the root organization mode. Note Chassis discovery policies can only be accessed from the root organization. |
| Step 2 | UCS-A /org # create server-disc-policy policy-name | Creates a server discovery policy with the specified policy name, and enters org server discovery policy mode. |
| Step 3 | UCS-A /org/server-disc-policy # set action {diag immediate user-acknowledged} | Specifies when the system will attempt to discover new servers. |
| Step 4 | UCS-A /org/chassis-disc-policy # set descr description | (Optional) Provides a description for the server discovery policy. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 5 | UCS-A /org/server-disc-policy # set qualifier qualifier | (Optional) Uses the specified server pool policy qualifications to associates this policy with a server pool. |
| Step 6 | UCS-A /org/server-disc-policy # set scrub-policy | Specifies the scrub policy to be used by this policy. The scrub policy defines whether the disk drive on a server should be scrubbed clean upon discovery. |
| Step 7 | UCS-A /org/server-disc-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a server discovery policy named ServDiscPolExample, sets it to immediately discover new servers, provides a description for the policy, specifies the server pool policy qualifications and scrub policy, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create server-disc-policy ServDiscPolExample
UCS-A /org/server-disc-policy* # set action immediate
```

```
UCS-A /org/server-disc-policy* # set descr "This is an example server discovery policy."
UCS-A /org/server-disc-policy* # set qualifier ExampleQual
UCS-A /org/server-disc-policy* # set scrub-policy NoScrub
UCS-A /org/server-disc-policy # commit-buffer
```

What to Do Next

Include the server discovery policy in a service profile and/or template.

Deleting a Server Discovery Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org# Delete server-disc-policy <i>policy-name</i> | Deletes the specified server discovery policy. |
| Step 3 | UCS-A /org/server-disc-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the server discovery policy named ServDiscPolExample and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete server-disc-policy ServDiscPolExample
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Server Inheritance Policies

Server Inheritance Policy

This policy is invoked during the server discovery process to create a service profile for the server. All service profiles created from this policy use the values burned into the blade at manufacture. The policy performs the following:

- Analyzes the inventory of the server
- If configured, assigns the server to the selected organization
- Creates a service profile for the server with the identity burned into the server at manufacture

You cannot migrate a service profile created with this policy to another server.

Configuring a Server Inheritance Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create server-inherit-policy <i>policy-name</i> | Creates a server inheritance policy with the specified policy name, and enters organization server inheritance policy mode. |
| Step 3 | UCS-A /org/server-inherit-policy # set descr <i>description</i> | (Optional) Provides a description for the policy. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /org/server-inherit-policy # set destination org <i>org-name</i> | (Optional) Specifies the organization for which the server is to be used. |
| Step 5 | UCS-A /org/server-inherit-policy # set qualifier <i>server-qual-name</i> | (Optional) Specifies server pool policy qualification to use for qualifying the server. |
| Step 6 | UCS-A /org/server-inherit-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a server inheritance policy named `InheritEngineering`, provides a description for the policy, specifies `engineering` as the destination organization and `ServPoolQual22` as the server pool policy qualification, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create server-inherit-policy InheritEngineering
UCS-A /org/server-inherit-policy* # set descr "Server Inheritance Policy for Engineering"
UCS-A /org/server-inherit-policy* # set destination org engineering
UCS-A /org/server-inherit-policy* # set qualifier ServPoolQual22
UCS-A /org/server-inherit-policy* # commit-buffer
UCS-A /org/server-inherit-policy #
```

Deleting a Server Inheritance Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete server-inherit-policy <i>policy-name</i> | Deletes the specified server inheritance policy. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the server inheritance policy named InheritEngineering and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # delete server-inherit-policy InheritEngineering
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring Server Pool Policies

Server Pool Policy

This policy is invoked during the server discovery process. It determines what happens if server pool policy qualifications match a server to the target pool specified in the policy.

If a server qualifies for more than one pool and those pools have server pool policies, the server is added to all those pools.

Configuring a Server Pool Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create pooling-policy <i>policy-name</i> | Creates a server pool policy with the specified name, and enters organization pooling policy mode. |
| Step 3 | UCS-A /org/pooling-policy # set descr <i>description</i> | (Optional) Provides a description for the server pool policy. |

| | Command or Action | Purpose |
|---------------|--|--|
| | | Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /org/pooling-policy # set pool <i>pool-distinguished-name</i> | Specifies the server pool to use with the server pool policy. You must specify the full distinguished name for the pool. |
| Step 5 | UCS-A /org/pooling-policy # set qualifier <i>qualifier-name</i> | Specifies the server pool qualifier to use with the server pool policy. |
| Step 6 | UCS-A /org/pooling-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a server pool policy named ServerPoolPolicy4 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create pooling-policy ServerPoolPolicy4
UCS-A /org/pooling-policy* # set pool org-root/compute-pool-pool13
UCS-A /org/pooling-policy* # set qualifier ServPoolQual8
UCS-A /org/pooling-policy* # commit-buffer
UCS-A /org/pooling-policy #
```

Deleting a Server Pool Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete pooling-policy <i>policy-name</i> | Deletes the specified server pool policy. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the server pool policy named ServerPoolPolicy4 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete pooling-policy ServerPoolPolicy4
UCS-A /org/pooling-policy* # commit-buffer
UCS-A /org/pooling-policy #
```

Configuring Server Pool Policy Qualifications

Server Pool Policy Qualifications

This policy qualifies servers based on the inventory of a server conducted during the discovery process. The qualifications are individual rules that you configure in the policy to determine whether a server meets the

selection criteria. For example, you can create a rule that specifies the minimum memory capacity for servers in a data center pool.

Qualifications are used in other policies to place servers, not just by the server pool policies. For example, if a server meets the criteria in a qualification policy, it can be added to one or more server pools or have a service profile automatically associated with it.

You can use the server pool policy qualifications to qualify servers according to the following criteria:

- Adapter type
- Chassis location
- Memory type and configuration
- CPU cores, type, and configuration
- Storage configuration and capacity
- Server model

Depending upon the implementation, you may configure several policies with server pool policy qualifications including the following:

- Autoconfiguration policy
- Chassis discovery policy
- Server discovery policy
- Server inheritance policy
- Server pool policy

Creating a Server Pool Policy Qualification

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create server-qual <i>server-qual-name</i> | Creates a server pool qualification with the specified name, and enters organization server qualification mode. |
| Step 3 | UCS-A /org/server-qual # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a server pool qualification named ServPoolQual22 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create server-qual ServPoolQual22
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

What to Do Next

Configure one or more of the following server component qualifications:

- Adapter qualification
- Chassis qualification
- Memory qualification
- Processor qualification
- Storage qualification

Deleting a Server Pool Policy Qualification

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete server-qual <i>server-qual-name</i> | Deletes the specified server pool qualification. |
| Step 3 | UCS-A /org/server-qual # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the server pool qualification named ServPoolQual22 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # delete server-qual ServPoolQual22
UCS-A /org* # commit-buffer
UCS-A /org #
```

Creating an Adapter Qualification

Before You Begin

Create a server pool policy qualification.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope server-qual <i>server-qual-name</i> | Enters organization server qualification mode for the specified server pool policy qualification. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 3 | UCS-A /org/server-qual # create adapter | Creates an adapter qualification and enters organization server qualification adapter mode. |
| Step 4 | UCS-A /org/server-qual/adapter # create cap-qual adapter-type | Creates an adapter capacity qualification for the specified adapter type and enters organization server qualification adapter capacity qualification mode. The <i>adapter-type</i> argument can be any of the following values: <ul style="list-style-type: none"> • fcoe—Fibre Channel over Ethernet • non-virtualized-eth-if—Non-virtualized Ethernet interface • non-virtualized-fc-if—Non-virtualized Fibre Channel interface • path-encap-consolidated—Path encapsulation consolidated • path-encap-virtual—Path encapsulation virtual • protected-eth-if—Protected Ethernet interface • protected-fc-if—Protected Fibre Channel interface • protected-fcoe—Protected Fibre Channel over Ethernet • virtualized-eth-if—Virtualized Ethernet interface • virtualized-fc-if—Virtualized Fibre Channel interface • virtualized-scsi-if—Virtualized SCSI interface |
| Step 5 | UCS-A /org/server-qual/adapter/cap-qual # set maximum {max-cap unspecified} | Specifies the maximum capacity for the selected adapter type. |
| Step 6 | UCS-A /org/server-qual/adapter/cap-qual # commit-buffer | Commits the transaction to the system configuration. |

The following example creates and configures an adapter qualification for a non-virtualized Ethernet interface and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create adapter
UCS-A /org/server-qual/adapter* # create cap-qual non-virtualized-eth-if
UCS-A /org/server-qual/adapter/cap-qual* # set maximum 2500000000
UCS-A /org/server-qual/adapter/cap-qual* # commit-buffer
UCS-A /org/server-qual/adapter/cap-qual #
```

Deleting an Adapter Qualification

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope server-qual <i>server-qual-name</i> | Enters organization server qualification mode for the specified server pool policy qualification. |
| Step 3 | UCS-A /org/server-qual # delete adapter | Deletes the adapter qualification from the server pool policy qualification. |
| Step 4 | UCS-A /org/server-qual # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the adapter qualification from the server pool policy qualification named ServPoolQual22 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete adapter
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

Configuring a Chassis Qualification

Before You Begin

Create a server pool policy qualification.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope server-qual <i>server-qual-name</i> | Enters organization server qualification mode for the specified server pool policy qualification. |
| Step 3 | UCS-A /org/server-qual # create chassis <i>min-chassis-num max-chassis-num</i> | Creates a chassis qualification for the specified chassis range and enters organization server qualification chassis mode. |
| Step 4 | UCS-A /org/server-qual/chassis # create slot <i>min-slot-num max-slot-num</i> | Creates a chassis slot qualification for the specified slot range and enters organization server qualification chassis slot mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 5 | UCS-A /org/server-qual/chassis/slot # commit-buffer | Commits the transaction to the system configuration. |

The following example configures a chassis qualification for slots 1 to 4 on chassis 1 and 2 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope server-qual ServPoolQual22
UCS-A /org/server-qual* # create chassis 1 2
UCS-A /org/server-qual/chassis* # create slot 1 4
UCS-A /org/server-qual/chassis/slot* # commit-buffer
UCS-A /org/server-qual/chassis/slot #
```

Deleting a Chassis Qualification

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope server-qual <i>server-qual-name</i> | Enters organization server qualification mode for the specified server pool policy qualification. |
| Step 3 | UCS-A /org/server-qual # delete chassis <i>min-chassis-num max-chassis-num</i> | Deletes the chassis qualification for the specified chassis range. |
| Step 4 | UCS-A /org/server-qual # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the chassis qualification for chassis 1 and 2 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete chassis 1 2
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

Creating a CPU Qualification

Before You Begin

Create a server pool policy qualification.

Procedure

| | Command or Action | Purpose |
|----------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope server-qual <i>server-qual-name</i> | Enters organization server qualification mode for the specified server pool policy qualification. |
| Step 3 | UCS-A /org/server-qual # create cpu | Creates a CPU qualification and enters organization server qualification processor mode. |
| Step 4 | UCS-A /org/server-qual/cpu # set arch { any dual-core-opteron intel-p4-c opteron pentium-4 turion-64 xeon xeon-mp } | Specifies the processor architecture type. |
| Step 5 | UCS-A /org/server-qual/cpu # set maxcores { <i>max-core-num</i> unspecified } | Specifies the maximum number of processor cores. |
| Step 6 | UCS-A /org/server-qual/cpu # set mincores { <i>min-core-num</i> unspecified } | Specifies the minimum number of processor cores. |
| Step 7 | UCS-A /org/server-qual/cpu # set maxprocs { <i>max-proc-num</i> unspecified } | Specifies the maximum number of processors. |
| Step 8 | UCS-A /org/server-qual/cpu # set minprocs { <i>min-proc-num</i> unspecified } | Specifies the minimum number of processors. |
| Step 9 | UCS-A /org/server-qual/cpu # set maxthreads { <i>max-thread-num</i> unspecified } | Specifies the maximum number of threads. |
| Step 10 | UCS-A /org/server-qual/cpu # set minthreads { <i>min-thread-num</i> unspecified } | Specifies the minimum number of threads. |
| Step 11 | UCS-A /org/server-qual/cpu # set stepping { <i>step-num</i> unspecified } | Specifies the processor stepping number. |
| Step 12 | UCS-A /org/server-qual/cpu # set model-regex <i>regex</i> | Specifies a regular expression that the processor name must match. |
| Step 13 | UCS-A /org/server-qual/cpu # commit-buffer | Commits the transaction to the system configuration. |

The following example creates and configures a CPU qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create processor
UCS-A /org/server-qual/cpu* # set arch xeon
UCS-A /org/server-qual/cpu* # set maxcores 8
UCS-A /org/server-qual/cpu* # set mincores 4
UCS-A /org/server-qual/cpu* # set maxprocs 2
UCS-A /org/server-qual/cpu* # set minprocs 1
UCS-A /org/server-qual/cpu* # set maxthreads 16
UCS-A /org/server-qual/cpu* # set minthreads 8
```

```
UCS-A /org/server-qual/cpu* # set stepping 5
UCS-A /org/server-qual/cpu* # commit-buffer
UCS-A /org/server-qual/cpu #
```

Deleting a CPU Qualification

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope server-qual <i>server-qual-name</i> | Enters organization server qualification mode for the specified server pool policy qualification. |
| Step 3 | UCS-A /org/server-qual # delete cpu | Deletes the processor qualification. |
| Step 4 | UCS-A /org/server-qual # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the processor qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete cpu
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

Creating a Memory Qualification

Before You Begin

Create a server pool policy qualification.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope server-qual <i>server-qual-name</i> | Enters organization server qualification mode for the specified server pool policy qualification. |
| Step 3 | UCS-A /org/server-qual # create memory | Creates a memory qualification and enters organization server qualification memory mode. |
| Step 4 | UCS-A /org/server-qual/memory # set clock <i>{clock-num unspec}</i> | Specifies the memory clock speed. |

| | Command or Action | Purpose |
|----------------|--|--|
| Step 5 | UCS-A /org/server-qual/memory # set maxcap { <i>max-cap-num</i> unspec } | Specifies the maximum capacity of the memory array. |
| Step 6 | UCS-A /org/server-qual/memory # set mincap { <i>min-cap-num</i> unspec } | Specifies the minimum capacity of the memory array. |
| Step 7 | UCS-A /org/server-qual/memory # set speed { <i>speed-num</i> unspec } | Specifies the memory data rate. |
| Step 8 | UCS-A /org/server-qual/memory # set units { <i>unit-num</i> unspec } | Specifies the number of memory units (DRAM chips mounted to the memory board). |
| Step 9 | UCS-A /org/server-qual/memory # set width { <i>width-num</i> unspec } | Specifies the bit width of the data bus. |
| Step 10 | UCS-A /org/server-qual/memory # commit-buffer | Commits the transaction to the system configuration. |

The following example creates and configures a memory qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create memory
UCS-A /org/server-qual/memory* # set clock 1067
UCS-A /org/server-qual/memory* # set maxcap 4096
UCS-A /org/server-qual/memory* # set mincap 2048
UCS-A /org/server-qual/memory* # set speed unspec
UCS-A /org/server-qual/memory* # set units 16
UCS-A /org/server-qual/memory* # set width 64
UCS-A /org/server-qual/memory* # commit-buffer
UCS-A /org/server-qual/memory #
```

Deleting a Memory Qualification

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope server-qual <i>server-qual-name</i> | Enters organization server qualification mode for the specified server pool policy qualification. |
| Step 3 | UCS-A /org/server-qual # delete memory | Deletes the memory qualification. |
| Step 4 | UCS-A /org/server-qual # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the memory qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete memory
```

```
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

Creating a Physical Qualification

Before You Begin

Create a server pool policy qualification.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope server-qual <i>server-qual-name</i> | Enters organization server qualification mode for the specified server pool policy qualification. |
| Step 3 | UCS-A /org/server-qual # create physical-qual | Creates a physical qualification and enters organization server qualification physical mode. |
| Step 4 | UCS-A /org/server-qual/physical-qual # set model-regex <i>regex</i> | Specifies a regular expression that the model name must match. |
| Step 5 | UCS-A /org/server-qual/physical-qual # commit-buffer | Commits the transaction to the system configuration. |

The following example creates and configures a physical qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create physical-qual
UCS-A /org/server-qual/physical-qual* # set model-regex
UCS-A /org/server-qual/physical-qual* # commit-buffer
UCS-A /org/server-qual/physical-qual #
```

Deleting a Physical Qualification

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope server-qual <i>server-qual-name</i> | Enters organization server qualification mode for the specified server pool policy qualification. |
| Step 3 | UCS-A /org/server-qual # delete physical-qual | Deletes the physical qualification. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 4 | UCS-A /org/server-qual # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes a physical qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete physical-qual
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

Creating a Storage Qualification

Before You Begin

Create a server pool policy qualification.

Procedure

| | Command or Action | Purpose |
|----------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope server-qual <i>server-qual-name</i> | Enters organization server qualification mode for the specified server pool policy qualification. |
| Step 3 | UCS-A /org/server-qual # create storage | Creates a storage qualification and enters organization server qualification storage mode. |
| Step 4 | UCS-A /org/server-qual/storage # set blocksize { <i>block-size-num</i> unspecified } | Specifies the storage block size. |
| Step 5 | UCS-A /org/server-qual/storage # set maxcap { <i>max-cap-num</i> unspecified } | Specifies the maximum capacity of the storage array. |
| Step 6 | UCS-A /org/server-qual/storage # set mincap { <i>min-cap-num</i> unspecified } | Specifies the minimum capacity of the storage array. |
| Step 7 | UCS-A /org/server-qual/storage # set numberofblocks { <i>block-num</i> unspecified } | Specifies the number of blocks. |
| Step 8 | UCS-A /org/server-qual/storage # set perdiskcap { <i>disk-cap-num</i> unspecified } | Specifies the per-disk capacity. |
| Step 9 | UCS-A /org/server-qual/storage # set units { <i>unit-num</i> unspecified } | Specifies the number of storage units. |
| Step 10 | UCS-A /org/server-qual/storage # commit-buffer | Commits the transaction to the system configuration. |

The following example creates and configures a storage qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # create storage
UCS-A /org/server-qual/storage* # set blocksize 512
UCS-A /org/server-qual/storage* # set maxcap 420000
UCS-A /org/server-qual/storage* # set mincap 140000
UCS-A /org/server-qual/storage* # set numberofblocks 287277984
UCS-A /org/server-qual/storage* # set perdiskcap 140000
UCS-A /org/server-qual/storage* # set units 1
UCS-A /org/server-qual/storage* # commit-buffer
UCS-A /org/server-qual/storage #
```

Deleting a Storage Qualification

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope server-qual <i>server-qual-name</i> | Enters organization server qualification mode for the specified server pool policy qualification. |
| Step 3 | UCS-A /org/server-qual # delete storage | Deletes the storage qualification. |
| Step 4 | UCS-A /org/server-qual/ # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the storage qualification and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope server-qual ServPoolQual22
UCS-A /org/server-qual # delete storage
UCS-A /org/server-qual* # commit-buffer
UCS-A /org/server-qual #
```

Configuring vNIC/vHBA Placement Profiles

vNIC/vHBA Placement Policies

vNIC/vHBA placement policies are used to assign vNICs or vHBAs to the physical adapters on a server. Each vNIC/vHBA placement policy contains two virtual network interface connections (vCons) that are virtual representations of the physical adapters. When a vNIC/vHBA placement policy is assigned to a service profile, and the service profile is associated to a server, the vCons in the vNIC/vHBA placement policy are assigned to the physical adapters. For servers with only one adapter, both vCons are assigned to the adapter; for servers with two adapters, one vCon is assigned to each adapter.

You can assign vNICs or vHBAs to either of the two vCons, and they are then assigned to the physical adapters based on the vCon assignment during server association. Additionally, vCons use the following selection preference criteria to assign vHBAs and vNICs:

| | |
|---------------------------|---|
| All | The vCon is used for vNICs or vHBAs assigned to it, vNICs or vHBAs not assigned to either vCon, and dynamic vNICs or vHBAs. |
| Assigned-Only | The vCon is reserved for only vNICs or vHBAs assigned to it. |
| Exclude-Dynamic | The vCon is not used for dynamic vNICs or vHBAs. |
| Exclude-Unassigned | The vCon is not used for vNICs or vHBAs not assigned to the vCon. The vCon is used for dynamic vNICs and vHBAs. |

For servers with two adapters, if you do not include a vNIC/vHBA placement policy in a service profile, or you do not configure vCons for a service profile, Cisco UCS equally distributes the vNICs and vHBAs between the two adapters.

Configuring a vNIC/vHBA Placement Profile

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create vcon-policy <i>policy-name</i> | Creates the specified vNIC/vHBA placement profile and enters organization vcon policy mode. |
| Step 3 | UCS-A /org/vcon-policy # set descr <i>description</i> | (Optional) Provides a description for the vNIC/vHBA Placement Profile. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /org/vcon-policy # set vcon {1 2} selection {all assigned-only exclude-dynamic exclude-unassigned} | Specifies the selection preference for the specified vCon. |
| Step 5 | UCS-A /org/vcon-policy # commit-buffer | Commits the transaction. |

The following example creates a vNIC/vHBA placement policy named Adapter1All, places all vNICs and vHBAs on adapter 1, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create vcon-policy Adapter1
UCS-A /org/vcon-policy* # set descr "This profile places all vNICs and vHBAs on adapter 1."
UCS-A /org/vcon-policy* # set vcon 1 selection all
UCS-A /org/vcon-policy* # commit-buffer
```

```
UCS-A /org/vcon-policy* #
UCS-A /org #
```

Deleting a vNIC/vHBA Placement Profile

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete vcon-policy <i>policy-name</i> | Deletes the specified vNIC/vHBA placement profile. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction. |

The following example deletes the vNIC/vHBA placement profile named Adapter1All and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete vcon-policy Adapter1All
UCS-A /org* # commit-buffer
UCS-A /org #
```



CHAPTER 25

Configuring Service Profiles

This chapter includes the following sections:

- [Service Profiles that Inherit Server Identity, page 271](#)
- [Service Profiles that Override Server Identity, page 272](#)
- [Service Profile Templates, page 272](#)
- [Creating a Service Profile Template, page 273](#)
- [Creating a Service Profile Instance from a Service Profile Template, page 275](#)
- [Creating a Service Profile, page 276](#)
- [Configuring a vNIC for a Service Profile, page 278](#)
- [Configuring a vHBA for a Service Profile, page 279](#)
- [Configuring a Local Disk for a Service Profile, page 281](#)
- [Configuring Serial over LAN for a Service Profile, page 282](#)
- [Service Profile Boot Definition Configuration, page 283](#)
- [Associating a Service Profile with a Server or Server Pool, page 288](#)
- [Disassociating a Service Profile from a Server or Server Pool, page 288](#)
- [Resetting the UUID Assigned to a Service Profile from a Pool in a Service Profile Template, page 289](#)
- [Resetting the MAC Address Assigned to a vNIC from a Pool in a Service Profile Template, page 290](#)
- [Resetting the WWPN Assigned to a vHBA from a Pool in a Service Profile Template, page 291](#)

Service Profiles that Inherit Server Identity

This hardware-based service profile is the simplest to use and create. This profile uses the default values in the server and mimics the management of a rack-mounted server. It is tied to a specific server and cannot be moved to another server.

You do not need to create pools or configuration policies to use this service profile.

This service profile inherits and applies the identity and configuration information that is present at the time of association, such as the following:

- MAC addresses for the two NICs
- For a converged network adapter or a virtual interface card, the WWN addresses for the two HBAs
- BIOS versions
- Server UUID



Important

The server identity and configuration information inherited through this service profile may not be the values burned into the server hardware at manufacture if those values were changed before this profile is associated with the server.

Service Profiles that Override Server Identity

This type of service profile provides the maximum amount of flexibility and control. This profile allows you to override the identity values that are on the server at the time of association and use the resource pools and policies set up in Cisco UCS Manager to automate some administration tasks.

You can disassociate this service profile from one server and then associate it with another server. This re-association can be done either manually or through an automated server pool policy. The burned-in settings, such as UUID and MAC address, on the new server are overwritten with the configuration in the service profile. As a result, the change in server is transparent to your network. You do not need to reconfigure any component or application on your network to begin using the new server.

This profile allows you to take advantage of and manage system resources through resource pools and policies, such as the following:

- Virtualized identity information, including pools of MAC addresses, WWN addresses, and UUIDs
- Ethernet and Fibre Channel adapter profile policies
- Firmware package policies
- Operating system boot order policies

Service Profile Templates

With a service profile template, you can quickly create several service profiles with the same basic parameters, such as the number of vNICs and vHBAs, and with identity information drawn from the same pools.



Tip

If you need only one service profile with similar values to an existing service profile, you can clone a service profile in the Cisco UCS Manager GUI.

For example, if you need several service profiles with similar values to configure servers to host database software, you can create a service profile template, either manually or from an existing service profile. You then use the template to create the service profiles.

Cisco UCS supports the following types of service profile templates:

- Initial template** Service profiles created from an initial template inherit all the properties of the template. However, after you create the profile, it is no longer connected to the template. If you need to make changes to one or more profiles created from this template, you must change each profile individually.
- Updating template** Service profiles created from an updating template inherit all the properties of the template and remain connected to the template. Any changes to the template automatically update the service profiles created from the template.

Creating a Service Profile Template

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create service-profile <i>profile-name</i> { initial-template updating-template } | Creates the specified service profile template and enters organization service profile mode. Enter a unique <i>profile-name</i> to identify this service profile template. This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved. |
| Step 3 | UCS-A /org/service-profile # set boot-policy <i>policy-name</i> | Associates the specified boot policy with the service profile. |
| Step 4 | UCS-A /org/service-profile # set descr <i>description</i> | (Optional) Provides a description for the service profile. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 5 | UCS-A /org/service-profile # set dynamic-vnic-conn-policy <i>policy-name</i> | Associates the specified dynamic vNIC connection policy with the service profile. |
| Step 6 | UCS-A /org/service-profile # set host-fw-policy <i>policy-name</i> | Associates the specified host firmware policy with the service profile. |
| Step 7 | UCS-A /org/service-profile # set identity { dynamic-uuid { <i>uuid</i> derived } dynamic-wwnn { <i>wwnn</i> derived } uuid-pool <i>pool-name</i> wwnn-pool <i>pool-name</i> } | Specifies how the server acquires a UUID or WWNN. You can do one of the following: <ul style="list-style-type: none"> • Create a unique UUID in the form <i>nnnnnnnnn-nnnnn-nnnnn-nnnnnnnnnnnnnnn</i>. |

| | Command or Action | Purpose |
|----------------|--|--|
| | | <ul style="list-style-type: none"> • Derive the UUID from the one burned into the hardware at manufacture. • Use a UUID pool. • Create a unique WWNN in the form <i>hh : hh : hh : hh : hh : hh : hh : hh</i>. • Derive the WWNN from one burned into the hardware at manufacture. • Use a WWNN pool. |
| Step 8 | UCS-A /org/service-profile # set ipmi-access-profile <i>profile-name</i> | Associates the specified IPMI access profile with the service profile. |
| Step 9 | UCS-A /org/service-profile # set local-disk-policy <i>policy-name</i> | Associates the specified local disk policy with the service profile. |
| Step 10 | UCS-A /org/service-profile # set mgmt-fw-policy <i>policy-name</i> | Associates the specified management firmware policy with the service profile. |
| Step 11 | UCS-A /org/service-profile # set scrub-policy <i>policy-name</i> | Associates the specified scrub policy with the service profile. |
| Step 12 | UCS-A /org/service-profile # set sol-policy <i>policy-name</i> | Associates the specified serial over LAN policy with the service profile. |
| Step 13 | UCS-A /org/service-profile # set stats-policy <i>policy-name</i> | Associates the specified statistics policy with the service profile. |
| Step 14 | UCS-A /org/service-profile # set vcon {1 2} selection {all assigned-only exclude-dynamic exclude-unassigned} | Specifies the selection preference for the specified vCon. |
| Step 15 | UCS-A /org/service-profile # set vcon-profile <i>policy-name</i> | <p>Associates the specified vNIC/vHBA placement profile with the service profile.</p> <p>Note You can either assign a vNIC/vHBA placement profile to the service profile, or set vCon selection preferences for the service profile, but you do not need to do both.</p> |
| Step 16 | UCS-A /org/service-profile # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a service profile template and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create service-profile ServTemp2 updating-template
UCS-A /org/service-profile* # set boot-policy BootPol32
UCS-A /org/service-profile* # set descr "This is a service profile example."
UCS-A /org/service-profile* # set dynamic-vnic-conn-policy MyDynVnicConnPolicy
UCS-A /org/service-profile* # set host-fw-policy Epuser987
UCS-A /org/service-profile* # set identity dynamic-uuid derived
```

```
UCS-A /org/service-profile* # set ipmi-access-profile IpmiProf16
UCS-A /org/service-profile* # set local-disk-policy LocalDiskPol133
UCS-A /org/service-profile* # set mgmt-fw-policy MgmtFwPol175
UCS-A /org/service-profile* # set scrub-policy ScrubPol155
UCS-A /org/service-profile* # set sol-policy SolPol2
UCS-A /org/service-profile* # set stats-policy StatsPol4
UCS-A /org/service-profile* # vcon-profile MyVconnProfile
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

What to Do Next

- (Optional) Configure a boot definition for the service profile. Use this option only if you have not associated a boot policy with the service profile.
- Create a service profile instance from the service profile template.

Creating a Service Profile Instance from a Service Profile Template

Before You Begin

Verify that there is a service profile template from which to create a service profile instance.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org org-name | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create service-profile profile-name instance | Creates the specified service profile instance and enters organization service profile mode. Enter a unique <i>profile-name</i> to identify this service profile template. This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved. |
| Step 3 | UCS-A /org/service-profile # set src-templ-name profile-name | Specifies the source service profile template to apply to the service profile instance. All configuration settings from the service profile template will be applied to the service profile instance. |
| Step 4 | UCS-A /org/service-profile # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a service profile instance named ServProf34, applies the service profile template named ServTemp2, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create service-profile ServProf34 instance
UCS-A /org/service-profile* # set src-templ-name ServTemp2
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

What to Do Next

Associate the service profile to a server or server pool.

Creating a Service Profile**Procedure**

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create service-profile <i>profile-name</i> instance | Creates the specified service profile instance and enters organization service profile mode. Enter a unique <i>profile-name</i> to identify this service profile template. This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved. |
| Step 3 | UCS-A /org/service-profile # set boot-policy <i>policy-name</i> | Associates the specified boot policy with the service profile. |
| Step 4 | UCS-A /org/service-profile # set descr <i>description</i> | (Optional) Provides a description for the service profile. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 5 | UCS-A /org/service-profile # set dynamic-vnic-conn-policy <i>policy-name</i> | Associates the specified dynamic vNIC connection policy with the service profile. |
| Step 6 | UCS-A /org/service-profile # set host-fw-policy <i>epuser-name</i> | Associates the specified host forwarding policy with the service profile. |
| Step 7 | UCS-A /org/service-profile # set identity { dynamic-uuid { <i>uuid</i> derived } dynamic-wwnn { <i>wwnn</i> derived } uuid-pool <i>pool-name</i> wwnn-pool <i>pool-name</i> } | Specifies how the server acquires a UUID or WWNN. You can do one of the following: <ul style="list-style-type: none"> • Create a unique UUID in the form <i>nnnnnnnn-nnnn-nnnn-nnnnnnnnnnnn</i>. • Derive the UUID from the one burned into the hardware at manufacture. • Use a UUID pool. |

| | Command or Action | Purpose |
|----------------|--|---|
| | | <ul style="list-style-type: none"> • Create a unique WWNN in the form <i>hh : hh : hh : hh : hh : hh</i>. • Derive the WWNN from one burned into the hardware at manufacture. • Use a WWNN pool. |
| Step 8 | UCS-A /org/service-profile # set ipmi-access-profile <i>profile-name</i> | Associates the specified IPMI access profile with the service profile. |
| Step 9 | UCS-A /org/service-profile # set local-disk-policy <i>policy-name</i> | Associates the specified local disk policy with the service profile. |
| Step 10 | UCS-A /org/service-profile # set mgmt-fw-policy <i>policy-name</i> | Associates the specified management forwarding policy with the service profile. |
| Step 11 | UCS-A /org/service-profile # set scrub-policy <i>policy-name</i> | Associates the specified scrub policy with the service profile. |
| Step 12 | UCS-A /org/service-profile # set sol-policy <i>policy-name</i> | Associates the specified serial over LAN policy with the service profile. |
| Step 13 | UCS-A /org/service-profile # set stats-policy <i>policy-name</i> | Associates the specified statistics policy with the service profile. |
| Step 14 | UCS-A /org/service-profile # set vcon {1 2} selection {all assigned-only exclude-dynamic exclude-unassigned} | Specifies the selection preference for the specified vCon. |
| Step 15 | UCS-A /org/service-profile # set vcon-profile <i>policy-name</i> | Associates the specified vNIC/vHBA placement policy with the service profile. Note You can either assign a vNIC/vHBA placement profile to the service profile, or set vCon selection preferences for the service profile, but you do not need to do both. |
| Step 16 | UCS-A /org/service-profile # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a service profile instance and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create service-profile ServInst90 instance
UCS-A /org/service-profile* # set boot-policy BootPol32
UCS-A /org/service-profile* # set descr "This is a service profile example."
UCS-A /org/service-profile* # set host-fw-policy Euser987
UCS-A /org/service-profile* # set identity dynamic-uuid derived
UCS-A /org/service-profile* # set ipmi-access-profile IpmiProf16
UCS-A /org/service-profile* # set local-disk-policy LocalDiskPol133
UCS-A /org/service-profile* # set mgmt-fw-policy MgmtFwPol175
UCS-A /org/service-profile* # set scrub-policy ScrubPol155
UCS-A /org/service-profile* # set sol-policy SolPol12
UCS-A /org/service-profile* # set stats-policy StatsPol14
UCS-A /org/service-profile* # vcon-profile MyVconnProfile
```

```
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

What to Do Next

- (Optional) Configure a boot definition for the service profile. Use this option only if you have not associated a boot policy with the service profile.
- Associate the service profile to a server or server pool.

Configuring a vNIC for a Service Profile

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope service-profile <i>profile-name</i> | Enters organization service profile mode for the specified service. |
| Step 3 | UCS-A /org/service-profile # create vnic <i>vnic-name</i> [eth-if <i>eth-if-name</i>] [fabric { a b }] | Creates a vNIC for the specified service profile and enters organization service profile vNIC mode. |
| Step 4 | UCS-A /org/service-profile/vnic # set adaptor-profile <i>policy-name</i> | Specifies the adapter policy to use for the vNIC. |
| Step 5 | UCS-A /org/service-profile/vnic # set identity { dynamic-mac { <i>mac-addr</i> derived } mac-pool <i>mac-pool-name</i> } | Specifies the identity (MAC address) for the vNIC. You can set the identity using one of the following options: <ul style="list-style-type: none"> • Create a unique MAC address in the form <i>nn:nn:nn:nn:nn:nn</i>. • Derive the MAC address from one burned into the hardware at manufacture. • Assign a MAC address from a MAC pool. |
| Step 6 | UCS-A /org/service-profile/vnic # set mtu <i>size-num</i> | Specifies the maximum transmission unit, or packet size, that the vNIC accepts. |
| Step 7 | UCS-A /org/service-profile/vnic # set nw-control-policy <i>policy-name</i> | Specifies the network control policy to use for the vNIC. |
| Step 8 | UCS-A /org/service-profile/vnic # set order { <i>order-num</i> unspecified } | Specifies the relative order for the vNIC. |
| Step 9 | UCS-A /org/service-profile/vnic # set pin-group <i>group-name</i> | Specifies the pin group to use for the vNIC. |

| | Command or Action | Purpose |
|----------------|---|---|
| Step 10 | UCS-A /org/service-profile/vnic # set qos-policy <i>policy-name</i> | Specifies the QoS policy to use for the vNIC. |
| Step 11 | UCS-A /org/service-profile/vnic # set stats-policy <i>policy-name</i> | Specifies the stats policy to use for the vNIC. |
| Step 12 | UCS-A /org/service-profile/vnic # set template-name <i>policy-name</i> | Specifies the dynamic vNIC connectivity policy to use for the vNIC. |
| Step 13 | UCS-A /org/service-profile/vnic # set vcon {1 2 any} | Assigns the vNIC to the specified vCon. Use the any keyword to have Cisco UCS Manager automatically assign the vNIC. |
| Step 14 | UCS-A /org/service-profile/vnic # commit-buffer | Commits the transaction to the system configuration. |

The following example configures a vNIC for a service profile and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServInst90
UCS-A /org/service-profile* # create vnic vnic3 fabric a
UCS-A /org/service-profile/vnic* # set adaptor-profile AdaptPol2
UCS-A /org/service-profile/vnic* # set identity mac-pool MacPool3
UCS-A /org/service-profile/vnic* # set mtu 8900
UCS-A /org/service-profile/vnic* # set nw-control-policy ncp5
UCS-A /org/service-profile/vnic* # set order 0
UCS-A /org/service-profile/vnic* # set pin-group EthPinGroup12
UCS-A /org/service-profile/vnic* # set qos-policy QosPol5
UCS-A /org/service-profile/vnic* # set stats-policy StatsPol2
UCS-A /org/service-profile/vnic* # set template-name VnicConnPol3
UCS-A /org/service-profile/vnic* # set set vcon any
UCS-A /org/service-profile/vnic* # commit-buffer
UCS-A /org/service-profile/vnic #
```

Configuring a vHBA for a Service Profile

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope service-profile <i>profile-name</i> | Enters organization service profile mode for the specified service. |
| Step 3 | UCS-A /org/service-profile # create vhma <i>vhba-name</i> [fabric {a b}] [fc-if <i>fc-if-name</i>] | Creates a vHBA for the specified service profile and enters organization service profile vHBA mode. |
| Step 4 | UCS-A /org/service-profile/vhba # set adaptor-profile <i>policy-name</i> | Specifies the adapter policy to use for the vHBA. |

| | Command or Action | Purpose |
|----------------|--|---|
| Step 5 | UCS-A /org/service-profile/vhba # set admin-vcon {1 2 any} | Assigns the vHBA to one or all virtual network interface connections. |
| Step 6 | UCS-A /org/service-profile/vhba # set identity {dynamic-wwpn {wwpn derived} wwpn-pool wwn-pool-name} | Specifies the storage identity (world wide port name [WWPN]) for the vHBA. You can set the storage identity using one of the following options: <ul style="list-style-type: none"> • Create a unique WWPN in the form <i>hh : hh : hh : hh : hh : hh</i>. • Derive the WWPN from one burned into the hardware at manufacture. • Assign a WWPN from a WWN pool. |
| Step 7 | UCS-A /org/service-profile/vhba # set max-field-size size-num | Specifies the maximum size of the Fibre Channel frame payload (in bytes) that the vHBA supports. |
| Step 8 | UCS-A /org/service-profile/vhba # set order {order-num unspecified} | Specifies the PCI scan order for the vHBA. |
| Step 9 | UCS-A /org/service-profile/vhba # set pers-bind {disabled enabled} | Disables or enables persistent binding to Fibre Channel targets. |
| Step 10 | UCS-A /org/service-profile/vhba # set pin-group group-name | Specifies the pin group to use for the vHBA. |
| Step 11 | UCS-A /org/service-profile/vhba # set qos-policy policy-name | Specifies the QoS policy to use for the vHBA. |
| Step 12 | UCS-A /org/service-profile/vhba # set stats-policy policy-name | Specifies the stats policy to use for the vHBA. |
| Step 13 | UCS-A /org/service-profile/vhba # set template-name policy-name | Specifies the vHBA SAN connectivity policy to use for the vHBA. |
| Step 14 | UCS-A /org/service-profile/vhba # commit-buffer | Commits the transaction to the system configuration. |

The following example configures a vHBA for a service profile and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServInst90
UCS-A /org/service-profile* # create vhba vha3 fabric b
UCS-A /org/service-profile/vhba* # set adaptor-profile AdaptPol2
UCS-A /org/service-profile/vhba* # set set admin-vcon any
UCS-A /org/service-profile/vhba* # set admin-vcon any
UCS-A /org/service-profile/vhba* # set identity wwpn-pool SanPool7
UCS-A /org/service-profile/vhba* # set max-field-size 2112
UCS-A /org/service-profile/vhba* # set order 0
UCS-A /org/service-profile/vhba* # set pers-bind enabled
UCS-A /org/service-profile/vhba* # set pin-group FcPinGroup12
UCS-A /org/service-profile/vhba* # set qos-policy QosPol5
UCS-A /org/service-profile/vhba* # set stats-policy StatsPol2
UCS-A /org/service-profile/vhba* # set template-name SanConnPol3
UCS-A /org/service-profile/vhba* # commit-buffer
UCS-A /org/service-profile/vhba #
```

Configuring a Local Disk for a Service Profile

Procedure

| | Command or Action | Purpose |
|----------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope service-profile <i>profile-name</i> | Enters organization service profile mode for the specified service profile. |
| Step 3 | UCS-A /org/service-profile # create local-disk-config | Creates a local disk configuration for the service profile and enters organization service profile local disk configuration mode. |
| Step 4 | UCS-A /org/service-profile/local-disk-config # set descr <i>description</i> | (Optional) Provides a description for the local disk configuration. |
| Step 5 | UCS-A /org/service-profile/local-disk-config # set mode { any-configuration no-local-storage no-raid raid-0-striped raid-1-mirrored raid-5-striped-parity raid-6-striped-dual-parity raid-10-mirrored-and-striped } | Specifies the mode for the local disk. |
| Step 6 | UCS-A /org/service-profile/local-disk-config # create partition | Creates a partition for the local disk and enters organization service profile local disk configuration partition mode. |
| Step 7 | UCS-A /org/service-profile/local-disk-config/partition # set descr <i>description</i> | (Optional) Provides a description for the partition. |
| Step 8 | UCS-A /org/service-profile/local-disk-config/partition # set size { <i>size-num</i> unspecified } | Specifies the partition size in MBytes. |
| Step 9 | UCS-A /org/service-profile/local-disk-config/partition # set type { ext2 ext3 fat32 none ntfs swap } | Specifies the partition type. |
| Step 10 | UCS-A /org/service-profile/local-disk-config/partition # commit-buffer | Commits the transaction to the system configuration. |

The following example configures a local disk for a service profile and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope service-profile ServInst90
UCS-A /org/service-profile # scope boot-definition
UCS-A /org/service-profile # create local-disk-config
UCS-A /org/service-profile/local-disk-config* # set mode raid-1-mirrored
```

```

UCS-A /org/service-profile/local-disk-config* # create partition
UCS-A /org/service-profile/local-disk-config/partition* # set size 1000000
UCS-A /org/service-profile/local-disk-config/partition* # set type ntfs
UCS-A /org/service-profile/local-disk-config/partition* # commit-buffer
UCS-A /org/service-profile/local-disk-config/partition #

```

Configuring Serial over LAN for a Service Profile

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope service-profile <i>profile-name</i> | Enters organization service profile mode for the specified service. |
| Step 3 | UCS-A /org/service-profile # create sol-config | Creates a serial over LAN configuration for the service profile and enters organization service profile SoL configuration mode. |
| Step 4 | UCS-A /org/service-profile/sol-config # {disable enable} | Disables or enables the serial over LAN configuration for the service profile. |
| Step 5 | UCS-A /org/service-profile/sol-config # set descr <i>description</i> | (Optional) Provides a description for the serial over LAN configuration. |
| Step 6 | UCS-A /org/service-profile/sol-config # set speed {115200 19200 38400 57600 9600} | Specifies the serial baud rate. |
| Step 7 | UCS-A /org/service-profile/sol-config # commit-buffer | Commits the transaction to the system configuration. |

The following example configures serial over LAN for the service profile named ServInst90 and commits the transaction:

```

UCS-A# scope org /
UCS-A /org # scope service-profile ServInst90
UCS-A /org/service-profile # create sol-config
UCS-A /org/service-profile/sol-config* # enable
UCS-A /org/service-profile/sol-config* # set descr "Sets serial over LAN to 9600 baud."
UCS-A /org/service-profile/sol-config* # set speed 9600
UCS-A /org/service-profile/sol-config* # commit-buffer
UCS-A /org/service-profile/sol-config #

```

Service Profile Boot Definition Configuration

Configuring a Boot Definition for a Service Profile

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope service-profile <i>profile-name</i> | Enters organization service profile mode for the the specified service. |
| Step 3 | UCS-A /org/service-profile # create boot-definition | Creates a boot definition for the service profile and enters organization service profile boot definition mode. |
| Step 4 | UCS-A /org/service-profile/boot-definition # set descr <i>description</i> | (Optional) Provides a description for the boot definition. |
| Step 5 | UCS-A /org/service-profile/boot-definition # set reboot-on-update {no yes} | (Optional) Specifies whether to automatically reboot all servers that use this boot definition after changes are made to the boot order. By default, the reboot on update option is disabled. |
| Step 6 | UCS-A /org/service-profile/boot-definition # commit-buffer | Commits the transaction to the system configuration. |

The following example configures a boot definition for a service profile and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServInst90
UCS-A /org/service-profile* # create boot-definition
UCS-A /org/service-profile/boot-definition* # set descr "This boot definition reboots on update."
UCS-A /org/service-profile/boot-definition* # set reboot-on-update yes
UCS-A /org/service-profile/boot-definition* # commit-buffer
UCS-A /org/service-profile/boot-definition #
```

What to Do Next

Configure one or more of the following boot options for the boot definition and set their boot order:

- **LAN Boot**—Boots from a centralized provisioning server. It is frequently used to install operating systems on a server from that server.

If you choose the LAN Boot option, continue to [Configuring a LAN Boot for a Service Profile Boot Definition](#), page 284.

- **Storage Boot**—Boots from an operating system image on the SAN. You can specify a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary.

We recommend that you use a SAN boot, because it offers the most service profile mobility within the system. If you boot from the SAN, when you move a service profile from one server to another, the new server boots from exactly the same operating system image. Therefore, the new server appears to be exactly the same server to the network.

If you choose the Storage Boot option, continue to [Configuring a Storage Boot for a Service Profile Boot Definition](#), page 285.

- **Virtual Media Boot**—Mimics the insertion of a physical CD into a server. It is typically used to manually install operating systems on a server.

If you choose the Virtual Media boot option, continue to [Configuring a Virtual Media Boot for a Service Profile Boot Definition](#), page 286.

Configuring a LAN Boot for a Service Profile Boot Definition

Before You Begin

Configure a boot definition for a service profile.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope service-profile <i>profile-name</i> | Enters organization service profile mode for the specified service profile. |
| Step 3 | UCS-A /org/service-profile # scope boot-definition | Enters organization service profile boot definition mode. |
| Step 4 | UCS-A /org/service-profile/boot-definition # create lan | Creates a LAN boot for the service profile boot definition and enters service profile boot definition LAN mode. |
| Step 5 | UCS-A /org/service-profile/boot-definition/lan # set order {1 2 3 4} | Specifies the boot order for the LAN boot. |
| Step 6 | UCS-A /org/service-profile/boot-definition/lan # create path {primary secondary} | Creates a primary or secondary LAN boot path and enters service profile boot definition LAN path mode. |
| Step 7 | UCS-A /org/service-profile/boot-definition/lan/path # set vnic <i>vnic-name</i> | Specifies the vNIC to use for the LAN image path. |
| Step 8 | UCS-A /org/service-profile/boot-definition/lan/path # commit-buffer | Commits the transaction to the system configuration. |

The following example enters the service profile named ServInst90, creates a LAN boot for the service profile boot definition, sets the boot order to 2, creates a primary path, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServInst90
UCS-A /org/service-profile* # scope boot-definition
UCS-A /org/service-profile/boot-definition* # create lan
UCS-A /org/service-profile/boot-definition/lan* # set order 2
UCS-A /org/service-profile/boot-definition/lan* # create path primary
UCS-A /org/service-profile/boot-definition/lan/path* # set vnic vnic3
UCS-A /org/service-profile/boot-definition/lan/path* # commit-buffer
UCS-A /org/service-profile/boot-definition/lan/path #
```

Configuring a Storage Boot for a Service Profile Boot Definition

Before You Begin

Configure a boot definition for a service profile.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope service-profile <i>profile-name</i> | Enters organization service profile mode for the specified service. |
| Step 3 | UCS-A /org/service-profile # scope boot-definition | Enters organization service profile boot definition mode. |
| Step 4 | UCS-A /org/service-profile/boot-definition # create storage | Creates a storage boot for the service profile boot definition and enters service profile boot definition storage mode. |
| Step 5 | UCS-A /org/service-profile/boot-definition/storage # set order {1 2 3 4} | Specifies the boot order for the storage boot. |
| Step 6 | UCS-A /org/service-profile/boot-definition/storage # create {local san-image {primary secondary}} | Creates a local storage boot or a SAN image boot. If a SAN image boot is created, it enters service profile boot definition storage SAN image mode. |
| Step 7 | UCS-A /org/service-profile/boot-definition/storage/san-image # create path {primary secondary} | Creates a primary or secondary SAN image path and enters service profile boot definition storage SAN image path mode. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device |

| | Command or Action | Purpose |
|----------------|--|--|
| | | class is determined by PCIe bus scan order. |
| Step 8 | UCS-A /org/service-profile/boot-definition/storage/san-image/path # set lun <i>lun-num</i> | Specifies the LUN used for the SAN image path. |
| Step 9 | UCS-A /org/service-profile/boot-definition/storage/san-image/path # set vhba <i>vhba-name</i> | Specifies the vHBA used for the SAN image path. |
| Step 10 | UCS-A /org/service-profile/boot-definition/storage/san-image/path # set wwn <i>wwn-num</i> | Specifies the WWN used for the SAN image path. |
| Step 11 | UCS-A /org/service-profile/boot-definition/storage/san-image/path # commit-buffer | Commits the transaction to the system configuration. |

The following example enters the service profile named ServInst90, creates a storage boot for the service profile boot definition, sets the boot order to 2, creates a primary path, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServInst90
UCS-A /org/service-profile/boot-definition* # scope boot-definition
UCS-A /org/service-profile/boot-definition* # create storage
UCS-A /org/service-profile/boot-definition/storage* # create san-image primary
UCS-A /org/service-profile/boot-definition/storage* # set order 2
UCS-A /org/service-profile/boot-definition/storage/san-image* # create path primary
UCS-A /org/service-profile/boot-definition/storage/san-image/path* # set lun 27512
UCS-A /org/service-profile/boot-definition/storage/san-image/path* # set vhba vhb3
UCS-A /org/service-profile/boot-definition/storage/san-image/path* # set wwn
20:00:00:00:20:00:00:23
UCS-A /org/service-profile/boot-definition/storage/san-image/path* # commit-buffer
UCS-A /org/service-profile/boot-definition/storage/san-image/path #
```

Configuring a Virtual Media Boot for a Service Profile Boot Definition

Before You Begin

Configure a boot definition for a service profile.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope service-profile <i>profile-name</i> | Enters organization service profile mode for the specified service. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 3 | UCS-A /org/service-profile # scope boot-definition | Enters organization service profile boot definition mode. |
| Step 4 | UCS-A /org/service-profile/boot-definition # create virtual-media {read-only read-write} | Creates a read-only or read-write virtual media boot for the service profile boot definition and enters service profile boot definition virtual media mode. |
| Step 5 | UCS-A /org/service-profile/boot-definition/virtual-media # set order {1 2 3 4} | Specifies the boot order for the virtual media boot. |
| Step 6 | UCS-A /org/service-profile/boot-definition/virtual-media # commit-buffer | Commits the transaction to the system configuration. |

The following example enters the service profile named ServInst90, creates a virtual media boot with read-only privileges for the service profile boot definition, sets the boot order to 3, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServInst90
UCS-A /org/service-profile* # scope boot-definition
UCS-A /org/service-profile/boot-definition* # create virtual-media read-only
UCS-A /org/service-profile/boot-definition/virtual-media* # set order 1
UCS-A /org/service-profile/boot-definition/virtual-media* # commit-buffer
UCS-A /org/service-profile/boot-definition/virtual-media #
```

Deleting a Boot Definition for a Service Profile

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org org-name | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope service-profile profile-name | Enters organization service profile mode for the specified service. |
| Step 3 | UCS-A /org/service-profile # delete boot-definition | Deletes the boot definition for the service profile. |
| Step 4 | UCS-A /org/service-profile # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the boot definition for a service profile and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope service-profile ServInst90
UCS-A /org/service-profile # delete boot-definition
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

Associating a Service Profile with a Server or Server Pool

Follow this procedure if you did not associate the service profile with a server or server pool when you created it, or to change the server or server pool with which a service profile is associated.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope service-profile <i>profile-name</i> | Enters organization service profile mode for the specified service profile. |
| Step 3 | UCS-A /org/service-profile # associate { server <i>chassis-id</i> <i>slot-id</i> server-pool <i>pool-name</i> <i>qualifier</i> } | Associates the service profile with a single server, or to the specified server pool with the specified server pool policy qualifications. |
| Step 4 | UCS-A /org/service-profile # commit-buffer | Commits the transaction to the system configuration. |

The following example associates the service profile named ServProf34 with the server in slot 4 of chassis 1 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServProf34
UCS-A /org/service-profile* # associate server 1/4
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

Disassociating a Service Profile from a Server or Server Pool

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope service-profile <i>profile-name</i> | Enters organization service profile mode for the specified service profile. |
| Step 3 | UCS-A /org/service-profile # disassociate | Disassociates the service profile from a server. |
| Step 4 | UCS-A /org/service-profile # commit-buffer | Commits the transaction to the system configuration. |

The following example disassociates the service profile named ServProf34 from the server to which it was associated and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServProf34
UCS-A /org/service-profile # disassociate
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

Resetting the UUID Assigned to a Service Profile from a Pool in a Service Profile Template

If you change the UUID suffix pool assigned to an updating service profile template, Cisco UCS Manager does not change the UUID assigned to a service profile created with that template. If you want Cisco UCS Manager to assign a UUID from the newly assigned pool to the service profile, and therefore to the associated server, you must reset the UUID. You can only reset the UUID assigned to a service profile and its associated server under the following circumstances:

- The service profile was created from an updating service profile template and includes a UUID assigned from a UUID suffix pool.
- The UUID suffix pool name is specified in the service profile. For example, the pool name is not empty.
- The UUID value is not 0, and is therefore not derived from the server hardware.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters the command mode for the organization for which you want to reset the UUID. If the system does not include multi-tenancy, type / as the <i>org-name</i> to enter the root organization. |
| Step 2 | UCS-A /org # scope service-profile <i>profile-name</i> | Enters the service profile that requires the UUID for the associated server to be reset to a different UUID suffix pool. |
| Step 3 | UCS-A /org/service-profile # set identity dynamic-uuid derived | Specifies that the service profile will obtain a UUID dynamically from a pool. |
| Step 4 | UCS-A /org/service-profile # commit-buffer | Commits the transaction to the system configuration. |

This example resets the UUID of a service profile to a different UUID suffix pool:

```
UCS-A# scope org /
UCS-A /org # scope service-profile ServInst90
UCS-A /org/service-profile # set identity dynamic-uuid derived
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

Resetting the MAC Address Assigned to a vNIC from a Pool in a Service Profile Template

If you change the MAC pool assigned to an updating service profile template, Cisco UCS Manager does not change the MAC address assigned to a service profile created with that template. If you want Cisco UCS Manager to assign a MAC address from the newly assigned pool to the service profile, and therefore to the associated server, you must reset the MAC address. You can only reset the MAC address assigned to a service profile and its associated server under the following circumstances:

- The service profile was created from an updating service profile template and includes a MAC address assigned from a MAC pool.
- The MAC pool name is specified in the service profile. For example, the pool name is not empty.
- The MAC address value is not 0, and is therefore not derived from the server hardware.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters the command mode for the organization that contains the service profile for which you want to reset the MAC address. If the system does not include multi-tenancy, type / as the <i>org-name</i> to enter the root organization. |
| Step 2 | UCS-A /org # scope service-profile <i>profile-name</i> | Enters the command mode for the service profile that requires the MAC address of the associated server to be reset to a different MAC address. |
| Step 3 | UCS-A /org/service-profile # scope vnic <i>vnic-name</i> | Enters the command mode for the vNIC for which you want to reset the MAC address. |
| Step 4 | UCS-A /org/service-profile/vnic # set identity dynamic-mac derived | Specifies that the vNIC will obtain a MAC address dynamically from a pool. |
| Step 5 | UCS-A /org/service-profile/vnic # commit-buffer | Commits the transaction to the system configuration. |

This example resets the MAC address of a vNIC in a service profile:

```
UCS-A# scope org /
UCS-A /org # scope service-profile ServInst90
UCS-A /org/service-profile # scope vnic dynamic-prot-001
UCS-A /org/service-profile/vnic # set identity dynamic-mac derived
UCS-A /org/service-profile/vnic* # commit-buffer
UCS-A /org/service-profile/vnic #
```

Resetting the WWPN Assigned to a vHBA from a Pool in a Service Profile Template

If you change the WWPN pool assigned to an updating service profile template, Cisco UCS Manager does not change the WWPN assigned to a service profile created with that template. If you want Cisco UCS Manager to assign a WWPN from the newly assigned pool to the service profile, and therefore to the associated server, you must reset the WWPN. You can only reset the WWPN assigned to a service profile and its associated server under the following circumstances:

- The service profile was created from an updating service profile template and includes a WWPN assigned from a WWPN pool.
- The WWPN pool name is specified in the service profile. For example, the pool name is not empty.
- The WWPN value is not 0, and is therefore not derived from the server hardware.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters the command mode for the organization that contains the service profile for which you want to reset the WWPN. If the system does not include multi-tenancy, type / as the <i>org-name</i> to enter the root organization. |
| Step 2 | UCS-A /org # scope service-profile <i>profile-name</i> | Enters the service profile of the vHBA for which you want to reset the WWPN. |
| Step 3 | UCS-A /org/service-profile # scope vhma <i>vhba-name</i> | Enters the command mode for vHBA for which you want to reset the WWPN. |
| Step 4 | UCS-A /org/service-profile/vhma # set identity dynamic-wwpn derived | Specifies that the vHBA will obtain a WWPN dynamically from a pool. |
| Step 5 | UCS-A /org/service-profile/vhma # commit-buffer | Commits the transaction to the system configuration. |

This example resets the WWPN of a vHBA in a service profile:

```
UCS-A# scope org /
UCS-A /org # scope service-profile ServInst90
UCS-A /org/service-profile # scope vhma vhma3
UCS-A /org/service-profile/vhma # set identity dynamic-wwpn derived
UCS-A /org/service-profile/vhma* # commit-buffer
UCS-A /org/service-profile/vhma #
```




CHAPTER 26

Configuring Server Power Usage

This chapter includes the following sections:

- [Server Power Usage, page 293](#)
- [Setting the Power Usage for a Server, page 293](#)
- [Viewing Server Power Usage, page 294](#)

Server Power Usage

You can set the level of power usage for each server in a Cisco UCS instance, as follows:

- | | |
|-----------------|---|
| Enabled | You can specify the maximum amount of power that the server can consume at one time. This maximum can be any amount between 0 watts and 1100 watts. |
| Disabled | No power usage limitations are imposed upon the server. The server can use as much power as it requires. |

If the server encounters a spike in power usage that meets or exceeds the maximum configured for the server, Cisco UCS Manager does not disconnect or shut down the server. Instead, Cisco UCS Manager reduces the power that is made available to the server. This reduction can slow down the server, including a reduction in CPU speed.

Setting the Power Usage for a Server

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope server <i>chassis-id/server-id</i> | Enters chassis server mode for the specified server. |
| Step 2 | UCS-A /chassis/server # set power-budget committed { disabled <i>watts</i> } | Commits the server to one of the following power usage levels: |

| | Command or Action | Purpose |
|---------------|--|---|
| | | <ul style="list-style-type: none"> • disabled—Does not impose any power usage limitations on the server. • watts—Allows you to specify the upper level for power usage by the server. If you choose this setting, enter the maximum number of watts that the server can use. The range is 100 to 1,100 watts. |
| Step 3 | UCS-A /chassis/server # commit-buffer | Commits the transaction to the system configuration. |
| Step 4 | UCS-A /chassis/server # show power-budget | (Optional) Displays the power usage level setting. |

The following example limits the power usage for a server to 1000 watts and commits the transaction:

```
UCS-A# scope server 2/4
UCS-A /chassis/server # set power-budget committed 1000
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server # show power-budget
Power Budget:
  Committed (W): 1100
  Oper Committed (W): Disabled
UCS-A /chassis/server #
```

Viewing Server Power Usage

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope server chassis-id/server-id | Enters chassis server mode for the specified server. |
| Step 2 | UCS-A /chassis/server # show stats mb-power-stats | Displays the power usage statistics collected for the server. |

The following example shows the server power usage:

```
UCS-A# scope server 2/4
UCS-A /chassis/server # show stats mb-power-stats

Mb Power Stats:
  Time Collected: 2010-04-15T21:18:04.992
  Monitored Object: sys/chassis-1/blade-2/board
  Suspect: No
  Consumed Power (W): 118.285194
  Input Voltage (V): 11.948000
  Input Current (A): 9.900000
  Thresholded: Input Voltage Min
UCS-A /chassis/server #
```



PART VI

VN-Link Configuration

- [Overview of VN-Link in Cisco UCS, page 297](#)
- [Configuring VN-Link Components and Connectivity, page 303](#)
- [Configuring Distributed Virtual Switches in Cisco UCS, page 311](#)
- [Configuring Port Profiles, page 323](#)
- [Configuring VN-Link Related Policies, page 331](#)
- [Managing Pending Deletions, page 333](#)



CHAPTER 27

Overview of VN-Link in Cisco UCS

This chapter includes the following sections:

- [Virtualization with a Virtual Interface Card Adapter, page 297](#)
- [Configuring Cisco UCS for VN-Link in Hardware, page 300](#)

Virtualization with a Virtual Interface Card Adapter

Virtual interface card (VIC) adapters support virtualized environments with VMware. These environments support the standard VMware integration with ESX installed on the server and all virtual machine management performed through the VMware vCenter.

This virtualized adapter supports the following:

- Dynamic vNICs in a virtualized environment with VM software, such as vSphere. This solution enables you to divide a single physical blade server into multiple logical PCIE instances.
- Static vNICs in a single operating system installed on a server.

With a VIC adapter, the solution you choose determines how communication works. This type of adapter supports the following communication solutions:

- Cisco VN-Link in hardware, which is a hardware-based method of handling traffic to and from a virtual machine. Details of how to configure this solution are available in this document.
- Cisco VN-Link in software, which is a software-based method of handling traffic to and from a virtual machine and uses the Nexus 1000v virtual switch. Details of how to configure this solution are available in the Nexus 1000v documentation.
- Single operating system installed on the server without virtualization, which uses the same methods of handling traffic as the other Cisco UCS adapters.

Cisco VN-Link

Cisco Virtual Network Link (VN-Link) is a set of features and capabilities that enable you to individually identify, configure, monitor, migrate, and diagnose virtual machine interfaces in a way that is consistent with the current network operation models for physical servers. VN-Link literally indicates the creation of a logical

link between a vNIC on a virtual machine and a Cisco UCS fabric interconnect. This mapping is the logical equivalent of using a cable to connect a NIC with a network port on an access-layer switch.

VN-Link in Hardware

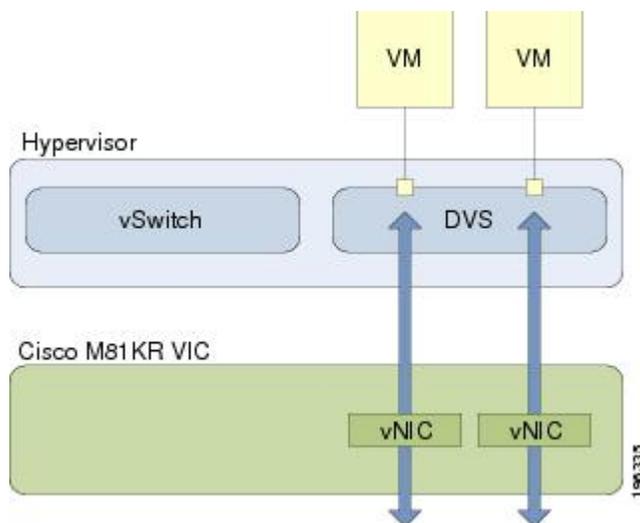
Cisco VN-Link in hardware is a hardware-based method of handling traffic to and from a virtual machine on a server with a VIC adapter. This method is sometimes referred to as pass-through switching. This solution replaces software-based switching with ASIC-based hardware switching and improves performance.

The distributed virtual switch (DVS) framework delivers VN-Link in hardware features and capabilities for virtual machines on Cisco UCS servers with VIC adapters. This approach provides an end-to-end network solution to meet the new requirements created by server virtualization.

With VN-Link in hardware, all traffic to and from a virtual machine passes through the DVS and the hypervisor, and then returns to the virtual machine on the server. Switching occurs in the fabric interconnect (hardware). As a result, network policies can be applied to traffic between virtual machines. This capability provides consistency between physical and virtual servers.

The following figure shows the traffic paths taken by VM traffic on a Cisco UCS server with a VIC adapter:

Figure 2: Traffic Paths for VM traffic with VN-Link in Hardware



Extension File for Communication with VMware vCenter

For Cisco UCS instances that use VIC adapters to implement VN-Link in hardware, you must create and install an extension file to establish the relationship and communications between Cisco UCS Manager and the VMware vCenter. This extension file is an XML file that contains vital information, including the following:

- Extension key
- Public SSL certificate

If you need to have two Cisco UCS instances share the same set of distributed virtual switches in a vCenter, you can create a custom extension key and import the same SSL certificate in the Cisco UCS Manager for each Cisco UCS instance.

Extension Key

The extension key includes the identity of the Cisco UCS instance. By default, this key has the value Cisco UCS GUID, as this value is identical across both fabric interconnects in a cluster configuration.

When you install the extension, vCenter uses the extension key to create a distributed virtual switch (DVS).

Public SSL Certificate

Cisco UCS Manager generates a default, self-signed SSL certificate to support communication with vCenter. You can also provide your own custom certificate.

Custom Extension Files

You can create a custom extension file for a Cisco UCS instance that does not use either or both of the default extension key or SSL certificate. For example, you can create the same custom key in two different Cisco UCS instances when they are managed by the same VMware vCenter instance.

**Important**

You cannot change an extension key that is being used by a DVS or vCenter. If you want to use a custom extension key, we recommend that you create and register the custom key before you create the DVS in Cisco UCS Manager to avoid any possibility of having to delete and recreate the associated DVS.

Distributed Virtual Switches

Each VMware ESX host has its own software-based virtual switch (vSwitch) in its hypervisor that performs the switching operations between its virtual machines (VMs). The Cisco UCS distributed virtual switch (DVS) is a software-based virtual switch that runs alongside the vSwitch in the ESX hypervisor, and can be distributed across multiple ESX hosts. Unlike vSwitch, which uses its own local port configuration, a DVS associated with multiple ESX hosts uses the same port configuration across all ESX hosts.

After associating an ESX host to a DVS, you can migrate existing VMs from the vSwitch to the DVS, and you can create VMs to use the DVS instead of the vSwitch. With the hardware-based VN-Link implementation, when a VM uses the DVS, all VM traffic passes through the DVS and ASIC-based switching is performed by the fabric interconnect.

In Cisco UCS Manager, DVSES are organized in the following hierarchy:

```
vCenter
  Folder (optional)
    Datacenter
      Folder (required)
        DVS
```

At the top of the hierarchy is the vCenter, which represents a VMware vCenter instance. Each vCenter contains one or more datacenters, and optionally vCenter folders with which you can organize the datacenters. Each datacenter contains one or more required datacenter folders. Datacenter folders contain the DVSES.

Port Profiles

Port profiles contain the properties and settings used to configure virtual interfaces in Cisco UCS for VN-Link in hardware. The port profiles are created and administered in Cisco UCS Manager. There is no clear visibility into the properties of a port profile from VMware vCenter.

In VMware vCenter, a port profile is represented as a port group. Cisco UCS Manager pushes the port profile names to vCenter, which displays the names as port groups. None of the specific networking properties or settings in the port profile are visible in VMware vCenter.

After a port profile is created, assigned to, and actively used by one or more DVSEs, any changes made to the networking properties of the port profile in Cisco UCS Manager are immediately applied to those DVSEs.

You must configure at least one port profile client for a port profile, if you want Cisco UCS Manager to push the port profile to VMware vCenter.

Port Profile Clients

The port profile client determines the DVSEs to which a port profile is applied. By default, the port profile client specifies that the associated port profile applies to all DVSEs in the vCenter. However, you can configure the client to apply the port profile to all DVSEs in a specific datacenter or datacenter folder, or only to one DVS.

VN-Link in Hardware Considerations

How you configure a Cisco UCS instance for VN-Link in hardware has several dependencies. The information you need to consider before you configure VN-Link in hardware includes the following:

- A Cisco UCS instance can have a maximum of 4 vCenters
- Each vCenter can have a maximum of 8 distributed virtual switches
- Each distributed virtual switch can have a maximum of 4096 ports
- Each port profile can have a maximum of 4096 ports
- Each Cisco UCS instance can have a maximum of 256 port profiles

Configuring Cisco UCS for VN-Link in Hardware

You must perform some of the following high-level steps in the VMware Virtual Center (vCenter). For more information about those steps, see the VMware documentation.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | Configure the VN-Link components and connectivity. | For more information, see the following chapter: Configuring VN-Link Components and Connectivity , page 303. |
| Step 2 | In VMware vCenter, create a vCenter and datacenter. | For more information, see the VMware documentation. |
| Step 3 | In Cisco UCS Manager create distributed virtual switches. | To create a distributed virtual switch (DVS), you must first create a vCenter, a datacenter under the vCenter, and a datacenter folder under the datacenter. You can then create a DVS in the datacenter folder. The vCenter name you specify in Cisco UCS Manager does not need to match the vCenter name specified in VMware vCenter; however, the datacenter name you specify in Cisco UCS Manager must match the |

| | Command or Action | Purpose |
|---------------|---|---|
| | | datacenter name specified in VMware vCenter. The datacenter folder and DVS you create in Cisco UCS Manager are pushed to VMware vCenter. For more information, see the following chapter: Configuring Distributed Virtual Switches in Cisco UCS , page 311. |
| Step 4 | In Cisco UCS Manager, create the port profile and profile clients. | The port profiles are pushed to their clients in VMware vCenter. They appear in VMware vCenter as port groups, not port profiles. For more information, see the following chapter: Configuring Port Profiles , page 323. |
| Step 5 | In VMware vCenter, add an ESX host to the DVS. | Configure the ESX host with the option to migrate to PTS/DVS. |
| Step 6 | In vCenter, create the virtual machines required for the VMs on the server. | As part of this configuration, ensure you select the port profiles (port groups) configured in Cisco UCS Manager. |



CHAPTER 28

Configuring VN-Link Components and Connectivity

This chapter includes the following sections:

- [Components of VN-Link in Hardware, page 303](#)
- [Configuring a VMware ESX Host for VN-Link, page 304](#)
- [Configuring a VMware vCenter Instance for VN-Link, page 305](#)
- [Configuring a Certificate for VN-Link in Hardware, page 306](#)
- [Connecting Cisco UCS Manager to VMware vCenter Using the Extension Key, page 308](#)

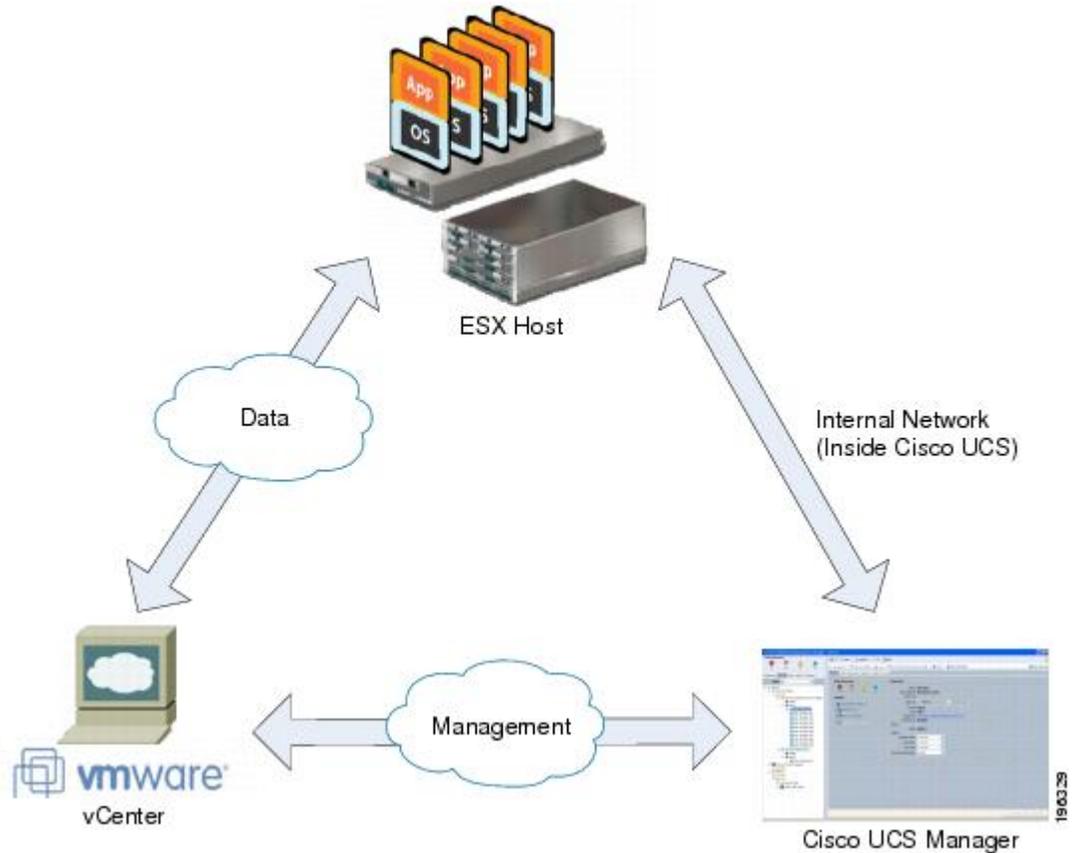
Components of VN-Link in Hardware

The following three main components must be connected for VN-Link in hardware to work:

- VMware ESX Host** A server with the VMware ESX installed. It contains a datastore and the virtual machines. The ESX host must have a Cisco M81KR VIC installed, and it must have uplink data connectivity to the network for communication with VMware vCenter.
- VMware vCenter** Windows-based software used to manage one or more ESX hosts. VMware vCenter must have connectivity to the UCS management port for management plane integration, and uplink data connectivity to the network for communication with the ESX Host. A vCenter extension key provided by Cisco UCS Manager must be registered with VMware vCenter before the Cisco UCS instance can be acknowledged.
- Cisco UCS Manager** The Cisco UCS management software that integrates with VMware vCenter to handle some of the network-based management tasks. Cisco UCS Manager must have management port connectivity to VMware vCenter for management plane integration. It also provides a vCenter extension key that represents the Cisco UCS identity. The extension key must be registered with VMware vCenter before the Cisco UCS instance can be acknowledged.

The following figure shows the three main components of VN-Link in hardware and the methods by which they are connected:

Figure 3: Component Connectivity for VN-Link in Hardware



Configuring a VMware ESX Host for VN-Link

Before You Begin

Ensure that Virtualization Technology is enabled in BIOS of the UCS server if you intend to run 64-bit VMs on the ESX host. An ESX host will not run 64-bit VMs unless Virtualization Technology is enabled.

Procedure

-
- Step 1** If not already present, install a Cisco M81KR VIC in the server you intend to use as the VMware ESX host. For more information about installing a Cisco M81KR VIC, see the *Cisco UCS 5108 Server Chassis Hardware Installation Guide*.
- Step 2** Configure and associate a service profile to the server. The service profile configuration must include the following:

- A Dynamic vNIC Connection policy that determines how the VN-link connectivity between VMs and dynamic vNICs is configured.
- Two static vNICs for each adapter on the ESX host. For ESX hosts with multiple adapters, your service profile must use either vCons or have an associated vNIC/vHBA placement profile that ensures the static vNICs are assigned to the appropriate adapters.

For more information, see the following chapter: [Configuring Service Profiles, page 271](#).

- Step 3** Install VMware ESX 4.0 or later on the blade server. No additional drivers are required during the installation.
-

Configuring a VMware vCenter Instance for VN-Link

Procedure

- Step 1** Configure a Windows-based machine to use a static IP address. Take note of the IP address. You will use it to connect to vCenter Server.
The Windows-based machine must have network connectivity to the Cisco UCS management port and to the uplink Ethernet port(s) being used by the ESX host. The management port connectivity is used for management plane integration between VMware vCenter and Cisco UCS Manager; the uplink Ethernet port connectivity is used for communication between VMware vCenter and the ESX host.
- Step 2** Install VMware vCenter (vCenter Server and vSphere Client 4.0 or later) on the Windows-based machine.
- Step 3** Launch vSphere Client.
- Step 4** On the vSphere Client launch page, enter the following information to connect to vCenter Server:
- a) Static IP address of the Windows-based machine.
 - b) Username and password specified while installing vCenter Server. If, during the vCenter Server installation, you chose to use the Windows logon credentials, you can check the **Use Windows session credentials** check box.
- Step 5** If a Security Warning dialog box appears, click **Ignore**.
-

What to Do Next

Do one of the following:

- (Optional) If you plan to use a custom certificate for VN-Link in hardware, configure the certificate for VN-Link in hardware.
- Connect Cisco UCS Manager to VMware vCenter using the extension key.

Configuring a Certificate for VN-Link in Hardware

Certificate for VN-Link in Hardware

Cisco UCS Manager generates a default, self-signed SSL certificate to support communication with vCenter. You can also create your own custom certificate to communicate with multiple vCenter instances. When you create a custom certificate, Cisco UCS Manager recreates the extension files to include the new certificate. If you subsequently delete the custom certificate, Cisco UCS Manager recreates the extension files to include the default, self-signed SSL certificate.

To create a custom certificate, you must obtain and copy an external certificate into Cisco UCS, and then create a certificate for VN-Link in hardware that uses the certificate you copied into Cisco UCS.

Copying a Certificate to the Fabric Interconnect

Before You Begin

Obtain a certificate.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# connect local-mgmt | Enters local management mode. |
| Step 2 | UCS-A(local-mgmt)# copy <i>from-filesystem:[from-path]filename</i> <i>to-filesystem:[to-path]filename</i> | <p>Copies the certificate from its source location to its destination location. For the <i>from-filesystem:</i> argument, use one of the following syntax:</p> <ul style="list-style-type: none"> • ftp://server-ip-addr • scp://username@server-ip-addr • sftp://username@server-ip-addr • tftp://server-ip-addr :port-num <p>For the <i>to-filesystem:</i> argument, use one of the following syntax:</p> <ul style="list-style-type: none"> • Volatile: • Workspace: |

The following example uses FTP to copy a certificate (certificate.txt) to the temp folder in the workspace:

```
UCS-A # connect local-mgmt
Cisco UCS 6100 Series Fabric Interconnect
```

```
TAC support: http://www.cisco.com/tac
```

```
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
```

```
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
```

Some parts of this software may be covered under the GNU Public License or the GNU Lesser General Public License. A copy of each such license is available at <http://www.gnu.org/licenses/gpl.html> and <http://www.gnu.org/licenses/lgpl.html>

```
UCS-A(local-mgmt) # copy ftp://192.168.10.10/certs/certificate.txt
workspace:/temp/certificate.txt
UCS-A(local-mgmt) #
```

What to Do Next

Create a certificate for VN-Link in hardware.

Creating a Certificate for VN-Link in Hardware

Before You Begin

Copy a certificate to the fabric interconnect.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt/vmware # scope cert-store | Enters system VM management VMware certificate store mode. |
| Step 5 | UCS-A /system/vm-mgmt/vmware/cert-store # create certificate certificate-name | Creates the specified certificate for VN-Link in hardware and enters system VM management VMware certificate store certificate mode. |
| Step 6 | UCS-A /system/vm-mgmt/vmware/cert-store/certificate # set location {volatile workspace} path path certfile file-name | Specifies the location and filename of an existing certificate to use as the certificate for VN-Link in hardware. |
| Step 7 | UCS-A /system/vm-mgmt/vmware/cert-store/certificate # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a certificate for VN-Link in hardware, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope cert-store
UCS-A /system/vm-mgmt/vmware/cert-store # create certificate VnLinkCertificate
UCS-A /system/vm-mgmt/vmware/cert-store/certificate* # set location workspace path /temp
certfile certificate.txt
UCS-A /system/vm-mgmt/vmware/cert-store/certificate* # commit-buffer
UCS-A /system/vm-mgmt/vmware/cert-store/certificate #
```

Deleting a Certificate for VN-Link in Hardware

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt /vmware # scope cert-store | Enters system VM management VMware certificate store mode. |
| Step 5 | UCS-A /system/vm-mgmt /vmware/cert-store # delete certificate certificate-name | Deletes the specified certificate for VN-Link in hardware. |
| Step 6 | UCS-A /system/vm-mgmt /vmware/cert-store # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes a certificate for VN-Link in hardware, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope cert-store
UCS-A /system/vm-mgmt/vmware/cert-store # delete certificate VnLinkCertificate
UCS-A /system/vm-mgmt/vmware/cert-store* # commit-buffer
UCS-A /system/vm-mgmt/vmware/cert-store #
```

Connecting Cisco UCS Manager to VMware vCenter Using the Extension Key

(Optional) Modifying the vCenter Extension Key

You can modify the vCenter extension key for the following reasons:

- To provide better system identification, you can name the vCenter extension key something more meaningful than the default ID string.
- If two Cisco UCS instances want to connect to the same VMware vCenter instance, they must use the same extension key and certificate.

Procedure

-
- Step 1** In the **Navigation** pane, click the **VM** tab.
- Step 2** On the **VM** tab, expand the **All** node.
- Step 3** On the **VM** tab, click **VMWare**.
- Step 4** In the **Work** pane, click the **General** tab.
- Step 5** In the **Actions** area, click **Modify Extension Key**.
- Step 6** In the **Modify Extension Key** dialog box, do the following:
- In the **Key** field, modify the key as needed.
A vCenter extension key can have a maximum length of 33 characters. These characters can be letters, numbers, or hyphens. No other characters or spaces are permitted in the extension key.
 - Click **OK**.
-

What to Do Next

Export the vCenter extension file or files from Cisco UCS Manager.

Exporting a vCenter Extension File from Cisco UCS Manager

Depending on the version of VMware vCenter you are using, you can either generate one extension file or a set of nine extension files.

Procedure

-
- Step 1** In the **Navigation** pane, click the **VM** tab.
- Step 2** On the **VM** tab, expand the **All** node.
- Step 3** On the **VM** tab, click **VMWare**.
- Step 4** In the **Work** pane, click the **General** tab.
- Step 5** In the **Actions** area, click one of the following links:

| Option | Description |
|---|---|
| Export vCenter Extension | For vCenter version 4.0 update 1 and later. |
| Export Multiple vCenter Extensions | For vCenter version 4.0. |

- Step 6** In the **Export vCenter Extension** dialog box, do the following:
- In the **Save Location** field, enter the path to the directory where you want to save the extension file or files.
If you do not know the path, click the **...** button and browse to the location.
 - Click **OK**.
Cisco UCS Manager generates the extension file(s) and saves them to the specified location.
-

What to Do Next

Register the vCenter extension file or files in VMware vCenter.

Registering a vCenter Extension File in VMware vCenter

In VMware vCenter, the vCenter extension files are called plug-ins.

Before You Begin

Export the vCenter extension file(s) from Cisco UCS Manager. Ensure that the exported vCenter extension files are saved to a location that can be reached by VMware vCenter.

Procedure

- Step 1** In VMware vCenter, choose **Plug-ins** ► **Manage Plug-ins**.
 - Step 2** Right-click any empty space below the Available Plug-ins section of the **Plug-in Manager** dialog box and click **New Plug-in**.
 - Step 3** Click **Browse** and navigate to the location where the vCenter extension file(s) are saved.
 - Step 4** Choose a vCenter extension file and click **Open**.
 - Step 5** Click **Register Plug-in**.
 - Step 6** If the **Security Warning** dialog box appears, click **Ignore**.
 - Step 7** Click **OK**.
The vCenter extension file registers as an available VMware vCenter plug-in. You do not need to install the plug-in, leave it in the available state. If you are registering multiple vCenter extension files, repeat this procedure until all files are registered.
-



CHAPTER 29

Configuring Distributed Virtual Switches in Cisco UCS

This chapter includes the following sections:

- [Distributed Virtual Switches](#), page 311
- [Configuring a Distributed Virtual Switch](#), page 312
- [Managing Distributed Virtual Switches](#), page 313

Distributed Virtual Switches

Each VMware ESX host has its own software-based virtual switch (vSwitch) in its hypervisor that performs the switching operations between its virtual machines (VMs). The Cisco UCS distributed virtual switch (DVS) is a software-based virtual switch that runs alongside the vSwitch in the ESX hypervisor, and can be distributed across multiple ESX hosts. Unlike vSwitch, which uses its own local port configuration, a DVS associated with multiple ESX hosts uses the same port configuration across all ESX hosts.

After associating an ESX host to a DVS, you can migrate existing VMs from the vSwitch to the DVS, and you can create VMs to use the DVS instead of the vSwitch. With the hardware-based VN-Link implementation, when a VM uses the DVS, all VM traffic passes through the DVS and ASIC-based switching is performed by the fabric interconnect.

In Cisco UCS Manager, DVSES are organized in the following hierarchy:

```
vCenter
  Folder (optional)
    Datacenter
      Folder (required)
        DVS
```

At the top of the hierarchy is the vCenter, which represents a VMware vCenter instance. Each vCenter contains one or more datacenters, and optionally vCenter folders with which you can organize the datacenters. Each datacenter contains one or more required datacenter folders. Datacenter folders contain the DVSES.

Configuring a Distributed Virtual Switch

Before You Begin

You must first create a datacenter in VMware vCenter. Do not create the folder inside the datacenter or the DVS in VMware vCenter.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt /vmware # create vcenter vcenter-name | Creates the specified vCenter and enters system VM management VMware vCenter mode. |
| Step 5 | UCS-A /system/vm-mgmt /vmware/vcenter # set hostname {hostname ip-addr} | Specifies the hostname or IP address of the remote vCenter Server instance associated to the vCenter object in Cisco UCS Manager. Note If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager. |
| Step 6 | UCS-A /system/vm-mgmt /vmware/vcenter # set description description | Provides a description for the vCenter. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 7 | UCS-A /system/vm-mgmt /vmware/vcenter # create folder folder-name | (Optional) Creates the specified vCenter folder. Note A vCenter can contain multiple datacenters, none of which must be contained in a vCenter folder, so the use of vCenter folders are optionally used only for organizational purposes. |
| Step 8 | UCS-A /system/vm-mgmt /vmware/vcenter/ # create data-center data-center-name | Creates the specified datacenter and enters system VM management VMware vCenter datacenter mode. The datacenter name that you specify in Cisco UCS Manager must exactly match the name of the datacenter previously created in VMware vCenter. |
| Step 9 | UCS-A /system/vm-mgmt /vmware/vcenter/data-center # create folder folder-name | Creates the specified datacenter folder and enters system VM management VMware vCenter datacenter folder mode. |

| | Command or Action | Purpose |
|----------------|---|---|
| | | Note At least one datacenter folder is required. You cannot create a distributed virtual switch (DVS) directly under a datacenter; you must create the DVS in a datacenter folder. |
| Step 10 | UCS-A /system/vm-mgmt /vmware/vcenter/data-center/folder # create distributed-virtual-switch <i>dvs-name</i> | Creates the specified DVS and enters system VM management VMware vCenter datacenter folder distributed virtual switch mode. |
| Step 11 | UCS-A /system/vm-mgmt /vmware/vcenter/data-center /folder/distributed-virtual-switch # { disable enable } | Disables or enables the DVS. If you disable the DVS, Cisco UCS Manager does not push any configuration changes related to the DVS to VMware vCenter. |
| Step 12 | UCS-A /system/vm-mgmt /vmware/vcenter/data-center/folder /distributed-virtual-switch # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a vCenter, a datacenter with the exact same name as the datacenter in VMware vCenter, a DVS in the datacenter folder named Engineering, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # create vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter* # set hostname 192.168.10.10
UCS-A /system/vm-mgmt/vmware/vcenter* # set description "vCenter running on my laptop"
UCS-A /system/vm-mgmt/vmware/vcenter* # create data-center MyDatacenter
UCS-A /system/vm-mgmt/vmware/vcenter/data-center* # create folder Engineering
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder* # create distributed-virtual-switch LabSwitch
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder/distributed-virtual-switch* # enable
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder/distributed-virtual-switch* # commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder/distributed-virtual-switch #
```

Managing Distributed Virtual Switches

Adding a Folder to a vCenter

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 4 | UCS-A /system/vm-mgmt /vmware # scope vcenter vcenter-name | Enters system VM management VMware vCenter mode for the specified vCenter. |
| Step 5 | UCS-A /system/vm-mgmt /vmware/vcenter # create folder folder-name | (Optional) Creates the specified vCenter folder and enters system VM management VMware vCenter folder mode. Note A vCenter can contain multiple datacenters, none of which must be contained in a vCenter folder, so the use of vCenter folders are optionally used only for organizational purposes. |
| Step 6 | UCS-A /system/vm-mgmt /vmware/vcenter/folder # commit-buffer | Commits the transaction to the system configuration. |

The following example adds a vCenter folder named Lab 5 to the vCenter named MyVcenter and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter* # create folder Lab5
UCS-A /system/vm-mgmt/vmware/vcenter/folder* # commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter/folder #
```

Deleting a Folder from a vCenter

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt /vmware # scope vcenter vcenter-name | Enters system VM management VMware vCenter mode for the specified vCenter. |
| Step 5 | UCS-A /system/vm-mgmt /vmware/vcenter # delete folder folder-name | (Optional) Deletes the specified vCenter folder. |
| Step 6 | UCS-A /system/vm-mgmt /vmware/vcenter # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the vCenter folder named Lab5 from the vCenter named MyVcenter and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
```

```
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter # delete folder Lab5
UCS-A /system/vm-mgmt/vmware/vcenter* # commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter #
```

Adding a Datacenter to a vCenter

Before You Begin

You must first create a datacenter in VMware vCenter. Do not create the folder inside the datacenter or the DVS in VMware vCenter.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt/vmware # scope vcenter vcenter-name | Enters system VM management VMware vCenter mode for the specified vCenter. |
| Step 5 | UCS-A /system/vm-mgmt/vmware/vcenter # scope folder folder-name | (Optional) Enters system VM management VMware vCenter folder mode for the specified folder. |
| Step 6 | UCS-A /system/vm-mgmt/vmware/vcenter/ # create data-center data-center-name | Creates the specified datacenter and enters system VM management VMware vCenter datacenter mode. The datacenter name that you specify in Cisco UCS Manager must exactly match the name of the datacenter previously created in VMware vCenter. |
| Step 7 | UCS-A /system/vm-mgmt/vmware/vcenter/data-center # commit-buffer | Commits the transaction to the system configuration. |

The following example adds a datacenter named SQA-Datacenter to the vCenter named MyVcenter and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter* # create data-center SQA-Datacenter
UCS-A /system/vm-mgmt/vmware/vcenter/data-center* # commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter/data-center #
```

Deleting a Datacenter from vCenter

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt/vmware # scope vcenter vcenter-name | Enters system VM management VMware vCenter mode for the specified vCenter. |
| Step 5 | UCS-A /system/vm-mgmt/vmware/vcenter # scope folder folder-name | (Optional) Enters system VM management VMware vCenter folder mode for the specified folder. |
| Step 6 | UCS-A /system/vm-mgmt/vmware/vcenter/ # delete data-center data-center-name | Deletes the specified datacenter. The datacenter name that you specify in Cisco UCS Manager must exactly match the name of a datacenter previously created in vCenter Server. |
| Step 7 | UCS-A /system/vm-mgmt/vmware/vcenter # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the datacenter named SQA-Datacenter from the vCenter named MyVcenter and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter* # delete data-center SQA-Datacenter
UCS-A /system/vm-mgmt/vmware/vcenter* # commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter #
```

Adding a Folder to a Datacenter

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt/vmware # scope vcenter vcenter-name | Enters system VM management VMware vCenter mode for the specified vCenter. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 5 | UCS-A /system/vm-mgmt /vmware/vcenter # scope folder <i>folder-name</i> | (Optional) Enters system VM management VMware vCenter folder mode for the specified folder. |
| Step 6 | UCS-A /system/vm-mgmt /vmware/vcenter/ # scope data-center <i>data-center-name</i> | Enters system VM management VMware vCenter datacenter mode for the specified datacenter. |
| Step 7 | UCS-A /system/vm-mgmt /vmware/vcenter/data-center # create folder <i>folder-name</i> | Creates the specified datacenter folder and enters system VM management VMware vCenter datacenter folder mode. |
| Step 8 | UCS-A /system/vm-mgmt /vmware/vcenter/data-center/folder # commit-buffer | Commits the transaction to the system configuration. |

The following example adds a datacenter folder named SoftwareQA to the datacenter named MyDatacenter and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter* # scope data-center MyDatacenter
UCS-A /system/vm-mgmt/vmware/vcenter/data-center* # create folder SoftwareQA
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder* # commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder #
```

Deleting a Folder from a Datacenter

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt /vmware # scope vcenter <i>vcenter-name</i> | Enters system VM management VMware vCenter mode for the specified vCenter. |
| Step 5 | UCS-A /system/vm-mgmt /vmware/vcenter # scope folder <i>folder-name</i> | (Optional) Enters system VM management VMware vCenter folder mode for the specified folder. |
| Step 6 | UCS-A /system/vm-mgmt /vmware/vcenter/ # scope data-center <i>data-center-name</i> | Enters system VM management VMware vCenter datacenter mode for the specified datacenter. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 7 | UCS-A /system/vm-mgmt /vmware/vcenter/data-center # delete folder <i>folder-name</i> | Deletes the specified datacenter folder. |
| Step 8 | UCS-A /system/vm-mgmt /vmware/vcenter/data-center # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the datacenter folder named SoftwareQA from the datacenter named MyDatacenter and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter # scope data-center MyDatacenter
UCS-A /system/vm-mgmt/vmware/vcenter/data-center # delete folder SoftwareQA
UCS-A /system/vm-mgmt/vmware/vcenter/data-center* # commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter/data-center #
```

Adding a Distributed Virtual Switch to a Datacenter Folder

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt/vmware # scope vcenter <i>vcenter-name</i> | Enters system VM management VMware vCenter mode for the specified vCenter. |
| Step 5 | UCS-A /system/vm-mgmt/vmware/vcenter # scope folder <i>folder-name</i> | (Optional) Enters system VM management |

| | Command or Action | Purpose |
|----------------|--|---|
| | | VMware vCenter folder mode for the specified folder. |
| Step 6 | UCS-A /system/vm-mgmt/vmware/vcenter/ # scope data-center <i>data-center-name</i> | Enters system VM management VMware vCenter datacenter mode for the specified datacenter. |
| Step 7 | UCS-A /system/vm-mgmt/vmware/vcenter/data-center # scope folder <i>folder-name</i> | Enters system VM management VMware vCenter datacenter folder mode for the specified datacenter folder. |
| Step 8 | UCS-A /system/vm-mgmt/vmware/vcenter/folder/data-center/folder # create distributed-virtual-switch <i>dvs-name</i> | Creates the specified DVS and enters system VM management VMware vCenter datacenter folder distributed virtual switch mode. |
| Step 9 | UCS-A /system/vm-mgmt/vmware/vcenter/folder/data-center/folder/distributed-virtual-switch # { disable enable } | Disables or enables the DVS. |
| Step 10 | UCS-A /system/vm-mgmt/vmware/vcenter/folder/data-center/folder/distributed-virtual-switch # commit-buffer | Commits the transaction to |

| | Command or Action | Purpose |
|--|-------------------|---------------------------|
| | | the system configuration. |

The following example adds a DVS named TestSwitch to the datacenter folder named Engineering, enables the DVS, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter* # scope data-center MyDatacenter
UCS-A /system/vm-mgmt/vmware/vcenter/data-center* # scope folder Engineering
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder* # create distributed-virtual-switch
TestSwitch
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder/distributed-virtual-switch* # enable
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder/distributed-virtual-switch* #
commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder/distributed-virtual-switch #
```

Deleting a Distributed Virtual Switch from a Datacenter Folder

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt/vmware # scope vcenter <i>vcenter-name</i> | Enters system VM management VMware vCenter mode for the specified vCenter. |
| Step 5 | UCS-A /system/vm-mgmt/vmware/vcenter # scope folder <i>folder-name</i> | (Optional) Enters system VM management VMware vCenter folder mode for the specified folder. |
| Step 6 | UCS-A /system/vm-mgmt/vmware/vcenter/ # scope data-center <i>data-center-name</i> | Enters system VM management VMware vCenter datacenter mode for the specified datacenter. |
| Step 7 | UCS-A /system/vm-mgmt/vmware/vcenter/data-center # scope folder <i>folder-name</i> | Enters system VM management VMware vCenter datacenter folder mode for the specified datacenter folder. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 8 | UCS-A /system/vm-mgmt/vmware/vcenter/folder/data-center/folder # delete distributed-virtual-switch <i>dvs-name</i> | Deletes the specified DVS. |
| Step 9 | UCS-A /system/vm-mgmt/vmware/vcenter/folder/data-center/folder # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the DVS named TestSwitch from the datacenter folder named Engineering and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope vcenter MyVcenter
UCS-A /system/vm-mgmt/vmware/vcenter* # scope data-center MyDatacenter
UCS-A /system/vm-mgmt/vmware/vcenter/data-center* # scope folder Engineering
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder* # delete distributed-virtual-switch
TestSwitch
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder* # commit-buffer
UCS-A /system/vm-mgmt/vmware/vcenter/data-center/folder #
```




CHAPTER 30

Configuring Port Profiles

This chapter includes the following sections:

- [Port Profiles, page 323](#)
- [Port Profile Clients, page 323](#)
- [Configuring a Port Profile, page 324](#)
- [Deleting a Port Profile, page 326](#)
- [Adding a Named VLAN to a Port Profile, page 326](#)
- [Deleting a Named VLAN from a Port Profile, page 327](#)
- [Adding a Port Profile Client to a Port Profile, page 328](#)
- [Deleting a Port Profile Client from a Port Profile, page 329](#)

Port Profiles

Port profiles contain the properties and settings used to configure virtual interfaces in Cisco UCS for VN-Link in hardware. The port profiles are created and administered in Cisco UCS Manager. There is no clear visibility into the properties of a port profile from VMware vCenter.

In VMware vCenter, a port profile is represented as a port group. Cisco UCS Manager pushes the port profile names to vCenter, which displays the names as port groups. None of the specific networking properties or settings in the port profile are visible in VMware vCenter.

After a port profile is created, assigned to, and actively used by one or more DVSEs, any changes made to the networking properties of the port profile in Cisco UCS Manager are immediately applied to those DVSEs.

You must configure at least one port profile client for a port profile, if you want Cisco UCS Manager to push the port profile to VMware vCenter.

Port Profile Clients

The port profile client determines the DVSEs to which a port profile is applied. By default, the port profile client specifies that the associated port profile applies to all DVSEs in the vCenter. However, you can configure

the client to apply the port profile to all DVSes in a specific datacenter or datacenter folder, or only to one DVS.

Configuring a Port Profile

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt/vmware # scope profile-set | Enters system VM management VMware profile set mode. |
| Step 5 | UCS-A /system/vm-mgmt/vmware/profile-set # create port-profile <i>profile-name</i> | Creates the specified port profile and enters system VM management VMware profile set port profile mode. |
| Step 6 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # set descr <i>description</i> | (Optional) Provides a description for the port profile. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 7 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # set max-ports <i>max-num</i> | Specifies the maximum number of ports the port profile can use. The maximum number of ports that can be associated with a single distributed virtual switch (DVS) is 4096. If the DVS has only one associated port profile, that port profile can be configured with up to 4096 ports. However, if the DVS has more than one associated port profile, the total number of ports associated with all of those port profiles combined cannot exceed 4096. |
| Step 8 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # set nw-control-policy <i>policy-name</i> | Specifies the network control policy to use for the port profile. |

| | Command or Action | Purpose |
|----------------|--|---|
| Step 9 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # set pin-group <i>group-name</i> | Specifies the LAN pin group to use for the port profile. |
| Step 10 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # set qos-policy <i>policy-name</i> | Specifies the QoS policy to use for the port profile. |
| Step 11 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # create client <i>client-name</i> | Creates the specified port profile client and enters system VM management VMware profile set port profile client mode. |
| Step 12 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client # set descr <i>description</i> | (Optional) Provides a description for the port profile client. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 13 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client # set data-center <i>data-center-name</i> | (Optional) Specifies the datacenter to which the port profile is applied. |
| Step 14 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client # set folder <i>folder-name</i> | (Optional) Specifies the datacenter folder to which the port profile is applied. |
| Step 15 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client # set dvs <i>folder-name</i> | (Optional) Specifies the DVS to which the port profile is applied. |
| Step 16 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client # commit-buffer | Commits the transaction. |

The following example creates a port profile client named MyClient that applies the port profile to all DVSes in the datacenter named MyDatacenter and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope profile-set
UCS-A /system/vm-mgmt/vmware/profile-set # create port-profile MyProfile
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # set descr "This is my port profile"
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # set max-ports 24
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # set nw-control-policy ncp5
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # set pin-group PinGroup54
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # set qos-policy QosPolicy34
```

```

UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # create client MyClient
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client* # set descr "This is the
client for my port profile"
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client* # set data-center MyDatacenter
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client* # commit-buffer
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client #

```

Deleting a Port Profile

You cannot delete a port profile if a VM is actively using that port profile.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt/vmware # scope profile-set | Enters system VM management VMware profile set mode. |
| Step 5 | UCS-A /system/vm-mgmt/vmware/profile-set # delete port-profile profile-name | Deletes the specified port profile. |
| Step 6 | UCS-A /system/vm-mgmt/vmware/profile-set # commit-buffer | Commits the transaction. Cisco UCS Manager deletes the port profile and all associated port profile clients. |

The following example deletes the port profile named MyProfile and commits the transaction:

```

UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope profile-set
UCS-A /system/vm-mgmt/vmware/profile-set # delete port-profile MyProfile
UCS-A /system/vm-mgmt/vmware/profile-set* # commit-buffer
UCS-A /system/vm-mgmt/vmware/profile-set #

```

Adding a Named VLAN to a Port Profile

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 4 | UCS-A /system/vm-mgmt/vmware # scope profile-set | Enters system VM management VMware profile set mode. |
| Step 5 | UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile <i>profile-name</i> | Enters system VM management VMware profile set port profile mode for the specified port profile. |
| Step 6 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # create vlan <i>vlan-name</i> | Specifies a named VLAN to use for the port profile. |
| Step 7 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/vlan # set native no | (Optional) Sets the named VLAN as a non-native VLAN. |
| Step 8 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/vlan # commit-buffer | Commits the transaction. |

The following example adds the VLAN named accounting to the port profile named MyProfile, sets the VLAN as non-native, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware# scope profile-set
UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile MyProfile
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # create vlan accounting
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/vlan* # set native no
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/vlan* # commit-buffer
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/vlan #
```

Deleting a Named VLAN from a Port Profile

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt/vmware # scope profile-set | Enters system VM management VMware profile set mode. |
| Step 5 | UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile <i>profile-name</i> | Enters system VM management VMware profile set port profile mode for the specified port profile. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 6 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # delete vlan <i>vlan-name</i> | Deletes the specified named VLAN from the port profile. |
| Step 7 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # commit-buffer | Commits the transaction. |

The following example deletes the VLAN named accounting from the port profile named MyProfile and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware# scope profile-set
UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile MyProfile
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # delete vlan accounting
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # commit-buffer
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile #
```

Adding a Port Profile Client to a Port Profile

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt/vmware # scope profile-set | Enters system VM management VMware profile set mode. |
| Step 5 | UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile <i>profile-name</i> | Enters system VM management VMware profile set port profile mode for the specified port profile. |
| Step 6 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # create client <i>client-name</i> | Creates the specified port profile client and enters system VM management VMware profile set port profile client mode. The port profile client determines the DVSEs to which the port profile is applied. By default, a port profile applies to all DVSEs in the vCenter; however, you can use the optional set data-center , set folder , and set dvs commands to apply the port profile to all DVSEs in a |

| | Command or Action | Purpose |
|----------------|---|---|
| | | specific datacenter or datacenter folder, or to a specific DVS. |
| Step 7 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client # set descr <i>description</i> | (Optional) Provides a description for the port profile client. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 8 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client # set data-center <i>data-center-name</i> | (Optional) Specifies the datacenter to which the port profile is applied. |
| Step 9 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client # set folder <i>folder-name</i> | (Optional) Specifies the datacenter folder to which the port profile is applied. |
| Step 10 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client # set dvs <i>folder-name</i> | (Optional) Specifies the DVS to which the port profile is applied. |
| Step 11 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client # commit-buffer | Commits the transaction. |

The following example creates a port profile client named OtherClient that applies the port profile named MyProfile to all DVSEs in the datacenter named OtherDatacenter and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope profile-set
UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile MyProfile
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # create client OtherClient
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client* # set descr "This is my other client for my port profile"
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client* # set data-center OtherDatacenter
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client* # commit-buffer
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile/client #
```

Deleting a Port Profile Client from a Port Profile

You cannot delete a port profile client if a VM is actively using the port profile with which the client is associated.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt/vmware # scope profile-set | Enters system VM management VMware profile set mode. |
| Step 5 | UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile <i>profile-name</i> | Enters system VM management VMware profile set port profile mode for the specified port profile. |
| Step 6 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # delete client <i>client-name</i> | Deletes the specified port profile client. |
| Step 7 | UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # commit-buffer | Commits the transaction. |

The following example deletes the port profile client named OtherClient from the port profile named MyProfile and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope profile-set
UCS-A /system/vm-mgmt/vmware/profile-set # scope port-profile MyProfile
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile # delete client OtherClient
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile* # commit-buffer
UCS-A /system/vm-mgmt/vmware/profile-set/port-profile #
```



CHAPTER 31

Configuring VN-Link Related Policies

This chapter includes the following sections:

- [Dynamic vNIC Connection Policy, page 331](#)
- [Configuring a Dynamic vNIC Connection Policy, page 331](#)
- [Deleting a Dynamic vNIC Connection Policy, page 332](#)

Dynamic vNIC Connection Policy

This policy determines how the VN-link connectivity between VMs and dynamic vNICs is configured. This policy is required for Cisco UCS instances that include servers with virtual interface card adapters on which you have installed VMs and configured dynamic vNICs.

Each Dynamic vNIC connection policy must include an adapter policy and designate the number of vNICs that can be configured for any server associated with a service profile that includes the policy.

Configuring a Dynamic vNIC Connection Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create dynamic-vnic-conn-policy <i>policy-name</i> | Creates the specified vNIC connection policy and enters organization vNIC connection policy mode. |
| Step 3 | UCS-A /org/dynamic-vnic-conn-policy # set adaptor-profile <i>policy-name</i> | Specifies the Ethernet adaptor policy to use for this policy. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 4 | UCS-A /org/dynamic-vnic-conn-policy # set dynamic-eth <i>dynamic-eth-num</i> off | Specifies the number of dynamic vNICs to use for this policy. |
| Step 5 | UCS-A /org/dynamic-vnic-conn-policy # commit-buffer | Commits the transaction. |

The following example creates a dynamic vNIC connection policy named MyDynVnicConnPolicy that uses the Ethernet adapter policy named EthPolicy19 for 12 dynamic vNICs and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # create dynamic-vnic-conn-policy MyDynVnicConnPolicy
UCS-A /org/dynamic-vnic-conn-policy* # set adaptor-profile EthPolicy19
UCS-A /org/dynamic-vnic-conn-policy* # set dynamic-eth 12
UCS-A /org/dynamic-vnic-conn-policy* # commit-buffer
UCS-A /org/dynamic-vnic-conn-policy #
```

Deleting a Dynamic vNIC Connection Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete dynamic-vnic-conn-policy <i>policy-name</i> | Deletes the specified vNIC connection policy. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction. |

The following example deletes the dynamic vNIC connection policy named MyDynVnicConnPolicy and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete dynamic-vnic-conn-policy MyDynVnicConnPolicy
UCS-A /org* # commit-buffer
UCS-A /org #
```



CHAPTER 32

Managing Pending Deletions

This chapter includes the following sections:

- [Pending Deletions for VN-Link Tasks, page 333](#)
- [Viewing Pending Deletions, page 334](#)
- [Viewing Properties for a Pending Deletion, page 334](#)
- [Deleting a Pending Deletion, page 335](#)
- [Changing Properties for a Pending Deletion, page 335](#)

Pending Deletions for VN-Link Tasks

When you delete a DVS from Cisco UCS Manager, either explicitly or by deleting any parent object in the hierarchy, Cisco UCS Manager initiates a connection with VMware vCenter to start the process of deleting the DVS. Until the DVS is successfully deleted from VMware vCenter, Cisco UCS Manager places the DVS in a pending deletion list.

However, Cisco UCS Manager cannot successfully delete a DVS from VMware vCenter if certain situations occur, including the following:

- VMware vCenter database was corrupted
- VMware vCenter was uninstalled
- The IP address for VMware vCenter was changed

If the DVS cannot be successfully deleted from VMware vCenter, the DVS remains in the pending deletion list until the pending deletion is deleted in Cisco UCS Manager or the properties for that pending deletion are changed in a way that allows the DVS to be successfully deleted from VMware vCenter. When you delete a pending deletion, the DVS is deleted from Cisco UCS Manager but is not deleted from VMware vCenter. If the DVS remains in VMware vCenter, you must delete the DVS manually.

You can view the pending deletion list, delete a pending deletion, or change the properties for a pending deletion in Cisco UCS Manager. For example, you can correct the VMware vCenter IP address for a pending deletion so that Cisco UCS Manager can successfully initiate a connection and delete the DVS from VMware vCenter. You cannot cancel the deletion of a DVS from Cisco UCS Manager.

Viewing Pending Deletions

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt/vmware # show pending-deletion | Displays the list of pending deletions. |

The following example displays the list of pending deletions:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # show pending-deletion

Pending Deletion:
  Id           Host           Distributed Virtual Switch
  -----
  1169232     192.168.10.10   LabDVS
  1176508     192.168.100.20  OpsDVS
  1176508     192.168.1.30   MyDVS
  1176508     192.168.1.40   OtherDVS
```

Viewing Properties for a Pending Deletion

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt/vmware # scope pending-deletion deletion-id | Enters system VM management VMware pending deletion mode for the specified pending deletion. |
| Step 5 | UCS-A /system/vm-mgmt/vmware/pending-deletion # show detail | Displays the properties for the pending deletion. |

The following example displays the properties for pending deletion 1169232:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
```

```

UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope pending-deletion 1169232
UCS-A /system/vm-mgmt/vmware/pending-deletion # show detail

Pending Deletion:
  Id: 1169232
  vCenter: vCenterLab
  Host: 192.168.10.10
  Data Center Folder:
  Data center: Lab
  Folder: LabFolder
  Distributed Virtual Switch: LabDVS
  Extension key: Cisco-UCSM-b32cc112-83bb-11de-acc_7
  Certificate:
  Current Task: external VM manager deletion from local fabric
(FSM-STAGE:sam:dme:ExtvmmSwitchDelTaskRemoveProvider:RemoveLocal)

```

Deleting a Pending Deletion

When you delete a pending deletion, the DVS is deleted from Cisco UCS Manager but is not deleted from VMware vCenter. If the DVS remains in VMware vCenter, you must delete the DVS manually.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt/vmware # delete pending-deletion <i>deletion-id</i> | Deletes the specified pending deletion. |
| Step 5 | UCS-A /system/vm-mgmt/vmware # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes pending deletion 1169232 and commits the transaction:

```

UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # delete pending-deletion 1169232
UCS-A /system/vm-mgmt/vmware* # commit-buffer
UCS-A /system/vm-mgmt/vmware #

```

Changing Properties for a Pending Deletion

You can change the properties of a pending deletion, if necessary, to ensure that Cisco UCS Manager can successfully initiate a connection and delete the DVS from VMware vCenter.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope vm-mgmt | Enters system VM management mode. |
| Step 3 | UCS-A /system/vm-mgmt # scope vmware | Enters system VM management VMware mode. |
| Step 4 | UCS-A /system/vm-mgmt /vmware # scope pending-deletion deletion-id | Enters system VM management VMware pending deletion mode for the specified pending deletion. |
| Step 5 | UCS-A /system/vm-mgmt /vmware/pending-deletion # set {certificate certificate-name data-center data-center-name data-center-folder folder-name folder folder-name host {hostname ip-addr}} | Changes the specified property for the pending deletion. Note If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager. |
| Step 6 | UCS-A /system/vm-mgmt /vmware/pending-deletion # commit-buffer | Commits the transaction to the system configuration. |

The following example changes the host IP address to 192.168.10.20 for pending deletion 1169232 and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope vm-mgmt
UCS-A /system/vm-mgmt # scope vmware
UCS-A /system/vm-mgmt/vmware # scope pending-deletion 1169232
UCS-A /system/vm-mgmt/vmware/pending-deletion # set host 192.168.10.20
UCS-A /system/vm-mgmt/vmware/pending-deletion* # commit-buffer
UCS-A /system/vm-mgmt/vmware/pending-deletion #
```



PART **VII**

System Management

- [Managing Time Zones, page 339](#)
- [Managing the Chassis, page 343](#)
- [Managing the Servers, page 347](#)
- [Managing the I/O Modules, page 355](#)
- [Configuring Call Home, page 357](#)
- [Backing Up and Restoring the Configuration, page 377](#)
- [Managing the System Event Log, page 391](#)
- [Configuring Settings for Faults, Events, and Logs, page 397](#)
- [Recovering a Lost Password, page 403](#)
- [Configuring Statistics-Related Policies, page 407](#)



CHAPTER 33

Managing Time Zones

This chapter includes the following sections:

- [Time Zones, page 339](#)
- [Setting the Time Zone, page 339](#)
- [Configuring an NTP Server, page 341](#)
- [Deleting an NTP Server, page 341](#)
- [Setting the System Clock Manually, page 342](#)

Time Zones

Cisco UCS requires an instance-specific time zone setting and an NTP server to ensure the correct time display in Cisco UCS Manager. If you do not configure both of these settings in a Cisco UCS instance, the time does not display correctly.

Setting the Time Zone

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope services | Enters system services mode. |
| Step 3 | UCS-A /system/services # set timezone | At this point, you are prompted to enter a number corresponding to your continent, country, and time zone region. Enter the appropriate information at each prompt. When you have finished specifying the location information, you are prompted to confirm that the correct time zone information is being set. Enter 1 (yes) to confirm, or 2 (no) to cancel the operation. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 4 | UCS-A /system/services # commit-buffer | Commits the transaction to the system configuration. |
| Step 5 | UCS-A /system/services # exit | Enters system mode. |
| Step 6 | UCS-A /system/services # exit | Enters EXEC mode. |
| Step 7 | UCS-A /system/services # show timezone | Displays the configured timezone. |

The following example configures the timezone to the Pacific time zone region, commits the transaction, and displays the configured timezone:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa                4) Arctic Ocean        7) Australia            10) Pacific Ocean
2) Americas              5) Asia                 8) Europe
3) Antarctica            6) Atlantic Ocean      9) Indian Ocean
#? Artic ocean
Please enter a number in range.
#? 2
Please select a country.
1) Anguilla              18) Ecuador            35) Paraguay
2) Antigua & Barbuda    19) El Salvador        36) Peru
3) Argentina            20) French Guiana     37) Puerto Rico
4) Aruba                 21) Greenland         38) St Kitts & Nevis
5) Bahamas              22) Grenada           39) St Lucia
6) Barbados             23) Guadeloupe        40) St Pierre & Miquelon
7) Belize               24) Guatemala         41) St Vincent
8) Bolivia              25) Guyana            42) Suriname
9) Brazil               26) Haiti              43) Trinidad & Tobago
10) Canada              27) Honduras          44) Turks & Caicos Is
11) Cayman Islands     28) Jamaica           45) United States
12) Chile               29) Martinique        46) Uruguay
13) Colombia            30) Mexico             47) Venezuela
14) Costa Rica         31) Montserrat        48) Virgin Islands (UK)
15) Cuba               32) Netherlands Antilles 49) Virgin Islands (US)
16) Dominica           33) Nicaragua
17) Dominican Republic 34) Panama
#? 45
Please select one of the following time zone regions.
1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Time - Kentucky - Wayne County
5) Eastern Standard Time - Indiana - most locations
6) Eastern Standard Time - Indiana - Crawford County
7) Eastern Standard Time - Indiana - Starke County
8) Eastern Standard Time - Indiana - Switzerland County
9) Central Time
10) Central Time - Michigan - Wisconsin border
11) Central Time - North Dakota - Oliver County
12) Mountain Time
13) Mountain Time - south Idaho & east Oregon
14) Mountain Time - Navajo
15) Mountain Standard Time - Arizona
16) Pacific Time
17) Alaska Time
18) Alaska Time - Alaska panhandle
19) Alaska Time - Alaska panhandle neck
20) Alaska Time - west Alaska
21) Aleutian Islands
22) Hawaii
```

#? 16

The following information has been given:

```

United States
Pacific Time

```

```

Therefore timezone 'America/Los Angeles' will be set.
Local time is now:   Fri May 15 07:39:25 PDT 2009.
Universal Time is now: Fri May 15 14:39:25 UTC 2009.
Is the above information OK?

```

```

1) Yes
2) No

```

#? 1

```

UCS-A /system/services* # commit-buffer
UCS-A /system/services # exit
UCS-A /system # exit
UCS-A# show timezone
Timezone: America/Los_Angeles (Pacific Time)
UCS-A#

```

Configuring an NTP Server

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope services | Enters system services mode. |
| Step 3 | UCS-A /system/services # create ntp-server {hostname ip-addr} | Configures the system to use the NTP server with the specified hostname or IP address. |
| Step 4 | UCS-A /system/services # commit-buffer | Commits the transaction to the system configuration. |

The following example configures an NTP server with the IP address 192.168.200.101 and commits the transaction:

```

UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # create ntp-server 192.168.200.101
UCS-A /system/services* # commit-buffer
UCS-A /system/services #

```

Deleting an NTP Server

Procedure

| | Command or Action | Purpose |
|---------------|---------------------------------------|------------------------------|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope services | Enters system services mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 3 | UCS-A /system/services # delete ntp-server {hostname ip-addr} | Deletes the NTP server with the specified IP address. |

The following example deletes the NTP server with the IP address 192.168.200.101 and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # delete ntp-server 192.168.200.101
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```

Setting the System Clock Manually

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope services | Enters system services mode. |
| Step 3 | UCS-A /system/services # set clock mon date <i>year hour min sec</i> | Configures the system clock. |
| Step 4 | UCS-A /system/services # commit-buffer | Commits the transaction to the system configuration. |

The following example configures the system clock and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope services
UCS-A /system/services # set clock apr 14 2010 15 27 00
UCS-A /system/services* # commit-buffer
UCS-A /system/services #
```



CHAPTER 34

Managing the Chassis

This chapter includes the following sections:

- [Acknowledging a Chassis, page 343](#)
- [Decommissioning a Chassis, page 344](#)
- [Removing a Chassis, page 344](#)
- [Recommissioning a Chassis, page 345](#)
- [Toggling the Locator LED, page 345](#)

Acknowledging a Chassis

Perform the following procedure if you increase or decrease the number of links that connect the chassis to the fabric interconnect. Acknowledging the chassis ensures that Cisco UCS Manager is aware of the change in the number of links and that traffics flows along all available links.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# acknowledge chassis <i>chassis-num</i> | Acknowledges the specified chassis. |
| Step 2 | UCS-A# commit-buffer | Commits the transaction to the system configuration. |

The following example acknowledges chassis 2 and commits the transaction:

```
UCS-A# acknowledge chassis 2  
UCS-A* # commit-buffer  
UCS-A #
```

Decommissioning a Chassis

This procedure decommissions the chassis and deletes it from the Cisco UCS configuration. The chassis hardware physically remains in the Cisco UCS instance. However, Cisco UCS ignores it and does not list it with the other commissioned chassis.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# decommission chassis <i>chassis-num</i> | Decommissions the specified chassis. |
| Step 2 | UCS-A# commit-buffer | Commits the transaction to the system configuration. |

The decommission may take several minutes to complete.

The following example decommissions chassis 2 and commits the transaction:

```
UCS-A# decommission chassis 2
UCS-A* # commit-buffer
UCS-A # show chassis

Chassis:
  Chassis   Overall Status      Admin State
  -----
           1 Operable          Acknowledged
           2 Accessibility Problem  Decommission
UCS-A #
```

Removing a Chassis

Before You Begin

Physically remove the chassis before performing the following procedure.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# remove chassis <i>chassis-num</i> | Removes the specified chassis. |
| Step 2 | UCS-A# commit-buffer | Commits the transaction to the system configuration. |

The removal may take several minutes to complete.

The following example removes chassis 2 and commits the transaction:

```
UCS-A# remove chassis 2
UCS-A* # commit-buffer
UCS-A #
```

Recommissioning a Chassis

This procedure returns the chassis to the configuration and applies the chassis discovery policy to the chassis. After this procedure, you can access the chassis and any servers in it.

Before You Begin

Collect the following information about the chassis to be recommissioned:

- Vendor name
- Model name
- Serial number

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# recommission chassis <i>vendor-name</i> <i>model-name serial-num</i> | Recommissions the specified chassis. |
| Step 2 | UCS-A# commit-buffer | Commits the transaction to the system configuration. |

The following example recommissions a Cisco UCS 5108 chassis and commits the transaction:

```
UCS-A# show chassis

Chassis:
Chassis   Overall Status           Admin State
-----
1 Accessibility Problem    Decommission

UCS-A# recommission chassis "Cisco Systems Inc" "Cisco UCS 5108" FOX1252GNNN
UCS-A* # commit-buffer
UCS-A #
```

oggling the Locator LED

Turning On the Locator LED for a Chassis

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope chassis <i>chassis-num</i> | Enters chassis mode for the specified chassis. |
| Step 2 | UCS-A /chassis # enable locator-led | Turns on the chassis locator LED. |
| Step 3 | UCS-A /chassis # commit-buffer | Commits the transaction to the system configuration. |

The following example turns on the locator LED for chassis 2 and commits the transaction:

```
UCS-A# scope chassis 2
UCS-A /chassis # enable locator-led
UCS-A /chassis* # commit-buffer
UCS-A /chassis #
```

Turning Off the Locator LED for a Chassis

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope chassis <i>chassis-num</i> | Enters chassis mode for the specified chassis. |
| Step 2 | UCS-A /chassis # disable locator-led | Turns off the chassis locator LED. |
| Step 3 | UCS-A /chassis # commit-buffer | Commits the transaction to the system configuration. |

The following example turns off the locator LED for chassis 2 and commits the transaction:

```
UCS-A# scope chassis 2
UCS-A /chassis # disable locator-led
UCS-A /chassis* # commit-buffer
UCS-A /chassis #
```



CHAPTER 35

Managing the Servers

This chapter includes the following sections:

- [Booting a Server, page 347](#)
- [Shutting Down a Server, page 348](#)
- [Power Cycling a Server, page 349](#)
- [Performing a Hard Reset on a Server, page 349](#)
- [Acknowledging a Server, page 350](#)
- [Removing a Server from a Chassis, page 350](#)
- [Decommissioning a Server, page 351](#)
- [Turning On the Locator LED for a Server, page 351](#)
- [Turning Off the Locator LED for a Server, page 351](#)
- [Resetting the CMOS for a Server, page 352](#)
- [Resetting the BMC for a Server, page 352](#)
- [Recovering the Corrupt BIOS on a Server, page 353](#)

Booting a Server

Before You Begin

Associate a service profile with a server or server pool.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 2 | UCS-A /org # scope service-profile <i>profile-name</i> | Enters organization service profile mode for the specified service profile. |
| Step 3 | UCS-A /org/service-profile # power up | Boots the server associated with the service profile. |
| Step 4 | UCS-A /org/service-profile # commit-buffer | Commits the transaction to the system configuration. |

The following example boots the server associated with the service profile named ServProf34 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope service-profile ServProf34
UCS-A /org/service-profile* # power up
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

Shutting Down a Server

When you use this procedure to shut down a server with an installed operating system, Cisco UCS Manager triggers the OS into a graceful shutdown sequence.

Before You Begin

Associate a service profile with a server or server pool.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope service-profile <i>profile-name</i> | Enters organization service profile mode for the specified service profile. |
| Step 3 | UCS-A /org/service-profile # power down | Shuts down the server associated with the service profile. |
| Step 4 | UCS-A /org/service-profile # commit-buffer | Commits the transaction to the system configuration. |

The following example shuts down the server associated with the service profile named ServProf34 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope service-profile ServProf34
UCS-A /org/service-profile # power down
UCS-A /org/service-profile* # commit-buffer
UCS-A /org/service-profile #
```

Power Cycling a Server

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope server <i>chassis-num</i> / <i>server-num</i> | Enters chassis server mode for the specified server. |
| Step 2 | UCS-A /chassis/server # cycle { cycle-immediate cycle-wait } | Power cycles the server. Use the cycle-immediate keyword to immediately begin power cycling the server; use the cycle-wait keyword to schedule the power cycle to begin after all pending management operations have completed. |
| Step 3 | UCS-A# commit-buffer | Commits the transaction to the system configuration. |

The following example immediately power cycles server 4 in chassis 2 and commits the transaction:

```
UCS-A# scope server 2/4
UCS-A /chassis/server # cycle cycle-immediate
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

Performing a Hard Reset on a Server

When you reset a server, Cisco UCS Manager sends a pulse on the reset line. You can choose to gracefully shutdown the operating system. If the operating system does not support a graceful shutdown, the server will be power cycled. The option to have Cisco UCS Manager complete all management operations before it resets the server does not guarantee that these operations will be completed before the server is reset.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope server <i>chassis-num</i> / <i>server-num</i> | Enters chassis server mode for the specified server. |
| Step 2 | UCS-A /chassis/server # reset { hard-reset-immediate hard-reset-wait } | Performs a hard reset of the server. Use the hard-reset-immediate keyword to immediately begin hard resetting the server; use the hard-reset-wait keyword to schedule the hard reset to begin after all pending management operations have completed. |
| Step 3 | UCS-A# commit-buffer | Commits the transaction to the system configuration. |

The following example performs an immediate hard reset of server 4 in chassis 2 and commits the transaction:

```
UCS-A# scope server 2/4
UCS-A /chassis/server # reset hard-reset-immediate
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

Acknowledging a Server

Perform the following procedure if you need to have Cisco UCS Manager rediscover the server and all endpoints in the server. For example, you can use this procedure if a server is stuck in an unexpected state, such as the discovery state.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# acknowledge server <i>chassis-num</i> / <i>server-num</i> | Acknowledges the specified server. |
| Step 2 | UCS-A# commit-buffer | Commits the transaction to the system configuration. |

The following example acknowledges server 4 in chassis 2 and commits the transaction:

```
UCS-A# acknowledge server 2/4
UCS-A* # commit-buffer
UCS-A #
```

Removing a Server from a Chassis

Before You Begin

Physically remove the server from its chassis before performing the following procedure.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# remove server <i>chassis-num</i> / <i>server-num</i> | Removes the specified server. |
| Step 2 | UCS-A# commit-buffer | Commits the transaction to the system configuration. |

The following example removes server 4 in chassis 2 and commits the transaction:

```
UCS-A# remove server 2/4
UCS-A* # commit-buffer
UCS-A #
```

What to Do Next

If you physically re-install the server, you must re-acknowledge the slot to have Cisco UCS Manager rediscover the server.

For more information, see [Acknowledging a Server](#), page 350.

Decommissioning a Server

This procedure decommissions a server and deletes it from the Cisco UCS configuration. The server hardware physically remains in the Cisco UCS instance. However, Cisco UCS Manager ignores it and does not list it with the other servers in the chassis.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# decommission server <i>chassis-num</i> / <i>server-num</i> | Decommissions the specified server. |
| Step 2 | UCS-A# commit-buffer | Commits the transaction to the system configuration. |

The following example decommissions server 4 in chassis 2 and commits the transaction:

```
UCS-A# decommission server 2/4
UCS-A* # commit-buffer
UCS-A #
```

Turning On the Locator LED for a Server

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope server <i>chassis-num</i> / <i>server-num</i> | Enters chassis server mode for the specified chassis. |
| Step 2 | UCS-A /chassis/server # enable locator-led | Turns on the server locator LED. |
| Step 3 | UCS-A /chassis/server # commit-buffer | Commits the transaction to the system configuration. |

The following example turns on the locator LED for server 4 in chassis 2 and commits the transaction:

```
UCS-A# scope server 2/4
UCS-A /chassis/server # enable locator-led
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

Turning Off the Locator LED for a Server

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope server <i>chassis-num</i> / <i>server-num</i> | Enters chassis mode for the specified chassis. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 2 | UCS-A /chassis/server # disable locator-led | Turns off the server locator LED. |
| Step 3 | UCS-A /chassis/server # commit-buffer | Commits the transaction to the system configuration. |

The following example turns off the locator LED for server 4 in chassis 2 and commits the transaction:

```
UCS-A# scope chassis 2/4
UCS-A /chassis/server # disable locator-led
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

Resetting the CMOS for a Server

On rare occasions, troubleshooting a server may require you to reset the CMOS. This procedure is not part of the normal maintenance of a server.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope server <i>chassis-num / server-num</i> | Enters chassis server mode for the specified chassis. |
| Step 2 | UCS-A /chassis/server # reset-cmos | Resets the CMOS for the server. |
| Step 3 | UCS-A /chassis/server # commit-buffer | Commits the transaction to the system configuration. |

The following example resets the CMOS for server 4 in chassis 2 and commits the transaction:

```
UCS-A# scope server 2/4
UCS-A /chassis/server # reset-cmos
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

Resetting the BMC for a Server

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the CIMC. This procedure is not part of the normal maintenance of a server. After you reset the CIMC, the server boots with the running version of the firmware for that server.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope server <i>chassis-num / server-num</i> | Enters chassis server mode for the specified chassis. |
| Step 2 | UCS-A /chassis/server # scope bmc | Enters chassis server BMC mode |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 3 | UCS-A /chassis/server/bmc # reset | Resets the BMC for the server. |
| Step 4 | UCS-A /chassis/server/bmc # commit-buffer | Commits the transaction to the system configuration. |

The following example resets the BMC for server 4 in chassis 2 and commits the transaction:

```
UCS-A# scope server 2/4
UCS-A /chassis/server # scope bmc
UCS-A /chassis/server/cimc # reset
UCS-A /chassis/server/cimc* # commit-buffer
UCS-A /chassis/server/cimc #
```

Recovering the Corrupt BIOS on a Server

On rare occasions, an issue with a server may require you to recover the corrupted BIOS. This procedure is not part of the normal maintenance of a server. After you recover the BIOS, the server boots with the running version of the firmware for that server.

Before You Begin



Important

Remove all attached or mapped USB storage from a server before you attempt to recover the corrupt BIOS on that server. If an external USB drive is attached or mapped from vMedia to the server, BIOS recovery fails.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope server <i>chassis-id/server-id</i> | Enters chassis server mode for the specified server in the specified chassis. |
| Step 2 | UCS-A /chassis/server # recover-bios <i>version [ignorecompcheck]</i> | Loads and activates the specified BIOS version. To activate the firmware without making sure that it is compatible first, include the ignorecompcheck keyword. We recommend that you use this option only when explicitly directed to do so by a technical support representative. |
| Step 3 | UCS-A /chassis/server # commit-buffer | Commits the transaction. |

The following example shows how to recover the BIOS:

```
UCS-A# scope server 1/7
UCS-A /chassis/server # recover-bios S5500.0044.0.3.1.010620101125
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```




CHAPTER 36

Managing the I/O Modules

This chapter includes the following sections:

- [Resetting the IOM, page 355](#)

Resetting the IOM

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope chassis <i>chassis-num</i> | Enters chassis mode for the specified chassis. |
| Step 2 | UCS-A /chassis # scope iom {a b} | Enters chassis IOM mode for the specified IOM. |
| Step 3 | UCS-A /chassis/iom # reset | Resets the IOM. |
| Step 4 | UCS-A /chassis/iom # commit-buffer | Commits the transaction to the system configuration. |

The following example resets the IOM on fabric A and commits the transaction:

```
UCS-A# scope chassis 1
UCS-A /chassis # scope iom a
UCS-A /chassis/iom # reset
UCS-A /chassis/iom* # commit-buffer
UCS-A /chassis/iom #
```




CHAPTER 37

Configuring Call Home

This chapter includes the following sections:

- [Call Home, page 357](#)
- [Call Home Considerations and Guidelines, page 359](#)
- [Cisco UCS Faults and Call Home Severity Levels, page 360](#)
- [Cisco Smart Call Home, page 361](#)
- [Configuring Call Home, page 362](#)
- [Disabling Call Home, page 363](#)
- [Enabling Call Home, page 364](#)
- [Configuring System Inventory Messages, page 364](#)
- [Configuring Call Home Profiles, page 366](#)
- [Sending a Test Call Home Alert, page 368](#)
- [Configuring Call Home Policies, page 369](#)
- [Example: Configuring Call Home for Smart Call Home, page 372](#)

Call Home

Call Home provides an email-based notification for critical system policies. A range of message formats are available for compatibility with pager services or XML-based automated parsing applications. You can use this feature to page a network support engineer, email a Network Operations Center, or use Cisco Smart Call Home services to generate a case with the Technical Assistance Center.

The Call Home feature can deliver alert messages containing information about diagnostics and environmental faults and events.

The Call Home feature can deliver alerts to multiple recipients, referred to as Call Home destination profiles. Each profile includes configurable message formats and content categories. A predefined destination profile is provided for sending alerts to the Cisco TAC, but you also can define your own destination profiles.

When you configure Call Home to send messages, Cisco UCS Manager executes the appropriate CLI **show** command and attaches the command output to the message.

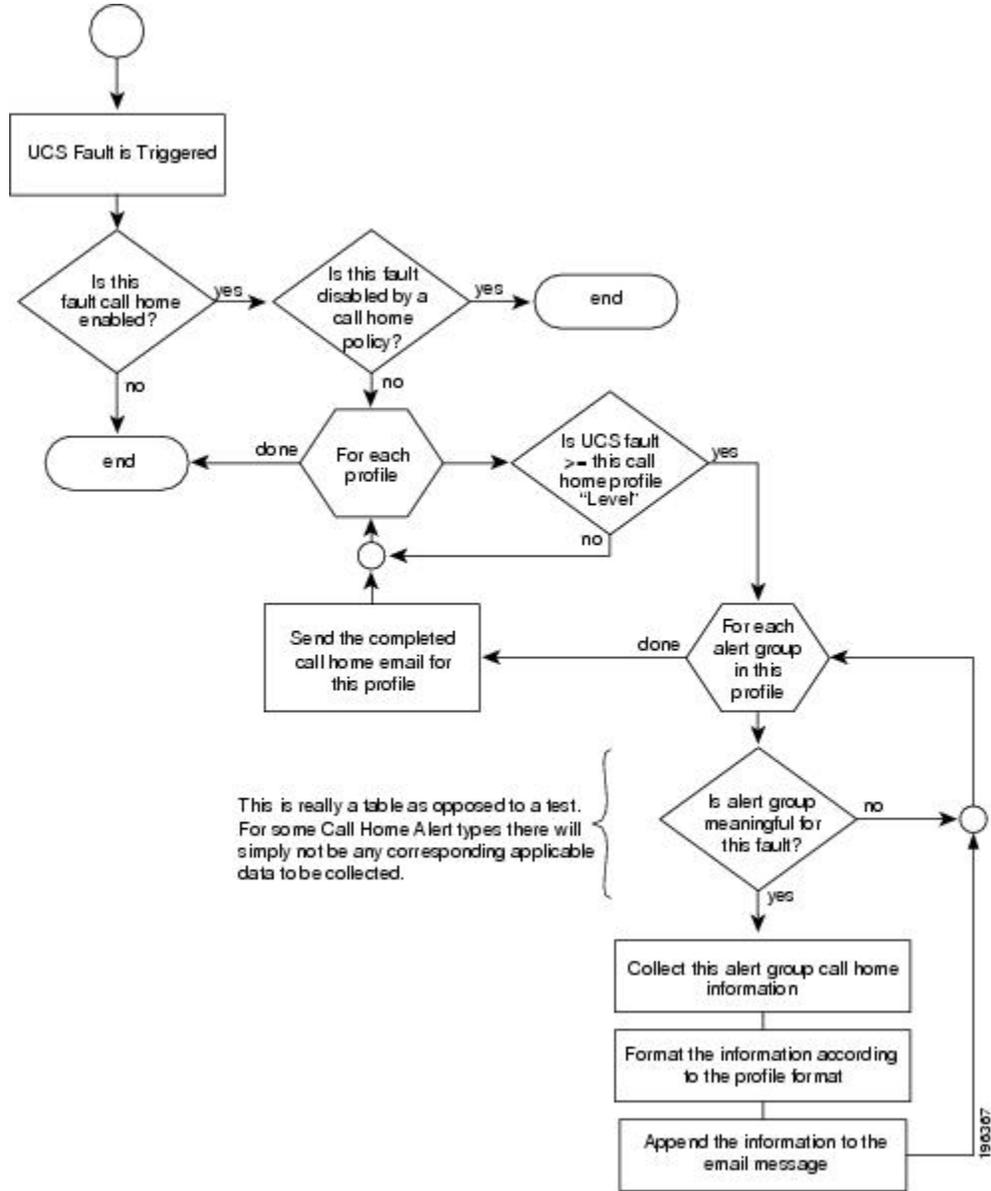
Cisco UCS delivers Call Home messages in the following formats:

- Short text format which provides a one or two line description of the fault that is suitable for pagers or printed reports.
- Full text format which provides fully formatted message with detailed information that is suitable for human reading.
- XML machine readable format that uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML schema definition (XSD). The AML XSD is published on the Cisco.com website at <http://www.cisco.com/>. The XML format enables communication with the Cisco Systems Technical Assistance Center.

For information about the faults that can trigger Call Home email alerts, see the *Cisco UCS Faults Reference*.

The following figure shows the flow of events after a Cisco UCS is triggered in a system with Call Home configured:

Figure 4: Flow of Events after a Fault is Triggered



Call Home Considerations and Guidelines

How you configure Call Home depends on how you intend to use the feature. The information you need to consider before you configure Call Home includes the following:

Destination Profile

You must configure at least one destination profile. The destination profile or profiles that you use depend upon whether the receiving entity is a pager, email, or automated service such as Cisco Smart Call Home.

If the destination profile uses email message delivery, you must specify a Simple Mail Transfer Protocol (SMTP) server when you configure Call Home.

Contact Information

The contact email, phone, and street address information should be configured so that the receiver can determine the origin of messages received.

IP Connectivity to Email Server or HTTP Server

The fabric interconnect must have IP connectivity to an email server or the destination HTTP server. In a cluster configuration, both fabric interconnects must have IP connectivity. This connectivity ensures that the current, active fabric interconnect can send Call Home email messages. The source of these email messages is always the IP address of a fabric interconnect. The virtual IP address assigned Cisco UCS Manager in a cluster configuration is never the source of the email.

Smart Call Home

If Cisco Smart Call Home is used, the following are required:

- An active service contract must cover the device being configured
- The customer ID associated with the Smart Call Home configuration in Cisco UCS must be the CCO (Cisco.com) account name associated with a support contract that includes Smart Call Home

Cisco UCS Faults and Call Home Severity Levels

Because Call Home is present across several Cisco product lines, Call Home has developed its own standardized severity levels. The following table describes how the underlying Cisco UCS fault levels map to the Call Home severity levels. You need to understand this mapping when you configure the Level setting for Call Home profiles.

Table 12: Mapping of Faults and Call Home Severity Levels

| Call Home Severity | Cisco UCS Fault | Call Home Meaning |
|--------------------|-----------------|--|
| (9) Catastrophic | N/A | Network-wide catastrophic failure. |
| (8) Disaster | N/A | Significant network impact. |
| (7) Fatal | N/A | System is unusable. |
| (6) Critical | Critical | Critical conditions, immediate attention needed. |
| (5) Major | Major | Major conditions. |
| (4) Minor | Minor | Minor conditions. |

| Call Home Severity | Cisco UCS Fault | Call Home Meaning |
|--------------------|-----------------|---|
| (3) Warning | Warning | Warning conditions. |
| (2) Notification | Info | Basic notifications and informational messages. Possibly independently insignificant. |
| (1) Normal | Clear | Normal event, signifying a return to normal state. |
| (0) debug | N/A | Debugging messages. |

Cisco Smart Call Home

Cisco Smart Call Home is a web application which leverages the Call Home feature of Cisco UCS. Smart Call Home offers proactive diagnostics and real-time email alerts of critical system events, which results in higher network availability and increased operational efficiency. Smart Call Home is a secure connected service offered by Cisco Unified Computing Support Service and Cisco Unified Computing Mission Critical Support Service for Cisco UCS.



Note Using Smart Call Home requires the following:

- A CCO ID associated with a corresponding Cisco Unified Computing Support Service or Cisco Unified Computing Mission Critical Support Service contract for your company.
- Cisco Unified Computing Support Service or Cisco Unified Computing Mission Critical Support Service for the device to be registered.

You can configure and register Cisco UCS Manager to send Smart Call Home email alerts to either the Smart Call Home System or the secure Transport Gateway. Email alerts sent to the secure Transport Gateway are forwarded to the Smart Call Home System using HTTPS.



Note For security reasons, we recommend using the Transport Gateway option. The Transport Gateway can be downloaded from Cisco.

To configure Smart Call Home, you must do the following:

- Enable the Smart Call Home feature.
- Configure the contact information.
- Configure the email information.
- Configure the SMTP server information.
- Configure the default CiscoTAC-1 profile.
- Send a Smart Call Home inventory message to start the registration process.

- Ensure that the CCO ID you plan to use as the Call Home Customer ID for the Cisco UCS instance has the contract numbers from the registration added to its entitlements. You can update the ID in the account properties under Additional Access in the Profile Manager on CCO.

Configuring Call Home

Procedure

| | Command or Action | Purpose |
|----------------|---|--|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # scope callhome | Enters monitoring call home mode. |
| Step 3 | UCS-A /monitoring/callhome # enable | Enables Call Home. |
| Step 4 | UCS-A /monitoring/callhome # set contact <i>name</i> | Specifies the name of the main Call Home contact person. |
| Step 5 | UCS-A /monitoring/callhome # set email <i>email-addr</i> | Specifies the email address of the main Call Home contact person. |
| Step 6 | UCS-A /monitoring/callhome # set phone-contact <i>phone-num</i> | Specifies the phone number of the main Call Home contact person. The phone number must be in international format, starting with a + (plus sign) and a country code. |
| Step 7 | UCS-A /monitoring/callhome # set street-address <i>street-addr</i> | Specifies the street address of the main Call Home contact person. |
| Step 8 | UCS-A /monitoring/callhome # set customer-id <i>id-num</i> | Specifies the CCO identification number that includes the contract numbers for the support contract in its entitlements. The number can be up to 255 alphanumeric characters in free format. |
| Step 9 | UCS-A /monitoring/callhome # set contract-id <i>id-num</i> | Specifies the contract identification number from the service agreement. The number can be up to 255 alphanumeric characters in free format. |
| Step 10 | UCS-A /monitoring/callhome # set site-id <i>id-num</i> | Specifies the site identification number from the service agreement. The number can be up to 255 alphanumeric characters in free format. |
| Step 11 | UCS-A /monitoring/callhome # set from-email <i>email-addr</i> | Specifies the email address to use for the From field in Call Home messages. |
| Step 12 | UCS-A /monitoring/callhome # set reply-to-email <i>email-addr</i> | Specifies the email address to use for the Reply To field in Call Home messages. |
| Step 13 | UCS-A /monitoring/callhome # set hostname { <i>hostname</i> <i>ip-addr</i> } | Specifies the hostname or IP address of the SMTP server that Call Home uses to send email messages. |

| | Command or Action | Purpose |
|----------------|---|---|
| Step 14 | UCS-A /monitoring/callhome # set port <i>port-num</i> | Specifies the SMTP server port that Call Home uses to send email messages. Valid port numbers are 1 to 65535. |
| Step 15 | UCS-A /monitoring/callhome # set throttling {off on} | Enables or disables Call Home throttling. When enabled, throttling prevents too many Call Home email messages from being sent for the same event. By default, throttling is enabled. |
| Step 16 | UCS-A /monitoring/callhome # set urgency {alerts critical debugging emergencies errors information notifications warnings} | Specifies the urgency level for Call Home email messages. In the context of a large UCS deployment with several pairs of fabric interconnects, the urgency level potentially allows you to attach significance to Call Home messages from one particular UCS instance versus another. In the context of a small UCS deployment involving only two fabric interconnects, the urgency level holds little meaning. |
| Step 17 | UCS-A /monitoring/callhome # commit-buffer | Commits the transaction to the system configuration. |

The following example configures Call Home and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # enable
UCS-A /monitoring/callhome* # set contact "Steve Jones"
UCS-A /monitoring/callhome* # set email admin@MyCompany.com
UCS-A /monitoring/callhome* # set phone-contact +1-001-408-555-1234
UCS-A /monitoring/callhome* # set street-address "123 N. Main Street, Anytown, CA, 99885"
UCS-A /monitoring/callhome* # set customer-id 1234567
UCS-A /monitoring/callhome* # set contract-id 99887766
UCS-A /monitoring/callhome* # set site-id 5432112
UCS-A /monitoring/callhome* # set from-email person@MyCompany.com
UCS-A /monitoring/callhome* # set reply-to-email person@MyCompany.com
UCS-A /monitoring/callhome* # set hostname 192.168.100.12
UCS-A /monitoring/callhome* # set port 25
UCS-A /monitoring/callhome* # set throttling on
UCS-A /monitoring/callhome* # set urgency information
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

Disabling Call Home

Procedure

| | Command or Action | Purpose |
|---------------|---|-----------------------------------|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # scope callhome | Enters monitoring call home mode. |
| Step 3 | UCS-A /monitoring/callhome # disable | Enables Call Home. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 4 | UCS-A /monitoring/callhome # commit-buffer | Commits the transaction to the system configuration. |

The following example disables Call Home and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # disable
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

Enabling Call Home

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # scope callhome | Enters monitoring call home mode. |
| Step 3 | UCS-A /monitoring/callhome # enable | Enables Call Home. |
| Step 4 | UCS-A /monitoring/callhome # commit-buffer | Commits the transaction to the system configuration. |

The following example enables Call Home and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # enable
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

Configuring System Inventory Messages

Configuring System Inventory Messages

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # scope callhome | Enters monitoring call home mode. |
| Step 3 | UCS-A /monitoring/callhome # scope inventory | Enters monitoring call home inventory mode. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 4 | UCS-A /monitoring/callhome/inventory # set send-periodically {off on} | Enables or disables the sending of inventory messages. When the on keyword is specified, inventory messages are automatically sent to the Call Home database. |
| Step 5 | UCS-A /monitoring/callhome/inventory # set interval-days <i>interval-num</i> | Specifies the time interval (in days) at which inventory messages will be sent. |
| Step 6 | UCS-A /monitoring/callhome/inventory # set timeofday-hour <i>hour</i> | Specifies the hour (using 24-hour format) that inventory messages are sent. |
| Step 7 | UCS-A /monitoring/callhome/inventory # set timeofday-minute <i>minute</i> | Specifies the number of minutes after the hour that inventory messages are sent. |
| Step 8 | UCS-A /monitoring/callhome/inventory # commit-buffer | Commits the transaction to the system configuration. |

The following example configures Call Home system inventory messages and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # scope inventory
UCS-A /monitoring/callhome/inventory* # set send-periodically on
UCS-A /monitoring/callhome/inventory* # set interval-days 15
UCS-A /monitoring/callhome/inventory* # set timeofday-hour 21
UCS-A /monitoring/callhome/inventory* # set timeofday-minute 30
UCS-A /monitoring/callhome/inventory* # commit-buffer
UCS-A /monitoring/callhome/inventory #
```

Sending a System Inventory Message

Use this procedure if you need to manually send a system inventory message outside of the scheduled messages.



Note

The system inventory message is sent only to those recipients defined in CiscoTAC-1 profile.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # scope callhome | Enters monitoring call home mode. |
| Step 3 | UCS-A /monitoring/callhome # scope inventory | Enters monitoring call home inventory mode. |
| Step 4 | UCS-A /monitoring/callhome/inventory # send | Sends the system inventory message to the Call Home database. |

The following example sends the system inventory message to the Call Home database:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # scope inventory
UCS-A /monitoring/callhome/inventory* # send
```

Configuring Call Home Profiles

Call Home Profiles

Call Home profiles determine which alert groups and recipients receive email alerts for events that occur at a specific severity. You can also use these profiles to specify the format of the alert for a specific set of recipients and alert groups.

By default, you must configure the Cisco TAC-1 profile. However, you can also create additional profiles to send email alerts to one or more specified groups when events occur at the level that you specify.

For example, you may want to configure two profiles for faults with a major severity:

- A profile that sends an alert to the Supervisor alert group in the short text format. Members of this group receive a one- or two-line description of the fault that they can use to track the issue.
- A profile that sends an alert to the CiscoTAC alert group in the XML format. Members of this group receive a detailed message in the machine readable format preferred by the Cisco Systems Technical Assistance Center.

Configuring a Call Home Profile

By default, you must configure the Cisco TAC-1 profile. However, you can also create additional profiles to send email alerts to one or more specified groups when events occur at the level that you specify.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # scope callhome | Enters monitoring call home mode. |
| Step 3 | UCS-A /monitoring/callhome # create profile <i>profile-name</i> | Enters monitoring call home profile mode. |
| Step 4 | UCS-A /monitoring/callhome/profile # set level { critical debug disaster fatal major minor normal notification warning } | Specifies the event level for the profile. Each profile can have its own unique event level. Cisco UCS faults that are greater than or equal to the event level will trigger this profile. |
| Step 5 | UCS-A /monitoring/callhome/profile # set alertgroups <i>group-name</i> • ciscotac • diagnostic | Specifies one or more groups that are alerted based on the profile. The <i>group-name</i> argument can be one or more of the following keywords entered on the same command line: |

| | Command or Action | Purpose |
|----------------|---|--|
| | <ul style="list-style-type: none"> • environmental • inventory • license • lifecycle • linecard • supervisor • syslogport • system • test | |
| Step 6 | UCS-A /monitoring/callhome/profile # add alertgroups <i>group-names</i> | (Optional) Adds one or more groups to the existing list of groups that are alerted based on the Call Home profile. Note You must use the add alertgroups command to add more alert groups to the existing alert group list. Using the set alertgroups command will replace any pre-existing alert groups with a new group list. |
| Step 7 | UCS-A /monitoring/callhome/profile # set format {shorttxt xml} | Specifies the formatting method to use for the e-mail messages. |
| Step 8 | UCS-A /monitoring/callhome/profile # set maxsize <i>id-num</i> | Specifies the maximum size (in characters) of the email message. |
| Step 9 | UCS-A /monitoring/callhome/profile # create destination <i>email-addr</i> | Specifies the email address to which Call Home alerts should be sent. Use multiple create destination commands in monitoring call home profile mode to specify multiple email recipients. Use the delete destination command in monitoring call home profile mode to delete a specified email recipient. |
| Step 10 | UCS-A /monitoring/callhome/profile/destination # commit-buffer | Commits the transaction to the system configuration. |

The following example configures a Call Home profile and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # create profile TestProfile
UCS-A /monitoring/callhome/profile* # set level normal
UCS-A /monitoring/callhome/profile* # set alertgroups test diagnostic
UCS-A /monitoring/callhome/profile* # set format xml
UCS-A /monitoring/callhome/profile* # set maxsize 100000
UCS-A /monitoring/callhome/profile* # create destination admin@MyCompany.com
UCS-A /monitoring/callhome/profile/destination* # commit-buffer
UCS-A /monitoring/callhome/profile/destination #
```

Deleting a Call Home Profile

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # scope callhome | Enters monitoring call home mode. |
| Step 3 | UCS-A /monitoring/callhome # delete profile <i>profile-name</i> | Deletes the specified profile. |
| Step 4 | UCS-A /monitoring/callhome # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the Call Home profile named TestProfile and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # delete profile TestProfile
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

Sending a Test Call Home Alert

Before You Begin

Configure Call Home and a Call Home Profile

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # scope callhome | Enters monitoring call home mode. |
| Step 3 | UCS-A /monitoring/callhome # send-test-alert {[alert-description <i>description</i>] [alert-group { diagnostic environmental }] [alert-level { critical debug fatal major minor normal notify warning }] [alert-message-subtype { delta full goldmajor goldminor goldnormal major minor nosubtype test }] [alert-message-type { conf diag env inventory syslog test }]} | Sends a test Call Home alert using one or more of the following alert parameters: <ul style="list-style-type: none"> • Alert description • Alert group • Event severity level • Message type • Message subtype <p>When a test Call Home alert is sent, Call Home responds as it would to any other alert and delivers it to the configured destination email addresses.</p> |

The following example sends a test Call Home alert to the configured destination email address of the environmental alert group:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # send-test-alert alert-description "This is a test alert"
alert-group environmental
```

Configuring Call Home Policies

Call Home Policies

Call Home policies determine whether or not Call Home alerts are sent for a specific type of fault or system event. By default, Call Home is enabled to send alerts for certain types of faults and system events. However, you can configure Cisco UCS not to process certain types.

To disable alerts for a type of fault or events, you must create a Call Home policy for that type, and you must first create a policy for that type and then disable the policy.

By default, Cisco UCS sends Call Home alerts for each of the following types of faults and system events:

- **association-failed**
- **configuration-failure**
- **connectivity-problem**
- **election-failure**
- **equipment-inaccessible**
- **equipment-inoperable**
- **equipment-problem**
- **fru-problem**
- **identity-unestablishable**
- **link-down**
- **management-services-failure**
- **management-services-unresponsive**
- **power-problem**
- **thermal-problem**
- **unspecified**
- **version-incompatible**
- **voltage-problem**

Configuring a Call Home Policy



Tip

By default, email alerts are sent for all critical system events. However, you can optionally configure Call Home policies to enable or disable sending email alerts for other critical system events.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # scope callhome | Enters monitoring call home mode. |
| Step 3 | UCS-A /monitoring/callhome # create policy { equipment-inoperable fru-problem identity-unestablishable thermal-problem voltage-problem } | Creates the specified policy and enters monitoring call home policy mode. |
| Step 4 | UCS-A /monitoring/callhome/policy # { disabled enabled } | Disables or enables the sending of email alerts for the specified policy. |
| Step 5 | UCS-A /monitoring/callhome/policy # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a Call Home policy that disables the sending of email alerts for system events pertaining to voltage problems and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # create policy voltage-problem
UCS-A /monitoring/callhome/policy* # disabled
UCS-A /monitoring/callhome/policy* # commit-buffer
UCS-A /monitoring/callhome/policy #
```

Disabling a Call Home Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # scope callhome | Enters monitoring call home mode. |
| Step 3 | UCS-A /monitoring/callhome # scope policy { equipment-inoperable fru-problem identity-unestablishable thermal-problem voltage-problem } | Enters monitoring call home policy mode for the specified policy. |
| Step 4 | UCS-A /monitoring/callhome/policy # disable | Disables the specified policy. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 5 | UCS-A /monitoring/callhome/policy # commit-buffer | Commits the transaction to the system configuration. |

The following example disables the Call Home policy named voltage-problem and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # scope policy voltage-problem
UCS-A /monitoring/callhome/policy # disable
UCS-A /monitoring/callhome/policy* # commit-buffer
UCS-A /monitoring/callhome/policy #
```

Enabling a Call Home Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # scope callhome | Enters monitoring call home mode. |
| Step 3 | UCS-A /monitoring/callhome # scope policy { equipment-inoperable fru-problem identity-unestablishable thermal-problem voltage-problem } | Enters monitoring call home policy mode for the specified policy. |
| Step 4 | UCS-A /monitoring/callhome/policy # enable | Enables the specified policy. |
| Step 5 | UCS-A /monitoring/callhome/policy # commit-buffer | Commits the transaction to the system configuration. |

The following example enables the Call Home policy named voltage-problem and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # scope policy voltage-problem
UCS-A /monitoring/callhome/policy # enable
UCS-A /monitoring/callhome/policy* # commit-buffer
UCS-A /monitoring/callhome/policy #
```

Deleting a Call Home Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|-----------------------------------|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # scope callhome | Enters monitoring call home mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 3 | UCS-A /monitoring/callhome # delete policy { equipment-inoperable fru-problem identity-unestablishable thermal-problem voltage-problem } | Deletes the specified policy |
| Step 4 | UCS-A /monitoring/callhome # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the Call Home policy named voltage-problem and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope callhome
UCS-A /monitoring/callhome # delete policy voltage-problems
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

Example: Configuring Call Home for Smart Call Home

Configuring Smart Call Home

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # scope callhome | Enters monitoring call home mode. |
| Step 3 | UCS-A /monitoring/callhome # enable | Enables Call Home. |
| Step 4 | UCS-A /monitoring/callhome # set contact name | Specifies the name of the main Call Home contact person. |
| Step 5 | UCS-A /monitoring/callhome # set email email-addr | Specifies the email address of the main Call Home contact person. |
| Step 6 | UCS-A /monitoring/callhome # set phone-contact phone-num | Specifies the phone number of the main Call Home contact person. The phone number must be in international format, starting with a + (plus sign) and a country code. |
| Step 7 | UCS-A /monitoring/callhome # set street-address street-addr | Specifies the street address of the main Call Home contact person. |
| Step 8 | UCS-A /monitoring/callhome # set customer-id id-num | Specifies the CCO identification number that includes the contract numbers for the support contract in its entitlements. The number can be up to 255 alphanumeric characters in free format. |

| | Command or Action | Purpose |
|----------------|---|--|
| Step 9 | UCS-A /monitoring/callhome # set contract-id <i>id-num</i> | Specifies the contract identification number from the service agreement. The number can be up to 255 alphanumeric characters in free format. |
| Step 10 | UCS-A /monitoring/callhome # set site-id <i>id-num</i> | Specifies the site identification number from the service agreement. The number can be up to 255 alphanumeric characters in free format. |
| Step 11 | UCS-A /monitoring/callhome # set from-email <i>email-addr</i> | Specifies the email address to use for the From field in Call Home messages. |
| Step 12 | UCS-A /monitoring/callhome # set reply-to-email <i>email-addr</i> | Specifies the email address to use for the Reply To field in Call Home messages. |
| Step 13 | UCS-A /monitoring/callhome # set hostname { <i>hostname</i> <i>ip-addr</i> } | Specifies the hostname or IP address of the SMTP server that Call Home uses to send email messages. |
| Step 14 | UCS-A /monitoring/callhome # set port <i>port-num</i> | Specifies the SMTP server port that Call Home uses to send email messages. Valid port numbers are 1 to 65535. |
| Step 15 | UCS-A /monitoring/callhome # set throttling { <i>off</i> <i>on</i> } | Enables or disables Call Home throttling. When enabled, throttling prevents too many Call Home email messages from being sent for the same event. By default, throttling is enabled. |
| Step 16 | UCS-A /monitoring/callhome # set urgency { <i>alerts</i> <i>critical</i> <i>debugging</i> <i>emergencies</i> <i>errors</i> <i>information</i> <i>notifications</i> <i>warnings</i> } | Specifies the urgency level for Call Home email messages. |
| Step 17 | UCS-A /monitoring/callhome # commit-buffer | Commits the transaction to the system configuration. |

The following example configures Call Home and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring* # scope callhome
UCS-A /monitoring/callhome* # enable
UCS-A /monitoring/callhome* # set contact "Steve Jones"
UCS-A /monitoring/callhome* # set email admin@MyCompany.com
UCS-A /monitoring/callhome* # set phone-contact +1-001-408-555-1234
UCS-A /monitoring/callhome* # set street-address "123 N. Main Street, Anytown, CA, 99885"
UCS-A /monitoring/callhome* # set customer-id 1234567
UCS-A /monitoring/callhome* # set contract-id 99887766
UCS-A /monitoring/callhome* # set site-id 5432112
UCS-A /monitoring/callhome* # set from-email person@MyCompany.com
UCS-A /monitoring/callhome* # set reply-to-email person@MyCompany.com
UCS-A /monitoring/callhome* # set hostname 192.168.100.12
UCS-A /monitoring/callhome* # set port 25
UCS-A /monitoring/callhome* # set throttling on
UCS-A /monitoring/callhome* # set urgency information
UCS-A /monitoring/callhome* # commit-buffer
UCS-A /monitoring/callhome #
```

What to Do Next

Continue to ["Configuring the Default Cisco TAC-1 Profile, page 374"](#) to configure a Call Home profile for use with Smart Call Home.

Configuring the Default Cisco TAC-1 Profile

The following are the default settings for the CiscoTAC-1 profile:

- Level is normal
- Only the CiscoTAC alert group is selected
- Format is xml
- Maximum message size is 5000000

Before You Begin

Complete the ["Configuring Smart Call Home, page 372"](#) section.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A /monitoring/callhome # scope profile CiscoTac-1 | Enters monitoring call home profile mode for the default Cisco TAC-1 profile. |
| Step 2 | UCS-A /monitoring/callhome/profile # set level normal | Specifies the normal event level for the profile. |
| Step 3 | UCS-A /monitoring/callhome/profile # set alertgroups ciscotac | Specifies the ciscotac alert group for the profile. |
| Step 4 | UCS-A /monitoring/callhome/profile # set format xml | Specifies the e-mail message format to xml . |
| Step 5 | UCS-A /monitoring/callhome/profile # set maxsize 5000000 | Specifies the maximum size of 5000000 for email messages. |
| Step 6 | UCS-A /monitoring/callhome/profile # create destination callhome@cisco.com | Specifies the email recipient to callhome@cisco.com . |
| Step 7 | UCS-A /monitoring/callhome/profile/destination # exit | Exits to monitoring call home profile mode. |
| Step 8 | UCS-A /monitoring/callhome/profile # exit | Exits to monitoring call home mode. |

The following example configures the default Cisco TAC-1 profile for use with Smart Call Home:

```
UCS-A /monitoring/callhome* # scope profile CiscoTac-1
UCS-A /monitoring/callhome/profile* # set level normal
UCS-A /monitoring/callhome/profile* # set alertgroups ciscotac
UCS-A /monitoring/callhome/profile* # set format xml
UCS-A /monitoring/callhome/profile* # set maxsize 5000000
UCS-A /monitoring/callhome/profile* # create destination callhome@cisco.com
UCS-A /monitoring/callhome/profile/destination* # exit
```

```
UCS-A /monitoring/callhome/profile* # exit
UCS-A /monitoring/callhome* #
```

What to Do Next

Continue to "[Configuring a System Inventory Message for Smart Call Home, page 375](#)" to configure system inventory messages for use with Smart Call Home.

Configuring a System Inventory Message for Smart Call Home

Before You Begin

Complete the "[Configuring the Default Cisco TAC-1 Profile, page 374](#)" section.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A /monitoring/callhome # scope inventory | Enters monitoring call home inventory mode. |
| Step 2 | UCS-A /monitoring/callhome/inventory # set send-periodically {off on} | Enables or disables the sending of inventory messages. When the on keyword is specified, inventory messages are automatically sent to the Call Home database. |
| Step 3 | UCS-A /monitoring/callhome/inventory # set interval-days <i>intervall-num</i> | Specifies the the time interval (in days) at which inventory messages will be sent. |
| Step 4 | UCS-A /monitoring/callhome/inventory # set timeofday-hour <i>hour</i> | Specifies the hour (using 24-hour format) that inventory messages are sent. |
| Step 5 | UCS-A /monitoring/callhome/inventory # set timeofday-minute <i>minute</i> | Specifies the number of minutes after the hour that inventory messages are sent. |
| Step 6 | UCS-A /monitoring/callhome/inventory # commit-buffer | Commits the transaction to the system configuration. |

The following example configures Call Home system inventory messages and commits the transaction:

```
UCS-A /monitoring/callhome* # scope inventory
UCS-A /monitoring/callhome/inventory* # set send-periodically on
UCS-A /monitoring/callhome/inventory* # set interval-days 15
UCS-A /monitoring/callhome/inventory* # set timeofday-hour 21
UCS-A /monitoring/callhome/inventory* # set timeofday-minute 30
UCS-A /monitoring/callhome/inventory* # commit-buffer
UCS-A /monitoring/callhome/inventory #
```

What to Do Next

Continue to "[Registering Smart Call Home, page 376](#)" to send an inventory message that starts the Smart Call Home registration process.

Registering Smart Call Home

Before You Begin

Complete the "[Configuring a System Inventory Message for Smart Call Home, page 375](#)" section.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A /monitoring/callhome/inventory # send | Sends the system inventory message to the Smart Call Home database. You will receive an email from Cisco that describes how to complete the registration process. |

The following example sends the system inventory message to the Smart Call Home database:

```
UCS-A /monitoring/callhome/inventory # send
```

What to Do Next

Follow the link in the email message to complete the SmartCall Home registration.



CHAPTER 38

Backing Up and Restoring the Configuration

This chapter includes the following sections:

- [Backup and Export Configuration, page 377](#)
- [Backup Types, page 377](#)
- [Considerations and Recommendations for Backup Operations, page 378](#)
- [Import Configuration, page 379](#)
- [Import Methods, page 379](#)
- [System Restore, page 379](#)
- [Required User Role for Backup and Import Operations, page 379](#)
- [Backup Operations, page 379](#)
- [Import Operations, page 383](#)
- [Restoring the Configuration for a Fabric Interconnect, page 387](#)
- [Erasing the Configuration, page 389](#)

Backup and Export Configuration

When you perform a backup through Cisco UCS Manager, you take a snapshot of all or part of the system configuration and export the file to a location on your network. You cannot use Cisco UCS Manager to back up data on the servers.

You can perform a backup while the system is up and running. The backup operation only saves information from the management plane. It does not have any impact on the server or network traffic.

Backup Types

You can perform one or more of the following types of backups through Cisco UCS Manager:

- **Full state**—A binary file that includes a snapshot of the entire system. You can use the file generated from this backup to restore the system during disaster recovery. This file can restore or rebuild the

configuration on the original fabric interconnect, or recreate the configuration on a different fabric interconnect. You cannot use this file for an import.

- **All configuration**—An XML file that includes all system and logical configuration settings. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.
- **System configuration**—An XML file that includes all system configuration settings such as usernames, roles, and locales. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.
- **Logical configuration**—An XML file that includes all logical configuration settings such as service profiles, VLANs, VSANs, pools, and policies. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.

Considerations and Recommendations for Backup Operations

Before you create a backup operation, consider the following:

| | |
|--|--|
| Backup Locations | The backup location is the destination or folder on the network where you want Cisco UCS Manager to export the backup file. You can maintain only one backup operation for each location where you plan to save a backup file. |
| Potential to Overwrite Backup Files | If you rerun a backup operation without changing the filename, Cisco UCS Manager overwrites the existing file on the server. To avoid overwriting existing backup files, change the filename in the backup operation or copy the existing file to another location. |
| Multiple Types of Backups | You can run and export more than one type of backup to the same location. You need to change the backup type before you rerun the backup operation. We recommend that you change the filename for easier identification of the backup type and to avoid overwriting the existing backup file. |
| Scheduled Backups | You cannot schedule a backup operation. You can, however, create a backup operation in advance and leave the admin state disabled until you are ready to run the backup. Cisco UCS Manager does not run the backup operation, save, or export the configuration file until you set the admin state of the backup operation to enabled. |
| Incremental Backups | You cannot perform incremental backups of the Cisco UCS Manager system configuration. |
| Backwards Compatibility | Starting with Release 1.1(1) of the Cisco UCS Manager, full state backups are encrypted so that passwords and other sensitive information are not exported as clear text. As a result, full state backups made from Release 1.1(1) or later cannot be restored to a Cisco UCS instance running an earlier software release. |

Import Configuration

You can import any configuration file that was exported from Cisco UCS Manager. The file does not need to have been exported from the same Cisco UCS Manager.

The import function is available for all configuration, system configuration, and logical configuration files. You can perform an import while the system is up and running. An import operation modifies information on the management plane only. Some modifications caused by an import operation, such as a change to a vNIC assigned to a server, can cause a server reboot or other operations that disrupt traffic.

You cannot schedule an import operation. You can, however, create an import operation in advance and leave the admin state disabled until you are ready to run the import. Cisco UCS Manager will not run the import operation on the configuration file until you set the admin state to enabled.

You can maintain only one import operation for each location where you saved a configuration backup file.

Import Methods

You can use one of the following methods to import and update a system configuration through Cisco UCS Manager:

- **Merge**—The information in the imported configuration file is compared with the existing configuration information. If there are conflicts, the import operation overwrites the information on the Cisco UCS instance with the information in the import configuration file.
- **Replace**—The current configuration information is replaced with the information in the imported configuration file one object at a time.

System Restore

You can restore a system configuration from any full state backup file that was exported from Cisco UCS Manager. The file does not need to have been exported from the Cisco UCS Manager on the system that you are restoring.

The restore function is only available for a full state backup file. You cannot import a full state backup file. You perform a restore through the initial system setup.

You can use the restore function for disaster recovery.

Required User Role for Backup and Import Operations

You must have a user account that includes the admin role to create and run backup and import operations.

Backup Operations

Creating a Backup Operation

Before You Begin

Obtain the backup server IP address and authentication credentials.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # create backup URL backup-type {disabled enabled} | <p>Creates a backup operation. Specify the <i>URL</i> for the backup file using one of the following syntax:</p> <ul style="list-style-type: none"> • ftp://username@hostname/path • scp://username@hostname/path • sftp://username@hostname/path • tftp://hostname:port-num/path <p>The <i>backup-type</i> argument can be one of the following values:</p> <ul style="list-style-type: none"> • all-configuration—Backs up the server-, fabric-, and system-related configuration • logical-configuration—Backs up the fabric- and service profile-related configuration • system-configuration—Backs up the system-related configuration • full-state—Backs up the full state for disaster recovery <p>Note Full-state backup files cannot be imported using an import operation. They are used only to restore the configuration for a fabric interconnect.</p> <p>You can save multiple backup operations, but only one operation for each hostname is saved.</p> <p>If you use the enable keyword, the backup operation automatically runs as soon as you enter the commit-buffer command. If you use the disable keyword, the backup operation will not run until it is enabled. When enabling a backup operation, you must specify the hostname you used when creating the backup operation.</p> |
| Step 3 | UCS-A /system # commit-buffer | Commits the transaction. |

The following example creates a disabled all-configuration backup operation for hostname host35 and commits the transaction:

```
UCS-A# scope system
UCS-A /system* # create backup scp://user@host35/backups/all-config9.bak all-configuration
disabled
Password:
UCS-A /system* # commit-buffer
UCS-A /system #
```

Running a Backup Operation

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope backup <i>hostname</i> | Enters system backup mode for the specified hostname. |
| Step 3 | UCS-A /system/backup # enable | Enables the backup operation. Note For backup operations using FTP, SCP, SFTP, you are prompted for the password. Enter the password before committing the transaction. |
| Step 4 | UCS-A /system/backup # commit-buffer | Commits the transaction. |

The following example enables a backup operation named host35, enters the password for the SCP protocol, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope backup host35
UCS-A /system/backup # enable
Password:
UCS-A /system/backup* # commit-buffer
UCS-A /system/backup #
```

Modifying a Backup Operation

You can modify a backup operation to save a file of another backup type to that location or to change the filename and avoid overwriting previous backup files.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope backup <i>hostname</i> | Enters system backup mode for the specified hostname. |
| Step 3 | UCS-A /system/backup # disable | (Optional) Disables an enabled backup operation so that it does not automatically run when the transaction is committed. |
| Step 4 | UCS-A /system/backup # enable | (Optional) Automatically runs the backup operation as soon as you commit the transaction. |

| | Command or Action | Purpose |
|----------------|--|---|
| Step 5 | UCS-A /system/backup # set descr <i>description</i> | (Optional) Provides a description for the backup operation. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 6 | UCS-A /system/backup # set protocol {ftp scp sftp tftp} | (Optional) Specifies the protocol to use when communicating with the remote server. |
| Step 7 | UCS-A /system/backup # set remote-file <i>filename</i> | (Optional) Specifies the name of the configuration file that is being backed up. |
| Step 8 | UCS-A /system/backup # set type <i>backup-type</i> | (Optional) Specifies the type of backup file to be made. The <i>backup-type</i> argument can be one of the following values: <ul style="list-style-type: none"> • all-configuration—Backs up the server, fabric, and system related configuration • logical-configuration—Backs up the fabric and service profile related configuration • system-configuration—Backs up the system related configuration • full-state—Backs up the full state for disaster recovery Note Full-state backup files cannot be imported using an import operation. They are used only to restore the configuration for a fabric interconnect. |
| Step 9 | UCS-A /system/backup # set preserve-pooled-values {no yes} | (Optional) Specifies whether pool-derived identity values, such as vHBA WWPN, vNIC MAC, WWNN, and UUID, will be saved with the backup. |
| Step 10 | UCS-A /system/backup # set user <i>username</i> | (Optional) Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used. |
| Step 11 | UCS-A /system/backup # set password <i>password</i> | (Optional) Specifies the password for the remote server username. This step does not apply if the TFTP protocol is used. |

| | Command or Action | Purpose |
|----------------|---|---|
| | | Note Cisco UCS Manager does not store this password. Therefore, you do not need to enter this password unless you intend to enable and run the backup operation immediately. |
| Step 12 | UCS-A /system/backup # commit-buffer | Commits the transaction. |

The following example adds a description and changes the protocol, username, and password for the host35 backup operation and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope backup host35
UCS-A /system/backup # set descr "This is a backup operation for host35."
UCS-A /system/backup* # set protocol sftp
UCS-A /system/backup* # set user UserName32
UCS-A /system/backup* # set password
Password:
UCS-A /system/backup* # set preserve-pooled-values no
UCS-A /system/backup* # commit-buffer
UCS-A /system #
```

Deleting a Backup Operation

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # delete backup hostname | Deletes the backup operation for the specified hostname. |
| Step 3 | UCS-A /system # commit-buffer | Commits the transaction. |

The following example deletes a backup operation for the host35 hostname and commits the transaction:

```
UCS-A# scope system
UCS-A /system # delete backup host35
UCS-A /system* # commit-buffer
UCS-A /system #
```

Import Operations

Creating an Import Operation

You cannot import a Full State configuration file. You can import any of the following configuration files:

- All configuration
- System configuration
- Logical configuration

Before You Begin

Collect the following information that you will need to import a configuration file:

- Backup server IP address and authentication credentials
- Fully qualified name of a backup file

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # create import-config <i>URL</i> { disabled enabled } { merge replace } | <p>Creates an import operation. Specify the URL for the file being imported using one of the following syntax:</p> <ul style="list-style-type: none"> • ftp://hostname/path • scp://username@hostname/path • sftp://username@hostname/path • tftp://hostname:port-num/path <p>You can save multiple import operations, but only one operation for each hostname is saved.</p> <p>If you use the enable keyword, the import operation automatically runs as soon as you enter the commit-buffer command. If you use the disable keyword, the import operation will not run until it is enabled. When enabling an import operation, you must specify the hostname you used when creating the import operation.</p> <p>If you use the merge keyword, the configuration information is merged with the existing information. If there are conflicts, the system replaces the information on the current system with the information in the import configuration file. If you use the replace keyword, the system takes each object in the import configuration file and overwrites the corresponding object in the current configuration.</p> |
| Step 3 | UCS-A /system/import-config# set descr <i>description</i> | <p>(Optional)</p> <p>Provides a description for the import operation.</p> <p>Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output.</p> |
| Step 4 | UCS-A /system/import-config # commit-buffer | Commits the transaction. |

The following example creates a disabled import operation for hostname host35 that replaces the existing configuration and commits the transaction:

```
UCS-A# scope system
UCS-A /system* # create import-config scp://user@host35/backups/all-config9.bak disabled
```

```

replace
Password:
UCS-A /system/import-config* # commit-buffer
UCS-A /system/import-config #
    
```

Running an Import Operation

You cannot import a Full State configuration file. You can import any of the following configuration files:

- All configuration
- System configuration
- Logical configuration

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope import-config <i>hostname</i> | Enters system backup mode for the specified hostname. |
| Step 3 | UCS-A /system/import-config # enable | Enables the import operation. |
| Step 4 | UCS-A /system/import-config # commit-buffer | Commits the transaction. |

The following example enables an import operation for the host35 hostname and commits the transaction:

```

UCS-A# scope system
UCS-A /system # scope import-config host35
UCS-A /system/import-config # enable
UCS-A /system/import-config* # commit-buffer
UCS-A /system/import-config #
    
```

Modifying an Import Operation

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # scope import-config <i>hostname</i> | Enters system import configuration mode for the specified hostname. |
| Step 3 | UCS-A /system/import-config # disable | (Optional) Disables an enabled import operation so that it does not automatically run when the transaction is committed. |
| Step 4 | UCS-A /system/import-config # enable | (Optional) Automatically runs the import operation as soon as you commit the transaction. |

| | Command or Action | Purpose |
|----------------|--|---|
| Step 5 | UCS-A /system/import-config # set action {merge replace} | (Optional) Specifies one of the following action types to use for the import operation: <ul style="list-style-type: none"> • Merge—The configuration information is merged with the existing information. If there are conflicts, the system replaces the information on the current system with the information in the import configuration file. • Replace—The system takes each object in the import configuration file and overwrites the corresponding object in the current configuration. |
| Step 6 | UCS-A /system/import-config # set descr <i>description</i> | (Optional) Provides a description for the import operation. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 7 | UCS-A /system/import-config # set password <i>password</i> | (Optional) Specifies the password for the remote server username. This step does not apply if the TFTP protocol is used. Note Cisco UCS Manager does not store this password. Therefore, you do not need to enter this password unless you intend to enable and run the import operation immediately. |
| Step 8 | UCS-A /system/import-config # set protocol {ftp scp sftp tftp} | (Optional) Specifies the protocol to use when communicating with the remote server. |
| Step 9 | UCS-A /system/import-config # set remote-file <i>filename</i> | (Optional) Specifies the name of the configuration file that is being imported. |
| Step 10 | UCS-A /system/import-config # set user <i>username</i> | (Optional) Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used. |
| Step 11 | UCS-A /system/import-config # commit-buffer | Commits the transaction. |

The following example adds a description, changes the password, protocol and username for the host35 import operation, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope import-config host35
UCS-A /system/import-config # set descr "This is an import operation for host35."
UCS-A /system/import-config* # set password
```

```

Password:
UCS-A /system/import-config* # set protocol sftp
UCS-A /system/import-config* # set user jforlenz32
UCS-A /system/import-config* # commit-buffer
UCS-A /system/import-config #

```

Deleting an Import Operation

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope system | Enters system mode. |
| Step 2 | UCS-A /system # delete import-config <i>hostname</i> | Deletes the import operation for the specified hostname. |
| Step 3 | UCS-A /system # commit-buffer | Commits the transaction. |

The following example deletes the import operation for the host35 hostname and commits the transaction:

```

UCS-A# scope system
UCS-A /system # delete import-config host35
UCS-A /system* # commit-buffer
UCS-A /system #

```

Restoring the Configuration for a Fabric Interconnect

Before You Begin

Collect the following information that you will need to restore the system configuration:

- Fabric interconnect management port IP address and subnet mask
- Default gateway IP address
- Backup server IP address and authentication credentials
- Fully qualified name of a Full State backup file



Note You must have access to a Full State configuration file to perform a system restore. You cannot perform a system restore with any other type of configuration or backup file.

Procedure

- Step 1** Connect to the console port.
- Step 2** If the fabric interconnect is off, power on the fabric interconnect.

You will see the power on self-test message as the fabric interconnect boots.

- Step 3** At the installation method prompt, enter **console**.
- Step 4** Enter **restore** to restore the configuration from a full-state backup.
- Step 5** Enter **y** to confirm that you want to restore from a full-state backup.
- Step 6** Enter the IP address for the management port on the fabric interconnect.
- Step 7** Enter the subnet mask for the management port on the fabric interconnect.
- Step 8** Enter the IP address for the default gateway.
- Step 9** Enter one of the following protocols to use when retrieving the backup configuration file:
 - **scp**
 - **ftp**
 - **tftp**
 - **sftp**
- Step 10** Enter the IP address of the backup server.
- Step 11** Enter the full path and filename of the Full State backup file.
- Step 12** Enter the username and password to access the backup server.
The fabric interconnect logs in to the backup server, retrieves a copy of the specified Full State backup file, and restores the system configuration. For a cluster configuration, you do not need to restore the secondary fabric interconnect. As soon as the secondary fabric interconnect reboots, Cisco UCS Manager synchronizes the configuration with the primary fabric interconnect.

The following example restores a system configuration from the Backup.bak file, which was retrieved from the 20.10.20.10 backup server using FTP:

```

Enter the configuration method. (console/gui) ? console

Enter the setup mode; setup newly or restore from backup. (setup/restore) ? restore

NOTE:
  To configure Fabric interconnect using a backup file on a remote server,
  you will need to setup management interface.
  The management interface will be re-configured (if necessary),
  based on information stored in the backup file.

Continue to restore this Fabric interconnect from a backup file (yes/no) ? yes

Physical Switch Mgmt0 IPv4 address : 192.168.10.10

Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 192.168.10.1

Enter the protocol to get backup file (scp/ftp/tftp/sftp) ? scp
Enter the IP address of backup server: 20.10.20.10
Enter fully qualified backup file name: Backup.bak
Enter user ID: user
Enter password:
  Retrieved backup configuration file.
  Configuration file - Ok

```

```

Cisco UCS 6100 Series Fabric Interconnect
UCS-A login:

```

Erasing the Configuration



Caution

You should erase the configuration only when it is necessary. Erasing the configuration completely removes the configuration and reboots the system in an unconfigured state. You must then either restore the configuration from a backup file or perform an initial system setup. For more information on performing an initial system setup, see [System Configuration, page 45](#).

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# connect local-mgmt | Enters the local management CLI. |
| Step 2 | UCS-A(local-mgmt)# erase configuration | Erases the configuration. You are prompted to confirm that you want to erase the configuration. Entering yes erases the configuration and reboots the system in an unconfigured state. |

The following example erases the configuration:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# erase configuration
All UCS configurations will be erased and system will reboot. Are you sure? (yes/no): yes
```




CHAPTER 39

Managing the System Event Log

This chapter includes the following sections:

- [System Event Log, page 391](#)
- [Viewing the System Event Log for a Server, page 392](#)
- [Configuring the SEL Policy, page 393](#)
- [Backing Up the System Event Log for a Server, page 395](#)
- [Clearing the System Event Log for a Server, page 396](#)

System Event Log

The system event log (SEL) resides on the CIMC in NVRAM. It records most server-related events, such as over and under voltage, temperature events, fan events, and events from BIOS. The SEL is mainly used for troubleshooting purposes.

SEL file is approximately 40KB in size, and no further events can be recorded when it is full. It must be cleared before additional events can be recorded.

You can use the SEL policy to backup the SEL to a remote server, and optionally clear the SEL after a backup operation occurs. Backup operations can be triggered based on specific actions, or they can occur at regular intervals. You can also manually backup or clear the SEL.

The backup file is automatically generated. The filename format is `sel-SystemName-ChassisID-ServerID-ServerSerialNumber-Timestamp`; for example, `sel-UCS-A-ch01-serv01-QCI12522939-20091121160736`.

Viewing the System Event Log for a Server

Viewing the System Event Log from Exec Mode

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# <code>show sel chassis-id/blade-id</code> | Displays the system event log for the specified server. |

The following example displays the system event log from Exec mode for blade 3 in chassis 1.

```
UCS-A# show sel 1/3
 1 | 01/01/1970 01:23:27 | System Event 0x83 | Timestamp clock synch | SEL timestamp
clock updated, event is f
irst of pair | Asserted
 2 | 01/01/1970 01:23:28 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to Degraded |
Asserted
 3 | 01/01/1970 01:23:28 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to On Line |
Deasserted
 4 | 01/01/1970 01:23:28 | Platform alert LED_SAS0_FAULT | LED is blinking fast |
Asserted
 5 | 01/01/1970 01:23:28 | Platform alert LED_SAS0_FAULT | LED is on | Deasserted
 6 | 01/01/1970 01:23:28 | Platform alert LED_FPID | LED is on | Asserted
 7 | 01/01/1970 01:23:28 | Platform alert LED_FPID | LED is off | Deasserted
 8 | 01/01/1970 01:23:29 | Entity presence MAIN_POWER | Device Absent | Asserted
 9 | 01/01/1970 01:23:29 | Entity presence MAIN_POWER | Device Present | Deasserted
 a | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED is on | Asserted
 b | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED color is green | Asserted
 c | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED is blinking fast |
Deasserted
 d | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED color is amber | Deasserted
 e | 01/01/1970 00:00:22 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to Degraded |
Asserted
 f | 01/01/1970 00:00:22 | Entity presence MEZZ_PRS | Device Present | Asserted
10 | 01/01/1970 00:00:22 | Entity presence HDD1_PRS | Device Absent | Asserted
```

Viewing the System Event Log from Chassis Server Mode

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# <code>scope server chassis-id/blade-id</code> | Enters chassis server mode for the specified server. |
| Step 2 | UCS-A /chassis/server # <code>show sel</code> | Displays the system event log. |

The following example displays the system event log from chassis server mode for blade 3 in chassis 1.

```
UCS-A# scope server 1/3
UCS-A /chassis/server # show sel
 1 | 01/01/1970 01:23:27 | System Event 0x83 | Timestamp clock synch | SEL timestamp
clock updated, event is f
irst of pair | Asserted
```

```

2 | 01/01/1970 01:23:28 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to Degraded |
  Asserted
3 | 01/01/1970 01:23:28 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to On Line |
  Deasserted
4 | 01/01/1970 01:23:28 | Platform alert LED_SAS0_FAULT | LED is blinking fast |
  Asserted
5 | 01/01/1970 01:23:28 | Platform alert LED_SAS0_FAULT | LED is on | Deasserted
6 | 01/01/1970 01:23:28 | Platform alert LED_FPID | LED is on | Asserted
7 | 01/01/1970 01:23:28 | Platform alert LED_FPID | LED is off | Deasserted
8 | 01/01/1970 01:23:29 | Entity presence MAIN_POWER | Device Absent | Asserted
9 | 01/01/1970 01:23:29 | Entity presence MAIN_POWER | Device Present | Deasserted
a | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED is on | Asserted
  b | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED color is green | Asserted
  c | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED is blinking fast |
  Deasserted
  d | 01/01/1970 01:23:29 | Platform alert LED_SAS0_FAULT | LED color is amber | Deasserted
  e | 01/01/1970 00:00:22 | Drive slot(Bay) SAS0_LINK_STATUS | Transition to Degraded |
  Asserted
  f | 01/01/1970 00:00:22 | Entity presence MEZZ_PRS | Device Present | Asserted
10 | 01/01/1970 00:00:22 | Entity presence HDD1_PRS | Device Absent | Asserted

```

Configuring the SEL Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope ep-log-policy sel | Enters organization endpoint log policy mode and scopes the SEL policy. |
| Step 3 | UCS-A /org/ep-log-policy # set description <i>description</i> | (Optional) Provides a description for the policy. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /org/ep-log-policy # set backup action [log-full] [on-change-of-association] [on-clear] [timer] [none] | Specifies an action or actions that will trigger a backup operation. |
| Step 5 | UCS-A /org/ep-log-policy # set backup clear-on-backup { no yes } | Specifies whether to clear the system event log after a backup operation occurs. |
| Step 6 | UCS-A /org/ep-log-policy # set backup destination <i>URL</i> | Specifies the protocol, user, password, remote hostname, and remote path for the backup operation. Depending on the protocol used, specify the URL using one of the following syntax: • ftp://hostname/path |

| | Command or Action | Purpose |
|----------------|---|---|
| | | <ul style="list-style-type: none"> • <code>scp://username@hostname/path</code> • <code>sftp://username@hostname/path</code> • <code>tftp://hostname:port-num/path</code> <p>Note You can also specify the backup destination by using the <code>set backup hostname</code>, <code>set backup password</code>, <code>set backup protocol</code>, <code>set backup remote-path</code>, <code>set backup user</code> commands, or by using the <code>set backup destination</code> command. Use either method to specify the backup destination.</p> |
| Step 7 | <code>UCS-A /org/ep-log-policy # set backup format {ascii binary}</code> | Specifies the format for the backup file. |
| Step 8 | <code>UCS-A /org/ep-log-policy # set backup hostname {hostname ip-addr}</code> | Specifies the hostname or IP address of the remote server. |
| Step 9 | <code>UCS-A /org/ep-log-policy # set backup interval {1-hour 2-hours 4-hours 8-hours 24-hours never}</code> | Specifies the time interval for the automatic backup operation. Specifying the never keyword means that automatic backups will not be made. |
| Step 10 | <code>UCS-A /org/ep-log-policy # set backup password password</code> | Specifies the password for the username. This step does not apply if the TFTP protocol is used. |
| Step 11 | <code>UCS-A /org/ep-log-policy # set backup protocol {ftp scp sftp tftp}</code> | Specifies the protocol to use when communicating with the remote server. |
| Step 12 | <code>UCS-A /org/ep-log-policy # set backup remote-path path</code> | Specifies the path on the remote server where the backup file is to be saved. |
| Step 13 | <code>UCS-A /org/ep-log-policy # set backup user username</code> | Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used. |
| Step 14 | <code>UCS-A /org/ep-log-policy # commit-buffer</code> | Commits the transaction. |

The following example configures the SEL policy to back up the system event log (in ascii format) every 24 hours or when the log is full and clear the system event log after a backup operation occurs and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope ep-log-policy sel
UCS-A /org/ep-log-policy # set backup destination scp://user@192.168.1.10/logs
Password:
UCS-A /org/ep-log-policy* # set backup action log-full
UCS-A /org/ep-log-policy* # set backup clear-on-backup yes
UCS-A /org/ep-log-policy* # set backup format ascii
UCS-A /org/ep-log-policy* # set backup interval 24-hours
UCS-A /org/ep-log-policy* # commit-buffer
UCS-A /org/ep-log-policy #
```

Backing Up the System Event Log for a Server

Backing Up the System Event Log from Exec Mode

Before You Begin

Configure the system event log policy. The manual backup operation uses the remote destination configured in the system event log policy.

Procedure

| | Command or Action | Purpose |
|---------------|---|------------------------------|
| Step 1 | UCS-A /chassis/server # backup sel <i>chassis-id/blade-id</i> | Clears the system event log. |
| Step 2 | UCS-A# commit-buffer | Commits the transaction. |

The following example backs up the system event log from exec mode for blade 3 in chassis 1 and commits the transaction.

```
UCS-A# backup sel 1/3
UCS-A* # commit-buffer
UCS-A#
```

Backing Up the System Event Log from Chassis Server Mode

Before You Begin

Configure the system event log policy. The manual backup operation uses the remote destination configured in the system event log policy.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope server <i>chassis-id/blade-id</i> | Enters chassis server mode for the specified server. |
| Step 2 | UCS-A /chassis/server # backup sel | Clears the system event log. |
| Step 3 | UCS-A /chassis/server # commit-buffer | Commits the transaction. |

The following example backs up the system event log from chassis server mode for blade 3 in chassis 1 and commits the transaction.

```
UCS-A# scope server 1/3
UCS-A /chassis/server # backup sel
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```

Clearing the System Event Log for a Server

Clearing the System Event Log from Exec Mode

Procedure

| | Command or Action | Purpose |
|---------------|---|------------------------------|
| Step 1 | UCS-A# <code>clear sel chassis-id/blade-id</code> | Clears the system event log. |
| Step 2 | UCS-A# <code>commit-buffer</code> | Commits the transaction. |

The following example clears the system event log from Exec mode for blade 3 in chassis 1 and commits the transaction:

```
UCS-A# clear sel 1/3
UCS-A* # commit-buffer
UCS-A#
```

Clearing the System Event Log from Chassis Server Mode

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# <code>scope server chassis-id/blade-id</code> | Enters chassis server mode for the specified server. |
| Step 2 | UCS-A /chassis/server # <code>clear sel</code> | Clears the system event log. |
| Step 3 | UCS-A /chassis/server # <code>commit-buffer</code> | Commits the transaction. |

The following example clears the system event log from chassis server mode for blade 3 in chassis 1 and commits the transaction:

```
UCS-A# scope server 1/3
UCS-A /chassis/server # clear sel
UCS-A /chassis/server* # commit-buffer
UCS-A /chassis/server #
```



CHAPTER 40

Configuring Settings for Faults, Events, and Logs

This chapter includes the following sections:

- [Configuring Settings for the Fault Collection Policy, page 397](#)
- [Configuring Settings for the Core File Exporter, page 398](#)
- [Configuring the Syslog, page 400](#)

Configuring Settings for the Fault Collection Policy

Fault Collection Policy

The fault collection policy controls the lifecycle of a fault in a Cisco UCS instance, including when faults are cleared, the flapping interval (the length of time between the fault being raised and the condition being cleared), and the retention interval (the length of time a fault is retained in the system).

A fault in Cisco UCS has the following lifecycle:

- 1 A condition occurs in the system and Cisco UCS Manager raises a fault. This is the active state.
- 2 When the fault is alleviated, it is cleared if the time between the fault being raised and the condition being cleared is greater than the flapping interval, otherwise, the fault remains raised but its status changes to soaking-clear. Flapping occurs when a fault is raised and cleared several times in rapid succession. During the flapping interval the fault retains its severity for the length of time specified in the fault collection policy.
- 3 If the condition reoccurs during the flapping interval, the fault remains raised and its status changes to flapping. If the condition does not reoccur during the flapping interval, the fault is cleared.
- 4 When a fault is cleared, it is deleted if the clear action is set to delete, or if the fault was previously acknowledged; otherwise, it is retained until either the retention interval expires, or if the fault is acknowledged.
- 5 If the condition reoccurs during the retention interval, the fault returns to the active state. If the condition does not reoccur, the fault is deleted.

Configuring the Fault Collection Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # scope fault policy | Enters monitoring fault policy mode. |
| Step 3 | UCS-A /monitoring/fault-policy # set clear-action {delete retain} | Specifies whether to retain or delete all cleared messages. If the retain option is specified, then the length of time that the messages are retained is determined by the set retention-interval command. |
| Step 4 | UCS-A /monitoring/fault-policy # set flap-interval seconds | Specifies the time interval (in seconds) the system waits before changing a fault state. Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change state until the flapping interval has elapsed after the last state change. If the fault is raised again during the flapping interval, it returns to the active state, otherwise, the fault is cleared. |
| Step 5 | UCS-A /monitoring/fault-policy # set retention-interval {days hours minutes seconds forever} | Specifies the time interval the system retains all cleared fault messages before deleting them. The system can retain cleared fault messages forever, or for the specified number of days, hours, minutes, and seconds. |
| Step 6 | UCS-A /monitoring/fault-policy # commit-buffer | Commits the transaction. |

This example configures the fault collection policy to retain cleared fault messages for 30 days, sets the flapping interval to 10 seconds, and commits the transaction.

```
UCS-A# scope monitoring
UCS-A /monitoring # scope fault policy
UCS-A /monitoring/fault-policy # set clear-action retain
UCS-A /monitoring/fault-policy* # set flap-interval 10
UCS-A /monitoring/fault-policy* # set retention-interval 30 0 0 0
UCS-A /monitoring/fault-policy* # commit-buffer
UCS-A /monitoring/fault-policy #
```

Configuring Settings for the Core File Exporter

Core File Exporter

Cisco UCS Manager uses the Core File Exporter to export core files as soon as they occur to a specified location on the network through TFTP. This functionality allows you to export the tar file with the contents of the core file.

Configuring the Core File Exporter

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # scope sysdebug | Enters monitoring system debug mode. |
| Step 3 | UCS-A /monitoring/sysdebug # enable core-export-target | Enables the core file exporter. When the core file exporter is enabled and an error causes the server to perform a core dump, the system exports the core file via TFTP to the specified remote server. |
| Step 4 | UCS-A /monitoring/sysdebug # set core-export-target path path | Specifies the path to use when exporting the core file to the remote server. |
| Step 5 | UCS-A /monitoring/sysdebug # set core-export-target port port-num | Specifies the port number to use when exporting the core file via TFTP. The range of valid values is 1 to 65,535. |
| Step 6 | UCS-A /monitoring/sysdebug # set core-export-target server-description description | Provides a description for the remote server used to store the core file. |
| Step 7 | UCS-A /monitoring/sysdebug # set core-export-target server-name hostname | Specifies the hostname of the remote server to connect with via TFTP. |
| Step 8 | UCS-A /monitoring/sysdebug # commit-buffer | Commits the transaction. |

The following example enables the core file exporter, specifies the path and port to use when sending the core file, specifies the remote server hostname, provides a description for the remote server, and commits the transaction.

```
UCS-A# scope monitoring
UCS-A /monitoring # scope sysdebug
UCS-A /monitoring/sysdebug # enable core-export-target
UCS-A /monitoring/sysdebug* # set core-export-target path /root/CoreFiles/core
UCS-A /monitoring/sysdebug* # set core-export-target port 45000
UCS-A /monitoring/sysdebug* # set core-export-target server-description CoreFile102.168.10.10
UCS-A /monitoring/sysdebug* # set core-export-target server-name 192.168.10.10
UCS-A /monitoring/sysdebug* # commit-buffer
UCS-A /monitoring/sysdebug #
```

Disabling the Core File Exporter

Procedure

| | Command or Action | Purpose |
|---------------|--------------------------------|-------------------------|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 2 | UCS-A /monitoring # scope sysdebug | Enters monitoring system debug mode. |
| Step 3 | UCS-A /monitoring/sysdebug # disable core-export-target | Disables the core file exporter. When the core file exporter is disabled core files are not automatically exported. |
| Step 4 | UCS-A /monitoring/sysdebug # commit-buffer | Commits the transaction. |

The following example disables the core file exporter and commits the transaction.

```
UCS-A# scope monitoring
UCS-A /monitoring # scope sysdebug
UCS-A /monitoring/sysdebug # disable core-export-target
UCS-A /monitoring/sysdebug* # commit-buffer
UCS-A /monitoring/sysdebug #
```

Configuring the Syslog

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A /monitoring # { enable disable } syslog console | Enables or disables the sending of syslog to the console. |
| Step 3 | UCS-A /monitoring # set syslog console level { emergencies alerts critical } | (Optional) Select the lowest message level that you want displayed. If syslogs are enabled, the system displays that level and above on the console. The level options are listed in order of decreasing urgency. The default level is Critical. |
| Step 4 | UCS-A /monitoring # { enable disable } syslog monitor | Enables or disables the monitoring of syslog information by the operating system. |
| Step 5 | UCS-A /monitoring # set syslog monitor level { emergencies critical errors warnings notifications information debugging } | (Optional) Select the lowest message level that you want displayed. If the monitor state is enabled, the system displays that level and above. The level options are listed in order of decreasing urgency. The default level is Critical. Note Messages at levels below Critical are displayed on the terminal monitor only if you have entered the terminal monitor command. |

| | Command or Action | Purpose |
|----------------|---|---|
| Step 6 | UCS-A /monitoring # {enable disable} syslog file | Enables or disables the writing of syslog information to a syslog file. |
| Step 7 | UCS-A /monitoring # set syslog file name filename | The name of the file in which the messages are logged. Up to 16 characters are allowed in the file name. |
| Step 8 | UCS-A /monitoring # set syslog file level {emergencies alerts critical errors warnings notifications information debugging} | (Optional) Select the lowest message level that you want stored to a file. If the file state is enabled, the system stores that level and above in the syslog file. The level options are listed in order of decreasing urgency. The default level is Critical. |
| Step 9 | UCS-A /monitoring # set syslog file size filesize | (Optional) The maximum file size, in bytes, before the system begins to write over the oldest messages with the newest ones. The range is 4096 to 4194304 bytes. |
| Step 10 | UCS-A /monitoring # {enable disable} syslog remote-destination {server-1 server-2 server-3} | Enables or disables the sending of syslog messages to up to three external syslog servers. |
| Step 11 | UCS-A /monitoring # set syslog remote-destination {server-1 server-2 server-3} level {emergencies alerts critical errors warnings notifications information debugging} | (Optional) Select the lowest message level that you want stored to the external log. If the remote-destination is enabled, the system sends that level and above to the external server. The level options are listed in order of decreasing urgency. The default level is Critical. |
| Step 12 | UCS-A /monitoring # set syslog remote-destination {server-1 server-2 server-3} hostname hostname | The hostname or IP address of the specified remote syslog server. Up to 256 characters are allowed in the hostname. |
| Step 13 | UCS-A /monitoring # set syslog remote-destination {server-1 server-2 server-3} facility {local0 local1 local2 local3 local4 local5 local6 local7} | (Optional) The facility level contained in the syslog messages sent to the specified remote syslog server. |
| Step 14 | UCS-A /monitoring # commit-buffer | Commits the transaction. |

This example shows how to enable the storage of syslog messages in a local file and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # disable syslog console
UCS-A /monitoring* # disable syslog monitor
UCS-A /monitoring* # enable syslog file
UCS-A /monitoring* # set syslog file name SysMsgsUCSA
UCS-A /monitoring* # set syslog file level notifications
UCS-A /monitoring* # set syslog file size 4194304
UCS-A /monitoring* # disable syslog remote-destination server-1
UCS-A /monitoring* # disable syslog remote-destination server-2
UCS-A /monitoring* # disable syslog remote-destination server-3
UCS-A /monitoring* # commit-buffer
UCS-A /monitoring #
```




CHAPTER 41

Recovering a Lost Password

This chapter includes the following sections:

- [Password Recovery for the Admin Account, page 403](#)
- [Determining the Leadership Role of a Fabric Interconnect, page 403](#)
- [Recovering the Admin Account Password in a Standalone Configuration, page 404](#)
- [Recovering the Admin Account Password in a Cluster Configuration, page 405](#)

Password Recovery for the Admin Account

The admin account is the system administrator or superuser account. If an administrator loses the password to this account, you can have a serious security issue. As a result, the procedure to recover the password for the admin account requires you to power cycle all fabric interconnects in a Cisco UCS instance.

When you recover the password for the admin account, you actually change the password for that account. You cannot retrieve the original password for that account.

You can reset the password for all other local accounts through Cisco UCS Manager. However, you must log in to Cisco UCS Manager with an account that includes aaa or admin privileges.



Caution

This procedure requires you to power down all fabric interconnects in a Cisco UCS instance. As a result, all data transmission in the instance is stopped until you restart the fabric interconnects.

Determining the Leadership Role of a Fabric Interconnect

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# <code>show cluster state</code> | Displays the operational state and leadership role for both fabric interconnects in a cluster. |

The following example displays the leadership role for both fabric interconnects in a cluster, where fabric interconnect A has the primary role and fabric interconnect B has the subordinate role:

```
UCS-A# show cluster state
Cluster Id: 0x4432f72a371511de-0xb97c000de1b1ada4

A: UP, PRIMARY
B: UP, SUBORDINATE

HA READY
```

Recovering the Admin Account Password in a Standalone Configuration

This procedure will help you to recover the password that you set for the admin account when you performed an initial system setup on the fabric interconnect. The admin account is the system administrator or superuser account.

Before You Begin

- 1 Physically connect the console port on the fabric interconnect to a computer terminal or console server
- 2 Determine the running versions of the following firmware:
 - The firmware kernel version on the fabric interconnect
 - The firmware system version



Tip

To find this information, you can log in with any user account on the Cisco UCS instance.

Procedure

- Step 1** Connect to the console port.
- Step 2** Power cycle the fabric interconnect:
 - a) Turn off the power to the fabric interconnect.
 - b) Turn on the power to the fabric interconnect.
- Step 3** In the console, press one of the following key combinations as it boots to get the loader prompt:
 - Ctrl+l
 - Ctrl+Shift+r

You may need to press the selected key combination multiple times before your screen displays the loader prompt.

- Step 4** Boot the kernel firmware version on the fabric interconnect.


```
loader > boot /installables/switch/kernel_firmware_version
```

Example:

```
loader > boot /installables/switch/ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin
```

- Step 5** Enter config terminal mode.


```
Fabric (boot) # config terminal
```

Step 6 Reset the admin password.

```
Fabric(boot) (config) # admin-passwordpassword
```

Choose a strong password that includes at least one capital letter and one number. The password cannot be blank.

The new password displays in clear text mode.

Step 7 Exit config terminal mode and return to the boot prompt.

Step 8 Boot the system firmware version on the fabric interconnect.

```
Fabric(boot) # load /installables/switch/system_firmware_version
```

Example:

```
Fabric(boot) # load /installables/switch/ucs-6100-k9-system.4.1.3.N2.1.0.211.bin
```

Step 9 After the system image loads, log in to Cisco UCS Manager.

Recovering the Admin Account Password in a Cluster Configuration

This procedure will help you to recover the password that you set for the admin account when you performed an initial system setup on the fabric interconnects. The admin account is the system administrator or superuser account.

Before You Begin

- 1 Physically connect a console port on one of the fabric interconnects to a computer terminal or console server
- 2 Obtain the following information:
 - The firmware kernel version on the fabric interconnect
 - The firmware system version
 - Which fabric interconnect has the primary leadership role and which is the subordinate



Tip

To find this information, you can log in with any user account on the Cisco UCS instance.

Procedure

Step 1 Connect to the console port.

Step 2 For the subordinate fabric interconnect:

- a) Turn off the power to the fabric interconnect.
- b) Turn on the power to the fabric interconnect.
- c) In the console, press one of the following key combinations as it boots to get the loader prompt:
 - Ctrl+l
 - Ctrl+Shift+r

You may need to press the selected key combination multiple times before your screen displays the loader prompt.

Step 3 Power cycle the primary fabric interconnect:

- a) Turn off the power to the fabric interconnect.
- b) Turn on the power to the fabric interconnect.

Step 4 In the console, press one of the following key combinations as it boots to get the loader prompt:

- Ctrl+l
- Ctrl+Shift+r

You may need to press the selected key combination multiple times before your screen displays the loader prompt.

Step 5 Boot the kernel firmware version on the primary fabric interconnect.

```
loader > boot /installables/switch/kernel_firmware_version
```

Example:

```
loader > boot /installables/switch/ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin
```

Step 6 Enter config terminal mode.

```
Fabric (boot) # config terminal
```

Step 7 Reset the admin password.

```
Fabric (boot) (config) # admin-password password
```

Choose a strong password that includes at least one capital letter and one number. The password cannot be blank.

The new password displays in clear text mode.

Step 8 Exit config terminal mode and return to the boot prompt.

Step 9 Boot the system firmware version on the primary fabric interconnect.

```
Fabric (boot) # load /installables/switch/system_firmware_version
```

Example:

```
Fabric (boot) # load /installables/switch/ucs-6100-k9-system.4.1.3.N2.1.0.211.bin
```

Step 10 After the system image loads, log in to Cisco UCS Manager.

Step 11 In the console for the subordinate fabric interconnect, do the following to bring it up:

- a) Boot the kernel firmware version on the subordinate fabric interconnect.

```
loader > boot /installables/switch/kernel_firmware_version
```

- b) Boot the system firmware version on the subordinate fabric interconnect.

```
Fabric (boot) # load /installables/switch/system_firmware_version
```



CHAPTER 42

Configuring Statistics-Related Policies

This chapter includes the following sections:

- [Statistics Collection Policies](#), page 407
- [Statistics Threshold Policies](#), page 408

Statistics Collection Policies

Statistics Collection Policy

A statistics collection policy defines how frequently statistics are to be collected (collection interval) and how frequently the statistics are to be reported (reporting interval). Reporting intervals are longer than collection intervals so that multiple statistical data points can be collected during the reporting interval, which provides Cisco UCS Manager with sufficient data to calculate and report minimum, maximum, and average values.

For NIC statistics, Cisco UCS Manager displays the average, minimum, and maximum of the change since the last collection of statistics. If the values are 0, there has been no change since the last collection.

Statistics can be collected and reported for the following five functional areas of the Cisco UCS system:

- Adapter—statistics related to the adapters
- Chassis—statistics related to the blade chassis
- Host—this policy is a placeholder for future support
- Port—statistics related to the ports, including server ports, uplink Ethernet ports, and uplink Fibre Channel ports
- Server—statistics related to servers



Note

Cisco UCS Manager has one default statistics collection policy for each of the five functional areas. You cannot create additional statistics collection policies and you cannot delete the existing default policies. You can only modify the default policies.

Configuring a Statistics Collection Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope monitoring | Enters monitoring mode. |
| Step 2 | UCS-A/monitoring # scope stats-collection-policy { adapter chassis host port server } | Enters statistics collection policy mode for the specified policy type. |
| Step 3 | UCS-A /monitoring/stats-collection-policy # set collection-interval { 1minute 2minutes 30seconds 5minutes } | Specifies the interval at which statistics are collected from the system. |
| Step 4 | UCS-A /monitoring/stats-collection-policy # set reporting-interval { 15minutes 30minutes 60minutes } | Specifies the interval at which collected statistics are reported. |
| Step 5 | UCS-A /monitoring/stats-collection-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example creates a statistics collection policy for ports, sets the collection interval to one minute, the reporting interval to 30 minutes, and commits the transaction:

```
UCS-A# scope monitoring
UCS-A /monitoring # scope stats-collection-policy port
UCS-A /monitoring/stats-collection-policy* # set collection-interval 1minute
UCS-A /monitoring/stats-collection-policy* # set reporting-interval 30minutes
UCS-A /monitoring/stats-collection-policy* # commit-buffer
UCS-A /monitoring/stats-collection-policy #
```

Statistics Threshold Policies

Statistics Threshold Policy

A statistics threshold policy monitors statistics about certain aspects of the system and generates an event if the threshold is crossed. You can set both minimum and maximum thresholds. For example, you can configure the policy to raise an alarm if the CPU temperature exceeds a certain value, or if a server is overutilized or underutilized.

These threshold policies do not control the hardware or device-level thresholds enforced by endpoints, such as the CIMC. Those thresholds are burned in to the hardware components at manufacture.

Cisco UCS enables you to configure statistics threshold policies for the following components:

- Servers and server components
- Uplink Ethernet ports
- Ethernet server ports, chassis, and fabric interconnects
- Fibre Channel port



Note You cannot create or delete a statistics threshold policy for Ethernet server ports, uplink Ethernet ports, or uplink Fibre Channel ports. You can only configure the existing default policy.

Server and Server Component Statistics Threshold Policy Configuration

Configuring a Server and Server Component Statistics Threshold Policy

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # create stats-threshold-policy <i>policy-name</i> | Creates the specified statistics threshold policy and enters organization statistics threshold policy mode. |
| Step 3 | UCS-A /org/stats-threshold-policy # set descr <i>description</i> | (Optional) Provides a description for the policy. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /org/stats-threshold-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example creates the server and server component statistics threshold policy named ServStatsPolicy, provides a description for the policy, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # create stats-threshold-policy ServStatsPolicy
UCS-A /org/stats-threshold-policy* # set descr "Server stats threshold policy."
UCS-A /org/stats-threshold-policy* # commit-buffer
UCS-A /org/stats-threshold-policy #
```

What to Do Next

Configure one or more policy classes for the statistics threshold policy. For more information, see "[Configuring a Server and Server Component Statistics Threshold Policy Class](#), page 410."

Deleting a Server and Server Component Statistics Threshold Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # delete stats-threshold-policy <i>policy-name</i> | Deletes the specified statistics threshold policy. |
| Step 3 | UCS-A /org # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the server and server component statistics threshold policy named ServStatsPolicy and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # delete stats-threshold-policy ServStatsPolicy
UCS-A /org* # commit-buffer
UCS-A /org #
```

Configuring a Server and Server Component Statistics Threshold Policy Class

Before You Begin

Configure or identify the server and server component statistics threshold policy that will contain the policy class. For more information, see "[Configuring a Server and Server Component Statistics Threshold Policy, page 409.](#)"

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope stats-threshold-policy <i>policy-name</i> | Enters organization statistics threshold policy mode. |
| Step 3 | UCS-A /org/stats-threshold-policy # create class <i>class-name</i> | Creates the specified statistics threshold policy class and enters organization statistics threshold policy class mode. The <i>class-name</i> argument can be any of the class name keywords available for the particular statistics threshold policy being configured. To see a list of the available class name keywords, enter the create class ? command in organization statistics threshold policy mode. Note You can configure multiple classes for the statistics threshold policy. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 4 | UCS-A /org/stats-threshold-policy /class # create property <i>property-name</i> | Creates the specified statistics threshold policy class property and enters organization statistics threshold policy class property mode. The <i>property-name</i> argument can be any of the property name keywords available for the particular policy class being configured. To see a list of the available property name keywords, enter the create property ? command in organization statistics threshold policy class mode. Note You can configure multiple properties for the policy class. |
| Step 5 | UCS-A /org/stats-threshold-policy/class/property # set normal-value <i>value</i> | Specifies the normal value for the class property. The <i>value</i> format can vary depending on the class property being configured. To see the required format, enter the set normal-value ? command in organization statistics threshold policy class property mode. |
| Step 6 | UCS-A /org/stats-threshold-policy /class/property # create threshold-value { above-normal below-normal } { cleared condition critical info major minor warning } | Creates the specified threshold value for the class property and enters organization statistics threshold policy class property threshold value mode. Note You can configure multiple threshold values for the class property. |
| Step 7 | UCS-A /org/stats-threshold-policy /class/property/threshold-value # set { deescalating escalating } <i>value</i> | Specifies the de-escalating or escalating class property threshold value. The <i>value</i> format can vary depending on the class property threshold value being configured. To see the required format, enter the set deescalating ? or set escalating ? command in organization statistics threshold policy class property threshold value mode. Note You can specify both de-escalating and escalating class property threshold values. |
| Step 8 | UCS-A /org/stats-threshold-policy /class/property/threshold-value # commit-buffer | Commits the transaction to the system configuration. |

The following example creates the server and server component statistics threshold policy class for CPU statistics, creates a CPU temperature property, specifies that the normal CPU temperature is 48.5° C, creates an above normal warning threshold of 50° C, and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope stats-threshold-policy ServStatsPolicy
UCS-A /org/stats-threshold-policy* # create class cpu-stats
UCS-A /org/stats-threshold-policy/class* # create property cpu-temp
UCS-A /org/stats-threshold-policy/class/property* # set normal-value 48.5
UCS-A /org/stats-threshold-policy/class/property* # create threshold-value above-normal
warning
UCS-A /org/stats-threshold-policy/class/property/threshold-value* # set escalating 50.0
UCS-A /org/stats-threshold-policy/class/property/threshold-value* # commit-buffer
UCS-A /org/stats-threshold-policy/class/property/threshold-value #
```

Deleting a Server and Server Component Statistics Threshold Policy Class

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope org <i>org-name</i> | Enters organization mode for the specified organization. To enter the root organization mode, type / as the <i>org-name</i> . |
| Step 2 | UCS-A /org # scope stats-threshold-policy <i>policy-name</i> | Enters the specified statistics threshold policy. |
| Step 3 | UCS-A /org/stats-threshold-policy # delete class <i>class-name</i> | Deletes the specified statistics threshold policy class from the policy. |
| Step 4 | UCS-A /org/stats-threshold-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the server and server component statistics threshold policy class for CPU statistics and commits the transaction:

```
UCS-A# scope org /
UCS-A /org* # scope stats-threshold-policy ServStatsPolicy
UCS-A /org/stats-threshold-policy* # delete class cpu-stats
UCS-A /org/stats-threshold-policy* # commit-buffer
UCS-A /org/stats-threshold-policy #
```

Uplink Ethernet Port Statistics Threshold Policy Configuration

Configuring an Uplink Ethernet Port Statistics Threshold Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # scope stats-threshold-policy default | Enters Ethernet uplink statistics threshold policy mode. Note You cannot create (or delete) an uplink Ethernet port statistics threshold policy. You can only enter (scope to) the existing default policy. |
| Step 3 | UCS-A /eth-uplink/stats-threshold-policy # set descr <i>description</i> | (Optional) Provides a description for the policy. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 4 | UCS-A /eth-uplink/stats-threshold-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example enters the default uplink Ethernet port threshold policy, provides a description for the policy, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink* # scope stats-threshold-policy default
UCS-A /eth-uplink/stats-threshold-policy* # set descr "Uplink Ethernet port stats threshold
policy."
UCS-A /eth-uplink/stats-threshold-policy* # commit-buffer
UCS-A /eth-uplink/stats-threshold-policy #
```

What to Do Next

Configure one or more policy classes for the statistics threshold policy. For more information, see "[Configuring an Uplink Ethernet Port Statistics Threshold Policy Class](#), page 413."

Configuring an Uplink Ethernet Port Statistics Threshold Policy Class

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # scope stats-threshold-policy default | Enters Ethernet uplink statistics threshold policy mode. |
| Step 3 | UCS-A /eth-uplink/stats-threshold-policy # create class class-name | Creates the specified statistics threshold policy class and enters Ethernet uplink statistics threshold policy class mode. The <i>class-name</i> argument can be any of the class name keywords available for the particular statistics threshold policy being configured. To see a list of the available class name keywords, enter the create class ? command in Ethernet uplink statistics threshold policy mode. Note You can configure multiple classes for the statistics threshold policy. |
| Step 4 | UCS-A /eth-uplink/stats-threshold-policy /class # create property property-name | Creates the specified statistics threshold policy class property and enters Ethernet uplink statistics threshold policy class property mode. The <i>property-name</i> argument can be any of the property name keywords available for the particular policy class being configured. To see a list of the available property name keywords, enter the create property ? command in Ethernet uplink statistics threshold policy class mode. Note You can configure multiple properties for the policy class. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 5 | UCS-A /eth-uplink/stats-threshold-policy /class/property # set normal-value <i>value</i> | Specifies the normal value for the class property. The <i>value</i> format can vary depending on the class property being configured. To see the required format, enter the set normal-value ? command in Ethernet uplink statistics threshold policy class property mode. |
| Step 6 | UCS-A /eth-uplink/stats-threshold-policy /class/property # create threshold-value { above-normal below-normal } { cleared condition critical info major minor warning } | Creates the specified threshold value for the class property and enters Ethernet uplink statistics threshold policy class property threshold value mode. Note You can configure multiple threshold values for the class property. |
| Step 7 | UCS-A /eth-uplink/stats-threshold-policy /class/property/threshold-value # set { deescalating escalating } <i>value</i> | Specifies the de-escalating or escalating class property threshold value. The <i>value</i> format can vary depending on the class property threshold value being configured. To see the required format, enter the set deescalating ? or set escalating ? command in Ethernet uplink statistics threshold policy class property threshold value mode. Note You can specify both de-escalating and escalating class property threshold values. |
| Step 8 | UCS-A /eth-uplink/stats-threshold-policy /class/property/threshold-value # commit-buffer | Commits the transaction to the system configuration. |

The following example creates the uplink Ethernet port statistics threshold policy class for Ethernet error statistics, creates a cyclic redundancy check (CRC) error count property, specifies that the normal CRC error count for each polling interval is 1000, creates an above normal warning threshold of 1250, and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink* # scope stats-threshold-policy default
UCS-A /eth-uplink/stats-threshold-policy* # create class ether-error-stats
UCS-A /eth-uplink/stats-threshold-policy/class* # create property crc-delta
UCS-A /eth-uplink/stats-threshold-policy/class/property* # set normal-value 1000
UCS-A /eth-uplink/stats-threshold-policy/class/property* # create threshold-value above-normal
warning
UCS-A /eth-uplink/stats-threshold-policy/class/property/threshold-value* # set escalating
1250
UCS-A /eth-uplink/stats-threshold-policy/class/property/threshold-value* # commit-buffer
UCS-A /eth-uplink/stats-threshold-policy/class/property/threshold-value #
```

Deleting an Uplink Ethernet Port Statistics Threshold Policy Class

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope eth-uplink | Enters Ethernet uplink mode. |
| Step 2 | UCS-A /eth-uplink # scope stats-threshold-policy default | Enters Ethernet uplink statistics threshold policy mode. |
| Step 3 | UCS-A /eth-uplink/stats-threshold-policy # delete class class-name | Deletes the specified statistics threshold policy class from the policy. |
| Step 4 | UCS-A /eth-uplink/stats-threshold-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the uplink Ethernet port statistics threshold policy class for Ethernet error statistics and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope stats-threshold-policy default
UCS-A /eth-uplink/stats-threshold-policy # delete class ether-error-stats
UCS-A /eth-uplink/stats-threshold-policy* # commit-buffer
UCS-A /eth-uplink/stats-threshold-policy #
```

Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Configuration

Configuring a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope eth-server | Enters Ethernet server mode. |
| Step 2 | UCS-A /eth-server # scope stats-threshold-policy default | Enters Ethernet server statistics threshold policy mode. Note You cannot create (or delete) a server port, chassis, and fabric interconnect statistics threshold policy. You can only enter (scope to) the existing default policy. |
| Step 3 | UCS-A /eth-server/stats-threshold-policy # set descr description | (Optional) Provides a description for the policy. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 4 | UCS-A /eth-server/stats-threshold-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example enters the default server port, chassis, and fabric interconnect statistics threshold policy, provides a description for the policy, and commits the transaction:

```
UCS-A# scope eth-server
UCS-A /eth-server* # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy* # set descr "Server port, chassis, and fabric
interconnect stats threshold policy."
UCS-A /eth-server/stats-threshold-policy* # commit-buffer
UCS-A /eth-server/stats-threshold-policy #
```

What to Do Next

Configure one or more policy classes for the statistics threshold policy. For more information, see "[Configuring a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Class](#), page 416."

Configuring a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Class

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | UCS-A# scope eth-server | Enters Ethernet server mode. |
| Step 2 | UCS-A /eth-server # scope stats-threshold-policy default | Enters Ethernet server statistics threshold policy mode. |
| Step 3 | UCS-A /eth-server/stats-threshold-policy # create class class-name | Creates the specified statistics threshold policy class and enters Ethernet server statistics threshold policy class mode. The <i>class-name</i> argument can be any of the class name keywords available for the particular statistics threshold policy being configured. To see a list of the available class name keywords, enter the create class ? command in Ethernet server statistics threshold policy mode. Note You can configure multiple classes for the statistics threshold policy. |
| Step 4 | UCS-A /eth-server/stats-threshold-policy /class # create property property-name | Creates the specified statistics threshold policy class property and enters Ethernet server statistics threshold policy class property mode. The <i>property-name</i> argument can be any of the property name keywords available for the particular policy class being configured. To see a list of the available property name keywords, enter the create property ? command in Ethernet server statistics threshold policy class mode. Note You can configure multiple properties for the policy class. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 5 | UCS-A /eth-server/stats-threshold-policy /class/property # set normal-value value | Specifies the normal value for the class property. The <i>value</i> format can vary depending on the class property being configured. To see the required format, enter the set normal-value ? command in Ethernet server statistics threshold policy class property mode. |
| Step 6 | UCS-A /eth-server/stats-threshold-policy /class/property # create threshold-value {above-normal below-normal} {cleared condition critical info major minor warning} | Creates the specified threshold value for the class property and enters Ethernet server statistics threshold policy class property threshold value mode. Note You can configure multiple threshold values for the class property. |
| Step 7 | UCS-A /eth-server/stats-threshold-policy /class/property/threshold-value # set {deescalating escalating} value | Specifies the de-escalating or escalating class property threshold value. The <i>value</i> format can vary depending on the class property threshold value being configured. To see the required format, enter the set deescalating ? or set escalating ? command in Ethernet server statistics threshold policy class property threshold value mode. Note You can specify both de-escalating and escalating class property threshold values. |
| Step 8 | UCS-A /eth-server/stats-threshold-policy /class/property/threshold-value # commit-buffer | Commits the transaction to the system configuration. |

The following example creates the server port, chassis, and fabric interconnect statistics threshold policy class for chassis statistics, creates an input power (Watts) property, specifies that the normal power is 8kW, creates an above normal warning threshold of 11kW, and commits the transaction:

```
UCS-A# scope eth-server
UCS-A /eth-server* # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy* # create class chassis-stats
UCS-A /eth-server/stats-threshold-policy/class* # create property input-power
UCS-A /eth-server/stats-threshold-policy/class/property* # set normal-value 8000.0
UCS-A /eth-server/stats-threshold-policy/class/property* # create threshold-value above-normal
warning
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value* # set escalating
11000.0
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value* # commit-buffer
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value #
```

Deleting a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Class

Procedure

| | Command or Action | Purpose |
|---------------|--------------------------------|------------------------------|
| Step 1 | UCS-A# scope eth-server | Enters Ethernet server mode. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 2 | UCS-A /eth-server # scope stats-threshold-policy default | Enters Ethernet server statistics threshold policy mode. |
| Step 3 | UCS-A /eth-server/stats-threshold-policy # delete class class-name | Deletes the specified statistics threshold policy class from the policy. |
| Step 4 | UCS-A /eth-server/stats-threshold-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the server port, chassis, and fabric interconnect statistics threshold policy class for chassis statistics and commits the transaction:

```
UCS-A# scope eth-server
UCS-A /eth-server* # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy* # delete class chassis-stats
UCS-A /eth-server/stats-threshold-policy* # commit-buffer
UCS-A /eth-server/stats-threshold-policy #
```

Fibre Channel Port Statistics Threshold Policy Configuration

Configuring a Fibre Channel Port Statistics Threshold Policy

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | UCS-A# scope fc-uplink | Enters Fibre Channel uplink mode. |
| Step 2 | UCS-A /fc-uplink # scope stats-threshold-policy default | Enters Fibre Channel uplink statistics threshold policy mode. Note You cannot create (or delete) an uplink Fibre Channel port statistics threshold policy. You can only enter (scope to) the existing default policy. |
| Step 3 | UCS-A /fc-uplink/stats-threshold-policy # set descr description | (Optional) Provides a description for the policy. Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output. |
| Step 4 | UCS-A /fc-uplink/stats-threshold-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example enters the default uplink Fibre Channel port statistics threshold policy, provides a description for the policy, and commits the transaction:

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink* # scope stats-threshold-policy default
UCS-A /fc-uplink/stats-threshold-policy* # set descr "Uplink Fibre Channel stats threshold policy."
```

```
UCS-A /fc-uplink/stats-threshold-policy* # commit-buffer
UCS-A /fc-uplink/stats-threshold-policy #
```

What to Do Next

Configure one or more policy classes for the statistics threshold policy. For more information, see "[Configuring a Fibre Channel Port Statistics Threshold Policy Class](#), page 419."

Configuring a Fibre Channel Port Statistics Threshold Policy Class

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | UCS-A# scope fc-uplink | Enters Fibre Channel uplink mode. |
| Step 2 | UCS-A /fc-uplink # scope stats-threshold-policy default | Enters Fibre Channel uplink statistics threshold policy mode. |
| Step 3 | UCS-A /fc-uplink/stats-threshold-policy # create class class-name | Creates the specified statistics threshold policy class and enters Fibre Channel uplink statistics threshold policy class mode. The <i>class-name</i> argument can be any of the class name keywords available for the particular statistics threshold policy being configured. To see a list of the available class name keywords, enter the create class ? command in Fibre Channel uplink statistics threshold policy mode. Note You can configure multiple classes for the statistics threshold policy. |
| Step 4 | UCS-A /fc-uplink/stats-threshold-policy /class # create property property-name | Creates the specified statistics threshold policy class property and enters Fibre Channel uplink statistics threshold policy class property mode. The <i>property-name</i> argument can be any of the property name keywords available for the particular policy class being configured. To see a list of the available property name keywords, enter the create property ? command in Fibre Channel uplink statistics threshold policy class mode. Note You can configure multiple properties for the policy class. |
| Step 5 | UCS-A /fc-uplink/stats-threshold-policy /class/property # set normal-value value | Specifies the normal value for the class property. The <i>value</i> format can vary depending on the class property being configured. To see the required format, enter the set normal-value ? command in Fibre Channel uplink statistics threshold policy class property mode. |
| Step 6 | UCS-A /fc-uplink/stats-threshold-policy /class/property # create threshold-value {above-normal below-normal} {cleared condition critical info major minor warning} | Creates the specified threshold value for the class property and enters Fibre Channel uplink statistics threshold policy class property threshold value mode. Note You can configure multiple threshold values for the class property. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 7 | UCS-A /fc-uplink/stats-threshold-policy /class/property/threshold-value # set { deescalating escalating } <i>value</i> | Specifies the de-escalating or escalating class property threshold value. The <i>value</i> format can vary depending on the class property threshold value being configured. To see the required format, enter the set deescalating ? or set escalating ? command in Fibre Channel uplink statistics threshold policy class property threshold value mode. Note You can specify both de-escalating and escalating class property threshold values. |
| Step 8 | UCS-A /fc-uplink/stats-threshold-policy /class/property/threshold-value # commit-buffer | Commits the transaction to the system configuration. |

The following example creates the uplink Fibre Channel port statistics threshold policy class for Fibre Channel statistics, creates an average bytes received property, specifies that the normal average number of bytes received for each polling interval is 150MB, creates an above normal warning threshold of 200MB, and commits the transaction:

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink* # scope stats-threshold-policy default
UCS-A /fc-uplink/stats-threshold-policy* # create class fc-stats
UCS-A /fc-uplink/stats-threshold-policy/class* # create property bytes-rx-avg
UCS-A /fc-uplink/stats-threshold-policy/class/property* # set normal-value 150000000
UCS-A /fc-uplink/stats-threshold-policy/class/property* # create threshold-value above-normal
warning
UCS-A /fc-uplink/stats-threshold-policy/class/property/threshold-value* # set escalating
200000000
UCS-A /fc-uplink/stats-threshold-policy/class/property/threshold-value* # commit-buffer
UCS-A /fc-uplink/stats-threshold-policy/class/property/threshold-value #
```

Deleting an Uplink Fibre Channel Port Statistics Threshold Policy Class

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | UCS-A# scope fc-uplink | Enters Fibre Channel uplink mode. |
| Step 2 | UCS-A /fc-uplink # scope stats-threshold-policy default | Enters Fibre Channel uplink statistics threshold policy mode. |
| Step 3 | UCS-A /fc-uplink/stats-threshold-policy # delete class class-name | Deletes the specified statistics threshold policy class from the policy. |
| Step 4 | UCS-A /fc-uplink/stats-threshold-policy # commit-buffer | Commits the transaction to the system configuration. |

The following example deletes the uplink Fibre Channel port statistics threshold policy class for Fibre Channel statistics and commits the transaction:

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope stats-threshold-policy default
UCS-A /fc-uplink/stats-threshold-policy # delete class fc-stats
```

```
UCS-A /fc-uplink/stats-threshold-policy* # commit-buffer  
UCS-A /fc-uplink/stats-threshold-policy #
```




INDEX

A

- accounts
 - admin [98](#)
 - expiration [98](#)
 - user [97, 98](#)
 - username guidelines [98](#)
- acknowledging
 - chassis [343](#)
 - server [350](#)
- activate firmware [117](#)
- activating
 - adapters [131](#)
 - board controller firmware [137](#)
 - CIMC [133](#)
 - fabric interconnects [139](#)
 - I/O modules [135](#)
 - UCS manager [138](#)
- adapter qualification
 - creating [259](#)
 - deleting [261](#)
- adapters
 - NIC [30](#)
 - updating and activating [131](#)
 - verifying status [128](#)
 - VIC [30, 297](#)
 - virtualization [30](#)
- administration [35](#)
- aging time
 - MAC address table [156](#)
- aging time, Mac address table
 - configuring [157](#)
- alert, call home test [368](#)
- all configuration [377](#)
- architectural simplification [3](#)
- authentication
 - primary [81](#)
 - remote [81](#)
- authentication service
 - selecting default [89](#)
- autoconfiguration policy
 - about [16, 251](#)

B

- backing up
 - about [377](#)
 - all-configuration [124](#)
 - considerations [378](#)
 - creating operations [379](#)
 - deleting operations [383](#)
 - modifying operations [381](#)
 - running operations [381](#)
 - types [377](#)
 - user role [379](#)
- backup operations
 - creating [379](#)
 - deleting [383](#)
 - modifying [381](#)
 - running [381](#)
- best effort system class [26, 176](#)
- BIOS
 - actual settings [232](#)
 - default settings [219](#)
 - policy [219](#)
 - scrub policy [247](#)
 - settings for servers [217](#)
- BIOS defaults
 - modifying [225](#)
- BIOS policy
 - creating [219](#)
- BIOS, recovering [353](#)
- BMC
 - resetting [352](#)
- board controllers, activating firmware [137](#)
- boot definitions
 - configuring [283](#)
 - deleting [287](#)
 - LAN boot [284](#)
 - storage boot [285](#)
 - virtual media boot [286](#)
- boot policies
 - about [9, 233](#)
 - configuring [234](#)
 - deleting [240](#)

boot policies (*continued*)

- LAN boot [236](#)
- storage boot [237](#)
- viewing [239](#)
- virtual media boot [238](#)

bronze system class [26, 176](#)

bundle, firmware [114](#)

burned in values [8, 271](#)

C

call home

- configuring [362](#)
- inventory messages, configuring [364](#)
- inventory messages, sending [365](#)
- policies, configuring [370](#)
- policies, deleting [371](#)
- policies, disabling [370](#)
- policies, enabling [371](#)
- profiles, configuring [366](#)
- profiles, deleting [368](#)
- sending test alert [368](#)
- smart call home, configuring [372](#)
- TAC-1 profile, configuring [374](#)

Call Home

- about [357](#)
- considerations [359](#)
- policies [369](#)
- profiles [366](#)
- severity levels [360](#)
- Smart Call Home [361](#)

capability catalog

- about [144](#)
- contents [144](#)
- restarting an update [147](#)
- updates [145](#)
- updating [145, 146](#)
- viewing provider [148](#)

capping server power usage [293](#)

catalog

- capability [144, 145](#)
- firmware images [114](#)

certificate

- about [69](#)
- VN-Link in hardware [306, 307, 308](#)

chassis

- acknowledging [343](#)
- decommissioning [344](#)
- discovery policy [10, 153](#)
- recommissioning [345](#)
- removing [344](#)
- turning off locator LED [346](#)

chassis (*continued*)

- turning on locator LED [345](#)

chassis discovery policy

- about [10, 153](#)
- discovery policies
 - chassis [154](#)

chassis management

- removing [344](#)

chassis qualification

- configuring [261](#)
- deleting [262](#)

CIM XML

- configuring [68](#)

CIMC

- updating and activating [133](#)

Cisco Discovery Protocol [15, 188](#)

Cisco UCS Manager

- about [35](#)
- impact of firmware upgrade [121](#)

Cisco VN-Link [31, 297, 298](#)

cisco-av-pair [82, 83](#)

CiscoAVPair [82](#)

clients, port profiles

- deleting [329](#)

clock

- setting manually [342](#)

cluster configuration

- about [38](#)

commands for object management [41](#)

communication services

- about [67](#)
- disabling [79](#)
- HTTPS [70, 71, 72](#)
- SNMP [75, 77, 78](#)

community, SNMP [75](#)

component, firmware [114](#)

configuration

- backing up [124, 379](#)
- erasing [389](#)
- import methods [379](#)
- importing [379, 383](#)
- restoring [379, 387](#)

configuring

- HTTPS [70, 71, 72](#)

considerations

- backup operations [378](#)
- Call Home [359](#)
- VN-Link in hardware [33, 300](#)

console authentication service

- selecting [88](#)

converged network adapters

- virtualization [30](#)

core file exporter

- configuring [399](#)

core file exporter (*continued*)

 disabling [399](#)

Core File Exporter

 about [398](#)

corrupt BIOS [353](#)

cpu qualification

 creating [262](#)

 deleting [264](#)

create [41](#)

D

database

 backing up [377](#)

 restoring [379](#)

decommissioning

 chassis [344](#)

 server [351](#)

default service profiles [8, 271](#)

delete [41](#)

deletion tasks

 about [333](#)

disaster recovery [377, 379](#)

discovery policy

 chassis [10, 153](#)

 server [16, 252](#)

disk scrub policy [247](#)

DNS servers

 about [151](#)

 configuring [151](#)

 deleting [152](#)

downgrading

 firmware [123](#)

 prerequisites [124](#)

download firmware [117](#)

DVS [312, 320](#)

dynamic vNIC connection policies

 configuring [331](#)

 deleting [332](#)

dynamic vNIC connection policy

 about [11, 331](#)

E

enabling

 SNMP [75](#)

endpoints

 direct firmware upgrade [118, 120](#)

 service profile upgrade [121](#)

enter [41](#)

Ethernet

 Fibre Channel over [5](#)

 flow control policies [19, 27, 180](#)

 server ports

 configuring [60](#)

 deleting [60](#)

 uplink port channels [62, 63, 64](#)

 configuring [62](#)

 deleting [63](#)

 member ports, adding [64](#)

 member ports, deleting [64](#)

 uplink ports [59, 61](#)

 configuring [61](#)

 deleting [61](#)

Ethernet adapter policies

 about [12, 185, 205](#)

Ethernet adapter policy

 configuring [186](#)

 deleting [188](#)

Ethernet switching mode [56, 57](#)

 about [56](#)

expiration, accounts [98](#)

exporting

 backup types [377](#)

 configuration [377](#)

 core file [399](#)

 extension files [309](#)

 user role [379](#)

extension files

 about [32, 298](#)

 exporting [309](#)

 modifying key [308](#)

F

fabric interconnects

 activating [139](#)

 admin password recover [404, 405](#)

 admin password recovery [403](#)

 cluster [38](#)

 determining leadership role [403](#)

 enabling standalone for cluster [54](#)

 Ethernet switching mode [56](#)

 high availability [38](#)

 host ID [159](#)

 impact of firmware upgrade [120](#)

 initial setup

 about [47](#)

 management port [48](#)

 setup mode [48](#)

 port licenses [159, 161, 162, 163](#)

 installing [161](#)

- fabric interconnects (*continued*)
 - port licenses (*continued*)
 - uninstalling [163](#)
 - viewing [162](#)
 - viewing usage [162](#)
 - system configuration type [48](#)
 - verifying high availability status and roles [125](#)
 - verifying operability [125](#)
- fault collection policy
 - about [18, 397](#)
 - configuring [398](#)
- faults
 - Call Home severity levels [360](#)
 - collection policy [18, 397](#)
 - Core File Exporter [398](#)
 - lifecycle [18, 397](#)
- FCoE [5](#)
- features
 - opt-in [27](#)
 - stateless computing [27](#)
- Fibre Channel
 - link-level flow control [5](#)
 - over Ethernet [5](#)
 - priority flow control [5](#)
 - statistics threshold policies [418](#)
 - statistics threshold policy classes [419](#)
 - uplink ports [59](#)
- Fibre Channel adapter policies
 - about [12, 185, 205](#)
- Fibre Channel adapter policy
 - configuring [206](#)
 - deleting [208](#)
- Fibre Channel system class [26, 176](#)
- firmware
 - about [113](#)
 - activating board controller [137](#)
 - adapters [131](#)
 - CIMC [133](#)
 - direct upgrade [118](#)
 - displaying [130](#)
 - displaying download status [129](#)
 - downgrades [123](#)
 - downloading [129](#)
 - fabric interconnects [139](#)
 - guidelines [115](#)
 - host package [13, 122, 140, 141](#)
 - I/O modules [135](#)
 - image headers [114](#)
 - images [114](#)
 - management [117](#)
 - management package [14, 122, 142, 143](#)
 - obtaining packages [128](#)
 - outage impacts [120](#)
 - prerequisites [124](#)

- firmware (*continued*)
 - service profiles [121](#)
 - UCS manager [138](#)
 - upgrade order [120](#)
 - upgrade stages [118, 123](#)
 - upgrades [115](#)
- firmwareadapters
 - verifying status [126, 127, 128](#)
- firmwarecluster configuration
 - verifying overall status [125](#)
- firmwarefabric interconnects
 - verifying overall status [125](#)
- firmwareI/O modules
 - verifying status [126, 127, 128](#)
- firmwareservers
 - verifying status [126, 127, 128](#)
- flexibility [4](#)
- flow control
 - link-level [5](#)
 - priority [5](#)
- flow control policies
 - configuring [181](#)
 - deleting [182](#)
- flow control policy
 - about [19, 27, 180](#)
- full state [377](#)

G

- gold system class [26, 176](#)
- guidelines
 - firmware upgrades [115](#)
 - local disk configuration policy [244](#)
 - oversubscription [24](#)
 - passwords [98](#)
 - pinning [26](#)
 - usernames [98](#)

H

- hardware-based service profiles [8, 271](#)
- hardware, stateless [27](#)
- headers, images [114](#)
- high availability [4, 38](#)
 - about [38](#)
- host firmware package
 - about [13, 122, 140](#)
 - creating and updating [141](#)
- host ID, obtaining [159](#)
- HTTP
 - configuring [69](#)

HTTPS

- certificate request [70](#)
- configuring [73](#)
- creating key ring [70](#)
- importing certificate [72](#)
- trusted point [71](#)

I

I/O modules

- updating and activating [135](#)
- verifying status [126](#)

IEEE 802.3x link-level flow control [5](#)images [113, 114, 128](#)

- bundle [114](#)
- component [114](#)
- contents [114](#)
- headers [114](#)
- obtaining [128](#)

import operations

- creating [383](#)
- deleting [387](#)
- modifying [385](#)
- running [385](#)

importing

- about [379](#)
- creating operations [383](#)
- deleting operations [387](#)
- modifying operations [385](#)
- restore methods [379](#)
- running operations [385](#)
- user role [379](#)

inheritance, servers [16, 254](#)inherited values [8, 271](#)

initial setup

- about [47](#)
- management port IP address [48](#)
- setup mode [48](#)

initial templates [8, 272](#)

inventory messages, call home

- configuring [364](#)
- sending [365](#)

inventory messages, smart call home

- configuring [375](#)

IOM

- resetting [355](#)

IP addresses

- management IP pool [22, 214](#)
- management port [48](#)

IP pools

- management [22, 214](#)

IPMI access profile

- configuring [240, 242](#)
- deleting [242, 243](#)

IPMI access profiles

- about [14, 240](#)

K

key ring

- about [69](#)
- certificate request [70](#)
- creating [70](#)
- deleting [74](#)
- importing certificate [72](#)
- trusted point [71](#)

L

LAN

- pin groups [171](#)
- VLANs [167](#)
- vNIC policy [18, 183](#)

LAN boot [284](#)LAN boot, boot policies [236](#)lanes, virtual [26, 175](#)

LDAP

- creating a provider [84](#)

LDAP provider

- about [81](#)
- configuring properties [83](#)
- user attribute [82](#)

licenses, port [159](#)lifecycle, faults [18, 397](#)link-level flow control [5](#)

local disk configuration policy

- about [14, 243](#)
- guidelines [244](#)

local disks

- policies [245, 246](#)
- service profiles [281](#)

locales

- about [102](#)
- adding an organization [105](#)
- assigning to user accounts [109](#)
- creating [104](#)
- deleting [106](#)
- deleting an organization from [105](#)
- removing from user accounts [110](#)

log, system [400](#)

log, system event

- about [391](#)

log, system event (*continued*)
 backing up
 chassis server mode [395](#)
 exec mode [395](#)
 clearing
 chassis server mode [396](#)
 exec mode [396](#)
 policy [393](#)
 viewing
 chassis server mode [392](#)
 exec mode [392](#)
 logical configuration [377](#)

M

MAC address pools [200](#)
 MAC address table
 aging time, about [156](#)
 MAC address table aging time
 configuring [157](#)
 MAC addresses
 pools [21, 173](#)
 MAC pools [173](#)
 management firmware package
 about [14, 122, 142](#)
 creating and updating [143](#)
 management IP pools
 about [22, 214](#)
 configuring [214](#)
 deleting [215](#)
 management port IP address [48, 55](#)
 changing [55](#)
 member ports, port channel
 adding [64](#)
 deleting [64](#)
 memory qualification
 creating [264](#)
 deleting [265](#)
 merging configuration [379](#)
 mobility [27](#)
 mode
 end-host [56](#)
 Ethernet switching [56](#)
 setup [48](#)
 modifying extension key [308](#)
 multi-tenancy
 about [28](#)
 name resolution [92](#)
 opt-in [29](#)
 opt-out [29](#)
 organizations [91](#)

N

name resolution [92, 151](#)
 named VLANs
 about [167](#)
 creating for dual fabric interconnects [167](#)
 creating for single fabric interconnect [168](#)
 deleting [169](#)
 named VSANs
 about [193](#)
 creating for dual fabric interconnects [194](#)
 creating for single fabric interconnect [194](#)
 deleting [195](#)
 network
 connectivity [6](#)
 named VLANs [167](#)
 named VSANs [193](#)
 network control policies
 configuring [189](#)
 deleting [190](#)
 network control policy [15, 188](#)
 NIC adapters
 virtualization [30](#)
 NTP servers
 about [339](#)
 configuring [341](#)
 deleting [341](#)

O

obtaining
 capability catalog updates [145](#)
 firmware image bundles [128](#)
 opt-in
 about [27](#)
 multi-tenancy [29](#)
 stateless computing [28](#)
 opt-out [27, 28, 29](#)
 multi-tenancy [29](#)
 stateless computing [28](#)
 organizations
 about [91](#)
 configuring under non-root [94](#)
 configuring under root [93](#)
 deleting [95](#)
 locales [102](#)
 multi-tenancy [28](#)
 name resolution [92](#)
 outage impacts
 firmware upgrade [120](#)
 Cisco UCS Manager [121](#)
 fabric interconnects [120](#)
 overriding server identity [7, 272](#)

- oversubscription
 - about [23](#)
 - considerations [23](#)
 - guidelines [24](#)
- overview [3](#)
- P**
- packages
 - obtaining [128](#)
- packs
 - host firmware [13, 122, 140](#)
 - management firmware [14, 122, 142](#)
- Palo adapter
 - extension files
 - exporting [309](#)
 - modifying key [308](#)
- pass-through switching [31, 298](#)
- passwords, guidelines [98](#)
- passwords, recovering admin [403, 404, 405](#)
- pending commands [42](#)
- pending deletions
 - about [333](#)
- PFC [5](#)
- physical qualification
 - creating [266](#)
 - deleting [266](#)
- pin groups
 - about [24](#)
 - LAN [171](#)
 - SAN [197](#)
- pinning
 - about [24](#)
 - guidelines [26](#)
 - servers to server ports [25](#)
- PKI [69](#)
- placement profiles, vNIC/VHBA
 - configuring [269](#)
 - deleting [270](#)
 - vcons [269](#)
- platinum system class [26, 176](#)
- policies
 - about [9](#)
 - autoconfiguration [16, 251](#)
 - BIOS [219](#)
 - boot [9, 233](#)
 - Call Home [369](#)
 - chassis discovery [10, 153](#)
 - dynamic vNIC connection
 - about [11, 331](#)
 - Ethernet [12, 185, 205](#)
 - fault collection [18, 397, 398](#)
 - policies (continued)*
 - Fibre Channel adapter [12, 185, 205](#)
 - flow control [19, 27, 180](#)
 - host firmware [13, 122, 140](#)
 - IPMI access [14, 240](#)
 - local disk configuration [14, 243](#)
 - local disks [245, 246](#)
 - management firmware [14, 122, 142](#)
 - network control [15, 188](#)
 - power [15, 155](#)
 - PSU [15, 155](#)
 - QoS [15, 27, 178](#)
 - scrub [19, 247](#)
 - serial over LAN
 - about [20, 248](#)
 - server discovery [16, 252](#)
 - server inheritance
 - about [16, 254](#)
 - server pool [16, 256](#)
 - server pool qualification [17, 257](#)
 - statistics collection [20, 407](#)
 - threshold [20, 408](#)
 - vHBA [17, 203](#)
 - VM lifecycle [17](#)
 - vNIC [18, 183](#)
 - vNIC/vHBA placement [18, 268](#)
 - policies, call home
 - configuring [370](#)
 - deleting [371](#)
 - disabling [370](#)
 - enabling [371](#)
 - policy classes
 - Fibre Channel port statistics, configuring [419](#)
 - server port statistics, configuring [416](#)
 - server port statistics, deleting [417](#)
 - server statistics, configuring [410](#)
 - server statistics, deleting [412](#)
 - uplink Ethernet port statistics, configuring [413](#)
 - uplink Ethernet port statistics, deleting [415, 420](#)
 - pools
 - about [21](#)
 - MAC [21, 173](#)
 - management IP [22, 214](#)
 - servers [21, 211](#)
 - UUID suffixes [21, 212](#)
 - WWN [22, 199](#)
 - port channels
 - configuring [62](#)
 - deleting [63](#)
 - member ports
 - adding [64](#)
 - deleting [64](#)
 - uplink Ethernet [62](#)

- port licenses
 - about [159](#)
 - installing [161](#)
 - obtaining [160](#)
 - obtaining host ID [159](#)
 - uninstalling [163](#)
 - viewing [162](#)
 - viewing usage [162](#)
 - port profiles
 - about [33, 299, 323](#)
 - clients
 - deleting [329](#)
 - configuring [324](#)
 - deleting [326](#)
 - Port profiles
 - VLANs
 - adding [326](#)
 - deleting [327](#)
 - ports
 - fabric interconnect [59](#)
 - licenses [159](#)
 - management [48](#)
 - pin groups [171, 197](#)
 - pinning server traffic [25](#)
 - port channels [62, 63](#)
 - configuring [62](#)
 - deleting [63](#)
 - server [59, 60](#)
 - configuring [60](#)
 - deleting [60](#)
 - uplink [59](#)
 - uplink Ethernet
 - configuring [61](#)
 - deleting [61](#)
 - ports,
 - port channels
 - member ports, adding [64](#)
 - member ports, deleting [64](#)
 - power cycling
 - server [349](#)
 - power policy [15, 155](#)
 - about [15, 155](#)
 - power usage
 - servers [293](#)
 - setting for server [293](#)
 - viewing [294](#)
 - primary authentication
 - about [81](#)
 - remote [81](#)
 - priority flow control [5](#)
 - privileges
 - about [100](#)
 - adding to user roles [103](#)
 - removing from user roles [103](#)
 - profiles [6, 33, 299, 323, 366](#)
 - Call Home [366](#)
 - port [33, 299, 323](#)
 - profiles, call home
 - configuring [366](#)
 - deleting [368](#)
 - profiles, TAC-1, smart call home
 - configuring [374](#)
 - provider, capability catalog [144, 148](#)
 - PSU policy [15, 155](#)
- ## Q
- QoS policies
 - about [15, 27, 178](#)
 - configuring [178](#)
 - deleting [180](#)
 - qualification
 - creating adapter [259](#)
 - creating cpu [262](#)
 - creating memory [264](#)
 - creating physical [266](#)
 - creating storage [267](#)
 - quality of service
 - about [26, 175](#)
 - flow control policies [19, 27, 180](#)
 - policies [15, 27, 178](#)
 - system classes [26, 175, 176, 177](#)
 - configuring [176](#)
 - disabling [177](#)
- ## R
- RADIUS
 - creating provider [86](#)
 - RADIUS provider
 - about [81](#)
 - configuring properties [85](#)
 - user attribute [82](#)
 - recommendations
 - backup operations [378](#)
 - recommissioning
 - chassis [345](#)
 - recovering admin password [403, 404, 405](#)
 - recovering BIOS [353](#)
 - remote authentication
 - user accounts [82](#)
 - user roles [82](#)
 - removing
 - chassis [344](#)
 - server [350](#)

- replacing configuration [379](#)
 - resetting
 - server [349](#)
 - resetting CMOS
 - server [352](#)
 - resolution, name [151](#)
 - restoring
 - about [379](#)
 - configuration [387](#)
 - user role [379](#)
 - role-based access control [97](#)
 - roles
 - about [99](#)
 - assigning to user accounts [108](#)
 - backing up [379](#)
 - privileges [100](#)
 - removing from user accounts [109](#)
 - RSA [69](#)
- ## S
- SAN
 - pin groups [197](#)
 - vHBA policy [17, 203](#)
 - VSANs [193](#)
 - scalability [4](#)
 - scope [41](#)
 - scrub policies
 - creating [247](#)
 - deleting [248](#)
 - scrub policy
 - about [19, 247](#)
 - SEL
 - about [391](#)
 - backing up
 - chassis server mode [395](#)
 - exec mode [395](#)
 - clearing
 - chassis server mode [396](#)
 - exec mode [396](#)
 - policy [393](#)
 - viewing
 - chassis server mode [392](#)
 - exec mode [392](#)
 - serial number, obtaining [159](#)
 - serial over LAN
 - policies [249](#)
 - service profiles [282](#)
 - serial over LAN policies
 - deleting [250](#)
 - serial over LAN policy
 - about [20, 248](#)
 - serial over LAN policy (*continued*)
 - viewing [250](#)
 - server
 - acknowledging [350](#)
 - BMC
 - resetting [352](#)
 - booting [347](#)
 - decommissioning [351](#)
 - power cycling [349](#)
 - removing [350](#)
 - resetting [349](#)
 - resetting CMOS [352](#)
 - setting power usage [293](#)
 - shutting down [348](#)
 - turning off locator LED [351](#)
 - turning on locator LED [351](#)
 - viewing power usage [294](#)
 - server autoconfiguration policies
 - configuring [251](#)
 - deleting [252](#)
 - server autoconfiguration policy
 - about [16, 251](#)
 - server discovery policies
 - configuring [253](#)
 - deleting [254](#)
 - discovery policies
 - server, configuring [253](#)
 - server, deleting [254](#)
 - server discovery policy
 - about [16, 252](#)
 - server inheritance policies
 - configuring [255](#)
 - deleting [256](#)
 - server inheritance policy
 - about [16, 254](#)
 - server pool policies
 - configuring [256](#)
 - deleting [257](#)
 - server pool policy
 - about [16, 256](#)
 - server pool policy qualification
 - about [17, 257](#)
 - creating [258](#)
 - deleting [259](#)
 - server pools
 - configuring [211](#)
 - deleting [212](#)
 - server ports
 - about [59](#)
 - configuring [60](#)
 - deleting [60](#)
 - server virtualization [4](#)
 - servers
 - actual BIOS settings [232](#)

- servers (*continued*)
 - adapters
 - updating and activating [131](#)
 - BIOS defaults [219, 225](#)
 - BIOS policies [219](#)
 - BIOS policy [219](#)
 - BIOS settings [217](#)
 - boot policies [9, 233](#)
 - CIMC
 - updating and activating [133](#)
 - configuration [6](#)
 - discovery policy [16, 252](#)
 - DNS [151](#)
 - inheritance policy [16, 254](#)
 - IPMI access [14, 240](#)
 - local disk configuration [14, 243](#)
 - multi-tenancy [28](#)
 - pinning [25](#)
 - pool policy [16, 256](#)
 - pool qualifications [17, 257](#)
 - pools [21, 211](#)
 - power usage [293](#)
 - recovering BIOS [353](#)
 - resetting UUID [289](#)
 - service profiles [6, 7, 272](#)
 - stateless [27](#)
 - verifying status [127](#)
- service profiles
 - about [6](#)
 - associating [288](#)
 - boot definitions [283, 287](#)
 - configuration [6](#)
 - creating [276](#)
 - disassociating [288](#)
 - firmware upgrades [121](#)
 - inherited values [8, 271](#)
 - instance, creating from template [275](#)
 - LAN boot [284](#)
 - local disks [281](#)
 - network connectivity [6](#)
 - override identity [7, 272](#)
 - resetting MAC address [290](#)
 - resetting UUID [289](#)
 - resetting WWPN [291](#)
 - serial over LAN [282](#)
 - storage boot [285](#)
 - template, creating [273](#)
 - templates [8, 272](#)
 - vHBAs [279](#)
 - virtual media boot [286](#)
 - vNICs [278](#)
- setup mode [48](#)
- severity levels, Call Home [360](#)
- silver system class [26, 176](#)
- smart call home
 - configuring [372](#)
 - inventory messages, configuring [375](#)
 - registering [376](#)
 - TAC-1 profile, configuring [374](#)
- Smart Call Home
 - about [361](#)
 - considerations [359](#)
 - severity levels [360](#)
- SNMP
 - community [75](#)
 - disabling [78](#)
 - enabling [75](#)
 - SNMPv3 users [78](#)
 - trap hosts
 - creating [76](#)
 - deleting [76](#)
 - users
 - creating [77](#)
 - deleting [78](#)
- software [113](#)
- SOL policies
 - deleting [250](#)
 - viewing [250](#)
- stages, firmware upgrades [118, 123](#)
- stateless computing
 - about [27](#)
 - opt-in [28](#)
 - opt-out [28](#)
- statelessness [27](#)
- statistics
 - threshold policies [20, 408](#)
- statistics collection policies
 - about [20, 407](#)
- statistics collection policy
 - configuring [408](#)
- statistics threshold policies
 - Fibre channel port, classes, configuring [419](#)
 - Fibre Channel port, configuring [418](#)
 - server classes, deleting [412](#)
 - server port classes, configuring [416](#)
 - server port classes, deleting [417](#)
 - server port, configuring [415](#)
 - server, classes, configuring [410](#)
 - server, configuring [409](#)
 - server, deleting [410](#)
 - uplink Ethernet port classes, deleting [415, 420](#)
 - uplink Ethernet port, classes, configuring [413](#)
 - uplink Ethernet port, configuring [412](#)
- statistics threshold policy classes
 - Fibre Channel port, configuring [419](#)
 - server port, configuring [416](#)
 - server port, deleting [417](#)
 - server, configuring [410](#)

statistics threshold policy classes (*continued*)
 server, deleting [412](#)
 uplink Ethernet port, configuring [413](#)
 uplink Ethernet port, deleting [415, 420](#)

storage boot [285](#)

storage boot, boot policies [237](#)

storage qualification

creating [267](#)

deleting [268](#)

supported tasks [36](#)

switching mode [57](#)

syslog [400](#)

system class

configuring [176](#)

disabling [177](#)

system classes [26, 175, 176](#)

best effort [26, 176](#)

bronze [26, 176](#)

Fibre Channel [26, 176](#)

gold [26, 176](#)

platinum [26, 176](#)

silver [26, 176](#)

system configuration [377](#)

system event log

about [391](#)

backing up

chassis server mode [395](#)

exec mode [395](#)

clearing

chassis server mode [396](#)

exec mode [396](#)

policy [393](#)

viewing

chassis server mode [392](#)

exec mode [392](#)

system name

changing [54](#)

T

TACACS+

creating provider [87](#)

TACACS+ provider

about [81](#)

configuring properties [87](#)

user attribute [83](#)

tasks

supported [36](#)

unsupported [38](#)

telnet

configuring [78](#)

templates

service profiles [8, 272](#)

test alert, call home [368](#)

TFTP Core Exporter [398](#)

threshold policies

about [20, 408](#)

time zones

about [339](#)

configuring NTP servers [341](#)

deleting NTP servers [341](#)

setting [339](#)

setting clock manually [342](#)

viewing [339](#)

traffic management

oversubscription [23, 24](#)

quality of service [26, 175](#)

system classes [26, 175](#)

virtual lanes [26, 175](#)

trap hosts

creating [76](#)

deleting [76](#)

trusted points

about [69](#)

creating [71](#)

deleting [75](#)

turning off locator LED

chassis [346](#)

server [351](#)

turning on locator LED

chassis [345](#)

server [351](#)

U

UCS manager

activating [138](#)

unified fabric

about [4](#)

Fibre Channel [5](#)

unsupported tasks [38](#)

updating

adapters [131](#)

capability catalog [145, 146](#)

CIMC [133](#)

firmware order [120](#)

I/O modules [135](#)

updating templates [8, 272](#)

upgrading

capability catalog [144, 145](#)

firmware [115, 118, 123](#)

firmware, direct [118](#)

firmware, guidelines [115](#)

- upgrading (*continued*)
 - prerequisites [124](#)
 - upgrading firmware
 - obtaining packages [128](#)
 - upgradng
 - firmware, service profiles [121](#)
 - uplink ports
 - about [59](#)
 - Ethernet
 - configuring [61](#)
 - deleting [61](#)
 - flow control policies [19, 27, 180](#)
 - pin groups [171, 197](#)
 - port channels
 - configuring [62](#)
 - deleting [63](#)
 - member ports, adding [64](#)
 - member ports, deleting [64](#)
 - uplink Ethernet [62](#)
 - usage, port licenses [162](#)
 - user accounts
 - about [97, 98](#)
 - creating [106](#)
 - deleting [108](#)
 - locales
 - assigning [109](#)
 - removing [110](#)
 - monitoring [110](#)
 - roles
 - assigning [108](#)
 - removing [109](#)
 - username guidelines [98](#)
 - user attribute
 - LDAP [82](#)
 - RADIUS [82](#)
 - TACACS+ [83](#)
 - user roles
 - about [99](#)
 - creating [102](#)
 - deleting [104](#)
 - privileges [100](#)
 - usernames, guidelines [98](#)
 - users
 - access control [97](#)
 - accounts [97, 98](#)
 - authentication [81](#)
 - guidelines [98](#)
 - locales
 - about [102](#)
 - privileges [100](#)
 - recovering admin password [403, 404, 405](#)
 - remote authentication [82](#)
 - roles [99](#)
 - SNMPv3 [77, 78](#)
 - UUID
 - resetting [289](#)
 - UUID suffix pools [21, 212, 213, 214](#)
 - about [21, 212](#)
- ## V
- vcons
 - vNIC/vHBA placement profiles [269](#)
 - vCons
 - about [18, 268](#)
 - vHBA SAN Connectivity policies
 - about [17, 203](#)
 - vHBA templates
 - about [17, 203](#)
 - configuring [203](#)
 - deleting [205](#)
 - vHBAs
 - resetting WWPN [291](#)
 - service profiles [279](#)
 - VIC adapters
 - virtualization [30, 297](#)
 - viewing
 - boot policies [239](#)
 - serial over LAN policies [250](#)
 - server power usage [294](#)
 - virtual lanes [26, 175](#)
 - virtual media boot [286](#)
 - virtual media boot, boot policies [238](#)
 - virtualization
 - about [29](#)
 - converged network adapters [30](#)
 - DVS [312, 320](#)
 - NIC adapters [30](#)
 - Palo adapter
 - extension file [309](#)
 - extension key [308](#)
 - support [30](#)
 - VIC adapter [30, 297](#)
 - VM lifecycle policy [17](#)
 - VN-Link
 - about [31, 297](#)
 - in hardware [31, 298](#)
 - VN-Link in hardware [33, 300, 303, 306, 307, 308, 312, 320, 333](#)
 - certificate [306](#)
 - components [303](#)
 - considerations [33, 300](#)
 - copying certificate [306](#)
 - creating a certificate [307](#)
 - deleting certificate [308](#)
 - pending deletions [333](#)

- VLANs
 - named
 - about [167](#)
 - port profiles
 - adding [326](#)
 - deleting [327](#)
 - VM lifecycle policy
 - about [17](#)
 - VMware [29, 308, 309](#)
 - extension files [309](#)
 - extension key [308](#)
 - VN-Link
 - about [31, 297](#)
 - extension file [32, 298](#)
 - port profiles [33, 299, 323](#)
 - VN-Link in hardware
 - about [31, 298](#)
 - certificate [306](#)
 - components [303](#)
 - considerations [33, 300](#)
 - copying certificate [306](#)
 - creating certificate [307](#)
 - deleting certificate [308](#)
 - DVS [312, 320](#)
 - pending deletions [333](#)
 - vNIC
 - policy [18, 183](#)
 - vNIC LAN Connectivity policies
 - about [18, 183](#)
 - vNIC templates
 - about [18, 183](#)
 - configuring [183](#)
 - deleting [185](#)
 - vNIC/vHBA placement policies
 - about [18, 268](#)
 - vCons [18, 268](#)
 - vNIC/vHBA placement profiles
 - configuring [269](#)
 - deleting [270](#)
 - vcons [269](#)
 - vNICs
 - dynamic vNIC connection policy [11, 331](#)
 - resetting MAC address [290](#)
 - service profiles [278](#)
 - VSANs
 - named [193](#)
- ## W
- WWN pools
 - about [22, 199](#)
 - WWNN pools
 - about [22, 199](#)
 - WWPN pools
 - about [22, 199](#)

