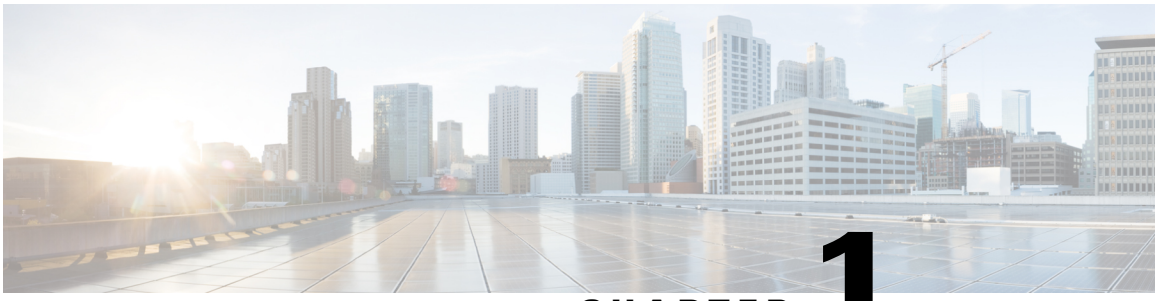
Cisco UCS Manager 2.2 Privileges

First Published: 2017-08-16

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

CONTENTS



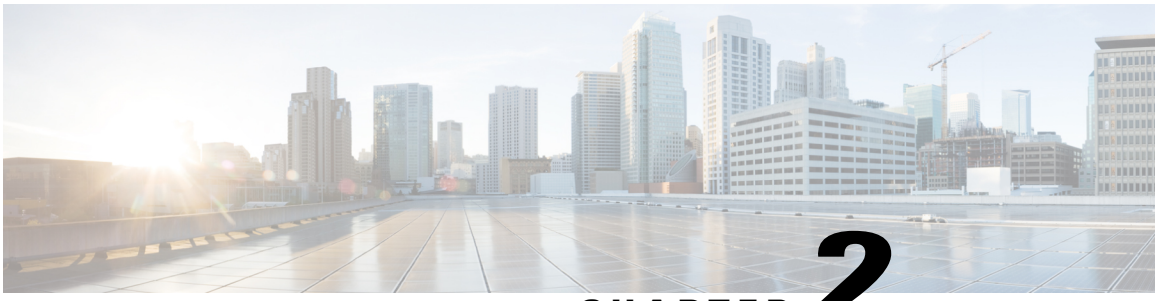
CHAPTER 1

Role-Based Access Control and Privileges

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 to access.

In Cisco UCS Manager, you do not directly assign privileges to users. Instead, you assign the roles, which contain one or more privileges, to the users. However, to understand which role to assign to a user, you need to know which system resources the privileges included in that role allow the user to access.

For example, in a company which is configured with locales for Engineering and Finance, a user who is assigned the Server Administrator role in the Engineering locale can update server configurations in the Engineering locale but cannot update server configurations in the Finance locale. If you want the user to be able to update server configurations in the Finance locale, you must assign that locale to the user as well.



CHAPTER 2

Cisco UCS Manager 2.2 Privileges

Aaa (aaa)

This privilege allows a user to perform provisioning operations related to Authentication, Authorization and Accounting. This includes managing users and roles, and configuring services that are exposed to the management interfaces.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Configure whether communication policies are resolved locally or through UCS Central.
- Configure DNS providers and DNS domain.
- Configure UCS management connectivity: HTTP, HTTPs, SSH, telnet, CIM, WS-MAN, event channel security.
- Configure users, roles, user locales, user sessions, login banner, authentication domains, authentication providers (LDAP, RADIUS, TACACS).
- Configure Key Ring. Import certificates of trusted authorities. Generate and import Certificates.
- Configure SNMP policy, SNMP users, SNMP trap destinations.

Admin (admin)

This privilege provides a user with full access to all operations in Cisco UCS Manager.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- This privilege has full access to all operations.

Ext Lan Config (ext-lan-config)

This privilege allows a user to configure LAN settings on a fabric interconnect, including Ethernet border ports, VLANs, LAN PIN groups, Ethernet SPAN sessions, LAN policies, and management interfaces.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Enable/Disable Ethernet/FC/iSCSI ports and port channels on a server adapter. Set port/port channel label.
- Specify the allowed range for virtual MAC addresses.
- Configure DNS providers and DNS domain.
- Configure Fabric Interconnect system name.
- Configure Ethernet monitoring sessions (SPAN).
- Configure Ethernet PIN Groups.
- Configure VLANs and VLAN groups.
- Configure management interfaces on the Fabric Interconnect.
- Configure Ethernet border ports on the Fabric Interconnect. Add/remove VLANs to border ports.
- Configure management interfaces monitoring policy.
- Configure MAC aging properties. Specify Ethernet end-host or switching mode. Enable/Disable VLAN compression.
- Enable/Disable Ethernet ports on a Fabric Interconnect or IO Module. Set port labels.

Ext Lan Policy (ext-lan-policy)

This privilege allows a user to configure LAN settings on a fabric interconnect, including Ethernet border ports, VLANs, LAN PIN groups, Ethernet SPAN sessions, LAN policies, and vNIC/vHBA placement policies

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Enable/Disable Ethernet/FC/iSCSI ports and port channels on a server adapter. Set port/port channel label.
- Specify the allowed range for virtual MAC addresses.
- Create/modify/delete vNIC/vHBA placement policies.
- Configure Ethernet monitoring sessions (SPAN).
- Configure Ethernet PIN Groups.
- Configure VLANs and VLAN groups.
- Configure Ethernet border ports on the Fabric Interconnect. Add/remove VLANs to border ports.
- Configure MAC aging properties. Specify Ethernet end-host or switching mode. Enable/Disable VLAN compression.
- Enable/Disable Ethernet ports on a Fabric Interconnect or IO Module. Set port labels.

Ext Lan Qos (ext-lan-qos)

This privilege allows a user to configure QoS classes of service for Ethernet and Fibre Channel and to configure Ethernet MTU.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- All tasks inherited from privilege: **ext-san-qos**

Ext Lan Security (ext-lan-security)

This privilege allows a user to configure NTP providers, and date and time zone settings.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Configure NTP providers, date and time zone.

Ext San Config (ext-san-config)

This privilege allows a user to configure SAN settings on a fabric interconnect, including FC/FCoE border ports, VSANs, SAN PIN groups, and Fibre Channel SPAN sessions.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- All tasks inherited from privilege: ext-san-policy

Ext San Policy (ext-san-policy)

This privilege allows a user to configure SAN settings on a fabric interconnect, including FC/FCoE border ports, VSANs, SAN PIN Groups, and Fibre Channel SPAN sessions.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Configure storage connection within a Service Profile.
- Configure Fibre Channel and FCoE ports on the Fabric Interconnect. Add/remove VSANs to FC ports. Configure the FCoE native VLAN.
- Specify the allowed range for virtual WWN addresses.
- Configure VSANs.
- Configure Fibre Channel PIN Groups.
- Configure Fibre Channel monitoring sessions.
- Create/modify/delete storage connection policies.
- Specify Fibre Channel end-host or switching mode. Specify FC trunking mode.

Ext San Qos (ext-san-qos)

This privilege allows a user to configure QoS classes of service for Ethernet and Fibre Channel and to configure Ethernet MTU.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Configure Ethernet and Fibre Channel QoS classes of service. Configures Ethernet MTU.

Fault (fault)

This privilege allows a user to configure fault policies, Call Home policies, and fault suppression policies. The user can also acknowledge faults in Cisco UCS Manager.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Configure whether fault policies are resolved locally or through UCS Central.
- Configure Call Home policies. Used to send call home events when a fault is raised.
- Acknowledge faults, configure fault policies (flap interval, soak interval, clear/ack action, limits, retention).

Service Profile Compute (ls-compute)

This privilege allows a user to configure most aspects of service profiles. However the user cannot create, modify or delete vNICs or vHBAs. You can use this privilege to enforce a strong separation between server, network, and storage provisioning activities. For example, a network administrator can create vNICs, a storage administrator can create vHBAs, and the server administrator can configure all other elements of a service profile

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Create/modify/delete Service Profiles/Templates. Assign policies to Service Profiles. Control power policies and placement. Acknowledge service profile pending tasks.
- Configure vHBA initiator groups.
- Configure schedules. Schedules can be used to trigger one-time or periodic tasks in the future.
- Associate and Disassociate Service Profiles.
- Create/modify/delete host firmware packages.
- Create/modify/delete Service Profile maintenance policies.
- Configure Service Profile BIOS policies.
- Create/modify/delete Service Profile dynamic vNICs within a Service Profile.
- Configure the vNIC/vHBA placement of a Service Profile.

Service Profile Config (ls-config)

This privilege allows a user to configure service profiles and to configure distributed virtual switches (DVSes) in a VM-FEX environment.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Configure VMware vCenter connections, datacenters, folders, switch.
- Configure vHBA initiator groups.
- Configure VMware vCenter cryptographic keys.

- Configure FC group templates.
- Configure the FC storage visibility for a vHBA initiator group.
- Configure the vNIC/vHBA placement of a Service Profile.
- Configure vHBA behavior policy when vHBAs are not explicitly defined.
- Configure vNIC behavior policy when vNICs are not explicitly defined.
- Create/modify/delete Service Profiles/Templates. Assign policies to Service Profiles. Control power policies and placement. Acknowledge service profile pending tasks.
- Configure schedules. Schedules can be used to trigger one-time or periodic tasks in the future.
- Assign port profiles to Distributed Virtual Switches.
- Associate and Disassociate Service Profiles.
- Configure Service Profile BIOS policies.
- Create/modify/delete Service Profile dynamic vNICs within a Service Profile.
- Within a service profile, specify if vNICs/vHBAs should be inherited from the hardware when vNICs/vHBAs are not explicitly defined.

Service Profile Config Policy (ls-config-policy)

This privilege allows a user to configure policies that are applied to Service Profiles, including host firmware packages, local disk policies, boot policies, and Serial over LAN policies

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Configure iSCSI authentication profile.
- Configure VMware vCenter connections, datacenters, folders, switch.
- Configure Service Profile boot policies.
- Create/modify/delete local disk policies.
- Associate and Disassociate Service Profiles.
- Assign port profiles to Distributed Virtual Switches.
- Create/modify/delete host firmware packages.
- Create/modify/delete adapter policies (Ethernet, FC and iSCSI).
- Create/modify/delete Service Profile maintenance policies.
- Configure VMware vCenter cryptographic keys.
- Create/modify/delete management firmware packages. This feature is deprecated.
- Configure Serial over LAN policies.

Service Profile Network (ls-network)

This privilege allows a user to configure network policies and network elements that are applied to service profile vNICs. A user can also configure other network elements that impact service profiles, such as server ports.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Configure VMware vCenter connections, datacenters, folders, switch.
- Specify the allowed range for virtual MAC addresses.
- Reset IO Module and FEX. Set IO Module/FEX labels.
- Create/modify/delete vNIC/vHBA placement policies.
- Assign port profiles to Distributed Virtual Switches.
- Create/modify/delete Network Control policies.
- Configure Ethernet server ports on the Fabric Interconnect.
- Create/modify/delete Service Profile dynamic vNICs within a Service Profile.
- Create/modify/delete Service Profile dynamic vNIC policies.
- Configure vNIC behavior policy when vNICs are not explicitly defined.
- Configure VLAN and VLAN group org permissions.

Service Profile Network Policy (ls-network-policy)

This privilege allows a user to configure network policies and network elements that are applied to service profile vNICs.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Specify the allowed range for virtual MAC addresses.
- Reset IO Module and FEX. Set IO Module/FEX labels.
- Create/modify/delete vNIC/vHBA placement policies.
- Create/modify/delete Network Control policies.
- Configure Ethernet server ports on the Fabric Interconnect.
- Configure pools of MAC addresses.
- Configure pools of IP addresses.
- Create/modify/delete Service Profile dynamic vNICs within a Service Profile.
- Create/modify/delete Service Profile dynamic vNIC policies.

Service Profile Qos Policy (ls-qos-policy)

Service Profile QOS policy

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Create/modify/delete QoS rate-limiting and Flow Control policies.

Service Profile Security (ls-security)

This privilege allows a user to configure IPMI policies.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- All tasks inherited from privilege: **ls-security-policy**

Service Profile Security Policy (ls-security-policy)

This privilege allows a user to configure IPMI policies.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Configure IPMI users and IPMI authentication profiles.

Service Profile Server (ls-server)

This privilege allows a user to configure service profiles.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Create/modify/delete Service Profiles/Templates. Assign policies to Service Profiles. Control power policies and placement. Acknowledge service profile pending tasks.
- Configure vHBA initiator groups.
- Configure schedules. Schedules can be used to trigger one-time or periodic tasks in the future.
- Associate and Disassociate Service Profiles.
- Configure Service Profile BIOS policies.
- Configure FC group templates.
- Create/modify/delete Service Profile dynamic vNICs within a Service Profile.
- Configure vNIC behavior policy when vNICs are not explicitly defined.
- Configure vHBA behavior policy when vHBAs are not explicitly defined.
- Configure the vNIC/vHBA placement of a Service Profile.
- Configure the FC storage visibility for a vHBA initiator group.
- Within a service profile, specify if vNICs/vHBAs should be inherited from the hardware when vNICs/vHBAs are not explicitly defined.

Service Profile Server Oper (ls-server-oper)

This privilege allows a user to control the power state of a service profile.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Control the power state of a Service Profile.

Service Profile Server Policy (ls-server-policy)

This privilege allows a user to control the power state of a service profile, associate and disassociate service profiles, and configure server-related policies.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Configure Service Profile boot policies.
- Control the power state of a Service Profile.
- Associate and Disassociate Service Profiles.
- Create/modify/delete host firmware packages.
- Create/modify/delete adapter policies (Ethernet, FC and iSCSI).
- Create/modify/delete server-related policies: power and power placement, maintenance, BIOS, iSCSI profiles, vNIC/vHBA placement.
- Create/modify/delete management firmware packages. This feature is deprecated.

Service Profile Storage (ls-storage)

This privilege allows a user to configure storage policies and storage elements that are applied to service profile vHBAs. The user can also configure other storage elements that impact service profiles.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Create/modify/delete local disk policies.
- Configure vHBA initiator groups.
- Specify the allowed range for virtual WWN addresses.
- Configure vHBA templates.
- Configure FC group templates.
- Create/modify/delete storage connection policies.
- Configure vHBA behavior policy when vHBAs are not explicitly defined.
- Configure the FC storage visibility for a vHBA initiator group.
- Specify the allowed range for UUIDs.
- Set labels for FC zones.

Service Profile Storage Policy (ls-storage-policy)

This privilege allows a user to configure storage policies and storage elements that are applied to service profile vHBAs.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Configure Service Profile boot policies.
- Create/modify/delete vNIC/vHBA placement policies.
- Configure storage connection within a Service Profile.
- Create/modify/delete local disk policies.
- Specify the allowed range for virtual WWN addresses.
- Configure vHBA templates.
- Configure FC group templates.
- Configure pools of WWN addresses.
- Configure pools of IQN addresses (for iSCSI).
- Create/modify/delete storage connection policies.
- Specify the allowed range for UUIDs.

Operations (operations)

This privilege allows a user to perform maintenance activities, such as SEL backup operations, and to configure system-level policies, such as call home, syslog, and log level, and to create tech support files.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Configure log file export policies. Export log files.
- Acknowledge faults.
- Create/modify/delete stats threshold policies.
- Configure core file export policies. Download core files.
- Configure the Catalog pack, specifying which catalog to be used.
- Configure the Syslog feature.
- Clear or backup SEL log files (FEX, IO Module, CIMC). Configure SEL log policy.
- Generate and download Tech Support files.
- Configure the logging level for debug log files on the Fabric Interconnect.
- Configure the statistics collection policies.
- Configure whether config, firmware and monitoring policies are resolved locally or through UCS Central.

Org Management (org-management)

This privilege allows a user to configure organizations in the org hierarchy.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Create/modify/delete organizations.

Server Equipment (pn-equipment)

This privilege allows a user to configure the power supply redundancy policy and to control the power state of network adapters.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Control power state of network adaptors.
- Configure Power Supply Redundancy policy. Configure whether PSU redundancy policies can be resolved through UCS Central.

Server Maintenance (pn-maintenance)

This privilege allows a user to perform maintenance operations on physical servers, such as acknowledging servers, configuring locator LEDs, and decommissioning servers.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Enable/Disable Ethernet/FC/iSCSI ports and port channels on a server adapter. Set port/port channel label.
- Reset server DIMM errors.
- Control the power state of a Service Profile.
- Reset IO Module and FEX. Set IO Module/FEX labels.
- Perform server maintenance operations: reset CIMC, reset KVM server, reset CMOS, perform diagnostic interrupt, reset server. Set blade and rack server labels.
- Configure locator, indicator and beacon LEDs.
- Acknowledge, decommission, recommission and recover blade servers and rack servers.
- Acknowledge Chassis and IO Module. Set Chassis labels and chassis IDs.
- Enable/Disable Ethernet ports on a Fabric Interconnect or IO Module. Set port labels.
- Configure diagnostics.

Server Policy (pn-policy)

This privilege allows a user to configure server-related policies.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Configure VMware vCenter connections, datacenters, folders, switch.
- Reset server DIMM errors.
- Control power state of network adaptors.
- Configure Service Profile disk and BIOS scrub policies.
- Perform server maintenance operations: reset CIMC, reset KVM server, reset CMOS, perform diagnostic interrupt, reset server. Set blade and rack server labels.
- Configure whether server/chassis discovery policies can be resolved through UCS Central.
- Configure UUID pools.
- Configure VMware vCenter cryptographic keys.
- Configure server/chassis discovery, acknowledgement and connectivity policies. Configure blade inheritance and auto-configuration policy.
- Configure Virtual Machine and Virtual Machine vNIC retention policy.
- Control the power state of a Service Profile.
- Configure Power Supply Redundancy policy. Configure whether PSU redundancy policies can be resolved through UCS Central.
- Reset IO Module and FEX. Set IO Module/FEX labels.
- Configure server pools, server pool policies, and server pool qualification policies.
- Assign port profiles to Distributed Virtual Switches.
- Configure locator, indicator and beacon LEDs.
- Configure Service Profile BIOS policies.
- Run diagnostics.
- Acknowledge, decommission, recommission and recover blade servers and rack servers.
- Acknowledge Chassis and IO Module. Set Chassis labels and chassis IDs.

Server Security (pn-security)

This privilege is currently not used.

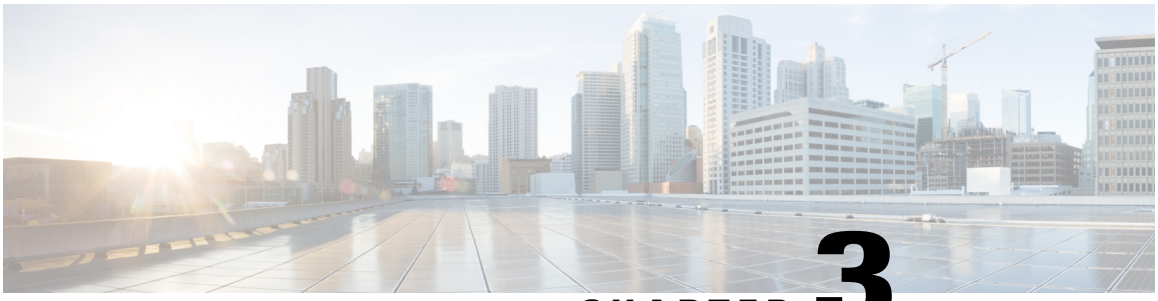
Power Mgmt (power-mgmt)

This privilege allows a user to configure power groups, the power budget, and power policies.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

- Configure Power Groups, power budget, and power policies.

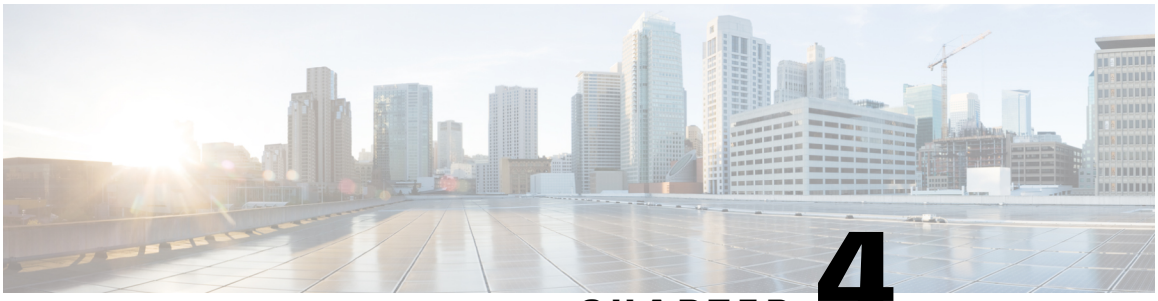


CHAPTER 3

Deprecated Privileges

The following privileges are not currently used by Cisco UCS Manager and are deprecated:

- pod-config
- pod-policy
- pod-security
- pod-qos
- ext-san-security
- ls-qos
- ls-ext-access



CHAPTER 4

Upgrading and Downgrading

This section describes the effects of upgrading to and downgrading from Cisco UCS, Release 2.2 on the new role and privileges introduced in this release.

Effect of Upgrading on Roles and Privileges

When upgrading Cisco UCS Manager from an earlier release to Cisco UCS 2.2, the server-compute role is added to the list of default roles in Cisco UCS Manager. By default, the following privileges are assigned to the server-compute role:

- Service Profile Compute (ls-compute)
- Service Profile Server Oper (ls-server-oper)
- Service Profile Server Policy (ls-server-policy)

The following new privileges are added to the list of privileges that you can add to a new or existing role:

- Org Management (org-management)
- Service Profile Compute (ls-compute)

Effect of Downgrading on the New Role

If you downgrade Cisco UCS Manager from Cisco UCS, Release 2.2 to an earlier release, the following occurs:

- If you have not made any changes to the server-compute role, that role is deleted and will not be available in the downgraded Cisco UCS Manager. Any user with this role is assigned read-only privileges.
- If you have customized the server-compute role by adding privileges to or deleting privileges from that role, the server-compute role remains in the downgraded Cisco UCS Manager and retains the privileges that you added to the role.
- If the server-compute role includes either of the privileges that were added in Cisco UCS, Release 2.2, those privileges are removed from the role when you downgrade.

Effect of Downgrading on Users Assigned with New Privileges

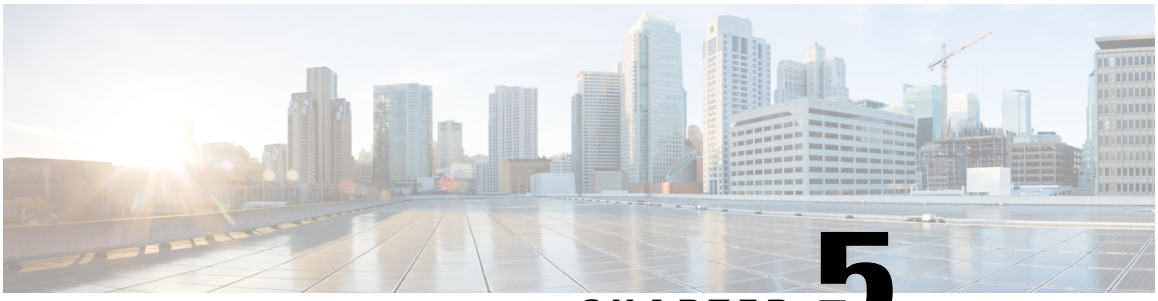
If you downgrade Cisco UCS Manager from Cisco UCS, Release 2.2 to an earlier release, the new privileges are not available in the downgraded Cisco UCS Manager. The following occurs to users who are assigned roles that include the new privileges:

- If the role includes other privileges that are available in the earlier release, the role and the user retains those privileges.
- If the role does not include other privileges that are available in the earlier release, the role and the user are assigned read-only privilege.

Effect of Upgrading Back to Cisco UCS Release 2.2 After a Downgrade

If you upgrade Cisco UCS Manager back to Cisco UCS, Release 2.2 after you have downgraded from that release, the following occurs to users who were assigned the new role or privileges:

- If the server-compute role was deleted during the downgrade, users retain read-only privileges. You must reassign the server-compute role to users.
- If the server-compute role was not deleted during the downgrade, users retain the privileges from the earlier release. However, the Service Profile Compute (ls-compute) privilege is not reassigned to that role. You must manually assign that privilege to the server-compute role. The server-compute role retains all other privileges assigned to it.
- If a user was assigned a custom role with either the Service Profile Compute (ls-compute) or Org Management (org-management), the users retain read-only privileges. You must manually assign the new privileges to the custom role.



CHAPTER 5

Related Documentation

For more information, you can access related documents from the Cisco UCS Documentation Roadmap.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Trademarks