Privileges in Cisco UCS, Release 2.1

First Published: November 16, 2012
Last Updated: November 16, 2012
Part Number: OL-28363-01

This document includes the following sections which describe the privileges in Cisco UCS, Release 2.(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.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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:

- All tasks inherited from privilege: **ls-security**
- Configure DNS providers and DNS domain
- Configure Key Ring. Import certificates of trusted authorities. Generate and import Certificates
- Configure SNMP policy, SNMP users, SNMP trap destinations
- 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 whether communication policies are resolved locally or through UCS Central

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:

- All tasks inherited from privilege: **ext-lan-security**
- Configure DNS providers and DNS domain
- Configure Ethernet PIN Groups

- Configure Ethernet border ports on the Fabric Interconnect. Add/remove VLANs to border ports
- Configure Ethernet monitoring sessions (SPAN)
- Configure Fabric Interconnect system name
- Configure MAC aging properties. Specify Ethernet end-host or switching mode. Enable/Disable VLAN compression
- Configure VLANs and VLAN groups
- Configure management interfaces monitoring policy
- Configure management interfaces on the Fabric Interconnect
- Enable/Disable Ethernet ports on a Fabric Interconnect or IO Module. Set port labels
- 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

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:

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

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

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:

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

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:

- All tasks inherited from privilege: **ls-server-oper**
- Associate and Disassociate Service Profiles
- Configure Service Profile BIOS policies
- Configure schedules. Schedules can be used to trigger one-time or periodic tasks in the future
- Configure the vNIC/vHBA placement of a Service Profile
- Configure vHBA initiator groups
- Create/modify/delete Service Profile dynamic vNICs within a Service Profile
- Create/modify/delete Service Profile maintenance policies

- Create/modify/delete Service Profiles/Templates. Assign policies to Service Profiles. Control power policies and placement. Acknowledge service profile pending tasks
- Create/modify/delete host firmware packages
- Specify boot devices, boot order and boot parameters 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:

- All tasks inherited from privilege: **ls-server**
- Assign port profiles to Distributed Virtual Switches
- Configure VMware vCenter connections, datacenters, folders, switch
- Configure VMware vCenter cryptographic keys

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:

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

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:

- All tasks inherited from privilege: **ls-qos-policy**
- Assign port profiles to Distributed Virtual Switches
- Configure Ethernet server ports on the Fabric Interconnect
- Configure LAN connectivity policies. Configure Service Profile vNICs and add/remove VLANs on vNICs
- Configure Service Profile iSCSI vNICs
- Configure VLAN and VLAN group org permissions
- Configure VM-FEX Port Profile policy
- Configure VMware vCenter connections, datacenters, folders, switch
- Configure iSCSI boot parameters
- Configure vNIC behavior policy when vNICs are not explicitly defined
- Configure vNIC templates
- Create/modify/delete Network Control policies
- Create/modify/delete Service Profile dynamic vNIC policies
- Create/modify/delete Service Profile dynamic vNICs within a Service Profile
- Create/modify/delete vNIC/vHBA placement policies
- Reset IO Module and FEX. Set IO Module/FEX labels
- Specify the allowed range for virtual MAC addresses

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:

- All tasks inherited from privilege: **ls-qos-policy**
- Configure Ethernet server ports on the Fabric Interconnect
- Configure VM-FEX Port Profile policy
- Configure pools of IP addresses
- Configure pools of MAC addresses

- Configure vNIC templates
- Create/modify/delete Network Control policies
- Create/modify/delete Service Profile dynamic vNIC policies
- Create/modify/delete Service Profile dynamic vNICs within a Service Profile
- Create/modify/delete vNIC/vHBA placement policies
- Reset IO Module and FEX. Set IO Module/FEX labels
- Specify the allowed range for virtual MAC addresses

Service Profile Qos Policy (ls-qos-policy)

This privilege allows a user to configure quality of service and flow control policies for service profiles.

Tasks Allowed with this Privilege

A user with this privilege can perform the following tasks:

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

- Create/modify/delete IPMI policies

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:

- All tasks inherited from privilege: **ls-server-oper**
- Associate and Disassociate Service Profiles
- Configure FC group templates
- Configure LAN connectivity policies. Configure Service Profile vNICs and add/remove VLANs on vNICs
- Configure SAN connectivity policies. Configure Service Profile vHBAs and add/remove VSANs on vHBAs
- Configure Service Profile BIOS policies
- Configure Service Profile iSCSI vNICs
- Configure schedules. Schedules can be used to trigger one-time or periodic tasks in the future
- 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 Profile dynamic vNICs within a Service Profile
- Create/modify/delete Service Profiles/Templates. Assign policies to Service Profiles. Control power policies and placement. Acknowledge service profile pending tasks
- Specify boot devices, boot order and boot parameters of 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 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:

- Allows the user to 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:

- All tasks inherited from privilege: **ls-server-oper**
- Associate and Disassociate Service Profiles
- Configure Service Profile boot policies
- Create/modify/delete adapter policies (Ethernet, FC and iSCSI)
- Create/modify/delete host firmware packages
- Create/modify/delete management firmware packages. This feature is deprecated
- Create/modify/delete server-related policies: power and power placement, maintenance, BIOS, iSCSI profiles, vNIC/vHBA placement

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:

- Configure FC group templates
- Configure SAN connectivity policies. Configure Service Profile vHBAs and add/remove VSANs on vHBAs
- Configure Service Profile iSCSI vNICs
- Configure vHBA behavior policy when vHBAs are not explicitly defined
- Configure vHBA templates
- Create/modify/delete local disk policies
- Create/modify/delete storage connection policies
- Set labels for FC zones
- Specify boot devices, boot order and boot parameters of a Service Profile
- Specify the allowed range for UUIDs
- Specify the allowed range for virtual WWN addresses

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

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:

- All tasks inherited from privilege: **ext-lan-security**
- Acknowledge faults
- Clear or backup SEL log files (FEX, IO Module, CIMC). Configure SEL log policy
- Configure core file export policies. Download core files
- Configure the Call Home feature
- Configure the Catalog pack, specifying which catalog to be used
- Configure the Syslog feature
- 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
- Create/modify/delete stats threshold policies
- Generate and download Tech Support files

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:

- All tasks inherited from privilege: **pn-maintenance**
- Configure Power Supply Redundancy policy. Configure whether PSU redundancy policies can be resolved through UCS Central
- Control power state of network adaptors

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:

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

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:

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

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

Deprecated Privileges

The following privileges are not currently used by Cisco UCS Manager and may be deprecated in a future release:

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

Effects of Upgrading and Downgrading

This section describes the effects of upgrading to and downgrading from Cisco UCS, Release 2.1 on the new role and privileges introduced in this release.

- Effect of Upgrading on Roles and Privileges, page 14
- Effect of Downgrading on the New Role, page 15
- Effect of Downgrading on Users Assigned the New Privileges, page 15
- Effect of Upgrading Back to Cisco UCS, Release 2.1 After a Downgrade, page 15

Effect of Upgrading on Roles and Privileges

When you upgrade Cisco UCS Manager from an earlier release to Cisco UCS 2.1, the following occurs:

- 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 2.1 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 2.1, those privileges are removed from the role when you downgrade.

Effect of Downgrading on Users Assigned the New Privileges

If you downgrade Cisco UCS Manager from Cisco UCS, Release 2.1 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 2.1 After a Downgrade

If you upgrade Cisco UCS Manager back to Cisco UCS, Release 2.1 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.

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 the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:

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

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

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