Cisco UCS Central Troubleshooting Reference Guide

First Published: 2015-01-30

Last Modified: 2016-06-17

Last Modified: 2017-05-02

Last Modified: 2018-07-31

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

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 NONINFRINGEMENT 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.

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.

CONTENTS

Preface

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

Conventions

Text Type	**Indication**
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.

Text Type	Indication
{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.
< >	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*. Notes contain helpful suggestions or references to material not covered in the document.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_rack_roadmap.html.

For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

Follow Cisco UCS Docs on Twitter to receive document update notifications.

Documentation Feedback

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

CHAPTER 1

General Troubleshooting

Guidelines for Troubleshooting

When you troubleshoot issues with Cisco UCS Central or a component that it manages, follow the guidelines listed in the following table.

Table 1: Troubleshooting Guidelines

Guideline	Description
Check the release notes to see if the issue is a known problem.	The release notes are available at: Cisco UCS Central Release Notes.
Take screenshots of the fault or error message dialog box, the FSM for the component, and other relevant areas.	These screenshots provide visual cues about the state of Cisco UCS Central when the problem occurred. If your computer does not have software to take screenshots, check the documentation for your operating system.

Guideline	Description
Record the steps that you took directly before the issue occurred.	If you have access to screen or keystroke recording software, repeat the steps you took and record what occurs in Cisco UCS Central. If you do not have access to that type of software, repeat the steps you took, make detailed notes of the steps and what happens in Cisco UCS Central after each step.
Create a technical support file.	The information about the current state of Cisco UCS Central and the Cisco UCS domains is helpful to Cisco support. It frequently provides the information to identify the source of the problem.

Technical Support Files

When you encounter an issue that requires troubleshooting, or a request for assistance to the Cisco Technical Assistance Center (Cisco Technical Assistance Center), collect as much information as possible. Cisco UCS Central outputs this information into a tech support file that you can send to TAC.

The following describes how to generate technical support log files through the HTML5 GUI and through the CLI. This guide does not support versions of Cisco UCS Central with the FLEX GUI.

Creating a Technical Support File in the Cisco UCS Central CLI

Use the **show tech-support** command to output information about a Cisco UCS domain that you can send to Cisco Technical Assistance Center.

Procedure

	Command or Action	Purpose
Step 1	UCS-A # **connect local-mgmt** {**a** | **b**}	Enters local management mode.
Step 2	UCS-A (local-mgmt) # **show tech-support detail**	Produces a detailed report (tgz file) that you can send to Cisco TAC to debug.
Step 3	UCS-A (local-mgmt) # **copy volatile:/**<*filename*>*.tar* {**scp** | **ftp** | **sftp** | **tftp**}: *user_name@IP_address* | *username*'s password: *password*	Copies the output file to an external location. The SCP and FTP commands require an absolute path for the target location. The path to your home directory cannot include special symbols, such as '~'.

Creating a Tech Support File in the Cisco UCS Central GUI

The following steps describe how to generate a tech support file in the HTML GUI.

Procedure

Step 1 Click on the **System Tools** icon and choose **Tech Support**.

In v1.4, the System Tools icon is called the Operations icon.

Step 2 From the Domain list, click a domain, or UCS Central.

Step 3 Click **Generate Tech Support**.
The Generate Tech Support dialog opens.

Step 4 Select **Include System data such as policies and inventory**.

Step 5 Click **Yes**.

Step 6 After Cisco UCS Central produces the report, select it.

Step 7 Click **Download** to download the report to your local system so you can email it to Cisco TAC.

Inventory Data Sync

When you register a Cisco UCS Manager domain to Cisco UCS Central, Cisco UCS Central performs a full inventory. After the initial inventory, Cisco UCS Central only performs a partial inventory, which consists of the delta between the previous inventory and the current one.

After an update, it's common to see an inventory out of sync. If inventory data is out of sync between Cisco UCS Manager and Cisco UCS Central, the status updates from Cisco UCS Manager do not display on Cisco UCS Central. On Cisco UCS Central, the inventory status displays as In Progress, but does not change to OK.

Note Acceptable latency between Cisco UCS Manager and Cisco UCS Central is less than 300ms.

Verify that the pmon state shows all of the Cisco UCS Central DME Logs processes in the CLI.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **connect local-mgmt**	Connects local management.
Step 2	UCSC(local-mgmt)# show pmon state	**Note** If your Cisco UCS domain is running Cisco UCS Manager v2.2.3 or earlier, and you are using a WAN environment with low bandwidth and high latency, inventory processing may timeout. To fix, install the latest version of Cisco UCS Manager.
Step 3	Alternatively, in the UI, click the Alerts icon, then click **Internal Services**.	

Refreshing the Inventory

Manually refresh the inventory for the specific Cisco UCS domain using the Cisco UCS Central CLI.

Procedure

	Command or Action	Purpose
Step 1	connect resource-mgr	Connects to the resource manager.
Step 2	scope domain-mgmt	Connects to domain management.
Step 3	show ucs-domain	Displays all registered domains and their IDs.
Step 4	scope ucs-domain <*domain-ID*>	Connects to the chosen domain.
Step 5	refresh-inventory	Refreshes the inventory.
Step 6	commit-buffer	Commits the transaction.

Disk Space Issues

The following describes disk space issues you could encounter:

Issue	Resolution
Scale issues	If you have many domains, enhance the VM configuration (memory, storage, etc.) to at least double the recommended numbers.
Excess images and files	Ensure that you clean up your unused images and technical support files.
Log files grew unbounded	Some users experienced a problem where syslog files grew larger than expected. These files consumed as much available space as possible, triggering alerts. This also prevented signing in and other admin functions. This issue has been fixed.

Boot Flash Full

If you enabled statistics collection with the internal statistics database, it could fill up the boot flash partition. To fix, drop the internal statistics database and disable statistics collection. Also, you could configure an external statistics database for statistics collection.

Attention Contact Cisco TAC if your /bootflash partition becomes full and you have stats collection enabled. Please note that the Statistics Management feature is being deprecated and will not be supported after Cisco UCS Central release 1.5.

Procedure

	Command or Action	Purpose
Step 1	UCSC# connect stats-mgr	Disables statistics collection.

	Command or Action	Purpose
Step 2	sc collection-policy	
Step 3	/collection-policy # set collection-interval never	
Step 4	/collection-policy* # commit-buffer	

Port Configuration with a Firewall

The following table lists the ports that you must configure:

Issue	Resolution
Ports open on Cisco UCS Central	• HTTPS_PORT=”https”(443) – Communications from Cisco UCS Central to Cisco UCS domain(s) and Cisco UCS Central GUI. Always required. • HTTP_PORT=”http”(80) – Communications from Cisco UCS Central to Cisco UCS domain(s). This port is configurable, and only required for the Flash-based Cisco UCS Central UI. • PRIVATE_PORT=(843) – Cisco UCS Central communications from Flash UI to Cisco UCS Central VM. Only required for the Flash-based Cisco UCS Central UI. This is not required if using the new HTML-5 UI. **Note** For Cisco UCS Manager domains v2.2(1b) and below, you also must open the following NFS ports: • LOCKD_TCPPORT=32803 – Linux NFS lock • MOUNTD_PORT=892 – Linux NFS mount • RQUOTAD_PORT=875 – Linux remote quota server port (NFS) • STATD_PORT=32805 – Linux – Used by NFS file locking service – lock recovery • NFS_PORT="nfs"(2049) – Linux NFS listening port • RPC_PORT="sunrpc"(111) – Linux RPCBIND listening port
Port open on Cisco UCS Manager	• HTTPS_PORT=”https”(443) – Communications from Cisco UCS Central to Cisco UCS domain(s). Always required.

DNS Troubleshooting

You can configure the DNS server from the Cisco UCS Central HTML-5 UI.

- If Cisco UCS Central fails to resolve domain names, check that the DNS server is added to the `/etc/resolve.conf` file.
- Check for any errors in the `/var/log/core/svc_cor_controllerAG.log`.

Host Firmware Package Policy Issues

Beginning with Cisco UCS Central release 1.4, you can exclude components from your host firmware package policy. When excluding components, be aware of the following:

- The global-default host firmware package policy includes all components. If you create a new custom host firmware package policy, it automatically excludes the local disk component.
- Host firmware package policies created in Cisco UCS Central v1.3, or previous versions, do not support excluding components. These policies do not change when you upgrade to Cisco UCS Central v1.4.
- If you create your own custom host firmware package policy with excluded components, you cannot include it in a service profile associated with a server running a Cisco UCS Manager version prior to 2.2.7. If you do, the following error displays during service profile association:

  ```
  ucs domain does not have the matching server capabilities for this service-profile
  ```

  You can either remove all excluded components in the host firmware package policy, or upgrade your version of Cisco UCS Manager to the latest version.

Private VLAN Issues

The following issues could cause PVLAN configuration to fail:

- VLAN referenced by a global service profile, port, or port channel that does not exist or has been deleted.
- VLAN referenced by a port or port channel that is not created in the appropriate cloud.
- VLAN referenced by a global service profile, port, or port channel that is not created under the appropriate domain groups.
- VLAN ID/Name is overlapping with other VLANs that exist locally on a Cisco UCS domain.
- More than one secondary VLAN is referring to the same primary VLAN.
- The secondary VLAN referenced by the global service profile, port, or port channel does not refer to a valid primary VLAN.
- The secondary VLAN referenced by global service profile, port, or port channel refers to a primary VLAN that was deleted.

Fixing Private VLAN Issues

To fix the PVLAN configuration issues:

Procedure

Step 1 Check the configuration and FSM status of the global service profiles, ports, or port channels.

Step 2 Analyze the domain and system faults for any related failures.

Smart Call Home Issues

The following table lists issues related to Smart Call Home:

Issues	Resolution
Configuration changes or issues	When you change a configuration, or enable or disable call home, you can check the status on the **System Configuration** > **Smart Call Home** > **Configuration Status**. Errors that are internally identified, such as "invalid certificate in the transport gateway" display here.
Registration email not received	When you enable Smart Call Home for the first time, you should receive an email confirming or requesting registration within five minutes. If you do not receive the email, create another inventory from **System Configuration** > **Smart Call Home** > **Basic** > **Operations** > **Send System Inventory Now**.
Viewing logs	• Smart Call Home logs are located at `/var/log/gch` and `/var/log/resource-mgr`. • Individual Data Management Engine (DME) logs specific call home events that are raised within the DME. For example, the core DME raises a process core dumped event. The information specific to the event is located in `/var/log/core/svc_core_dme.log`. • Audit logs and tech support files capture specific configuration changes made in the Smart Call Home section.

Smart Software Licensing Issues

The first five Cisco UCS Central domains are currently licensed at no charge. For more domains, there is a charge. Support for the initial, or additional domains, is available as a paid option with the licenses.

Note There is a 120-day grace period after the registration of the first domain. You can register any number of domains during this grace period. After the grace period expires, a license is required to prevent licensing fault alarms.

The following table lists issues related to Smart Software licensing:

Issues	Resolution
Registration failed due to network issue	Review the network connectivity to the Cisco Smart Software Licensing portal.
Deregistration failed due to network issue	Manually remove the product instance from the Cisco Smart Software Licensing portal.

Issues	Resolution

Smart Software Licensing tech support commands	`(resource-mgr) /smart-license # generate techsupport`
	`(resource-mgr) /smart-license* # commit-buffer`

Smart Software Licensing show commands	`(policy-mgr) /org/device-profile/smart-license # show smart-license`
	`(resource-mgr) /smart-license # show license usage`
	`(resource-mgr) /smart-license # show license summary`
	`(resource-mgr) /smart-license # show license status`
	`(resource-mgr) /smart-license # show license udi`
	`(resource-mgr) /smart-license # show license techsupport`
	`(resource-mgr) /smart-license # show license all`

Smart Software Licensing logs	`/var/log/resource-mgr/svc_sam_cloudAG.log` `/var/log/resource-mgr/svc_rsrcMgr_dme.log`

DME Logs

The following table lists the Data Management Engine (DME) logs used in Cisco UCS Central:

Issue	Resolution
Mgmt-controller (core) DME	Applies VM settings like IP address, DNS, NTP. • Located in /var/log/core • svc_core_dme.log – DME log • svc_core_controllerAG.log – runs scripts to configure VM • svc_core_secAG.log – authentication errors (local/ldap)
Policy-mgr DME	Policy management, ID Pool management. • Located in /var/log/policy-mgr • svc_pol_dme.log – DME log • svc_sam_pkiAG.log – certificate maintenance.
Resource-mgr DME	Service profiles, VLANS/VSANS, Inventory. • Located in /var/log/resource-mgr • svc_rsrcMgr_dme.log – DME log
Identifier-mgr DME	Management for IDs. • Located in /var/log/identifier-mgr • svc_idm_dme.log – DME log

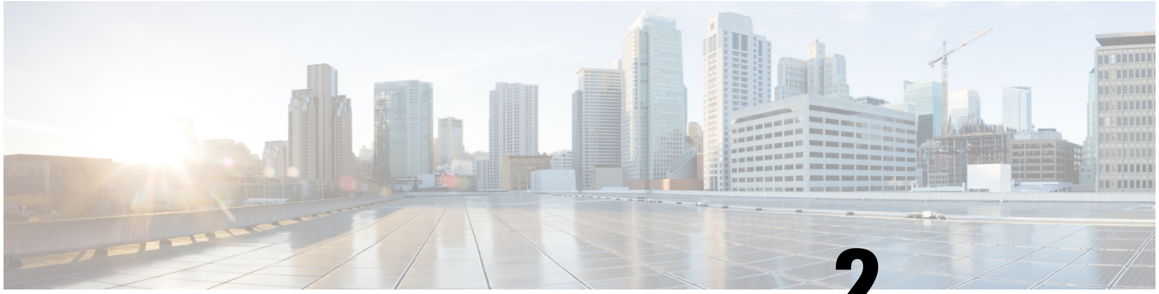
Issue	Resolution
Service Registry DME	Monitors DME status, registered domain status. • Located in /var/log/service-reg • svc_reg_dme.log – DME log
Operation-mgr DME	Backup, and firmware management. • Located in /var/log/operation-mgr • svc_ops_dme.log – DME log • svc_ops_imgMgmtAG.log - image management
Stats-mgr DME	Statistics collection from Cisco UCS domains. • Located in /var/log/stats-mgr • svc_statsMgr_dme.log – DME log
Central-mgr DME	Single entry point for XML API. • Located in /var/log/central-mgr • svc_centralMgr_dme.log – DME log

Cisco UCS Central Processes

The following table lists the Cisco UCS Central processes:

Service Name	Description
core-svc_cor_secAG	Implements authentication related feature, such as local auth and remote auth
identifier-mgr-svc_idm_dme	Manages ID pools and allocates unique IDs in the system
core-solr.sh	SOLR process
resource-mgr-svc_sam_snmpTrapAG	Sends SNMP traps from resource-mgr
central-mgr-svc_centralMgr_dme	Cisco UCS Central NBAPI provider forwards the NBAPI to a specific DME
policy-mgr-svc_pol_dme	Manages Cisco UCS Central policies
identifier-mgr-svc_sam_snmpTrapAG	Sends SNMP traps from identifier-mgr
core-svc_cor_snmpTrapAG	Sends SNMP traps from mgmt-controller
operation-mgr-svc_ops_dme	Operations manager DME

Service Name	Description
policy-mgr-svc_sam_pkiAG	Provides PKI related service for policy-mgr DME
core-httpd.sh	Starts httpd process
gch-call_home	Cisco GCH call home process, which forwards the callhome/smartlicense message to Cisco Cloud Smartlicense Manager
service-reg-svc_sam_snmpTrapAG	Sends SNMP trap from service-reg
core-svc_cor_sessionmgrAG	Session auditing for Cisco UCS Central HA implementation
core-svc_cor_dme	Manages the configuration for Cisco UCS Central VM (mgmt-control DME)
resource-mgr-svc_sam_cloudAG	GCH callhome, smartlicense application gateway
stats-mgr-svc_sam_snmpTrapAG	Sends SNMP trap from stats-mgr
service-reg-svc_reg_dme	Implements registration service for different DME and UCSM
operation-mgr-svc_ops_imgMgmtAG	Image management application gateway for operations manager
resource-mgr-svc_rsrcMgr_dme	Resource manager DME where Cisco UCS Manager inventory is kept and which manages GSP
core-tomcat.sh	Controlling script for tomcat process
service-reg-svc_sam_controller	AG to implement Cisco UCS Central HA service
operation-mgr-svc_sam_snmpTrapAG	Sends SNMP trap from operation manager
sam_cores_mon.sh	Script to monitor and manage Cisco UCS Central coredump file
core-svc_cor_controllerAG	AG to configure Cisco UCS Central VM policies
service-reg-svc_sam_licenseAG	License AG for domain base license.
core-sam_nfs_mon.sh	Script to monitor NFS
gch-xosdsd	Infrastructure process for implementing GCH smartlicense feature
policy-mgr-svc_sam_snmpTrapAG	Sends SNMP Trap from policy-mgr
stats-mgr-svc_statsMgr_dme	Statistics manager which collects statistics from different Cisco UCS Manager domains and generates the statistics report



CHAPTER 2

Installation

Initial Setup in Cluster Installation for RDM

The following table lists issues you could encounter during initial setup in a cluster installation with raw device mapping (RDM):

Issue	Resolution
In ISO installation, I/O error on shared LUN.	Click **Ignore** and normal installation proceeds.
High Availability or other RDM-related feature is not ready.	Make sure that multipath is **not** enabled.
Cannot convert standalone mode to HA cluster.	Check if you have multipath enabled. If yes, contact Cisco Technical Assistance Center to disable multipath.
Validations on Node A	
No shared storage devices detected during first node installation.	Check if the RDM and shared disk have been added with required configuration. See Installation and Upgrade Guide, specific to the Cisco UCS Central release version you are using.
Failed to write on disk.	• RDM may have persistent writing or LUN ownership issues. Verify that the RDM has the same specifications as mentioned in the "Adding and Setting up an RDM Shared Storage on VMware" in the Installation and Upgrade Guide. • Verify that you disabled SCSI filtering in Hyper-V. • Verify that the path selection policy for the RDM hard disk is **fixed (VMware)**.
Validations on Node B	

Issue	Resolution
Peer node unreachable.	Verify the following: • Installation is complete on node A. • Network connectivity between both nodes is active.
Expected shared storage device not found.	Make sure that you configure the same shared storage device (same LUN) for both nodes.
Node cannot be added to the cluster.	Verify the following: • Both nodes are at the same Cisco UCS Central release version. • The IP address configured on the second node matches the value of peer node IP entered during first node setup. • Username and password for the peer node is correct.
You have enabled multipath while setting up HA.	Contact Cisco Technical Assistance Center.

Cluster State Issues

The following table lists issues that you could encounter in cluster state:

Issue	Resolution
Node state - down.	Verify the following: • Peer node is powered up. • Network connectivity between both nodes is active.

Management Services State - DOWN. This means that one or more services are down on the node.	Use the **show pmon state** command to verify the process states in local management.
	`UCSC# connect local-mgmt`
	`UCSC(local-mgmt)# show pmon state`

High Availability is not ready. No devices found for quorum.	For HA, you must have at least one registered Cisco UCS Manager domain in Cisco UCS Central. Check the current registration status for registered domains.
I/O error in quorum devices.	Check the availability of the Cisco UCS domains with quorum, using either one or both cluster nodes.
I/O error in shared storage.	Verify that the LUN is unaltered. Only the VMs in the cluster nodes can share the LUN.

Network Access

The following table lists issues related to accessing the network after installation:

Issues	Resolution
Cisco UCS Central GUI or CLI is not accessible through a virtual IP.	Check if election completed successfully and primary node is selected. It can take up to 5 minutes after election to enable virtual IP.

VM IPs are not reachable.	Run the **reset-network***<IP><Mask><Gateway>* local-mgmt command on the affected VMs console in VSphere Client.
	`UCSC# connect local-mgmt`
	`UCSC(local-mgmt)# reset-network <IP><Mask><Gateway>`

CHAPTER 3

Registration Issues

Date and Time Mismatch

Date and time mismatch is the most common issue with registration. If the certificate is not valid, regenerate the default keyring certificate from Cisco UCS Central:

Before you begin

To ensure that the date and time between Cisco UCS Central and Cisco UCS domains are in sync, ensure that you have a valid NTP configuration with Cisco UCS Central and the Cisco UCS domains.

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope keyring default**	Enters key ring security mode for the default key ring.
Step 6	UCSC(policy-mgr) /org/device-profile/security/keyring # **set regenerate yes**	Regenerates the default key ring.
Step 7	UCSC(policy-mgr) /org/device-profile/security/keyring* # **commit-buffer**	Commits the transaction to the system configuration.

Updating Shared Secret

If you have issues after correcting the configuration, you may need to update the shared secret in Cisco UCS Manager.

Procedure

	Command or Action	Purpose
Step 1	UCSM#**scope system**	Enters system mode.
Step 2	UCSM /system #**scope control-ep policy**	Scopes the control-ep policy.
Step 3	UCSM /system/control-ep #**set shared-secret**	Sets the shared secret. Shared Secret for Registration:
Step 4	UCSM system/control-ep #**commit-buffer**	Enters security mode.

What to do next

Important

Before calling Cisco TAC, make sure that:

- You synchronize the date and time in Cisco UCS Central and registered Cisco UCS domains.
- Cisco UCS Domain is not in suspended or lost visibility state.
- The registration status for the domain displays **Registered**.

TCP Packet Loss Issues

Sometimes, TCP package loss may result in registration failure. If this happens, contact Cisco TAC.

Other Registration Issues

The following issues may also affect registration:

- Port 443 must be open between Cisco UCS Manager and Cisco UCS Central.
    - To check TCP connectivity on Cisco UCS Manager (from root shell or from primary node), type:

      ```
      (local-mgmt) # test ucsm-connectivity <ip_address_of_UCSM_machine>
      ```

- If the Cisco UCS domains are over WAN, upgrade to Cisco UCS Central release 1.3(1a) to avoid a timeout issue over the slow speed connection.
- View the log files in the following locations:
    - Cisco UCS Manager Log files (`/var/sysmgr/sam_logs/`):
        - `svc_sam_dme.log` (looks for curl errors)

    - `svc_sam_dcosAG.log` (invokes cert-gen.pl script)
    - `pa_setup.log` (contains cert generation errors)

- Cisco UCS Central log files (`/var/log/`):
    - `core/httpd.log`
    - `core/error_log.1442275635`
    - `Service-reg/svc_reg_dme.log`

CHAPTER 4

LDAP Authentication and 3rd Party Certificates

Verifying LDAP Configurations

Note You can only perform this procedure through the Cisco UCS Central CLI.

It verifies the configuration of the Lightweight Directory Access Protocol (LDAP) provider or the LDAP provider group.

Verifying LDAP Native Authentication

When LDAP fails, verify that Cisco UCS Central can communicate with the LDAP provider:

- The server responds to the authentication request if you provide the correct username and password.
- The roles and locales defined on the user object in the LDAP are downloaded.
- The LDAP group authorization is turned on and the LDAP groups are downloaded.

The first step is to verify that Cisco UCS Central is configured with native authentication.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope auth-realm**	Enters authentication realm security mode.

Step 6	UCSC(policy-mgr) /org/device-profile/security/auth-realm # **show default-auth**	Following is an example of the result
		`Default Authentication:`
		`    Realm Authentication Server Group`
		`    ----- --------------------------`
		`    Local`

Verifying the LDAP Provider Configuration

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters LDAP mode.

Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **show server detail**	Shows server detail:
		`  Hostname or IP address: provider1`
		`    Order: 1`
		`    bindDN:`
		`CN=Administrator,CN=Users,DC=qasamlab,DC=com`
		`    Password:`
		`    Port: 389`
		`    SSL: No`
		`    Basedn: DC=qasamlab,DC=com`
		`    User profile attribute: ciscoavpair`
		`    Filter: cn=$userid`
		`    LDAP Vendor: Open Ldap`

3rd Party Certificates

The following table lists issues related to 3rd party certificates:

Issues	Resolution

Registered Cisco UCS domain fails to register or changes to lost visibility status	Keyring, or certificate configured in Cisco UCS Central, has expired. If the keyring is configured to default, execute the following command to regenerate the default certificate:
	`UCSC # connect policy-mgr`
	`UCSC(policy-mgr)# scope org`
	`UCSC(policy-mgr) /org# scope device-profile`
	`UCSC(policy-mgr) /org/device-profile # scope security`
	`UCSC(policy-mgr) /org/device-profile/security # scope keyring default`
	`UCSC(policy-mgr) /org/device-profile/security/keyring* # set regenerate yes`
	`UCSC(policy-mgr) /org/device-profile/security/keyring* #commit-buffer`
	If the configured keyring is issued by a third party CA, make sure to renew the certificate from the third-party.

Certificate status displays **Not Yet Valid**.	Occurs when Cisco UCS Central is behind in time with CA server. Cisco UCS Central, Cisco UCS domain and the CA server must be synchronized to a valid NTP server.
Certificate status displays **Empty Cert**.	Occurs when the certificate field is empty. Provide content for issued certificates.
Certificate status displays **Failed to Verify with TP**.	Occurs when the configured **Trusted Point** is not the one from which the certificate is issued. Configure the correct **Trusted Point**.
Certificate status displays **Failed to Verify with Private Key**.	Occurs when the certificate contents are wrong and does not match with the certificate request you had created. Make sure to update the certificate information from the certificate request created in the keyring.
Certificate status displays **Certificate Chain Too Long**.	Occurs when the configured **Trusted Point** has a bundled certificate with a depth of 10 or more. This is a product boundary limitation by design.
There are no options to upload or specify CRL.	Cisco UCS Central does not support revoked certificates, so the option to specify CRL is not available.

The `regenerate certificate` command does not work	This command is removed from Cisco UCS Central. Use the following:
	`UCSC # connect policy-mgr`
	`UCSC(policy-mgr)# scope org`
	`UCSC(policy-mgr) /org# scope device-profile`
	`UCSC(policy-mgr) /org/device-profile # scope security`
	`UCSC(policy-mgr) /org/device-profile/security # scope keyring default`
	`UCSC(policy-mgr) /org/device-profile/security/keyring* # set regenerate yes`
	`UCSC(policy-mgr) /org/device-profile/security/keyring* #commit-buffer`

Multidomain certificate does not work.	Cisco UCS Central does not accept multiple DNS entries in a certificate request.

Issues	Resolution
Wildcard certificate does not work.	Cisco UCS Central does not accept wildcards in DNS or subject fields.
Trusted point certificate does not work.	Make sure you have the following order to specify the bundled certificate: **1.** Specify the self-signed primary certificate. **2.** Specify the subordinate certificate.
Cisco UCS domain registration fails or changes to lost visibility when the configured trust point contains a bundled certificate with depth 2 or more.	Q: If certificate sync fails on both nodes in a cluster setup, what do I do? • When you convert a standalone installation to cluster installation, make sure to recreate the certificate after completing installation on node B. • For an existing cluster setup, contact Cisco Technical Assistance Center.
Certificate sync fails on both the nodes in an HA Cisco UCS Central setup.	Certificate sync fails on both nodes when standalone to HA conversion occurs for Cisco UCS Central setup due to a known issue. Recreate the certificate after HA is ready. For an HA setup that is running, if certificate sync fails, contact Cisco Technical Assistance Center. You can identify certificate sync failure when the browser throws a certificate error. This occurs when you use the IP address of one of the nodes to open the application. It also fails when Cisco UCS Manager registration fails with Cisco UCS Central node IPs of an HA setup.
Certificate is valid, but Cisco UCS Manager still fails to register.	If a certificate configured on Cisco UCS Central contains extra space characters at the end of the certificate, these are incorrectly translated into extra lines on the certificate issued to Cisco UCS Manager, resulting in registration failure. Remove extra space characters, and re-configure it on Cisco UCS Central.

SSL Issues

UCSC third-party certificate request contains required key usages set.

If Customer uses an internal PKI provider, they must use the appropriate template to set both the SSL client, and the SSL server key usages.

Note

For Microsoft Enterprise CA, use the computer template to issue third-party certificates.

Cisco UCS Central does not allow you to configure third-party certificates without an SSL client and SSL server key usages.

CHAPTER 5

Globally Identified Issues

Global Policy Resolution

If global policy resolution is not working, verify the following:

- On the Cisco UCS Manager Registration page, make sure that policy resolution control for the category is set to Global.
- Place Cisco UCS domain into the correct domain group in Cisco UCS Central.
- Define the global policies for Cisco UCS Central for that category.
- In Cisco UCS Manager, if the local service profiles refer to global policies, and the global policies are not resolving down to Cisco UCS Manager from Cisco UCS Central, verify if:
    - The registered Cisco UCS domain is in a suspended state.
    - The Cisco UCS Manager GUI displays cached data.
    - The Cisco UCS domain has lost visibility.
- Local service profiles refer to maintenance policies and schedulers from the domain group from which the Cisco UCS domain is a member. From Cisco UCS Central release 1.3(1a) and above, host firmware policies resolve from the org hierarchy.
- All global policies work in entirety, and not partially across nested domain-groups.

  For example, a Cisco UCS domain is part of subdomain group root/DG1. DG1 has time zone settings defined without an NTP server, while domain group root has NTP servers defined. Only the time zone is resolved at the Cisco UCS domain. The NTP server settings should not be pushed down to Cisco UCS Manager.

Global ID Pools

Global ID pools include:

- Global IP pools
- MAC pools
- WWN pools
- IQN pools
- UUID pools

Issue	Resolution
The local service profiles in Cisco UCS Manager refer to global ID pools, but the IDs are not allocated.	Check the following: • The registered Cisco UCS domain is not in lost visibility or suspended state. • No local pools with the same name exist with available IDs. If they do, the IDs are issued from the local pool instead of the global ID pool. • No initial vNIC or vHBA template is used for references. Global initial templates for vNICs and vHBAs have a caveat that prevents ID requests from MAC or FC pools. • Make sure that the global pools contain enough IDs.
IDs not getting pulled from the pools assigned for the global service profile.	Verify the blocks in the pools do not have an ID range qualifier assigned. Global service profiles cannot consume IDs from the blocks with an ID range qualifier assigned.
You see the following fault: `ID is defined in multiple systems`	This fault occurs when the same ID is defined in two registered domains, or is defined in both Cisco UCS Central and registered Cisco UCS Manager. Avoid this fault by removing the duplicate IDs.
You see the following fault: `ID is duplicated assigned`	This fault occurs when the same ID is defined and assigned to service profiles in two registered domains. Avoid this fault by removing duplicate IDs.
You have deleted service profiles and released the consumed IDs, but newly created service profiles are not fetching the IDs that were released.	This occurs when the interval between service profile creation and deletion is small. The ID state updates after a short period. The IDs may not be available if they have not yet updated.

CHAPTER 6

HA Issues

HA Issues with Initial Setup

The following table lists issues that you could encounter with the initial setup of HA:

Environment	Issue	Resolution
ISO installation	I/O error on shared LUN	Ignore this error. Installation proceeds as normal after clicking **Ignore**.
Validating first node	No shared storage devices detected during first node installation	Check if the RDM disk (shared disk) was added with the specified configuration.
	Failed to write on disk	• RDM may have persistent writing or LUN ownership issues. Verify if the RDM has the same specifications as mentioned in the UCSC Installation and Upgrade Guide. • Refer to “Adding a Shared Storage on VMware” and “Adding a Shared Storage on Hyper-V” in the UCSC Installation and Upgrade Guide. • Verify "Disabling SCSI Filtering" in Hyper-V and "Path Selection Policy" in VMware, according to the UCSC Installation and Upgrade Guide.

Environment	Issue	Resolution
Validating second Node	Peer node unreachable	• Verify that installation is complete on first node. • Verify network connectivity for the two nodes.
	Expected shared storage device not found	Verify that the same shared storage device is configured on both nodes (same LUN)
	Node not added to the cluster	Verify if the IP address configured on the second node matches the value of the peer node IP entered during first node setup. Verify that username and password for peer node is correct. Verify that both of the nodes contain the same version of Cisco UCS Central.

HA Issues with NFS

The following table lists issues that you could encounter with NFS:

Issue	Resolution
Using NFS shared storage for HA	• You can only mount the NFS point using IPv4 address. • During restore, you cannot configure RDM if the backup was taken on NFS HA. • You cannot switch back to RDM from NFS. • As part of tech support, the file `sharedStorage.txt` contains the result of the performance diagnostic on the NFS server that you are using as shared storage.
Boot failures	If UCS Central shuts down due to an ungraceful shutdown, or unexpected reboot, it could fail to boot due to file system errors. Contact Cisco TAC for help recovering from a file system error.

Issue	Resolution
Firewall Issues	When Cisco UCS Manager is registered with Cisco UCS Central, the NFS mount definition MO disables. When you move Cisco UCS Manager to a domain group root, or a subgroup, from an ungrouped domain, then NFS mount enables so you can mount the following partitions: • `/bootflash/images`—Used for storing the firmware images needed for copying over to Cisco UCS domains. • `/bootflash/cfg`—Used to store the Cisco UCS Manager scheduled configuration and full state backups. This mount can fail due to multiple reasons, including that the required NFS ports are not opened between Cisco UCS Manager and Cisco UCS Central. The following TCP ports must be open between Cisco UCS Central and a registered Cisco UCS domain for the firmware management and backup functionality to work correctly: • LOCKD_TCPPORT=32803 • MOUNTD_PORT=892 • RQUOTAD_PORT=875 • STATD_PORT=32805 • NFS_PORT="nfs"(2049) • RPC_PORT="sunrpc"(111)
Cisco UCS Manager in lost visibility state	Sometimes Cisco UCS Manager loses visibility with Cisco UCS Central due to various communication failures or network failures. Check the FSM status under the control-ep policy and fix the problem. The NFS mounts recover automatically.

Internal NFS server issues	Sometimes, all of the communication channels look fine, but you observe NFS mount failures on Cisco UCS Manager.
	The dcos AG logs would look similar to the following:
	`mount: 10.193.190.211:/bootflash/cfg/10.193.23.70 failed, reason given by server: Permission denied`
	`+ '[' 32 -ne 0 ']’`
	Contact Cisco TAC for help.