cisco.



Cisco Integrated System for Microsoft Azure Stack Hub Operations Guide

First Published: 2018-09-17 Last Modified: 2021-05-13

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018-2021 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	Overview 1	
	Overview of the Guide 1	
CHAPTER 2	Support Guidance 3	
	Support Case Creation 3	
	Support Case Manager 3	
	Logging in to Support Case Manager 4	
	Opening a Case through Support Case Manager 4	
	Related Cisco Integrated System for Microsoft Azure Stack Hub Documentation	5
CHAPTER 3	Start and Stop Azure Stack Hub 7	
	Start and Stop Azure Stack Hub 7	
	Stop Azure Stack Hub 7	
	Start Azure Stack Hub 8	
	Get the Startup Status for Azure Stack Hub 10	
	Troubleshoot Startup and Shutdown of Azure Stack Hub 10	
CHAPTER 4	Secret Rotation 11	
	Secret Rotation 11	
	Rotating Secrets of Cisco Nexus Top of Rack Switch 12	
	Rotating Secrets of Cisco UCS manager 12	
CHAPTER 5	Upgrade Firmware 17	
	Firmware Upgrade Overview 17	
	Identifying Installed Firmware 18	
	UCS Infrastructure and Server Firmware 18	

	Top-of-Rack Nexus Switch Firmware 19
	Known Behavior During Firmware Upgrade 19
	Cisco Azure Stack Hub Platform Upgrade Automation 20
	Configuring Cisco Azure Stack Hub Platform Upgrade Automation 22
CHAPTER 6	
0	Physical Memory Canacity Management 27
	Add Scale Unit Nodes 27
	Extending Management IP Pools 29
	Adding a Scale Unit Node 30
CHAPTER 7	Configuring Cisco Intersight Monitoring 35
	Cisco Intersight Overview 35
	Network Requirements for using Cisco Intersight 36
	Creating an Intersight Account 36
	Obtaining Device ID and Claim Code 36
	Claiming a UCSM Managed Domain 37
	Creating and Associating an Organization with Cisco UCS Manager Instance 37
	Customize Dashboard Widgets 38
CHAPTER 8	Replace Hardware 39
	Replace Hardware 39
	Replace Disk 39
CHAPTER 9	Manage System 41
	Call Home in UCS Overview 41
	Call Home Considerations and Guidelines 42
	Cisco UCS Faults and Call Home Severity Levels 43
	Configuring Call Home 44
	Enabling Call Home 47

I



Overview

• Overview of the Guide, on page 1

Overview of the Guide

This guide is intended for Azure Stack Hub operators who own and maintain the life cycle of Azure Stack Hub hardware. This guide is supplemental to the **How-to guides** > **Manage Azure Stack Hub** section of the Azure Stack Hub operator documentation at https://docs.microsoft.com/en-us/azure-stack/operator/.

I



Support Guidance

- Support Case Creation, on page 3
- Support Case Manager, on page 3
- Related Cisco Integrated System for Microsoft Azure Stack Hub Documentation, on page 5

Support Case Creation

After the installation is completed, you must go through the digital onboarding process with the professional services engineer as part of the handover process. This will ensure that your system is covered under a Cisco Service Contract, and that your contract number and contact information are updated in the Cisco Service Contract System (CSCC).

There are three ways to open a Cisco support case:

- Contact TAC by Phone: Cisco Worldwide Contacts
- Contact TAC by Email: tac@cisco.com (additional language support in Worldwide contact link)
- Open Case through Support Case Manager

Support Case Manager

Support Case Manager (SCM) provides end-to-end case management functionality. To use SCM, you need the user ID and password of your Cisco profile, a valid service contract number, the serial number or virtual license number of the product that requires support, and a supported Internet browser. Supported browsers include Mozilla Firefox Versions 10 and later, Google Chrome Versions 20 and later, Safari Versions 5 and later, and the latest version of Microsoft Internet Explorer.

- To register for a Cisco user ID for SCM, open this url in your browser: https://idreg.cloudapps.cisco.com/ idreg/register.do
- To request access to SCM, provide your Cisco user ID and contract number to web-help-sr@cisco.com

See SCM At-A-Glance for screenshots of this process.

Logging in to Support Case Manager

Procedure

Step 1	Open this URL in your browser: https://mycase.cloudapps.cisco.com.
Step 2	Enter the user ID and password of your Cisco profile, and click Log In.

Opening a Case through Support Case Manager

Before you begin

Log in to Support Case Manager.

Procedure

Step 1	On the home page, click Open New Case to advance to the Entitlement page.			
Step 2	In the Find Product by Serial Number field, enter the server or switch serial number.			
	This information is provided on the service contract.			
Step 3	Click Search.			
Step 4	In the list of search results, click the desired product for this case.			
Step 5	Click Next.			
	This brings you to the Describe Problem page. A severity is assigned based on the product type, contract and user permissions.			
Step 6	Enter the required case details such as Title and Description that summarizes the request. The Title accepts a maximum of 80 characters and Description accepts a maximum of 32,000 characters.			
Step 7	In the Technology field, click Browse to open the Select Technology window and search for Azure Stack.			
Step 8	Select Azure Stack - (Solution Support Contract Required) and click Select.			
Step 9	From the Problem Area drop-down list, select the appropriate failure.			
Step 10	Review the Contact Preference area. Contact information that you enter here overrides the default information and applies only to this case.			
Step 11	Click Submit.			

Based on your entitlement level a Cisco Solution Support engineer will contact you. Cisco Solution Support is the single point of contact for managing Cisco product issues and coordinating with the Microsoft Azure Stack support team.

Related Cisco Integrated System for Microsoft Azure Stack Hub Documentation

The complete list of all Cisco Integrated System for Microsoft Azure Stack Hub documentation is available at the following URL:

Cisco Integrated System for Microsoft Azure Stack Hub



Start and Stop Azure Stack Hub

- Start and Stop Azure Stack Hub, on page 7
- Stop Azure Stack Hub, on page 7
- Start Azure Stack Hub, on page 8
- Get the Startup Status for Azure Stack Hub, on page 10
- Troubleshoot Startup and Shutdown of Azure Stack Hub, on page 10

Start and Stop Azure Stack Hub

You can shut down and restart Azure Stack Hub services in the Cisco Integrated System for Microsoft Azure Stack Hub. Shutting down physically powers off the entire Azure Stack Hub environment. Starting up powers on all the infrastructure and returns tenant resources to the power state that they were in before shutdown. The following procedures illustrate how you can properly shut down and restart Azure Stack Hub services.

For the latest version of the Microsoft specific steps, refer to the Microsoft documentation.

Stop Azure Stack Hub

To shut down Azure Stack Hub, do the following:

Procedure

Step 1	Prepare all workloads running on your Azure Stack Hub environment's tenant resources for the upcoming shutdown.					
Step 2	Open a VMs.	Open a Privileged Endpoint (PEP) session from a machine with network access to the Azure Stack Hub ERCS VMs.				
	For det	For detailed information, see Using the privileged endpoint in Azure Stack Hub.				
Step 3	From the PEP, run Stop-AzureStack .					
Step 4	Wait for all physical Azure Stack Hub nodes to power down.					
Step 5	Log into Cisco UCS Manager (https:// <ucs_manager_ip>) by using the admin credentials.</ucs_manager_ip>					
	Note	The Cisco UCS Manager IP Address is available in the Cisco deployment worksheet addendum document provided during the deployment.				

- **Step 6** From the Cisco UCS Manager GUI, in the **Navigation** pane, click **Equipment**.
- **Step 7** Expand **Equipment** > **Rack Mounts** > **Servers**, and ensure that all the servers are in the **Power Off** state.
- **Step 8** After all the physical servers are in the **Power Off** state, you can remove power from the Azure Stack Hub



Start Azure Stack Hub

To start Azure Stack Hub, do the following regardless of how Azure Stack Hub stopped:

Procedure

Log into Cisco UCS Manager (https:// <ucs_manager_ip>) by using the admin credentials.</ucs_manager_ip>			
Note	The Cisco UCS Manager IP Address is available in the Cisco deployment worksheet addendum document provided during the deployment.		
In the	Navigation pane, click Equipment.		
Expand Equipment > Rack Mounts > Servers.			
Choose the server that you want to boot.			
In the	In the Work pane, click the General tab.		
In the Actions area, click Boot Server.			

Equipment / Rack-Mounts / Servers	/ Server 1			
General Inventory Virtual	Machines	Hybrid Display	Installed Firmware	SEL Logs
Fault Summary		Physical Disp	play	
	0			
Status		-shade		
Status Details		<		
Actions		Properties	: 1	
Create Service Profile		Product Nam	ne : Cisco l	JCS C240 M5L
Associate Service Profile		Vendor	: Cisco S	Systems Inc
Set Desired Power State		Revision	: 0	
Boot Server		Asset Tag	:	

After the server has booted, the **Overall Status** field on the **General** tab displays an **OK** status in a few minutes.



Step 7 Wait until the Azure Stack Hub infrastructure services starts.

Azure Stack Hub infrastructure services can require two hours to finish the start process. You can verify the start status of Azure Stack Hub with the Get-ActionStatus cmdlet.

9

Step 8 Ensure that all your tenant resources have returned to the state that they were in before shutdown. Workloads running on tenant resources may need to be reconfigured after startup by the workload manager.

Get the Startup Status for Azure Stack Hub

Get the status for the Azure Stack Hub startup routine with the following steps:

	Procedure
Step 1	Open a Privileged Endpoint (PEP) session from a machine with network access to the Azure Stack Hub ERCS VMs.
	For detailed information, see Using the privileged endpoint in Azure Stack Hub.
Step 2	From the PEP, run Get-ActionStatus Start-AzureStack.

Troubleshoot Startup and Shutdown of Azure Stack Hub

Perform these steps if the infrastructure and tenant services do not successfully start 2 hours after you power on your Azure Stack Hub environment.

Procedure

Step 1	Open a Privileged Endpoint (PEP) session from a machine with network access to the Azure Stack Hub ERCS VMs.
	For detailed information, see Using the privileged endpoint in Azure Stack Hub.
Step 2	From the PEP, run Test-AzureStack.
Step 3	Review the output, and resolve any health errors.
	For more information, see Run a validation test of Azure Stack Hub.
Step 4	From the PEP, run Start-AzureStack .
Step 5	If running Start-AzureStack results in a failure, contact Microsoft Customer Services Support.



Secret Rotation

- Secret Rotation, on page 11
- Rotating Secrets of Cisco Nexus Top of Rack Switch, on page 12
- Rotating Secrets of Cisco UCS manager, on page 12

Secret Rotation

Azure Stack Hub uses internal and external secrets to maintain secure communication between the Azure Stack Hub infrastructure resources and services. For more information on Azure Stack Hub specific secret rotation, see https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-rotate-secrets?view=azs-2002.

Cisco recommends using strong passwords for all the user accounts. This chapter covers the instructions to rotate the secrets of hardware management user accounts.

Cisco Azure Stack Hub has the following default user accounts created during the installation. The user accounts are configured with the customer provided password during the installation.

Device	Account	Purpose	
Cisco UCS	admin	Default administrator account with the administrator role on Cisco UCS manager	
	UCSAzSAdmin	Additional administrator account with the administrator role on UCS manager	
	IpmiUser	Baseboard management controller (BMC) user account.	
Nexus	admin Default administrator acco the network-administrator		
	azsadmin-<5 character random string>	Additional administrator account with the network-administrator role	

Rotating Secrets of Cisco Nexus Top of Rack Switch

To rotate passwords for each user account in Cisco Nexus Top of Rack switch, run the following command:

n9k-1# conf t n9k-1(config)# username <username> password <new password>

Note

Cisco Nexus Top of Rack switches are setup to allow only strong passwords. Ensure that you replace an existing password with a strong password which meets the requirements documented at the Enabling Password-Strength Checking section in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

Rotating Secrets of Cisco UCS manager

Cisco UCS Manager is the control center for the UCS server infrastructure. Cisco UCS manager can be accessed using supported browser on any computer which has access to the out-of-band management network of Azure Stack Hub.

Note

Never reboot any servers or other components using Cisco UCS manager, unless requested by Cisco support technician. Any reboot operation from Cisco UCS manager can result in the temporary or permanent data loss.

As described in the Table, Cisco UCS manager has three user accounts. To change the passwords on the user accounts, perform the following tasks:

Procedure

- Step 1 In any supported browser, enter https://<UCS Manager IP> and log into Cisco UCS manager using admin credentials.
- Step 2
 In the Navigation pane, click Admin. Expand All > User Management > User Services > Locally

 Authenticated Users and then select admin user. In the Properties area on the right, enter the new password in the Password and Confirm Password fields. Click Save Changes to complete the password change.



Step 3Under All > User Management > User Services > Locally Authenticated Users , select UCSAzSadmin
user. In the Properties area on the right, enter the new password in the Password and Confirm Password
fields. Click Save Changes to complete the password change.

cisco	UCS Manager		🛞 🔽 🙆 🔇 1 41 8 8	• = Q Q
æ	All	All / User Management / User Services /	Locally Authenticated Users / UCSAzSAdmin	
Ē	 ▼ All ▶ Faults, Events and Audit Log 	General Events		
모		Actions	Properties	
	 Authentication 	Clear Password History	Login ID : UCSAzSAdmin	
	▶ LDAP	Delete	First Name : Azure Stack	
	▶ RADIUS		Last Name : Administrator	
	▶ TACACS+		Email : azurestackadmin@azurestack.local	
_	▼ User Services		Phone :	
=	 Locales 		Password :	Set Yes
	 Locally Authenticated Users 		Confirm Decouverd :	
_	admin			
20	UCSAzSAdmin			
	Login Profile		Account Expires .	
	 Remotely Authenticated Users 		Roles Locales	
	 Roles 		aaa	
	✓ Key Management		 ✓ admin facilitv-manager 	
	KeyRing AzureStack		network	
	KeyRing default		operations	
	TP AzureStack		server-compute	
	 Communication Management 		server-equipment	
	 Stats Management 		server-prome server-security	
	 Collection Policies 		storage	
	Collection Policy Chassis			
	Collection Policy Fex			
	Collection Policy Host		SSH	
	Collection Policy Port			
	Collection Policy Server			

Step 4In the Navigation pane, click Servers. Expand Servers > Policies > root > Sub-Organizations >
[Organization name provided during the deployment] > IPMI/Redfish Access Profiles and then select
IPMI/Redfish profile IpmiId. In the Properties area on the right, under the IPMI/Redfish Users sub-area,
select IpmiUser and click info.

cisco.	UCS Manager		😢 👽 🙆 📀 1 41 8 8	• •
Æ	All	Servers / Policies / root / Sub-Orga	anizations / RTAZS2 / IPMI/Redfish Acce / IPMI/Redfish Profi	
-	 Power Control Policies Power Sync Policies 	General Events		
윪	 Scrub Policies Serial over LAN Policies 	Actions Create User	Name : Ipmild	
₽	 Server Pool Policies Server Pool Policy Qualifications 	Delete Show Policy Usage	Description : Owner : Local	
	Threshold Policies ISCSI Authentication Profiles		IPMI/Redfish Over LAN : O Disable O Enable IPMI/Redfish Users	
=	 vMedia Policies 		+ - Ty Advanced Filter 🔶 Export 🚔 Print	
	 vNIC/vHBA Placement Policies 		Name	Role
	 Sub-Organizations 		IpmiUser	Admin
20	▼ RTAZS2			
	 Adapter Policies 			
	 BIOS Policies 			
	 Boot Policies 			
	 Diagnostics Policies 			
	 Graphics Card Policies 			+ Add i Delete 🗊 Info
	Host Firmware Packages			
	 IPMI/Redfish Access Profiles 			
	IPMI/Redfish Profile Ipmild			
	 KVM Management Policies 			
	 Local Disk Config Policies 			

Step 5 Enter the new password in the **Password** and **Confirm Password** fields. Click **Save Changes** to complete the password change.

General Events			
Actions	Properties		
Delete	Name	: IpmiUser	
	Passwor	Set : Yes	
	Confirm Passwor	:	
	Role	: CRead Only Admin	
	Description	:	

Step 6 Open an Elevated PowerShell window and connect to the Azure Stack Hub Emergency Recovery console using a "Cloudadmin" account. Update the baseboard management controller (BMC) credential by running the set-bmccredential command with the -BypassBMCUpdate flag.

Note The order should be first update BMC credentials on each server from Cisco UCS Manager (Step 4 and 5) and then run the set-bmccredential command (Step 6). For more information, refer to Microsoft documentation.

In the generic Azure Stack Hub, the set-bmccredential command is capable of updating BMC credentials on the BMC controller of each server along with the update to its internal credential store. But, in Cisco Azure Stack Hub, the credentials update on each server is not possible as the server BMC controllers are controlled using Cisco UCS Manager. Hence, set the new credentials on the BMC controller using Cisco UCS manager and then use the set-bmccredential command to update the internal credential store on Azure Stack Hub.



Upgrade Firmware

- Firmware Upgrade Overview, on page 17
- Identifying Installed Firmware, on page 18
- Known Behavior During Firmware Upgrade, on page 19
- Cisco Azure Stack Hub Platform Upgrade Automation, on page 20
- Configuring Cisco Azure Stack Hub Platform Upgrade Automation, on page 22

Firmware Upgrade Overview

This section includes the firmware and driver update procedure for Cisco Integrated System for Microsoft Azure Stack Hub. Cisco periodically releases system update for the Azure Stack Hub platform. These system updates include updated firmware and drivers that improve the platform lifecycle and resolve known defects. Customers are required to update their systems to the latest system update within 60 days of the system update release date.

The following components of the Cisco appliance require periodic firmware updates to resolve known functional and security issues:

- Top-of-Rack Switches
- Cisco UCS
 - Cisco UCS Manager
 - UCS Fabric Interconnects
 - UCS Fabric Extenders
 - UCS C-Series rack server components, including BIOS, SAS HBA, NIC, HDD, and SSD
 - Server device drivers

For assistance with firmware upgrade issues or errors, refer the Support Guidance chapter to open a Cisco TAC case for Azure Stack Hub support.



Note

Cisco recommends performing firmware upgrade during the scheduled maintenance window.

Cisco Integrated System for Microsoft Azure Stack Hub firmware download portal can be accessed by selecting Integrated System Azure Stack - System Updates on UCS C-Series Rack-Mount UCS-Managed Server Software Download page. Also, it can be set up to notify you about the availability of the new firmware. Cisco highly recommends that you sign up for these notifications.

The following software components hosted on Microsoft Azure Stack Hub firmware download portal are required for the firmware upgrade procedure:

Component	Description
ucs-6300-k9-bundle-infra. <version number="">.A.bin</version>	UCS Infrastructure Firmware
ucs-k9-bundle-c-series. <version number="">.C.bin</version>	UCS Server Firmware
nxos. <version number="">.bin</version>	ToR Switch Firmware
<i><oem extension="" number="" version=""></oem></i> .zip	Zip file containing the OEM Extensions Package. The OEM Extensions Package is made of two files. One zip file and one xml file.
Cisco_UCS_AzureStack_FwUpdate_ <version number>.zip</version 	Firmware and Driver Update Automation (CASPU)

Identifying Installed Firmware

Based on when the system is installed and updated, some of the components or all the components of Micorsoft Azure Stack Hub hardware requires firmware upgrade. This section provides the procedure to identify installed firmware.

UCS Infrastructure and Server Firmware

Procedure

 Step 1
 Log into Cisco UCS Manager (https://<UCS_Manager_IP>) by using the admin credentials, through a SSH client, such as Putty.

Step 2 Check the version using the show version command.

UCS-B# show version System version: 4.0(4b)

Step 3 On the Microsoft Azure Stack Hub firmware download portal, check for the latest firmware version from the posted Cisco UCS firmware files (ucs-6300-k9-bundle-infra.4.0.4g.A.bin or ucs-k9-bundle-c-series.4.0.4g.C.bin).

The firmware version of bundle image files are same. If the posted firmware version is greater than the installed firmware version, the system requires UCS firmware upgrade. For example, if the installed UCS firmware version is 4.0(4b) and the posted firmware version is 4.0(4g), the system requires UCS firmware upgrade from 4.0(4b) to 4.0(4g).

Note The OEM extension package installation is required to complete UCS firmware upgrade.

Top-of-Rack Nexus Switch Firmware

Procedure

Step 1 Log into Top-of-Rack Nexus switch A by using the admin credentials, through a SSH client, such as Putty.

```
Step 2 Check the version using the show version | inc NXOS command.
```

```
ToR-1# show version | inc NXOS
NXOS: version 7.0(3)I7(4)
NXOS image file is: bootflash:///nxos.7.0.3.I7.4.bin
NXOS compile time: 6/14/2018 2:00:00 [06/14/2018 10:49:04]
```

Step 3 On the Microsoft Azure Stack Hub firmware download portal, check for the latest Nexus switch firmware version from the Nexus switch firmware file (nxos.7.0.3.17.8.bin). If the posted firmware version is greater than the installed firmware version, the system requires Nexus switch firmware upgrade.

Known Behavior During Firmware Upgrade

- During ToR switch upgrade, the admin portal may show a route publication failure alert. This behavior is expected and can be safely ignored. This alert will clear automatically after firmware upgrade.
- During UCS infrastructure firmware upgrade, Cisco UCS Manager shows an alert message to acknowledge server reboot. This alert message must be ignored, as rebooting servers from Cisco UCS manger may result in a down time for Azure Stack Hub and possible data loss. The safe reboot of servers is triggered automatically during OEM extension package installation.
- During UCS infrastructure firmware upgrade, the Azure Stack Hub admin portal may generate the alert shown in the following figure. This behavior is expected and can be safely ignored. This alert will clear automatically after firmware upgrade.

Network interface	disconnected \Box ×
🗙 Close alert	
NAME	Network interface disconnected
SEVERITY	Critical
STATE	Active
CREATED TIME	7/12/2019 11:06:04 PM
UPDATED TIME	7/12/2019 11:06:04 PM
COMPONENT	s-cluster
DESCRIPTION	The network interface Manufacturer 'QLogic Corporation', Product Name Cisco FastLinQ QL45412H 40GbE Adapter (NDIS) is disconnected. The node is unavailable and there is less capacity available for tenant workloads. A process has been started to move tenant workloads from this node to other nodes. If there is no available capacity, some workloads may not restart.
REMEDIATION	Reconnect the network cable.

Cisco Azure Stack Hub Platform Upgrade Automation

Firmware upgrade for Cisco Integrated System for Microsoft Azure Stack Hub is a non-disruptive operation, which is fully automated using Cisco Azure Stack Hub Platform Upgrade (CASPU) automation software. With CASPU Cisco customers can upgrade all the components of Azure Stack Hub all at once or in three parts:

- Top-of-Rack Nexus switch upgrade (flag: UpdateNexus)
- UCS infrastructure upgrade (flag: UpdateUCSManager)
- Server firmware upgrade and driver installation (flag: UpdateOEMExtension)

Running CASPU in parts is particularly useful when the host running CASPU cannot access the admin portal and the management IPs of UCS and ToR switches all at the same time. The CASPU configuration file FirmwareUpdateInputs.xml consists of flags **UpdateNexus**, **UpdateUCSManager**, and **UpdateOEMExtension** to configure the three-part execution of CASPU. By default, all the flags are marked true, and CASPU tries to upgrade all the components at the same time.



Important

Execution order is important for the Azure Stack Hub firmware upgrade. If all the flags are marked true, CASPU automatically selects the correct order. While running CASPU in parts, ensure that you run UCS infrastructure upgrade and server firmware upgrade staging before Server firmware upgrade and driver installation using OEM extension package.

When CASPU is executed in parts, manually invoke the Azure Stack Hub validation tool (Test-AzureStack) (https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-diagnostic-test?view=azs-2005) before and after every step to ensure that the Azure Stack Hub is healthy after each operation. When CASPU is executed in default mode (all flags true), CASPU ensures that Azure Stack Hub is healthy before and after each operation.

Azure Stack Hub systems must be running Azure Stack Hub version 1.1907.17.54 or higher before CASPU utilities can be used to update the firmware and OEM Extensions package.

CASPU is written in PowerShell and can be executed from any Microsoft Windows environment that meets the following requirements:

MS Windows 10, 2016 or 2019 Operating System



Note Ensure that the Operating System has all the latest patches.

- · Network connectivity to Management IPs of Nexus ToR switches and UCS
- · Network connectivity to the Azure Stack Hub admin portal and privileged endpoints
- All Azure Stack Hub PKI certificates installed
- PowerShell version 5.1 or later installed
- The latest version of PowerShell for Azure Stack Hub installed (https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-powershell-install)



Note The host running CASPU adds customer provided privileged endpoint VM IP address to the trusted host.

Ensure that the host running CASPU has a reliable wired network connection to Azure Stack Hub. Running CASPU from a computer that connects to Azure Stack Hub over a VPN or an unreliable network is not supported.

In addition to firmware upgrade, CASPU makes the following configuration changes to Azure Stack Hub:

- Sets 9216 MTU for all SVIs and peer link port channel (po10) on both ToR switches. This update addresses the new requirements for ToR switch configuration.
- Makes ACL changes to implement the latest ToR switch security settings required by Microsoft.
- Configures QoS class for the cluster communication traffic on ToR switches and Fabric Interconnects.
- · Changes UCS server boot policy settings from Local Disk to Embedded LUN

Configuring Cisco Azure Stack Hub Platform Upgrade Automation

Procedure

- **Step 1** In the Microsoft Windows environment that meets the earlier mentioned requirements, download the following firmware upgrade components into a folder (for example, c:\azsfirmwareupgrade):
 - ucs-6300-k9-bundle-infra.<version number>.A.bin
 - ucs-k9-bundle-c-series.<version number>.C.bin
 - nxos.<version number>.bin
 - < OEM extension version number>.zip
 - Cisco_UCS_AzureStack_FwUpdate_<version number>.zip
- Step 2 Run gci -path c:\azsfirmwareupgrade -recurse | unblock-file and unblock all the components.
- Step 3 Extract the Cisco_UCS_AzureStack_FwUpdate_<version>.zip package.
- **Step 4** Extract the OEM extension package to the C:\ azsfirmwareupgrade\OEM folder from the <OEM extension version number>.zip file.
- Step 5 Update the FirmwareUpdateInputs.xml file located inside the C:\ azsfirmwareupgrade
 \Cisco UCS AzureStack FwUpdate <version>\FirmwareUpdate folder.

Field Name	Description
UpdateNexus (True/False)	Flag to perform Nexus firmware upgrade
UpdateUCSManager (True/False)	Flag to perform UCS infrastructure firmware upgrade and server firmware upgrade staging
UpdateOEM (True/False)	Flag to perform rolling server firmware and driver update
RunAzureStackHubHealthCheck (True/False)	Flag to run Test-AzureStack before Nexus and UCS infrastructure firmware upgrade If the host running CASPU does not have access to the ERCS VM, set this flag to False
ToRSwitch1IP	IP address for the Nexus Top-of-Rack switch 1
ToRSwitch1UserName	Nexus switch 1 admin username
ToRSwitch2IP	IP address for the Nexus Top-of-Rack switch 2
ToRSwitch2UserName	Nexus switch 2 admin username
ToRImageFilePath	File path for the Top-of-Rack switch firmware image

Field Name	Description
UCSMIP	IP address of Cisco UCS Manager
UCSMUserName	Cisco UCS Manager admin username
ImagePathInfraBundle	File path for the UCS infrastructure firmware bundle
ImagePathHostBundle	File path for the UCS server firmware bundle
AdminResourceManagerURI	URI for the Azure Stack Hub admin resource manager. Normally located in the AzureStackStampInformation.json provided to you after deployment. For example, https://adminmanagement.usw.m4l.rtazslab.net/
OEMExtensionFolderPath	Folder path for the OEM Extension package C:\ azsfirmwareupgrade\OEM
AzureRMUserName	Azure Stack Hub global administrator username
ERCSIPAddress	IP address of ERCS VM
ERCSUserName	ERCS cloud admin username. For example, <local domain="">\cloudadmin</local>
TenantId	(Optional). This option is intended for use in a Cloud Solution Provider (CSP) scenario where the operator does not own the tenant domain. In this case, this option allows the tenant ID to be specified for the login. When not specified, the Tenant ID associated with
Subscription	(Optional). The optional Subscription field allows a specific subscription GUID to be specified when a none-default subscription needs to be used. The default value is Default Provider Subscription .

Step 6 (Optional) If configured for the duration of the firmware upgrade, disable UCS Call Home to avoid unnecessary alerts.

-1 1-1 1- CISCO.	UCS Manager							
ж	Al 🗸	All / Comm	unication Ma	nagement / Call Home				
•	All Faults, Events and Audit Log Exuits	General Admin	Profiles	Call Home Policies	System Inventory	Anonymous Reporting	Events	FSM
55 =	Events	States	: • •	l 🔿 On				
	Syslog Core Files TechSupport Files	ciares -						
	Settings • User Management • Authentication							
J 0	 LDAP RADIUS TACACS+ 							
	User Services Locales Locally Authenticated Users Locally Authenticated Users							
	Remotely Authenticated Users Roles Key Macagement							
	KeyRing AzureStack KeyRing default							
	TP AzureStack Communication Management Call Home							
	Communication Services DNS Management Management Interfaces							

Step 7 Run C:\ azsfirmwareupgrade

\Cisco_UCS_AzureStack_FwUpdate_<version>\FirmwareUpdate
\RunFirmwareUpdate.ps1 from an elevated PowerShell window. Provide the required credentials:

Module	Credential Details
UpdateUCSManager	Admin credentials for Cisco UCS Manager
UpdateNexus	Admin credentials for each Nexus ToR switch
UpdateOEMExtension	Azure Stack Hub Global administrator
	Cloudadmin account credentials for Privileged Endpoint access

Note RunFirmwareUpdate.ps1 can auto install the required PowerShell modules. By default, the script waits for user acknowledgement before installation. If you want the script to install all the required modules without user acknowledgement, you can use the "force" parameter while running the script. For example, **RunFirmwareUpdate.ps1 -force**.

The **UpdateOEMExtension** module only starts the installation on the OEM Extension on Azure Stack Hub. It does not wait for the OEM Extension update to complete. You must monitor the status of the OEM Extension update from the admin portal.

Server firmware upgrade is not complete until the OEM Extension is successfully updated.

Configuring Cisco Azure Stack Hub Platform Upgrade Automation



Manage Capacity

- Physical Memory Capacity Management, on page 27
- Add Scale Unit Nodes, on page 27
- Extending Management IP Pools, on page 28
- Adding a Scale Unit Node, on page 30

Physical Memory Capacity Management

Cisco supports memory expansion on Azure Stack Hub servers. Memory expansion is a disruptive operation, and involves shutdown of the Azure Stack Hub system. Following are the guidelines for memory expansion or upgrade:

- All the servers in the Azure Stack Hub have homogeneous hardware configuration. For this reason, you cannot perform memory upgrade only on a single server. You must upgrade the memory on all the servers at the same time.
- Upgrade only to increments supported for M5 384 GB, 512 GB and 768 GB using 32 GB DIMMS, 1024 GB or 1536 GB using 64 GB DiMMS.
- You cannot mix and match 32 GB and 64 GB DIMMS

Review the Cisco memory expansion best practices from following links:

https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/ memory-guide-c220-c240-b200-m5.pdf

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C240M4/install/C240M4/replace.html

After supported memory is procured, follow the instructions from the following Microsoft guide to perform the memory expansion:

https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-manage-storage-physical-memory-capacity

Add Scale Unit Nodes

With Azure Stack Hub update 1807 Microsoft supports addition of physical servers to an existing Azure Stack Hub. Cisco customers running Azure Stack Hub version 1807 and above can now order and add nodes to their existing Azure Stack Hub. In the current version of the Add Node capability, Microsoft allows the existing

cluster to be expanded up to a maximum of 16 servers per scale unit. This section covers detailed instructions for the addition of new nodes to an existing Azure Stack Hub system.

Prerequisites for Adding a Node

The following prerequisites must be complete before adding a node:

- Verify that Azure Stack Hub is running update 1807 or above with no errors or warnings on the Azure Stack Hub admin portal.
- Verify that the following components are received as a part of the add node package:
 - · Server with the exact same components as other servers in the existing Azure Stack Hub
 - Two QSFP-H40G-CU3M cables
 - UCS port license for 2 ports
- Obtain two CAT 6 cables.
- Ensure that there are no errors or warnings displayed on Cisco UCS Manager. Cisco UCS Manager can be accessed using any computer that has access to the Azure Stack Hub Out-of-Band-Management network. To access Cisco UCS Manager using a Web browser, open https://<Cisco_UCS_Manager_IP>.
 You can find the Cisco UCS Manager IP and admin login credentials in the customer handover information.
- Verify that the UCS service profile template has enough Cisco IMC (Integrated Management Controller)/BMC IPs for newly added nodes. Most of the new deployments after September 2018 will have Cisco IMC IP pools large enough to support 16 servers. However, for older deployments, Cisco IMC IP pools require manual expansion. Each Cisco Azure Stack Hub server requires two Cisco IMC IPs:
 - Out-of-Band Management IP
 - Inband Management IP

Extending Management IP Pools

You can have one IP pool for each type of Cisco IMC IP. Cisco IMC IP pools should already exist on all Cisco Azure Stack Hub appliances.

To extend the Out-of-Band management IP pool, review the Out-of-Band management IP subnet provided on the Cisco deployment worksheet addendum and find unused IP blocks in that subnet. It is recommended to make the total pool size 16 IPs.

From Cisco UCS Manager, navigate to LAN > Pools > Sub-Organizations > AzureStack Org > IP Pools.Locate the Out-of-Band management IP pool and ensure that the pool size is 16.

Procedure

Step 1 From Cisco UCS Manager, navigate to LAN > Pools > Sub-Organizations > AzureStack Org > IP Pools.
 Step 2 Locate the Out-of-Band management IP pool and ensure that the pool size is 16.

	Owned Robberry Riberts facts facts		
LAN Deuf			
Applances	Actions	Properties	
Internal LAN	Delete	Name	AS_008_MGMT
Policies	Create Block of Pul Addresses	Description	Cisco MC Out-Of Band Management Pls for manage
Posts	Create Black of Pv8 Addresses	949	
• rest 😋	Create DNS Suffix	504	· · · · · · · · · · · · · · · · · · ·
· P Pools		Asseyed Assessed Online	Contra a langesta
· P Pod ext-mant	Show Pool Usege		(Comment of the state of the s
· P Pod aca-interaction			
 MAC Room 			
 Sub-Organizations 			
 Aparelitecking 			
 # Pools 			
P Not AS, COL, MONT			
 IP Pool Assemblack. 			
 MAC Pools 			
 Sub-Organizations 			
Traffic Monitoring Sessions			
+ Patric A			
fatric 8			
Netfox Monitoring			
Rev Record Definitions			
Pos Exporters			
Pow Montana			
A Real Manager Transport			

Step 3 If the pool size is not 16, add more IP addresses using the **Create Block of IPv4 Addresses** option in the UI. Add enough IP addresses to make the pool size 16. Leave the DNS values at the default "0.0.0.0".

-	M .	LNN / Pools / root / Sub-Organizations / Association	I PPerce I PPercet COLMENT	
m	· ·			
	• LAN	General P Addresses P Books Paulos	Lasts	
	· LAN Cloud	Actions	Properties	
añs -	· Approves	Delete	Name	: AS ODE MGMT
	- Printer	Course Block of Pul Addresses	Description	Claco IAC Out-Of Band Management Pla for manage
	* Poole	Create Block of Pv6 Addresses	000	
•		Cristia DNS Suffix	Sav	
	. B facto		Asspect	
	 B Dui an more 	Show Pool Usege	Assignment Or	der: [] Delout in Sequental
	· Ritur according and			
-	- 104 from			
	Sub-Dramation			
	• Another s			
	· P-Paula			
	P Prof AS COR MONT			
	 If find do collects 			
	 MAC Broke 			
	 Sub-Organizations 			
	· Traffic Information Generate			
	+ fature A			
	+ false #			
	Netfau Maniation			
	Fine Record Definitions			
	 For Econtral 			
	Row Montees			
	Pose Monter Sessions			
6	rooto Ploak	of IDv4 Addross		
	Jeale DIOCK	on IPV4 Address	65	
1	From : 0.0.0.0		Size : 1	÷
	Subnet Mask : 255.25	5.255.0	Default Gateway : 0.0.	0.0
	Primary DNS : 0.0.0.0		Secondary DNS : 0.0.	0.0
		antional		
		- optional		
				Cancel

Step 4 Repeat these steps to extend the Inband management IP pool.

To determine the Inband management IPs for the pool expansion review the deployment worksheet completed before the deployment. It includes the BMC IP addresses for each server in the IP usage section. If the IP addresses for all 16 servers are not listed on the worksheet, select the next consecutive unused IP addresses after the last used BMC IP to extend the pool. For example, if you have a 4-node system and currently you

have a fully-consumed IP pool of 4 IP addresses 192.168.26.3 - 192.168.26.6, use IP addresses 192.168.26.7 - 192.168.26.18 to expand the Inband IP pool.

LAN Could	General P Addresses P Books Parts Evens	
· Applances	Actions	Properties
 Internal LAN 	Delete	Norre : AzureStuck
· Pulcies	Create Block of IDvil Addresses	Description Cisco IAC Management IPs for management
* Pacis	Grade Book of IPv8 Addresses	00 : 0000000-0000-0000-0000-0000-00000000
- reet 🗢		Sol 96 Provide Contraction
 IP Pools 	Create PVI WIG Server	Assignment Oxfer: Default # Sequence
 IP Posted-reget 	Show Pool Usage	
 IP Paol acsi-initiatur-pool 		
 MAC Pools 		
 Sub-Organizations 		
 ApyreTeck-si 		
· P Pools		
 IP Post A5, COB, VOVT 		
P Ded Assectant		
 MAC Poots 		
 Sub-Organizations 		
 Traffic Monitoring Sessions 		
 Fabric A 		
+ Fabric B		
 Netflow Monitoring 		
 Flow Record Definitions 		
 Fox Dipoters 		
 Rew Monitors 		
 Fox Montor Sessions 		

Adding a Scale Unit Node

Before you begin

Complete the list of prerequisites listed in Add Scale Unit Nodes.

Procedure

Step 1Login to Cisco UCS Manager and navigate to Admin > License Management > Fabric Interconnect A >
General tab.



Step 2 Click Download License and install the UCS port license on Fabric Interconnect A.

Step 3 Repeat Steps 1 and 2 for Fabric Interconnect B.

After installing the license on each Fabric Interconnect, check the license status for the newly added server port by verifying the port properties.

**	UCS Manager	8 8 9 9	
	A - - Same - Own - Same - - Same - <tr< th=""><th>Recent for the former of the f</th><th></th></tr<>	Recent for the former of the f	
	+ Free Kobin + Strenec Forts + PEnec + PEne	Million Islandjulan Sector Sector Sector Millionska Alf Sector Se	

Step 4

Install the server into the existing Azure Stack Hub rack, but do not connect the power. Refer to the Cisco Azure Stack Hub cabling guide for additional information on server placement and cabling. Connect the QLogic and management ports to the Fabric Interconnect and Fabric Extender. The new server will take up the next consecutive ports on the Fabric Interconnects and Fabric Extenders. For example, if you are installing the fifth server on the 4-node Azure Stack Hub system, the cabling for the server will look like this:



Step 5 Connect the power and wait for the UCS server discovery to finish.

During the discovery phase, Cisco UCS Manager automatically performs the following actions:

- a. Inventories the server and server components
- **b.** Adds the server to the appropriate server pool
- **c.** Creates a new service profile for the server
- d. Associates the service profile to the server
- e. During service profile association, upgrades server firmware to match other servers in the stamp

Server discovery can take anywhere from 40 minutes to 2 hours, depending upon the number of server components that require firmware upgrade.

Step 6 After discovery is complete, verify the Association state under **Equipment** > **Rack-Mounts** > **Servers** > *Server <newly added server number* > > **General**

The Assoc State should be Associated.



Step 9

I

Step 7 From the **Server** tab in the navigation pane, select the service profile associated with the newly installed server and note the Inband management IP address.



Step 8 Login to the Azure Stack Hub admin portal as an Azure Stack Hub operator.

Navigate to New > Capacity > Scale Unit Node Microsoft Azure Stack - Administration New = x New + New III Dashbo Azure Marketplace Featured All resources Get started E Resource aroups Offers + Plans Virtu al machine Compute Ξ Data + Storage E Plans Networking Offers Custom Marketplace ma Security + Ide Capacity Recent More services >

Step 10 On the **Add Node** pane, select the **Region** and then select the **Scale Unit** that you want to add the node to. Also, specify the BMC IP Address (InBand management IP address noted in Step 7) for the scale unit node that you are adding.

Note You can only add one node at a time.

Microsoft Azure Stack -	Administration New > Add node
Microsoft Azure Stack -	
	Add node
+ New	
Dashboard	Adds new node(s) to a scale unit and configures the required settings. Learn more
All resources	
(Resource groups	* Region
Virtual machines	* Scale unit
i≡ Plans	×
🥏 Offers	BMC IP ADDRESS
in Marketplace management	BMC IP addresses can't be empty
Recent	····
More services >	

Step 11 You can also add a node using PowerShell. Refer to the Microsoft Add node documentation for additional details.

Note During node addition, the scale unit will show status as **Expanding**, and this scale unit expansion takes a very long time. A new node can be added to the cluster as long as the last added node shows status as **Running** and it is not required to wait for cluster expansion to finish.

Aiere	osoft Azure Stack - Adm	inistration we sale with 3 solution	P Search resources ×	Q @ O annutherrows
	s-cluster	* 0 ×	Notifical	tons
	+ Add node			Danie Incolution Completes All
	Exertisk A			constuly added node 1130 PM
	Anglin une Type Hyper converged	knaringool sons 192 194 1940 menung 1920 557 68	Land	Ay added node 192 MILIS.3
	Nodes			
	-	POWER EXAMIN		
	AG-No.4C1	l 🔒 Ranning		
	AG-NOAK2	 Burning 		
	Ad Noted	Rening		
	Ad-Nodels	 Revelag 		
	Ad-NotedS	• funning		



Configuring Cisco Intersight Monitoring

- Cisco Intersight Overview, on page 35
- Network Requirements for using Cisco Intersight, on page 36
- Creating an Intersight Account, on page 36
- Obtaining Device ID and Claim Code, on page 36
- Claiming a UCSM Managed Domain, on page 37
- Creating and Associating an Organization with Cisco UCS Manager Instance, on page 37
- Customize Dashboard Widgets, on page 38

Cisco Intersight Overview

Cisco Intersight^m is a software-as-a-service (SaaS) infrastructure lifecycle management platform that delivers simplified monitoring and support of Cisco Unified Computing System^m (Cisco UCS[®]). Cisco Intersight can be used for monitoring the UCS components that are part of the Cisco Integrated System for Azure Stack Hub.

The following features are part of Cisco Intersight Base License and can be used with Cisco UCS components:

- · Global Monitoring of Health and Basic Inventory Status
- Integration with Cisco Technical Assistance Center (TAC) and Proactive TAC Support
- Proactive Support enabled through Intersight
- User Customizable Dashboard
- Custom Metrics Widgets
- Alarms
- Search and Tagging
- Launch Virtual KVM

For more information about Cisco Intersight, see Getting Started

Network Requirements for using Cisco Intersight

All device connectors must properly resolve svc.intersight.com and allow outbound initiated HTTPS connections on port 443. To resolve svc.intersight.com, you must configure DNS on the managed targets. If a proxy is required for an HTTPS connection to svc.intersight.com, the proxy can be configured in the Device Connector user interface.

For more information, see Intersight FAQ.

Creating an Intersight Account

You must have a Cisco Intersight account to configure Intersight Monitoring for Azure Stack Hub UCS Platform.

To create a Cisco Intersight account, do the following:

Procedure

Step 1 Log in to https://intersight.com/.

You must have a valid Cisco ID to create a Cisco Intersight account. If you do not have a Cisco ID, create one here.

Step 2 Click Create an Account, accept the Cisco End User License Agreement, and enter the account name in the Account Creation dialog box.

Step 3 Click Create.

You can create multiple accounts using the same Cisco ID. Click **Create an Account** on https://intersight.com/ and follow the step 2 to create another Intersight account.

After creating an Intersight account, you can begin claiming targets to manage your endpoints.

Obtaining Device ID and Claim Code

To obtain the Domain Device ID and Claim Code, do the following:

Procedure

Step 1	Log in to Cisco UCS Manager in a web browser.	
Step 2	In the Navigation pane, click Admin.	
Step 3	Expand Communication Management category and select DNS Management.	
	Verify the DNS server entries. If there are no DNS server entries, add minimum one DNS server IP address	
Step 4	In the Navigation pane, expand All and select Device Connector .	

The **Device Connector** tab displays the device ID, claim code, connection status and the set access mode.

If the Device Connector does not show green dots to the Internet icon even with DNS entries, click **Retry Connection** to re-establish the Internet connection. Once the connection is established, the device ID and claim code will be displayed.

Claiming a UCSM Managed Domain

To initiate the Cisco UCS Domain (UCSM Managed) target claim, do the following:

Procedure

Step 1	In Cisco Intersight, navigate to ADMIN > Targets > Claim Target .			
	The Se	lect Target Type window is displayed.		
Step 2	In the filter column, select Compute / Fabric and select Cisco UCS Domain (UCSM Managed), and then click Start.			
	Note	Do not select the Cisco UCS Domain (Intersight Managed) target.		
Step 3	Enter th Device	ne Device ID and Claim Code obtained from Cisco UCS Manager. For more information, see Obtaining ID and Claim Code, on page 36.		
Step 4	Click (The Ci	Claim. sco UCS Domain (UCSM Managed) instance will be added to the Intersight Managed devices.		

Creating and Associating an Organization with Cisco UCS Manager Instance

The organization represents the Cisco UCS Manager instance to which it belongs to. When a Cisco UCS Manager instance is claimed in Cisco Intersight, you can assign the Cisco UCS Manager instance to an organization different from the default organization.

To create and associate a claimed Cisco UCS Manager instance to an organization, do the following:

Procedure

- Step 1 Log in to Cisco Intersight.
- Step 2 Click the gear icon in the upper right of the home screen and choose Settings from the drop-down list.
- Step 3 In the Account Details screen, click the Organizations in the middle pane and perform the following:
 - a) Click Create Organization.
 - b) Enter the name of the organization. For example, Azure-Stack-Hub.

- c) Enter the description of the organization.
- d) Select the claimed Cisco UCSM Managed Domain.
- e) Click **Create** to create and associate the Cisco UCSM Managed Domain with the new organization. Click Fabric Interconnects in the right pane to view the claimed Fabric Interconnects and its status.

Customize Dashboard Widgets

Cisco Intersight provides dashboard for real-time health and inventory status monitoring. You can create, customize, rename, and manage multiple dashboard views by adding, removing, or rearranging widgets. In the Widget Library, you can select the widget(s) that you want to pin to the dashboard, preview the details for a server or a cluster, search for a widget, and add a custom title to a widget. You can toggle between the detail and list view of the available widgets in the library. You can add multiple instances of a widget to monitor different targets. You can add a maximum of 30 widgets per dashboard.

- Use Add Widget button on the top right of the dashboard to add a widget.
- Hover the cursor on the widget, click **X** that appears on the top right corner of the widget to remove the widget.



Replace Hardware

- Replace Hardware, on page 39
- Replace Disk, on page 39

Replace Hardware

Use the following link and follow Microsoft instructions for replacement of faulty components:

https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-replace-component?view=azs-1908

The only customer-replaceable component of the Cisco Azure Stack Hub is the front and rear loading SAS disk drive. For all other component failures, contact Cisco Support.

Replace Disk

Disk failure alert on the Azure Stack Hub admin portal provides the server slot information and serial number of the faulty disk.

Procedure

Step 1 Step 2	Locate and remove the faulty disk from the server. Order the replacement disk using serial number of the faulty disk.	
	Use the following portal to order the replacement disk: https://mycase.cloudapps.cisco.com/case. Alternatively, you can also contact Cisco Support.	
Step 3	After the replacement disk is received, install the replacement disk in the server and follow Microsoft instructions to activate the disk.	

I



Manage System

- Call Home in UCS Overview, on page 41
- Configuring Call Home, on page 44
- Enabling Call Home, on page 47
- Disabling Call Home, on page 47

Call Home in UCS Overview

Call Home provides an email-based notification for critical system policies. A range of message formats are available for compatibility with pager services or XML-based automated parsing applications. You can use this feature to page a network support engineer, email a Network Operations Center, or use Cisco Smart Call Home services to generate a case with the Technical Assistance Center.

C C

Important Call Home does not use a secure protocol. It is disabled by default.

The Call Home feature can deliver alert messages containing information about diagnostics and environmental faults and events.

The Call Home feature can deliver alerts to multiple recipients, referred to as Call Home destination profiles. Each profile includes configurable message formats and content categories. A predefined destination profile is provided for sending alerts to the Cisco TAC, but you also can define your own destination profiles.

When you configure Call Home to send messages, Cisco UCS Manager executes the appropriate CLI **show** command and attaches the command output to the message.

Cisco UCS delivers Call Home messages in the following formats:

- Short text format which provides a one or two line description of the fault that is suitable for pagers or printed reports.
- Full text format which provides fully formatted message with detailed information that is suitable for human reading.
- XML machine-readable format that uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML Schema Definition (XSD). The AML XSD is published on the Cisco.com website. The XML format enables communication with the Cisco Systems Technical Assistance Center.

For information about the faults that can trigger Call Home email alerts, see the *Cisco UCS Faults and Error Messages Reference*.

The following figure shows the flow of events after a Cisco UCS fault is triggered in a system with Call Home configured:





C)

Important Call Home is configured as **Off** by default. It is a non-secure feature, and must be explicitly enabled.

Call Home Considerations and Guidelines

How you configure Call Home depends on how you intend to use the feature. The information you need to consider before you configure Call Home includes the following:

Destination Profile

You must configure at least one destination profile. The destination profile or profiles that you use depends upon whether the receiving entity is a pager, email, or automated service such as Cisco Smart Call Home. If the destination profile uses email message delivery, you must specify a Simple Mail Transfer Protocol (SMTP) server when you configure Call Home.

Contact Information

The contact email, phone, and street address information should be configured so that the receiver can determine the origin of messages received from the Cisco UCS domain.

Cisco Smart Call Home sends the registration email to this email address after you send a system inventory to begin the registration process.

If an email address includes special characters, such as # (hash), spaces, or & (ampersand), the email server might not be able to deliver email messages to that address. Cisco recommends that you use email addresses which comply with RFC2821 and RFC2822 and include only 7bit ASCII characters.

IP Connectivity to Email Server or HTTP Server

The fabric interconnect must have IP connectivity to an email server or the destination HTTP server. In a cluster configuration, both fabric interconnects must have IP connectivity. This connectivity ensures that the current, active fabric interconnect can send Call Home email messages. The source of these email messages is always the IP address of a fabric interconnect. The virtual IP address assigned to Cisco UCS Manager in a cluster configuration is never the source of the email.

Smart Call Home

If Cisco Smart Call Home is used, the following are required:

- An active service contract must cover the device being configured.
- The customer ID associated with the Smart Call Home configuration in Cisco UCS must be the CCO (Cisco.com) account name associated with a support contract that includes Smart Call Home.

Cisco UCS Faults and Call Home Severity Levels

Because Call Home is present across several Cisco product lines, Call Home has its own standardized severity levels. The following table describes how the underlying Cisco UCS fault levels map to the Call Home severity levels. You need to understand this mapping when you configure the Level setting for Call Home profiles.

Call Home Severity	Cisco UCS Fault	Call Home Meaning
(9) Catastrophic	N/A	Network-wide catastrophic failure.
(8) Disaster	N/A	Significant network impact.
(7) Fatal	N/A	System is unusable.
(6) Critical	Critical	Critical conditions, immediate attention needed.
(5) Major	Major	Major conditions.
(4) Minor	Minor	Minor conditions.

Table 1: Mapping of Faults and Call Home Severity Levels

Call Home Severity	Cisco UCS Fault	Call Home Meaning
(3) Warning	Warning	Warning conditions.
(2) Notification	Info	Basic notifications and informational messages. Possibly independently insignificant.
(1) Normal	Clear	Normal event, signifying a return to normal state.
(0) debug	N/A	Debugging messages.

Configuring Call Home

Procedure

Step 1	In the Navigation pane, click Admin.		
Step 2	Expand All > Communication Management > Call Home.		
Step 3	In the Work pane, click the General tab.		
Step 4	In the Admin area, complete the following fields to enable Call Home:		
	Important Call Home is configured as Off by default. It is a non-secure feature, and must be explicitly enabled		

Name	Descript	ion
State field	This can be one of the following:	
	• Off—Call Home is not used for this Cisco UCS domain.	
	• On —Cisco UCS generates Call Home alerts based on the Call Home policies and profiles defined in the system.	
	Note If this field is set to On , Cisco UCS Manager GUI displays the rest of the fields on this tab.	

Name	Description
Switch Priority drop-down list	This can be one of the following:
	• Alerts
	• Critical
	• Debugging
	• Emergencies
	• Errors
	• Information
	Notifications
	• Warnings
Throttling field	Indicates whether the system limits the number of duplicate messages received for the same event. This can be one of the following:
	• On —If the number of duplicate messages sent exceeds 30 messages within a 2-hour timeframe, then the system discards further messages for that alert type.
	• Off—The system sends all duplicate messages, regardless of how many are encountered.

a) In the **State** field, click **On**.

Note If this field is set to **On**, Cisco UCS Manager GUI displays the rest of the fields on this tab.

- b) From the Switch Priority drop-down list, select one of the following levels:
 - Alerts
 - Critical
 - Debugging
 - Emergencies
 - Errors
 - Information
 - Notifications
 - Warnings

For a large Cisco UCS deployment with several pairs of fabric interconnects, this field enables you to attach significance to messages from one particular Cisco UCS domain, so that message recipients can gauge the priority of the message. This field may not be as useful for a small Cisco UCS deployment, such as a single Cisco UCS domain.

Step 5 In the **Contact Information** area, complete the following fields with the required contact information:

I

Name	Description	
Contact field	The main Call Home contact person.	
	Enter up to 255 ASCII characters.	
Phone field	The telephone number for the main contact.	
	Enter the number in international format, starting with a + (plus sign) and a country code. You can use hyphens but not parentheses.	
Email field	The email address for the main contact.	
	Cisco Smart Call Home sends the registration email to this email address.	
	Note If an email address includes special characters, such as # (hash), spaces, or & (ampersand), the email server might not be able to deliver email messages to that address. Cisco recommends that you use email addresses which comply with RFC2821 and RFC2822 and include only 7bit ASCII characters.	
Address field	The mailing address for the main contact.	
	Enter up to 255 ASCII characters.	

Step 6 In the **Ids** area, complete the following fields with the identification information that Call Home should use:

Tip If you are not configuring Smart Call Home, this step is optional.

Name	Description
Customer Id field	The Cisco.com ID that includes the contract numbers for the support contract in its entitlements.
	Enter up to 510 ASCII characters.
Contract Id field	The Call Home contract number for the customer.
	Enter up to 510 ASCII characters.
Site Id field	The unique Call Home identification number for the customer site.
	Enter up to 510 ASCII characters.

Step 7 In the **Email Addresses** area, complete the following fields with email information for Call Home alert messages:

Name	Description
From field	The email address that should appear in the From field on Call Home alert messages sent by the system.
Reply To field	The return email address that should appear in the To field on Call Home alert messages sent by the system.

Step 8 In the **SMTP Server** area, complete the following fields with information about the SMTP server where Call Home should send email messages:

Name	Description
Host (IP Address or Hostname) field	 The IPv4 or IPv6 address, or the hostname of the SMTP server. Note If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to local, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS central and DNS management is set to global, configure a DNS server in Cisco UCS central.
Port field	The port number the system should use to talk to the SMTP server. Enter an integer between 1 and 65535. The default is 25.

Step 9

Click Save Changes.

Enabling Call Home

This step is optional. You only need to enable Call Home if you disabled it before you began the firmware upgrades.

Procedure

Step 1	In the I	In the Navigation pane, click Admin.		
Step 2	Expand All > Communication Management > Call Home.			
Step 3	In the Work pane, click the General tab.			
Step 4	In the Admin area, click On in the State field.			
	Note	If this field is set to On , Cisco UCS Manager GUI displays the rest of the fields on this tab.		
Step 5	Click Save Changes.			

Disabling Call Home

This step is optional.

When you upgrade a Cisco UCS domain, Cisco UCS Manager restarts the components to complete the upgrade process. This restart causes events that are identical to service disruptions and component failures that trigger Call Home alerts to be sent. If you do not disable Call Home before you begin the upgrade, you can ignore the alerts generated by the upgrade-related component restarts.

Procedure

Step 1	In the Navigation pane, click Admin.	
Step 2	Expand All > Communication Management > Call Home.	
Step 3	In the Work pane, click the General tab.	
Step 4	In the Admin area, click Off in the State field.	
	Note	If this field is set to Off, Cisco UCS Manager hides the rest of the fields on this tab.

Step 5 Click Save Changes.

Cisco Integrated System for Microsoft Azure Stack Hub Operations Guide