HITACHI
Inspire the Next

Unified Compute Platform 3.5.1

UCP Administration Manual

Hitachi Data Systems

MK-92UCP021-05

Contents

Preface

This book explains how **Hitachi Unified Compute Platform (UCP)** functions. The information contained is intended to help UCP administrators better understand how the system works, including concepts that are needed to configure and manage UCP. It is not a solution design guide or a replacement for the release notes.

This book also covers concepts and instructions on using UCP Director Console in with both vCenter and SCVMM to administer manage the system, including switch, storage system, server, server profile, image, and service template inventory.

Intended audience

This book is intended for UCP system administrators who configure, monitor, and manage UCP systems. It assumes that they understand the hypervisor manager they use (vCenter and SCVMM), as well as the hardware components managed.

Default names and accounts

While it is possible to rename some components in UCP, such as the VM names on the UCPManagement VM on the management block or the sysadmin account, this book will use the default name.

Product version

This guide applies to UCP version 3.5.1.

Document organization

This book contains eleven chapters and four appendixes.

Chapter/Appendix	Description
Part I: "UCP overview"	
Chapter 1, "Introduction to UCP"	Contains an overview of UCP.
Chapter 2, "UCP hardware components"	Provides an overview of the hardware configurations for UCP and its related components.
Chapter 3, "UCP software components"	Contains an overview of UCP Director and other third-party software used in UCP.
Chapter 4, "UCP DOC and UCP Disaster Recovery"	Contains an overview of UCP DOC and UCP Disaster Recovery.
Part II: "Using UCP Director"	
Chapter 5, "UCP Director Console"	Describes how to use UCP Director Console to control UCP Director. Also details the **Status Monitor** page and explains how to monitor component health.
Part III: "Image management"	
Chapter 6, "Images overview"	Provides an overview of how images work in UCP.
Chapter 7, "Prepare images for deployment"	Explains how to set up Windows, Linux and ESXi images.
Chapter 8, "Deploy images in UCP Director"	Explains image deployment and post-deployment steps.
Part IV: "Resource administration"	
Chapter 9, "Physical network administration"	Explains how to administer Ethernet, Fibre Channel, and converged switches.
Chapter 10, "Logical network administration"	Explains how to administer logical networks.
Chapter 11, "Storage system administration"	Explains how to administer the storage system.
Chapter 12, "Server administration"	Explains how to administer servers.
Chapter 13, "Server profile administration"	Explains how to administer server profiles.
Chapter 14, "Service template administration"	Explains how to administer service templates.

(Continued)

Chapter/Appendix	Description
Part V: "Host deployment"	
Chapter 15, "Host deployment"	Explains how to prepare servers for deployment, deploy a host OS, and configure the host after deployment.
Part VI: "Appendices"	
Appendix A, "Jobs"	Lists and describes UCP Director tasks.
Appendix B, "Events"	Lists and describes UCP Director events.
Appendix C, "VMware alarms"	Lists and describes UCP Director alarms when using vCenter.
Appendix D, "VMware privileges"	Describes the permissions necessary to access the different features of UCP Director when using vCenter.

UCP document set

The following documents from UCP 3.5 Patch 2 contain information that applies to UCP 3.5.1:

- *UCP Pre-Installation Requirements and Configuration* — Contains information and procedures you need to be aware of for a successful UCP installation.
- *UCP Administration Manual* — Contains technical and usage information for UCP and UCP Director. Describes how to administer UCP Director through UCP Director Console with both VMware vCenter and Microsoft SCVMM.
- *UCP Director API Reference* — Describes how to use the UCP Director API.
- *UCP Director CLI Reference* — Describes how to use the UCP Director CLI.
- *UCP Director Third-Party Copyrights and Licences* — Contains copyright and license information for the third-party software distributed with or embedded in UCP Director.

- *UCP DOC Administration Manual* — Contains technical and usage information for Unified Compute Platform Director Operations Center (UCP DOC). Describes how to administer UCP DOC through UCP DOC Console.

- *UCP DOC API Reference* — Describes how to use the UCP DOC API.

- *UCP DOC CLI Reference* — Describes how to use the UCP DOC CLI.

Getting help

If you need to call the Hitachi Data Systems® support center, please have your site ID and provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure

- The exact content of any returned messages

The Hitachi Data Systems customer support staff is available 24 hours a day, seven days a week. If you need technical support, please call:

- United States: (800) 446-0744

- Outside the United States: (858) 547-4526

Comments

Please send us your comments on this document:

UCPDocumentationFeedback@hds.com

Include the document title, number, and revision, and refer to specific sections and paragraphs whenever possible.

Thank you! (All comments become the property of Hitachi Data Systems.)

Part I: UCP overview

This part contains these chapters:

1

Introduction to UCP

Hitachi Unified Compute Platform (UCP) is a turnkey converged infrastructure solution. It uses centralized management software to virtualize and integrate the server, storage, and networking resources that comprise the physical infrastructure of UCP with the hypervisor manager that you use to administer your virtual infrastructure. This enables you to centrally administer and configure both physical and virtual resources from a single interface.

This chapter contains an overview of UCP and explains the following:

About UCP

In a traditional datacenter you need to use different management platforms and interfaces to administer virtual resources and hardware elements. Some hardware elements, such as servers, may be able to be administered through a single element manager, such as Hitachi Compute Systems Manager (HCSM). Others, such as switches, often need to be administered individually.

UCP solves this by integrating the configuration and administration of your physical infrastructure with the hypervisor manager that you use to administer your virtual infrastructure, either vCenter and System Center Virtual Machine Manager (SCVMM). This enables the scalable, automated deployment and administration of both your physical and virtual resources from the same platform.

UCP Director is the software that is used to aggregate the administration of your physical infrastructure. Because it is integrated with your hypervisor manager, it is able to bring hardware awareness fully into the platform.

For more information on UCP Director, see Chapter 3, “UCP software components,” on page 41.

UCP hardware

UCP comes as a complete solution that contains all of the servers and networking equipment needed to support both your virtual infrastructure and the management components that administer it. This section covers the fundamental physical and hardware components that are core to understanding the UCP infrastructure.

Networking

Depending on the networking equipment that your infrastructure uses, UCP comes in different configurations to support your business needs. This enables you to select the networking components that are best able to integrate with the rest of your infrastructure.

UCP supports the following networking equipment:

- Cisco converged
- Cisco Ethernet
- Brocade Ethernet

Servers

Servers, also referred to as blade servers, are the hardware entities in a rack that are used to support a host OS. Because each server is located in a rack and a rack can support up to 8 servers, the number of servers supported by UCP depends on the number of racks that have been added to UCP.

Storage

Storage is an fundamental component of your UCP solution because it provides the necessary storage resources used by blade servers and host VMs in UCP.

UCP supports the following storage system models:

- Hitachi Unified Storage (HUS) 100 series
  - HUS 130
  - HUS 150
- Enterprise storage systems
  - HUS-VM
  - VSP
  - VSP G1000

Racks

Racks contain modules that enable servers to share basic resources, such as power and fan modules. Each rack is able to contain up to eight servers. Racks contain all of the physical hardware that make up the chasis installed on-site.

Before shipping, all components in each rack are assembled, configured, and tested. Testing ensures that all components function correctly and that any firmware or hardware issues are detected prior to shipment. After UCP arrives on site, an HDS technician will reassemble and test each component again to ensure that it still functions correctly before being put into production.

The networking, server and storage components described earlier will be housed in one or more compute racks based on the UCP model you have.

UCP comes in two expandable rack configurations:

- Base compute racks
- Expansion compute racks

For more information about each of the components in each configuration, see Chapter 2, “UCP hardware components,” on page 11.

Base compute racks

The core unit of each configuration is the base compute rack. In addition to containing server and networking hardware, the base compute rack contains the management block, which is used to run the UCP Director software.

UCP is available with the following base compute rack models:

- UCP 4000E for VMware vSphere with Cisco Networking
- UCP 4000E for Microsoft Private Cloud with Cisco Networking

Software features supported by base compute rack model

The following table lists the supported software features in the 3.5.1 release of UCP based on the base compute rack models that are available.

Feature	UCP 4000E for VMware vSphere (Cisco)	UCP 4000E for Microsoft Private Cloud (Cisco)
Provisioning		
Server profiles	Yes	Yes
ESXi host templates	Yes	N/A
ESXi cluster templates	Yes	N/A
Windows/Linux bare metal templates	Yes	Yes
Hyper-V host templates	N/A	Yes
Hyper-V cluster templates	N/A	No
Data Protection		
Storage Replication (ESXi)	No	No
Storage Replication (Bare metal)	No	No

Feature	UCP 4000E for VMware vSphere (Cisco)	UCP 4000E for Microsoft Private Cloud (Cisco)
Monitoring		
Health monitoring	Yes	Yes
Performance monitoring	Yes (via VC OPs)	No
Topology	Yes (via VC OPs)	No
Infrastructure Management		
Firmware upgrades	No	No
Ethernet switch backups	Yes	Yes

Expansion compute racks

Additional compute racks, known as expansion compute racks, can be added to Cisco Ethernet and Brocade Ethernet equipment to increase the number of servers in the system.

UCP is available with the following expansion compute rack models:

- UCP 4000 for VMware vSphere with Brocade Networking
- UCP 4000 for VMware vSphere with Cisco Networking
- UCP 4000 for Microsoft Private Cloud with Brocade Networking
- UCP 4000 for Microsoft Private Cloud with Cisco Networking

Software features supported by expansion compute rack model

The following table lists the supported software features in the 3.5.1 release of UCP based on the type of expansion compute rack models that are available.

Feature	UCP 4000 for VMware vSphere		UCP 4000E for Microsoft Private Cloud	
	Brocade	Cisco	Brocade	Cisco
Provisioning				
Server profiles	Yes	Yes	Yes	Yes
ESXi host templates	Yes	Yes	N/A	N/A
ESXi cluster templates	Yes	Yes	N/A	N/A

Feature	UCP 4000 for VMware vSphere		UCP 4000E for Microsoft Private Cloud	
	Brocade	Cisco	Brocade	Cisco
Windows/Linux bare metal templates	Yes	Yes	Yes	Yes
Hyper-V host templates	N/A	N/A	Yes	Yes
Hyper-V cluster templates	N/A	N/A	No	No
Data Protection				
Storage Replication (ESXi)	Yes*	Yes*	No	No
Storage Replication (Bare metal)	Yes*	Yes*	No	No
Monitoring				
Health monitoring	Yes	Yes	Yes	Yes
Performance monitoring	Yes (via VC OPs)	Yes (via VC OPs)	No	No
Topology	Yes (via VC OPs)	Yes (via VC OPs)	No	No
Infrastructure Management				
Firmware upgrades	Yes	Yes	No	No
Ethernet switch backups	Yes	Yes	Yes	Yes

UCP software

The UCP compute rack offerings described earlier come pre-configured with software developed by Hitachi Data Systems and other third-party software to help you manage all aspects of your virtual and UCP hardware infrastructure.

UCP Director

UCP Director is the main software component that is used to provision, monitor, protect and operate all elements of your UCP compute rack solution from within a single dashboard. It can be administered using the UI, via the UCP Director Console, or programmatically through the UCP Director API or UCP Director CLI. Any action or data collection that can be performed through the UCP Director Console can also be done directly through the API or the CLI.

Depending on your specific virtual management preferences, the UCP Director Console can be launched from directly within either of the hypervisor managers discussed below.

VMWare VSphere

UCP Director tightly integrates with VMware vSphere to enable faster deployment of cloud infrastructure and efficient resource allocation. Although VMware does provide API and CLI interfaces, VMware vSphere is typically administered using either the thick client, referred to as the VSphere Client, or through a thin client, VSphere Web Client.

Most UCP features are accessible using both vSphere client types, however, there are some exceptions. The following table describes which features are available based on the VSphere client you are using.

Feature	UCP 4000 for VMware vSphere (Brocade & Cisco)				UCP 4000E for VMware vSphere (Cisco)			
	5.1 Web Client	5.1 Thick Client	5.5 Web Client	5.5 Thick Client	5.1 Web Client	5.1 Thick Client	5.5 Web Client	5.5 Thick Client
Provisioning								
Server profiles		✓	✓	✓		✓	✓	✓
ESXi host templates		✓	✓	✓		✓	✓	✓
ESXi cluster templates		✓	✓	✓		✓	✓	✓
Windows/Linux bare metal templates		✓	✓	✓		✓	✓	✓
Data Protection								
Storage Replication (ESXi)	via Datacenter Operations Center				Not supported			
Storage Replication (Bare metal)								
Monitoring								
Health monitoring	✓	✓	✓	✓	✓	✓	✓	✓
Performance monitoring	via stand-alone vC Ops adapter							
Topology								
Infrastructure Management								
Firmware upgrades	✓		✓					
Ethernet switch backups	✓	✓	✓	✓	✓	✓	✓	✓

Microsoft SCVMM

SCVMM is a virtual management solution provided by Microsoft that is used to manage virtualization-related hosts, networking and storage resources. UCP Director can be imported as an SCVMM add-in.

All UCP features are accessible from within the SCVMM console.

For more information about UCP software and to see a breakdown of additional included third-party software, see Chapter 3, “UCP software components,” on page 41.

2

UCP hardware components

Understanding the physical components in UCP is essential to administering them and supporting your virtual infrastructure.

This chapter contains an overview of the physical system architecture, as well as details regarding the following components:

- Management block
- Chassis and servers
- Networking and switches
- Storage system

Physical architecture overview

UCP comes in three configurations that are powered by either Cisco Ethernet, Brocade Ethernet, or converged Cisco switches. These configurations are designed to be able to integrate with the Ethernet technology used in the rest of your infrastructure. The following sections detail the hardware components that are used by each configuration. For more information on the networks that these configurations support, see Chapter 10, “Configuring Fibre Channel zones on a hypervisor host,” on page 158.

Cisco converged configuration

Designed to be cost effective, Cisco converged configurations use converged Cisco switches to handle all network traffic. They also come in one self-contained rack and do not make use of expansion racks. Because the storage system is located in the base compute rack, Cisco converged configurations can support a total of 2 chassis and 16 servers.

The base compute rack contains the following components:

- Management block
- 2 10G access converged switches: Cisco Nexus 5548
- Storage system (one of the following):
  - HUS 130
  - HUS-VM

  An storage rack can be added when using a HUS-VM for additional storage.
- 2 to 16 servers (housed in 1 or 2 chassis)

  Each server contains two 2 or 4-port Emulex Converged Network Adapters (CNA). When using 4-port CNA, a Cisco converged configuration is limited to one chassis.

  In addition to servers, chassis contain fan, power, and management modules, as well as two Ethernet pass-through modules.

Cisco Ethernet configuration

Designed to support the maximum number of servers, Cisco Ethernet configurations use Cisco Ethernet switches and can support up to three expansion racks for a total of four racks. Because each rack can support up to 4 chassis and 32 servers, a Cisco converged configuration can support a total of 16 chassis and 128 servers.

The base and optional expansion compute racks contain the following components:

- Base compute rack:
  - Management block
  - 2 1G management Ethernet switches: Cisco Nexus 3048
  - 2 10G Ethernet FEX (when more than one rack is used): Cisco Nexus 2232
  - 2 10G access Ethernet switches: Cisco Nexus 5548
  - 2 8G core Fibre Channel switches: Brocade 6510
  - 2 to 32 servers (housed in 1 to 4 chassis)
- Expansion compute racks:
  - 2 10G Ethernet FEX: Cisco Nexus 2232
  - 2 10G access Ethernet switches: Cisco Nexus 5548
  - 2 8G core Fibre Channel switches: Brocade 6510
  - 1 to 32 servers (housed in 1 to 4 chassis)

Each server contains the following network adapters:

- 2-port Emulex Converged Network Adapters (CNA)
- Hitachi FiVE Fibre Channel HBA

Chassis contain fan, power, and management modules, as well as the following networking components:

- 2 Ethernet pass-through modules

- 2 8G edge Fibre Channel switches: Brocade 5460

In addition to the compute racks, at least one storage system rack is needed to accommodate your storage system. UCP supports the following storage systems:

- Hitachi Unified Storage (HUS) 100 series
  - HUS 130
  - HUS 150
- Enterprise storage systems
  - HUS-VM
  - VSP
  - VSP G1000

  Only enterprise storage systems support UCP Disaster Recovery or can be shared.

The networking components are connected, as follows:

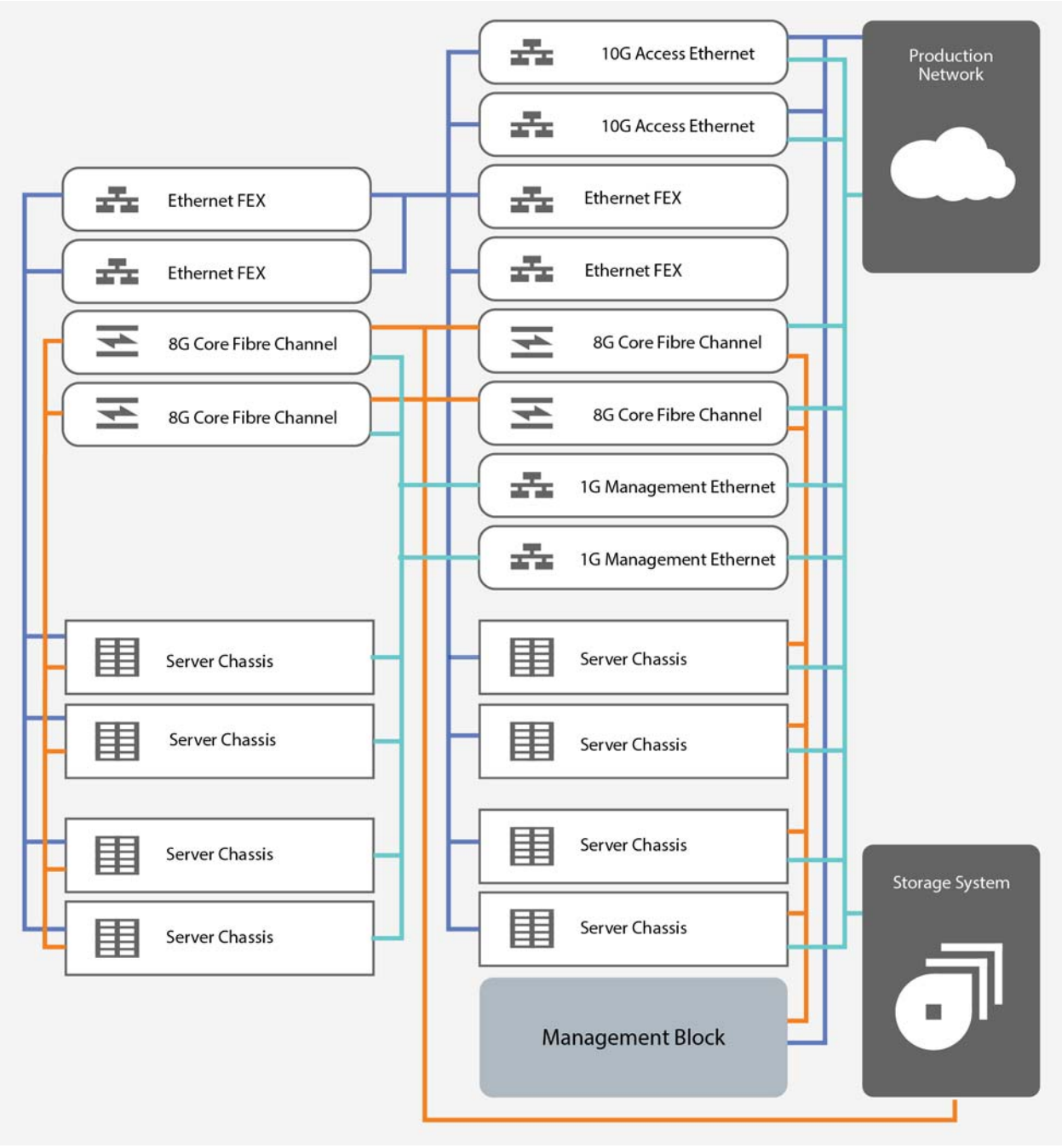
- When using one rack:

  The Ethernet pass-through modules in each chassis are connected directly to the access Ethernet switches. The access Ethernet switches are connected to the production network.

- When using two racks:

  The Ethernet pass-through modules in each chassis are connected to the Ethernet FEX, which are then connected to the access Ethernet switches. The access Ethernet switches are connected to the production network.

The following diagram shows the layout of the physical components in the base compute rack and one expansion compute rack when using a Cisco Ethernet configuration. It also shows the how the access, storage, and management networks connect to each component and the production network.



The previous diagram showed the access, storage, and management networks as follows:

- Teal — 1G Ethernet
- Blue — 10G Ethernet
- Orange — 8G Fibre Channel

Brocade Ethernet configuration

Designed to use Brocade Ethernet switches, Brocade Ethernet configurations can support one expansion rack for a total of two racks. Because each rack can support up to 4 chassis and 32 servers, a Brocade Ethernet configuration can support a total of 8 chassis and 64 servers.

The base and optional expansion compute racks contain the following components:

- Base compute rack:
  - Management block
  - 2 1G management Ethernet switches: Brocade FCX648
  - 2 10G aggregate Ethernet switches: Brocade 6740
  - 2 8G core Fibre Channel switches: Brocade 6510
  - 2 to 32 servers (housed in 1 to 4 chassis)
- Expansion compute racks:
  - 2 10G aggregate Ethernet switches: Brocade 6740
  - 2 8G core Fibre Channel switches: Brocade 6510
  - 1 to 32 servers (housed in 1 to 4 chassis)

Each server contains the following network adapters:

- 2-port Emulex Converged Network Adapters (CNA)
- Hitachi FiVE Fibre Channel HBA

Chassis contain fan, power, and management modules, as well as the following networking components:

- 2 10G access Ethernet switches: Brocade 6746
- 2 8G edge Fibre Channel switches: Brocade 5460

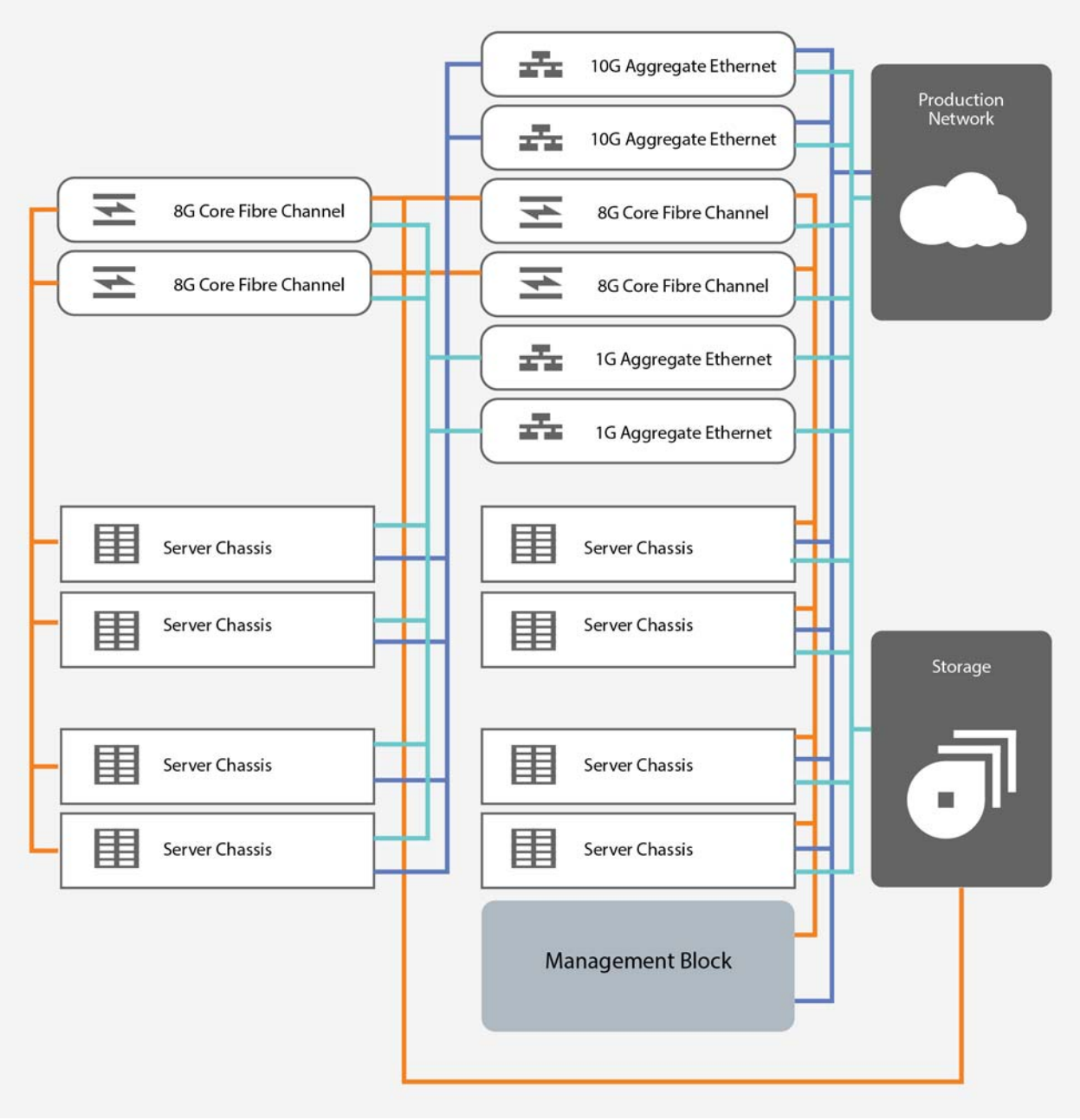
In addition to the compute racks, at least one storage system rack is needed to accommodate your storage system. UCP supports the following storage systems:

- Hitachi Unified Storage (HUS) 100 series
  - HUS 130
  - HUS 150
- Enterprise storage systems
  - HUS-VM
  - VSP
  - VSP G1000

  Only enterprise storage systems support UCP Disaster Recovery or can be shared.

The access Ethernet switches in each chassis are connected to the aggregate Ethernet switches. The aggregate Ethernet switches are connected to the production network.

The following diagram shows the layout of the physical components in the base compute rack and one expansion compute rack when using a Brocade configuration. It also shows the how the access, storage, and management networks connect to each component and the production network.



The previous diagram showed the access, storage, and management networks as follows:

- Teal — 1G Ethernet

- Blue — 10G Ethernet
- Orange — 8G Fibre Channel

Management block

The management block hosts VMs that contain UCP Director, as well as the software that supports its operation. In a Cisco Ethernet or Brocade Ethernet configuration, it consists of two servers that are clustered together to ensure reliable operation. A Cisco converged configuration consists of one server with the option to add a second server.

Depending on the hypervisor manager that you use, the servers that comprise the management block are configured as follows:

- vCenter — One of the following:
  - ESXi 5.1 clustered and managed using vCenter Server 5.1.
  - ESXi 5.5 clustered and managed using vCenter Server 5.5.
- SCVMM — Windows Server 2012R2 SP1 configured in a stand-alone cluster.

The host operating systems on the management block are installed to drives that are internal to the servers in the management block. All VMs hosted by the management block are stored on the storage system. UCP Director requires that the storage pool used by the management block is dedicated to the management block. As a result, it is not configured to be visible in UCP Director Console.

For more information on UCP Director and its supporting software, see Chapter 3, “UCP software components,” on page 41.

Chassis and servers

To maximize the server density of a rack, UCP uses blade servers that are located in chassis. All servers in a chassis have the same hardware configuration, although different CPU types and memory capacities can be selected for each chassis. UCP Director leverages HCSM to administer the servers and chassis.

The following sections explain how servers and chassis are configured in UCP.

Chassis configuration

Each chassis is able to contain up to eight servers. In addition to increasing server density, chassis contain modules that enable servers to share basic resources, such as power and fan modules. Specifically, chassis are configured as follows:

- 6 fan modules
- Switch modules
  - In a Cisco converged configuration: 2 Ethernet pass-through modules
  - In a Cisco Ethernet configuration:
    - 2 Ethernet pass-through modules
    - 2 edge Fibre Channel switches
  - In a Brocade Ethernet configuration:
    - 2 access Ethernet switches
    - 2 edge Fibre Channel switches
- 4 power modules
- 2 management (SVP) modules

Server configuration

Servers are the hardware entities that are used to support a host OS. Because each server is located in a chassis and a chassis can support up to 8 servers, the number of servers supported by UCP depends on the number of chassis that have been added to UCP.

Before a server can function as a host and support VMs, it will need to be configured for use in UCP Director. Configuring a server for use requires the following:

- A server profile that virtualizes and defines the identifying information for the server. Because server identities are virtualized in UCP Director, server profiles are a logical entity that are used to define the identifying information about a server, such as the IP address and WWPNs. For more information on server profiles, see "Server profiles" on page 47.

- A service template will need to be created to define the image, networking, and storage configuration that will be applied to the server. Service templates define the basic storage and networking configuration options of a server and ensure consistency in the datacenter. For more information on service templates, see "Service templates" on page 50.

- An image containing the host OS to be installed on the server through the service template. For more information on images, see "Images" on page 52.

Because UCP Director leverages HCSM to administer server inventory, for UCP Director to see a server, it must first be added in HCSM. Likewise, to remove a server from UCP, it must be removed from HCSM.

HCSM also monitors server status and reports hardware events to UCP Director. UCP Director then collects and reports this information to your hypervisor manager. This enhances the limited subset of hardware events that the hypervisor manager is able to receive through a host alone.

Server boot configurations

Servers can be configured to function as hosts as follows:

- Hypervisor hosts — Depending on your hypervisor manager, a server can function as either an ESXi or Hyper-V host, as follows:

  – When using vCenter, hypervisor hosts are configured to boot stateless ESXi images through Auto Deploy. UCP automatically configures the necessary Auto Deploy rules so that a server loads the correct image each time it boots. As a result, manually changing or adding auto deploy rules is not advisable.

  - When using SCVMM, hypervisor hosts are configured to boot Windows 2012 R2 SP1 Datacenter images with the Hyper-V role enabled through Windows Deployment Server (WDS). Customization of the Hyper-V image is done manually through WDS.

- Non-hypervisor (Windows or Linux) hosts — In both vCenter and SCVMM, servers can be configured to boot Windows or Linux images through WDS. Customization of Windows and Linux images is handled manually through WDS.

- Custom hosts — A server can be configured as a custom host to disable automated UCP image deployment on that server. You can configure as a custom host when you want to manually manage the server. UCP Director continues to monitor health and SNMP traps from custom hosts.

For more information on:

- Images, see Chapter 6, “Images overview,” on page 91.

- Host deployment, see Chapter 15, “Host deployment,” on page 241.

The following table shows which host types are available in each hypervisor manager.

Host type	Available using vCenter	Available using SCVMM
ESXi cluster	X	
ESXi standalone	X	
Hyper-V		X
Windows	X	X
Linux	X	X
Custom	X	X

Server identity virtualization

UCP is deployed with pools of MAC addresses, WWNs, UUIDs, and IP addresses. When a server profiles are created, they can use IDs from these pools or IDs that are manually entered. A server profile can then be applied to a server. When a server profile is applied to a server, it is actually applied to the slot in the chassis that the server is located in. This enables server virtualization because servers can then be moved or replaced in the chassis and the new server will automatically resume the identity of the server that it replaced.

Because a server profile is associated with the slot, and not the actual server, if a server fails or is removed, the server profile will still be associated with the slot. To remove a server profile, a new server will have to be inserted into the slot so that the server profile can be removed. A server profile can only be manually removed from a slot and applied to another slot when a functioning server is in the slot.

Server host names

When a new host is created, there are different ways that hosts and their names show up in either virtualization platform.

For Hyper-V, the Windows Deployment Server (WDS) tells the new host to generate a name during the unattended installation process. Then, through the domain join process, the new host registers its name with DNS and SCVMM will pick up that name from DNS.

vCenter, on the other hand, will look for DNS records that match the IP address for the new host. If there are no records in DNS that match the IP address for the host, vCenter will use the host's IP address as its name.

There are some situations where you may need to use a specific host name and apply it to a host. You can do this today, but the steps vary depending on which hypervisor you are using for the host.

Configure a custom host name for a vCenter host

When using vCenter as the hypervisor, you will need to:

1. Use UCP Director to pre-stage the host name and corresponding IP address with the DNS server. The Auto Deploy process will then pick up the DNS name and show it in the VMware inventory

For more information, see Chapter 12, "Setting a non-hypervisor host name," on page 205.

Configure a custom host name for a SCVMM host

UCP Director does not currently provide a mechanism for you to pre-stage a custom host name for a host in SCVMM. Therefore, to set a custom host name for a SCVMM host, you will need to:

1. Remove the host from SCVMM

2. On the host, dis-join it from the Active Directory Domain, and then reboot

3. On the host, change the host name and reboot

4. On the host, join it back to the Active Directory Domain, and then reboot

5. Add the host back to SCVMM

Note: Each reboot will take approximately five minutes to complete.

Networking and switches

The following sections describe the physical and logical networks used by UCP.

Physical networking

UCP Director uses three different physical networks to support the virtual networks, as follows:

- 1G Ethernet

  Connects switches to the following management ports:

  – Chassis SVP

  – CR210 BMC

  – Storage array SVP

  – Switch management interface

- 10G Ethernet

- 8G Fibre Channel

These networks are connected to different switches, depending on the configuration used, as follows:

- Cisco converged

  1G Ethernet, 10G Ethernet, and 8G Fibre Channel — Access converged switches

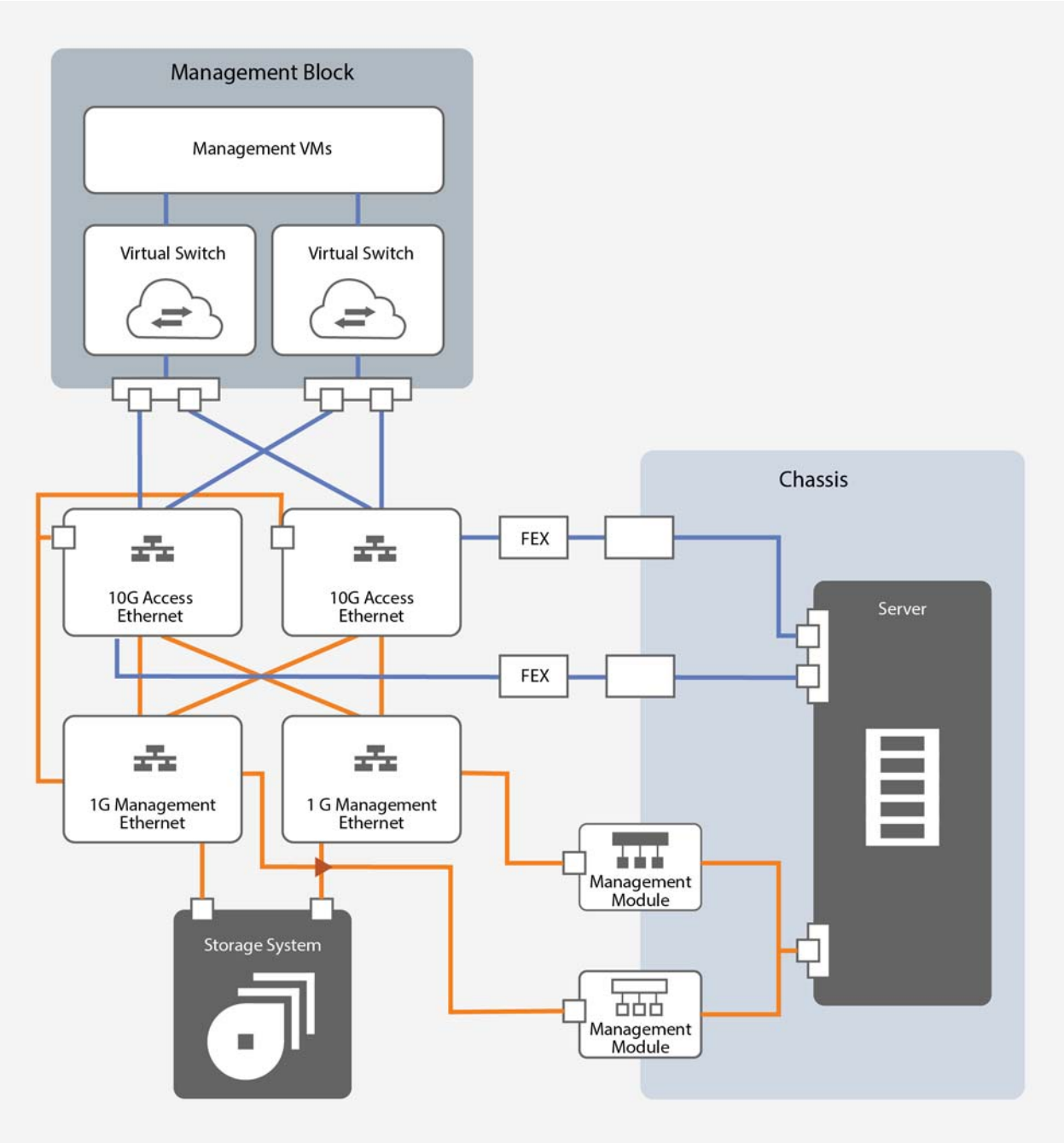
- Cisco Ethernet and Brocade Ethernet

  – 1G Ethernet — Management Ethernet switches

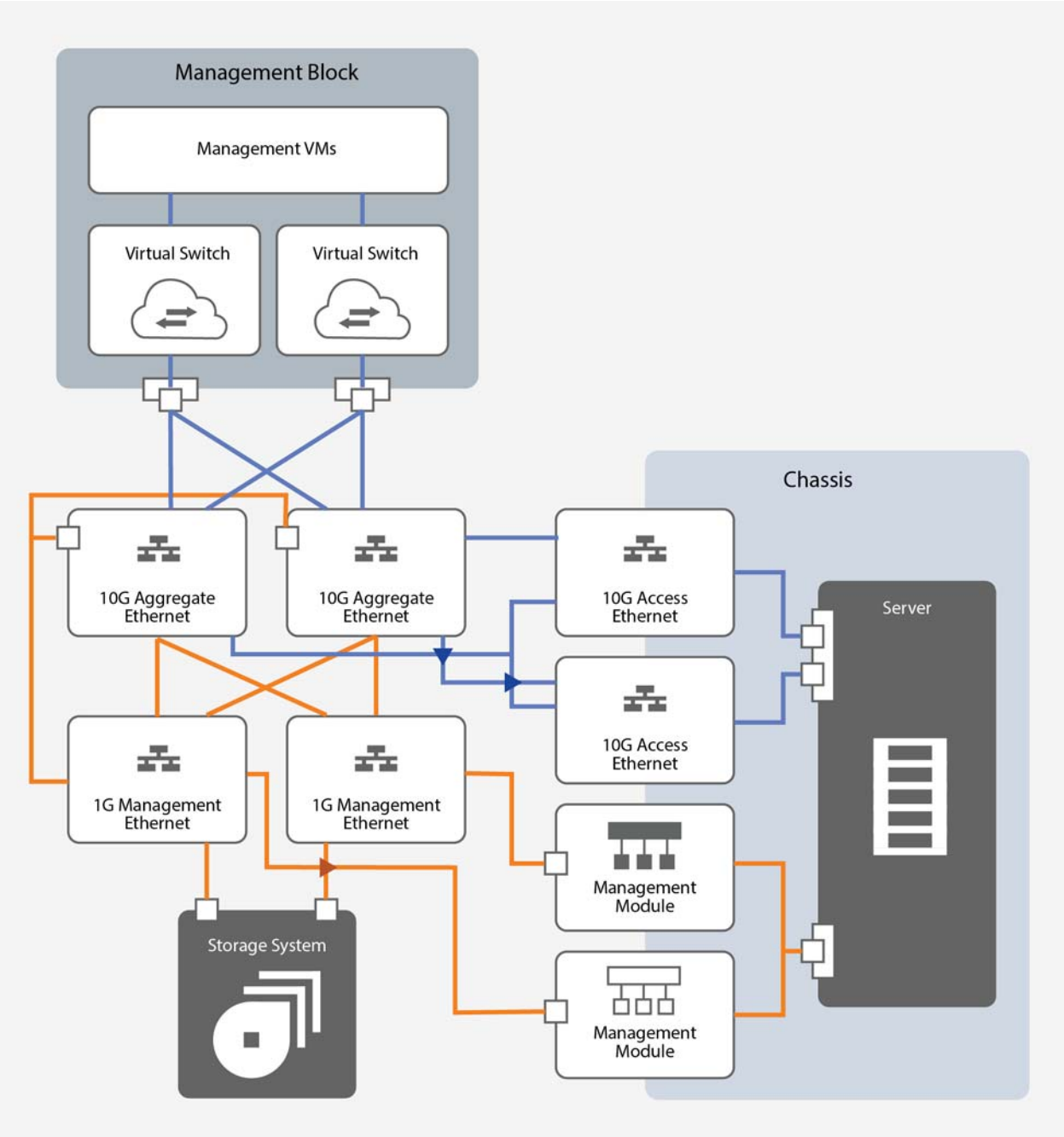
  – 10G Ethernet — Access and, in the case of a Brocade Ethernet configuration, aggregate Ethernet switches

  – 8G Fibre Channel — Fibre Channel switches

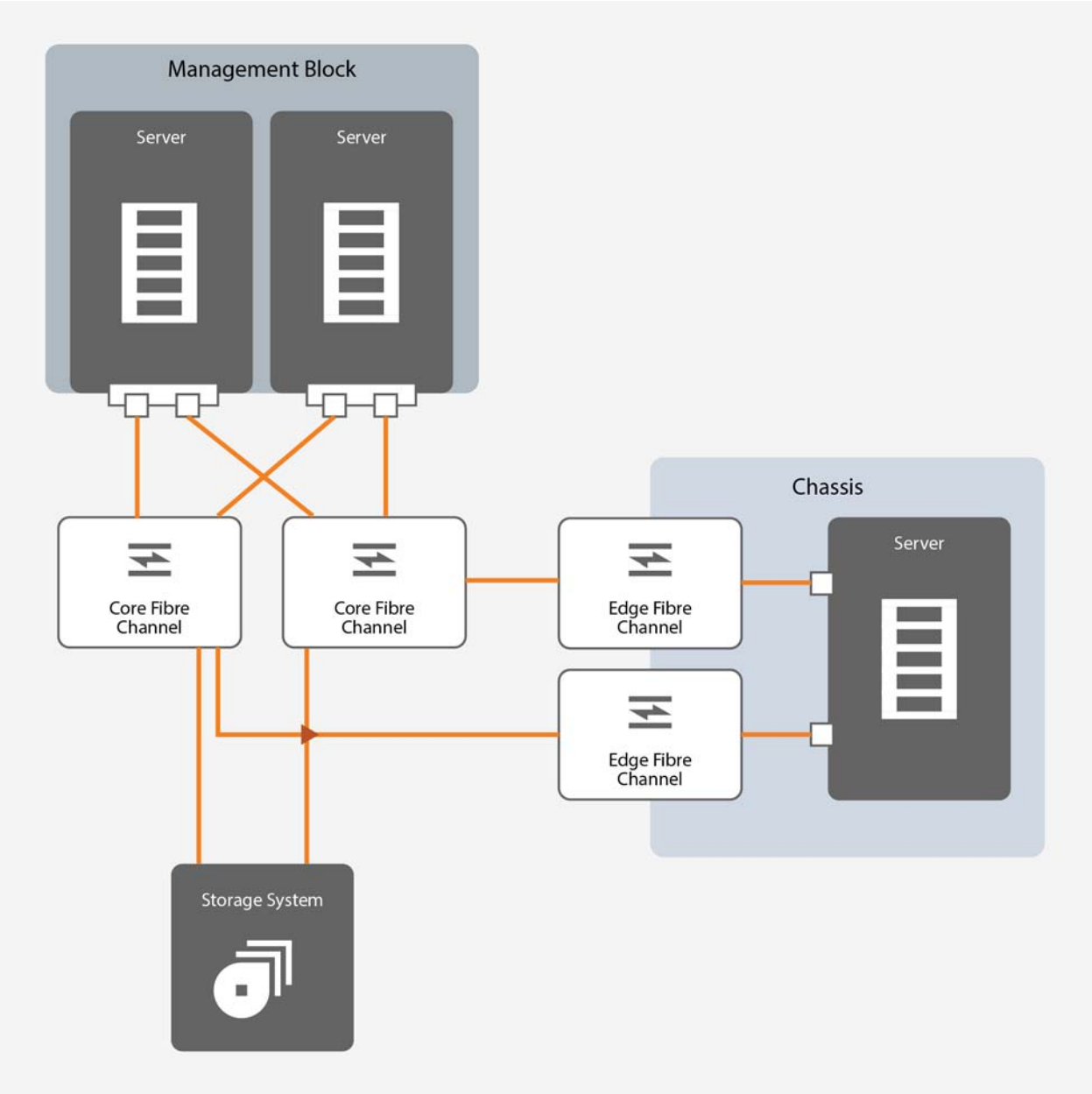
The following network diagram shows how the management block, a server, and the storage array are connected to the 1G Ethernet and 10G Ethernet networks in a Cisco Ethernet configuration.



The following network diagram shows how the management block, a server, and the storage array are connected to the access and management networks in a Brocade configuration.



The following diagram shows how the management block and a server are connected to the storage system through the storage network in Cisco Ethernet and Brocade Ethernet configurations.



Logical networking

UCP Director uses several logical networks for component communications. Depending on the hypervisor manager used, UCP Director uses either four or five logical networks, as follows:

- VM migration

  Used for workload migration on clustered servers. It is powered by vMotion when using vCenter, or Live Migration when using SCVMM. The VM migration network is supported by the 10G Ethernet network.

- Cluster (Hyper-V only)

  When using SCVMM, used for cluster communication for Hyper-V clusters. The cluster network is supported by the 10G Ethernet network.

- Management

  Used by UCP Director to manage the physical components in UCP. This includes such jobs as configuring switches, rebooting servers, and managing storage volumes. The management network is supported by the 1G Ethernet network, and is accessed by the VMs on the management block through the 10G Ethernet network.

- Data

  Used to support connectivity between VMs and the production network, as well as hypervisor deployment.

- Storage

  Used for communication with the storage system. Supported by the 8GB Fibre Channel network.

These networks are connected through the physical networks, as shown in the following table.

Logical network	1G Ethernet	10G Ethernet	8G Fibre Channel
Data		X	
Storage			X
Management	X	X	
VM migration		X	

Logical network	1G Ethernet	10G Ethernet	8G Fibre Channel
Cluster		X	

Switches

UCP Director acts as an interface between the switches that are included in your configuration and your hypervisor manager. The following sections explain how switches are configured in UCP.

Management Ethernet

In Cisco Ethernet and Brocade Ethernet configurations, redundant 1G Ethernet switches are located in the base compute rack to support the management network. The first 1G Ethernet switch is the primary switch and it is connected to all hardware components in UCP. All hardware components that have a redundant management port, such as chassis and some storage systems, are also connected to the second 1G Ethernet switch. Management Ethernet switches are not added to UCP Director inventory.

Access and aggregate Ethernet

Access and aggregate Ethernet switches support the 10G Ethernet network and are used to provide connectivity between components within UCP as well as between UCP and the production network.

Fibre Channel

In Cisco Ethernet or Brocade Ethernet configurations, a combination of edge and core Fibre Channel switches, as follows:

- **Edge** - Two Fibre Channel switches are located in each chassis that are used to connect the servers to the core Fibre Channel switches.
- **Core** - Two 8GB Fibre Channel switches are located in each rack that are used to connect the edge Fibre Channel switches to the storage system.

The Fibre Channel switches are used to enable both the management block and all UCP servers to access the storage system. Because UCP Director is integrated with both the Fibre Channel switches and the hypervisor manager, it is able to automate storage networking functions such as the creation of Fibre Channel zones.

Converged

Converged switches support the 10G Ethernet, 1G Ethernet, and 8G Fibre Channel networks and are used to provide connectivity between components within UCP as well as between UCP and the production network.

Switch configuration

SNMP settings are configured on all switches (Brocade Ethernet, Cisco Ethernet, Fibre Channel, Cisco converged) directly by UCP Director based on the corresponding SNMP settings. All switches of the same type (Ethernet, Fibre Channel, or converged) need to use the same username and password for SNMP access.For more information on SNMP settings, see "SNMP monitoring" on page 55.

In addition to SNMP settings, UCP Director configures different settings and protocols to optimize logical networking, as follows:

- VLANs are configured on Ethernet and converged switches, as follows:

  UCP Director automates the VLAN configuration on Ethernet and converged switches during host deployment. After a host has been deployed, you can configure VLANs by host or cluster.

  For hypervisor hosts, the management, or native, VLAN ID is set when UCP is deployed. It is used for all management traffic. The management VLAN ID is set automatically when creating a hypervisor service template.

  Because the hypervisor manager does not manage non-hypervisor hosts, you can manually configure the management VLAN ID when creating a non-hypervisor Windows, Linux, or custom host service template. If you use the same management VLAN ID that is configured for UCP, then the host's management IP address will be configured by UCP. If a different management VLAN ID is set, then the management IP address of the host will need to be configured manually.

  In addition to the management VLAN ID, you can set the trunk VLAN IDs that will be used for VM network traffic when creating a service template. UCP supports VLANs 2-4094 and UCP Director will return an error when setting any VLANs outside of this range.

- The following are configured on Cisco Ethernet and converged switches:

  – Cisco discovery protocol (CDP)

    UCP Director enables CDP along with LLDP. Cisco switches use CDP to determine what ports and devices the converged switch is connected to. When using vCenter, if CDP is configured on Cisco Ethernet switches, UCP Director will also enable it on all vSwitches and virtual distributed switches.

  – Virtual port channel configuration (vPC)

    vPC is used by Cisco converged switches to treat links that are connected between different Ethernet components to appear as a single port channel. This enables UCP Director to treat redundant connections between the access converged switches, the Ethernet FEX, and the chassis as a single path.

- The following are configured on Brocade and Cisco Ethernet switches:

  – Rapid spanning tree protocol (RSTP)

    Ethernet switches managed by UCP Director are configured with RSTP to provide redundancy in the case of link failure.

  – VDS configuration

    Servers in UCP have two Ethernet ports each. To achieve redundant paths through both physical Ethernet switches, the associated vSwitch and VDS switches should be configured with both NICs attached as uplinks. In a Brocade Ethernet configuration, each access Ethernet switch is connected to a different aggregate Ethernet switch.

    The following teaming methods are supported:

    - Route, based on the originating virtual port (port ID hash)
    - Route, based on the source MAC hash (MAC hash)
    - Explicit failover order (failover order)
    - Route, based on the physical NIC load (LBT)

    Route, based on IP hash, is not supported.

- The following are configured on Brocade Ethernet switches:

  – Port channel groups

    UCP Director uses port channel groups consisting of four ports each to provide connectivity between access and aggregate switches.

  – Link layer discovery protocol (LLDP)

    UCP Director enables LLDP on Brocade Ethernet switches. This is used to determine what ports and devices the Ethernet switch is connected to.

- Fibre Channel zones are configured on Fibre Channel and Cisco converged switches, as follows:

  The SAN design in UCP is based on using multiple fabrics between a host and the storage system. Each storage system controller (referred to as cluster 1 and cluster 2) are connected to each fabric to maximize path redundancy. UCP Director supports:

  – Automatic provisioning to create the Fibre Channel zones and attach the volume to a host or cluster

  – Manual provisioning to support traditional Fibre Channel zone creation for hypervisor hosts

    When creating a zone manually, only one zone per initiator/target pair is needed. The target port must be visible to the initiator port.

  When automating Fibre Channel zone creation, UCP Director determines if a zone currently exists for the selected initiator and target port pair, and creates a new zone if one does not exist. When creating the zone, UCP Director only creates single initiator/single target zones.

- The following are configured on Fibre Channel switches:

  – Virtual fabrics

    UCP uses vFabs, or virtual fabrics, to logically segregate core Fibre Channel switches into multiple logical switches. By default, each core Fibre Channel switch is divided into two virtual fabrics, as follows:

    - Virtual Fabric #128 (default) — Used for all compute Fibre Channel ports

- Virtual Fabric #1 — Used for management Fibre Channel ports

  Modifying the virtual fabrics may make the storage system unstable.

Note: Edge Fibre Channel switches are part of the virtual fabric of the core Fibre Channel switch they are connected to.

- Load balancing

  UCP Director engages in load balancing on Fibre Channel switches to ensure that there is the minimum number of paths to each storage system port.

Network adapters

The network adapters used in a server are configured differently depending on the hardware configuration selected. Specifically, the network adapters are connected as follows:

- Brocade Ethernet

  Server contains both CNA and Fibre Channel network adapters. They are connected as follows:

  - 2-port CNA adapter — Connected to the in-chassis access Ethernet switches
  - Fibre Channel adapter — Connected to the in-chassis edge Fibre Channel switches

- Cisco Ethernet

  Server contains both Ethernet and Fibre Channel network adapters. They are connected as follows:

  - 2-port CNA adapter — Connected to the in-chassis Ethernet pass-through modules
  - Fibre Channel adapter — Connected to the in-chassis edge Fibre Channel switches

- Cisco converged

  Servers contain two 2-port or 4-port CNA adapters. Each adapter is connected to the in-chassis Ethernet pass-through modules.

Storage system

UCP Director is designed to connect to one storage system to provide the storage resources used by servers in UCP. Depending on the configuration, the storage system is configured as follows:

- In a Cisco converged configuration, the storage system is located inside the base compute rack.
- In a Brocade Ethernet or Cisco Ethernet configuration, the storage system is located in at least one external storage rack. The compute racks are then connected to the storage rack through the storage network to access storage pools.

Additional storage systems can be virtualized through Hitachi enterprise storage systems.

HDvM configuration

UCP Director leverages HDvM to control interactions with the storage system, such as managing Fibre Channel zones or creating and attaching volumes. This also enables changes that are made to the storage system in HDVM to be reported to UCP Director, and for UCP Director to leverage key storage technologies, such as:

- Hitachi Dynamic Provisioning (HDP) pools
- Hitachi Dynamic Tiering (HDT) pools
- Hitachi Thin Imaging (HTI) pools
- Universal Volume Manager (UVM)

Because storage resources are leveraged through HDvM, HDvM can be used to modify those resources, such as storage pools, after UCP is deployed.

UCP Director requires the following HDvM configuration to interact with storage resources:

- HDvM needs to be configured to administer the storage system.
- HDvM credentials need to be added to UCP Director. UCP Director can connect to only one instance of HDvM.
- In addition to the storage pool used by the management block, at least one storage pool needs to be configured on the storage system for UCP Director to administer host volumes in.

Storage system configuration

When using a Brocade Ethernet or Cisco Ethernet configuration, UCP requires two dedicated resource groups to be configured in the storage system to separate the management and compute elements:

- Management resource group:
  - 4 Storage system ports
    - If using a VSP storage system, the ports are: CL1-A, CL2-A, CL3-A, and CL4-A
    - If using an HUS-150 or HUS-VM storage system, the ports are: CTL0-A, CTL0-B, CTL1-A, and CTL1-B
  - 1 Parity Group (PG 1-1, 8 spindles, RAID6)
  - LDEV IDs are created for boot-from-SAN volumes and datastores for management nodes
  - Host storage domain (HSD) IDs (All HSD IDs for above 4 ports)
- Compute resource group:
  - All remaining storage ports if a dedicated storage system is used, or specifically assigned ports if a shared storage system is used
  - All remaining parity groups if a dedicated storage system is used, or specifically assigned ports if a shared storage system is used
  - All remaining logical device (LDEV) IDs if a dedicated storage system is used, or specifically assigned LDEV IDs if a shared storage system is used
  - All HSD IDs for the assigned compute ports

If an enterprise storage system is shared with non-UCP resources, then those resources will need to use other resource groups. Modifying the default resource group configuration can have unpredictable effects and should only be done with the assistance of Hitachi Data Systems personnel.

Shared storage requirements

Hitachi enterprise storage systems can be shared with non-UCP resources. A Hitachi enterprise storage system must meet the following requirements to be shared:

- 4 Dedicated storage ports for management nodes
- 9 x 600Gb SAS in R6 parity group (6+2 for data, 1 for hot spare)
- 12 Dedicated storage ports for compute nodes.

Storage pools

The initial Storage pools are configured in the storage system when UCP is deployed. A storage pool is comprised of logical devices that are created from physical parity groups. Parity groups cross multiple HDDs (hard disk drives) that are grouped together to act as one.

At least two pools are required for UCP to function. The management pool is the first pool. It is not displayed in inventory and instead is only used to support the management block.

Additional pools are added to inventory to store your data and store the volumes that you administer from within UCP. These pools are accessible to UCP servers only.

When defining these pools, you can select either Hitachi dynamic provisioning (HDP) or Hitachi dynamic tiering (HDT) pools. Both HDP and HDT pools are made up of multiple physical drives and enable:

- Wide-striping to achieve a high aggregate input/output (IO) throughput from all of the hard disk drives (HDDs) that make up the storage pool.
- Overprovisioning to reduce wasted capacity in the storage system. This is done by logically allocating more virtual space to a volume than is physically allocated. Instead, through overprovisioning, space is taken up in the storage system as data is written to it. To keep you from running out of space, alerts can be configured on the storage system.

HDT pools are also capable of dynamic tiering. When dynamic tiering is used, up to three tiers can be created with different types of drives based on the cost and speed of the drives. For example, an HDT pool could have SSD, SAS, and SATA drives. Dynamic tiering would then move data to the appropriate drive type based on its access characteristics. When a block of data is frequently accessed, it could be migrated to the high-speed SSD drives for quicker response times. As the data ages and becomes less frequently accessed, it could be migrated to the lower-cost SATA drives.

When defining storage pools, you can commit more storage capacity to HDP and HDT pools than is physically reserved on the storage system. When a pool is overprovisioned, space can be allocated to volumes on the storage system, but the capacity will be dynamically used as data is written. This enables more flexibility, more complete use of the pool, and reduced up-front storage requirements.

If a pool becomes full, all input and output for the pool will cease, which can cause VMs to fail. To avoid this, it is important to set realistic subscription limits and monitor pool use.

Tip: Try to keep physical pool utilization <70% to provide a buffer in the event of sudden data growth.

Enterprise Hitachi storage systems also support Hitachi Thin Provisioning (HTI) pools. HTI pools are created by HDS personnel when two UCP sites are configured for replication using UCP Disaster Recovery. Test volumes can be created in HTI pools when conservation of storage space is important. Because HTI pools and test volumes are used by UCP Disaster Recovery, UCP Director does not enable the manual deletion, expansion, or attachment of volumes in an HTI pool.

Volumes

Volumes are virtual storage resources that UCP Director can allocate from a storage pool. They can be created and attached to or detached from a single host, multiple hosts, or all hosts in a cluster.

When a volume is attached to a host, UCP Director is able to automatically:

- Create Fibre Channel zones and select appropriate ports on the Fibre Channel or converged switches.

  When automatically selecting ports, UCP Director selects ports to present to volumes based on:

  – The existence of usable zones for the initiator and target ports.

  - The existence of usable host storage domains (HSDs) for initiator and target ports.

  - If there are no usable zones or HSDs, UCP Director:

    - Creates the volume with the defined size.

    - Uses 4 ports on the least used paths per point (calculated based on the number of volumes to number of hosts on a per-port basis). UCP Director requires the use of one even and one odd port per Fibre Channel fabric to ensure path redundancy in connecting to the volume.

    - Creates the appropriate zones in the Fibre Channel infrastructure.

    - Creates the appropriate host storage domains (HSDs) on the storage system.

    - Sets the HSD optimization mode (ESXi, Windows, or Linux).

    - Presents and mounts the volume on the host or all hosts in the cluster.

    - Formats the volume if indicated.

- Create corresponding Hitachi Storage Domains (HSDs) in the storage system.

- Add the LDEV ID of the volume, as well as the WWPNs of the host and storage system to the HSD.

For redundancy, each host is allocated a set of four Fibre Channel zones and HSDs for each attached volume.

When UCP Director attaches an ESXi, Windows, or Linux image to a server, the volumes will be configured to be optimized for that OS type. When a volumes configured for a custom host, you can use Storage Navigator to customize the optimization settings for the type of OS that you deploy to the server.

Important: Volumes should not be shared between different operating system types.

Supported vs unsupported HSDs

UCP Director is not able to attach a volume to a host if one of its host adapter port WWPNs is contained in an unsupported HSD. UCP only supports HSDs created on a per-host basis. In other words, supported HSDs are defined as HSDs that contain all of the host adapter port WWPNs for that host. HSDs that only have a subset of host adapter port WWPNs or have WWPNs from another host are unsupported.

3

UCP software components

UCP Director is the software that administers server, storage, and networking resources in UCP and integrates them into your hypervisor manager. This enables jobs to be run across hardware elements, such as configuring network VLANs, deploying images to servers, or automatically provisioning storage resources. UCP Director also monitors health and performance data to better facilitate hardware troubleshooting and administration.

This chapter contains an overview of the following core software for UCP:

- UCP Director software
- Overview of UCP software components

In addition, this chapter contains an explanation of:

- Inventory
- Monitoring
- Jobs, events, and reporting
- Firmware update management in vSphere Web Client
- Security

UCP Director software

UCP Director can be administered either graphically, through UCP Director Console, or programmatically through the UCP Director API or UCP Director CLI. Because all three interfaces are developed in tandem, functional parity is maintained across all three interfaces. This means that any action that can be performed through UCP Director Console can also be performed

For more information on the UCP Director CLI, see UCP Director CLI Reference.

through the UCP Director API or UCP Director CLI. In addition, because the API and CLI are programmatic interfaces, they can be scripted to perform repetitious actions.

UCP Director Console

UCP Director Console is integrated into your hypervisor manager. This enables you to administer UCP resources graphically from within the same user interface (UI) that you use to administer your virtual resources.

For more information on UCP Director Console, see "UCP Director Console" on page 73.

The UCP Director API

The UCP Director API is a REST-based API. The UCP Director API enables you to request the current state of a resource or to change the state of a resource using standard HTTP methods.

For more information on the UCP Director API, see *UCP Director API Reference*.

The UCP Director CLI

The UCP Director CLI provides full access to hardware resources. This enables you to perform the same actions through the UCP Director CLI that you can perform through the API.

For more information on the UCP Director CLI, see *UCP Director CLI Reference*.

Overview of UCP software components

UCP Director and the software components that it works with to monitor and administer your physical infrastructure is stored in a collection of VMs that are run in the management block. For more information about the management block, see "Management block" on page 19.

The following is a list of the software that runs on each of the VMs in the management block.

- **UCPManagement** — Hosts the following services:
  - UCP Director - A central administration interface used to support rapid enterprise data center scalability and virtual machine deployment.
  - AMQP — Used to organize UCP Director events and messages, including SNMP events and monitor states.

    SNMP events and monitor states are organized into queues and exchanges that you can post or subscribe to. For example, when a UCP site is registered with UCP DOC, UCP DOC subscribes to the SNMP messaging exchange in that site.
- **A hypervisor manager VM**. This is used to deploy and manage hypervisor hosts. UCP supports both VMware and Microsoft solutions, as follows:
  - vCenter — Hosts the VMware vCenter server and all related vCenter modules, such as single sign on (SSO). It only exists when using vCenter as your hypervisor manager.
  - SCVMM – Hosts the Microsoft SCVMM server. It only exists when using SCVMM as your hypervisor manager.
- **UCPUtility** — Hosts the following services:
  - Syslog — Used to receive syslogs from hardware elements.
  - TFTP — Used for Auto Deploy.
  - DHCP — Used to dynamically assign IP addresses to servers.
  - SCP — Used to restore Ethernet switch configuration backups and Fibre Channel and Ethernet switch firmware downloads.

- **ServiceVM** — Hosts the UCP deployment and maintenance tools that are used by Hitachi Data Systems personnel to support UCP.
- **HCS** — Hitachi Command Suite (HCS), hosts the following services:
  - Hitachi Device Manager (HDvM), which is used to coordinate volume management with the storage system.
  - Hitachi Compute Systems Manager (HCSM), which is used to administer servers.
  - Hitachi Storage Navigator Modular 2 (SNM2), which is used for lower-level administration of the storage array, such as administering licensing, parity groups, or pool creation.
  - Hitachi vSphere APIs for Storage Awareness (VASA), which is used with vCenter only to provide storage details for vCenter to understand storage system capabilities.
- **SQL** — Hosts the SQL databases used by both UCP Director and your selected hypervisor manager.
- **AD1** — Included if UCP is not integrated with the production domain to host the following services:
  - Active Directory
  - DNS
- **WDS** — Hosts the following services:
  - Windows Deployment Service (WDS), which is used to deploy Windows images.
  - PXE Linux, which is used to deploy Linux images.
- **HTnM** — Hosts the Hitachi Tuning Manager (HTnM) service that is used to provide performance metrics about the storage system.

- **WSUS** — Hosts the Windows Server Update Services (WSUS) service.

Important: The proper functioning of these VMs is critical to UCP Director performance. As a result, while some configuration changes may need to be made to ensure that the services running on them function properly in their environment, they should not be used as a workstation. Any additional software that could disrupt their operation should not be installed.

Additional VMs and services will be added if UCP DOC and UCP Disaster Recovery have been added. For more information on UCP DOC and UCP Disaster Recovery, see Chapter 4, “UCP DOC and UCP Disaster Recovery,” on page 69.

In addition to the active VMs on the management block, there is a deployable OVF file that contains the workstation VM. It uses Windows Server 2012 R2 and can be freely edited to be used as needed. The primary purpose of it is to function as a workstation that is capable of accessing UCP resources in isolated installations where external workstations are not able to access UCP. If needed, it can be configured with an extra connection to function as a remote access server.

To see the VMs on the management block, when using:

- vCenter, your account must have UCP system administrator access. For more information on access credentials, see “Security” on page 65.

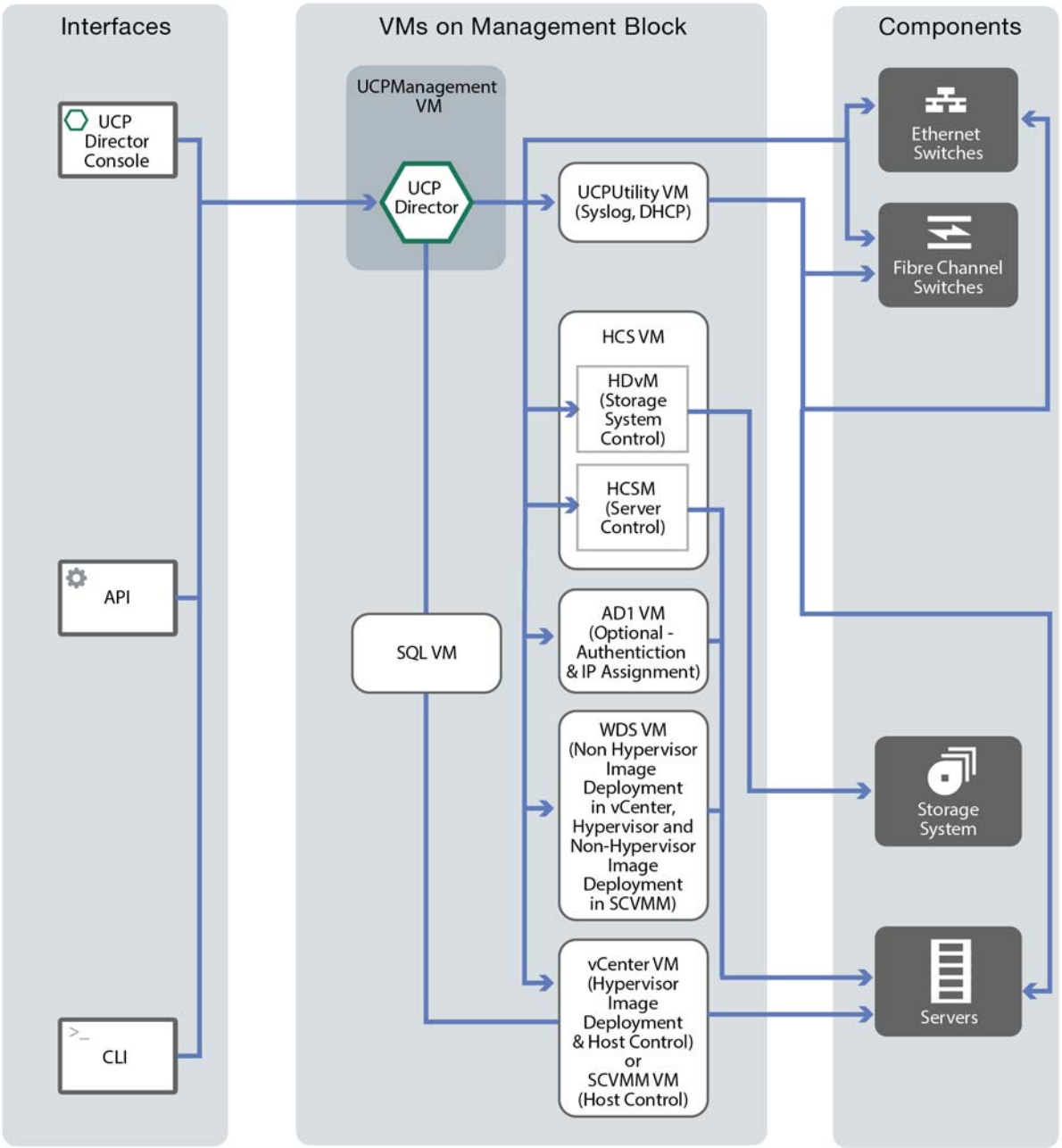
- SCVMM, you will need to add the clustered servers in the management block to a separate instance of Microsoft Windows Failover Cluster Manager.

For more information on the third-party services hosted on these VMs, see their respective documentation.

UCP is set to use the UTC time zone by default.

Important: When using UCP Director Console, the system time of the hypervisor manager will be displayed. As a result, when reviewing system logs, the difference in the time zone will need to be taken into account.

The following diagram depicts the major interactions between UCP Director and its supporting software with the system components.



Inventory

By adding physical and virtual components to inventory, UCP Director is able to perform end-to-end administration, provisioning, and monitoring of all components in inventory.

Switches

Depending on the configuration, UCP supports adding Ethernet, Fibre Channel, or converged switches to inventory to support networking.

For technical information on networking and switches, see "Networking and switches" on page 24.

For instructions on how to configure and administer switches, see Chapter 9, "Physical network administration," on page 129.

Storage system

UCP supports directly interfacing with one storage system in UCP inventory.

For technical information on the storage system, see "Storage system" on page 34.

For instructions on how to configure and administer the storage system, see Chapter 11, "Storage system administration," on page 161.

Chassis and servers

UCP supports adding both servers and the chassis that contain them to inventory.

For technical information on servers and chassis, see "Chassis and servers" on page 19.

For instructions on how to configure and administer servers and chassis, see Chapter 12, "Server administration," on page 189.

Server profiles

A server profile is assigned to each physical server to abstract the uniquely identifiable attributes of a server, such as the MAC, WWPN, WWNN, UUID, and IP addresses. These identifiers are used by other components to communicate with the host that is operating on the server.

For example, the WWPN is a unique identifier of a server that is added to a Fibre Channel zone on a Fibre Channel or converged switch and to the host storage domain (HSD) on the storage system. Through it, volumes that have been added to the HSD can be presented to the server. If a server were to fail, any volumes attached to the server would be disconnected.

By assigning the WWPN to a server profile instead of the physical server itself, the server profile can be assigned to another server if the first server fails or is replaced. This enables the second server to be able to access the volumes that the first server had access to and, for non-ESXi hosts, the replacement will boot using the previous server's boot volume.

Because server profiles abstract the network identities of a server, as well as the EFI settings that control how it boots, UCP is able to treat servers as logical identities. As a result, if a server fails, the server profile can be assigned to another server without having to manually reconfigure these dependencies.

In addition to assisting in recovering from a server failure, server profiles can be manually removed from a server. By manually removing a server profile, you can:

- Transfer the server profile to another server. If a server profile is applied to a different server, it will cause the second server to identify and function as if it were the first server. This can help when migrating from one server to another, such as when migrating hosts from one chassis to another.

- Store the server profile. By storing a server profile you can free the server up to function as another host by applying a different server profile to it. Then, when you want to return the server to its previous function, apply the first server profile again and it will resume operation.

A server in UCP cannot be deployed unless a server profile is assigned to it during deployment. To configure multiple servers with the same server profile settings, such as servers in a cluster, either manually create each server profile through UCP Director, or script the procedure using the CLI.

Upgraded servers without a server profile

If your UCP installation has been upgraded, server profiles will not be associated with the servers by default. This is done because applying a server profile requires rebooting the server. Instead, when a server does not have a server profile applied, you can manually virtualize the server by applying a server profile during a maintenance window.

To create and apply a server profile to a server, extract a server profile from the server that you want to apply a server profile to, and then apply the extracted server profile to the server.

Just to confirm, is this how this works? Should something more be said?

For more information on extracting a server profile, see "Extract server profile" on page 219.

Identity pools

UCP Director maintains pools of the IP addresses, MAC addresses, and WWNs that can be assigned to server profiles. In addition to these identity pools, UCP Director is also capable of auto-generating UUIDs. When a server profile is assigned to a server, these IDs are then associated with the server and are used to identify the server to network and storage resources. When assigned through a server profile, each server requires the following IDs:

- One IP address
- One UUID
- One MAC address for each NIC port
- Two WWPNs
- Two WWNNs

These IDs can either be drawn from UCP Director or manually entered. UCP Director maintains these identities as follows:

- IP addresses — A pool of static IP addresses that are designated when UCP is deployed. These IP addresses are mirrored on the DHCP server, which is configured with the IP address and corresponding MAC address during server profile application. UCP Director enables you to add IP address pools through the API and CLI.
- UUIDs — UUIDs are not maintained in a pool. Instead, they can be manually entered or dynamically generated each time they are added to a server profile.
- MAC addresses — MAC addresses are stored in a pre-configured MAC address pool. When a MAC address is associated with a server profile, UCP Director automatically assigns the corresponding IP address.

- WWPNs and WWNNs — WWPNs and WWNNs are stored in a WWN pool.

Service templates

Service templates standardize and simplify the configuration and deployment of hosts and clusters, ensuring uniformity. They assign the image, server profile, and define the basic storage, networking, and, when applicable, clustering configuration.

Different service template types are used depending on the type of host that is deployed. This enables the settings specified in the service template to be tailored to the host type. The following table lists each of the service template types, along with the hypervisor manager they are available to and the properties that can be set in them.

Template job	ESXi cluster	ESXi standalone	Hyper-V hosts	Windows	Linux	Custom
Available using vCenter	X	X		X	X	X
Available using SCVMM			X	X	X	X
Deploy image	X	X	X	X	X	
Form cluster	X					
Create/attach volume	X	X	X	X	X	
Apply trunk VLAN IDs to switches	X	X	X	X	X	X
Make and attach hosts to a VDS	X					

A service template can be used to configure and apply an image to multiple servers. Because of this, the settings that are configured in a service template are generic to the hardware, while the server profile contains identifiable information that is unique to the server.

This enables the easy configuration of servers or clusters by reducing the variability in server configuration. By including network and storage resource definitions with the service template, all servers in a cluster can be provisioned simultaneously. After being provisioned, all servers in the cluster will share access to the specified resources. This eliminates errors that can arise from configuration differences.

Service templates only affects the initial configuration of a server or cluster. After the server or cluster is operational, the server or cluster can be customized as needed. Because of this, service templates are only used

when they are applied to a server and a lasting relationship is not maintained between the service template and servers that have been deployed from it. As a result, any changes to a service template will not affect the hosts that it has already been applied to.

ESXi cluster service templates in vCenter

ESXi cluster service templates:

- Configure vMotion and the ESXi image that is deployed to all ESXi hosts in the cluster.
- Form a cluster with the deployed hosts.
- Configure HA settings.
- Define the VLAN IDs that will be assigned to the ports on the connected Ethernet switches and the VDS and associated port groups that the cluster will be attached to. One port group is created for each VLAN ID configured by the service template.
- Define the ESXi storage cluster settings, if selected.

ESXi standalone service templates in vCenter

ESXi standalone service templates configure the ESXi image that is deployed to hosts deployed from it. They also define the VLAN IDs that will be assigned to the ports on the connected Ethernet switches.

Hyper-V service templates in SCVMM

Hyper-V service templates deploy Windows with the Hyper-V role enabled, attach storage, and configure VLAN IDs the connected Ethernet switches. After deploying a Hyper-V service template, you can manually configure the hosts into clusters, configure virtual networking, and deploy virtual machines.

Windows, Linux, or custom host service templates

When creating a Windows, Linux, or custom host service template, you can define the VLAN configuration that will be applied to the Ethernet switches that the host is connected to. For Windows and Linux service templates, the boot and data volumes as well as the image that will be applied to the host is also defined.

Instead of defining the image or storage configuration, a custom host service template is used to configure the physical server so that you can manually attach storage and install an image.

Images

Images are applied to a server to enable it to function as a host. To ensure that images are up-to-date, UCP Director administers and automates the image deployment process. In addition, when using vCenter, UCP Director also automates the image update process. This saves you from having to manually check and update images when updates become available.

Hyper-V, Windows, and Linux images

Hyper-V, Windows, and Linux images and image deployment are administered through Windows Deployment Server (WDS). This includes the boot process, as well as adding, updating, or removing images.

For more information about how to administer images, see Chapter 6, "Images overview," on page 91.

Refreshing inventory

UCP automatically scans and refreshes inventory to make sure component status, configuration, and relationships are up-to-date. Updated information will not be displayed until the job is complete.

Different components have different refresh intervals. The following table lists refresh interval for each component type:

Component	Refresh interval
Servers	30 minutes
Switches	30 minutes
Storage system	30 minutes
Images	User configurable

You can also manually initiate an inventory refresh. For information on how to manually refresh:

- Switch inventory, see "Refreshing switch inventory" on page 142.
- Storage inventory, see "Refreshing storage inventory" on page 180.
- Server inventory, see "Refreshing server inventory" on page 203.

- Image inventory, see “Refresh image inventory” on page 119.

Note: Only manual and failed automatic inventory refreshes are reported to your hypervisor manager.

Standard component properties

UCP Director monitors and reports numerous properties regarding each component in the system. Some properties are unique to the component being monitored, while other properties are standard for most components in UCP. The following is a list of standard component properties that are monitored by UCP Director:

- **Monitoring State** — The monitoring state of the component. The monitoring state of the element is reported as follows:
  - OK — UCP Director is able to communicate with the element and it is functioning properly.
  - Error — UCP Director is able to communicate with the element and it is reporting an error.
  - Warning — UCP Director is able to communicate with the indicator but there is a issue. In the case of storage, server, or chassis resources, this means that the corresponding element manager has detected a warning. In the case of storage pools, this means that the storage pool is shrinking.
  - Unknown — UCP Director is not able to communicate with the element.

  For more information on monitoring state, see “Monitoring” on page 54.

- **Firmware** — The software version of the component. This is dynamically retrieved from the component.

- **Available Firmware** — If applicable, the updated version of the software version of the component that is available to be applied if the firmware is updated.

- **ID** — The UCP Director ID number assigned to the component. This number is dynamically assigned by UCP Director to the component.

- **Global ID** — The fully qualified UCP Director ID associated with the component. This identifies the instance of UCP Director that it is associated with, as well as the element type and type ID.

Monitoring

UCP Director monitors the status and health of all hardware components in UCP. It also monitors performance of Ethernet switches, Fibre Channel switches, converged switches, and the storage system. This enables you to detect when a component may be ready to fail and replace it without impacting the operation of UCP.

Monitoring indicators and monitoring state

UCP Director tracks both health and performance details for Ethernet switches, Fibre Channel switches, converged switches, and the storage system as monitoring indicators. Health and performance data for chassis and servers is tracked through HCSM. UCP Director records the following monitoring indicator types for each of these components, as follows:

- Health — Data regarding the status of a component that impacts the functionality of a component, such as whether or not that component has generated an error or warning.

- Performance — Data regarding the performance of a component that may or may not impact the health of a component, such as the throughput of a port.

- Composite — An aggregate of health and performance monitoring.

Monitoring the health and performance of each hardware element individually gives you:

- Visibility into the hardware characteristics of UCP

- Rapid discovery of infrastructure issues

- Awareness of the health and performance characteristics of UCP components

The overall, cumulative health of a component. For Ethernet switches, Fibre Channel switches, converged switches, and the storage system, this is an aggregate of all health and performance monitoring indicators related to the component. For servers, this information is retrieved from HCSM.

Note: For a performance monitoring indicator to be used in calculating the monitoring state of a component, the threshold of that indicator needs to be set using the API or CLI.

Thresholds

UCP Director enables you to set thresholds for performance monitoring indicators through the API and CLI. Thresholds enable you to indicate when the monitoring state of a component will be reported as healthy, or when a warning or error message will be generated.

Threshold values are not an industry standard and acceptable ranges are unique for each environment. Before setting thresholds, determine what monitoring indicators you want to set thresholds for and what the values should be.

For more information on setting performance metrics, see:

- *UCP Director API Reference*
- *UCP Director CLI Reference*

SNMP monitoring

When enabled, UCP monitors SNMP traps related to the hardware components that are added to inventory. This enables UCP Director to report events related to SNMP traps from the hardware to vCenter. SNMP traps are also used to feed health monitoring indicators. For more information on health monitoring, see “Health monitoring” on page 60.

Natively, server resources are monitored by HCSM. UCP Director passively monitors the SNMP traps sent by HCSM. Because UCP Director does not make any changes to the element manager, all changes must first be manually made in HCSM before being made in UCP Director.

Storage resources are monitored by the storage system. UCP Director does not make any changes to the storage system, and instead passively monitors the SNMP traps sent by the storage system. Because UCP

Director does not make any monitoring changes to the storage system, all changes must first be manually made in the storage system before being made in UCP Director.

SNMP settings are set and configured in the switches in inventory directly by UCP Director.

UCP Director updates SNMP settings in switches as follows:

- As new switches are added to inventory if SNMP monitoring is enabled.
- As switches are removed, UCP Director removes SNMP settings, including the account used for SNMP communication.
- When refreshing inventory, if SNMP monitoring is disabled, UCP Director removes the SNMP configuration from the corresponding switches.

UCP Director configures switches to report SNMP traps to the IP address that UCP uses to listen to SNMP traps.

Important: When configuring SNMP settings or monitoring mode on switches, UCP Director needs to be able to communicate with all switches of the corresponding type. To communicate with a switch, the switches must be turned on and active. Switches that UCP Director is unable to communicate with will not be updated until communications resume during an inventory refresh.

The SNMP monitoring mode can be adjusted for the following element types:

- Compute — All elements inside a chassis: servers, as well as fan, management, power, and server modules.
- Storage — The storage system, as well as the storage system processor, parity groups, pools, drives, and ports in the storage system.
- Ethernet switches — The Ethernet switches and Ethernet switch ports.
- Fibre Channel switches — The Fibre Channel switches and Fibre Channel switch ports.
- Converged switches — The converged switches and Fibre Channel, Ethernet, and FCOE ports.

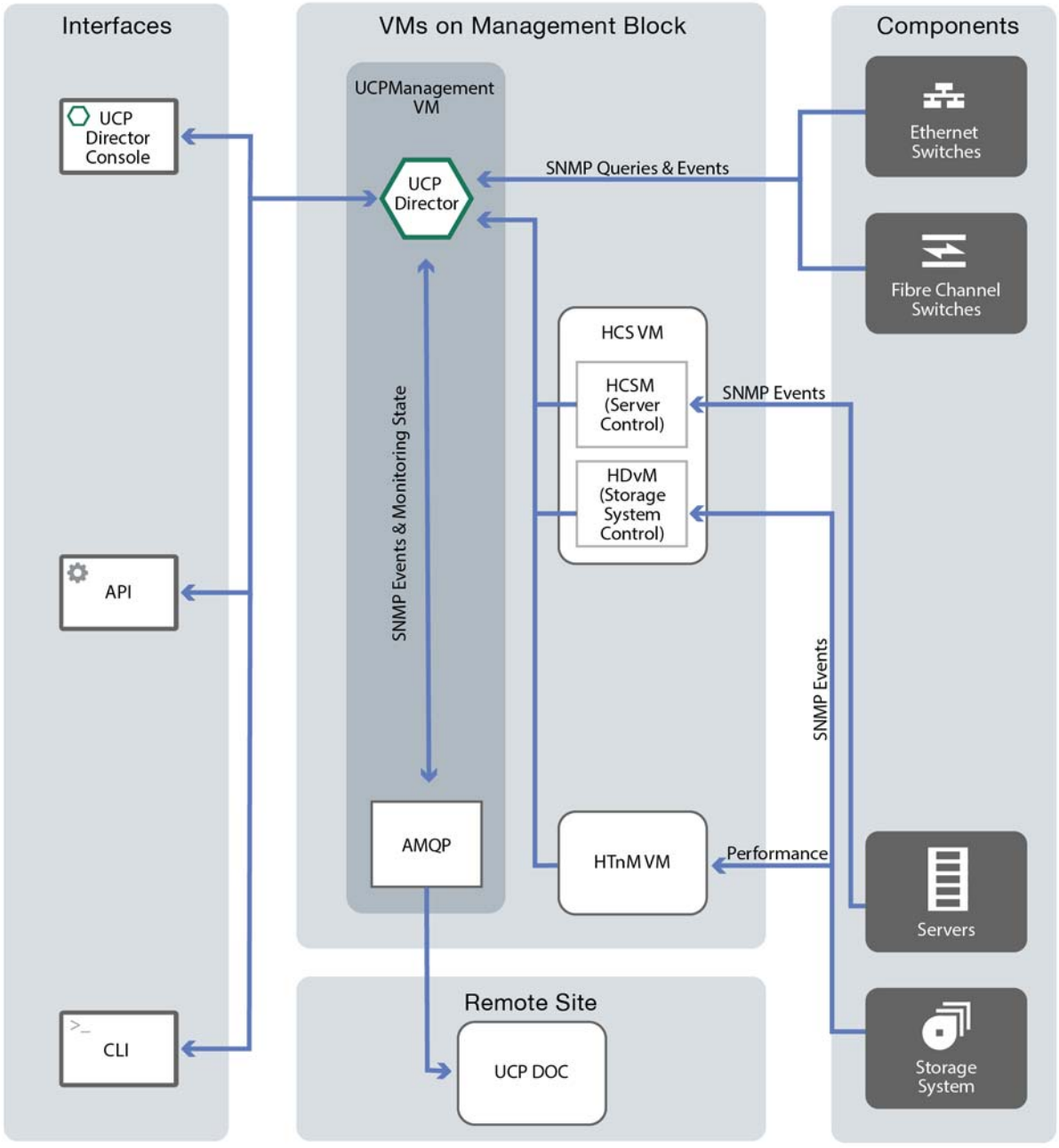
When performing maintenance on a component, you may want to disable monitoring or reporting to avoid receiving component errors that you are aware of. You can select the following monitoring modes:

- Monitoring and reporting — All SNMP events received are logged in the syslog. Events that are received are forwarded to the hypervisor manager and aggregated to form the overall health state of a resource type.
- Monitoring only — All SNMP events received are logged in the syslog. Events are not forwarded to the hypervisor manager.
- Monitoring off — Events are not received or logged in the syslog. Events are not forwarded to the hypervisor manager.

Notes:

- Monitoring needs to be enabled for reporting to be enabled.
- By default, SNMP monitoring and reporting are enabled in UCP.
- For more information regarding SNMP version support, see *UCP Release Notes*.

Both monitoring and reporting must be enabled for UCP Director Console to display SNMP events and the current monitoring state of elements. The following diagram shows how monitoring and event information are received by UCP Director and UCP DOC.



UCP Director refreshes monitoring indicators every 5 minutes.

Note: Only manual and failed refreshes are reported in your hypervisor manager.

Performance monitoring

UCP Director uses SNMP to monitor switch performance, and monitors HTnM for performance information, as follows:

- SNMP — Performance data from SNMP queries is used to populate switch performance monitoring indicators. For UCP Director to be able to monitor health and performance data from switches, SNMP monitoring and reporting needs to be enabled.

- HTnM — Performance data from HTnM is used to populate storage system performance monitoring indicators.

In addition to the data received from health monitoring indicators, performance monitoring indicators can be used to determine potential component failures. For example, the **Link Failures** performance monitoring indicator can be monitored to look for an increase in failures, which may indicate a component is failing.

Data from performance monitoring indicators is consolidated every 30 minutes.

Performance data can be collected from either the UCP Director API or UCP Director CLI, or viewed in UCP Director Console. If you use VMware vCenter Operations Management Suite (vC Ops) with vCenter as your hypervisor manager, you can also view performance data in Hitachi Converged Adapter for VMware vCenter Operations Management Suite (HCA for vC Ops).

Performance data for each performance monitoring indicator in UCP Director Console is displayed graphically.The information shown on these graphs is different based on the component and performance monitoring indicator being viewed. For more information on:

- Switch performance monitoring, see “Switch performance monitoring in vSphere Web Client” on page 137.

- Storage system performance monitoring, see “Storage system performance monitoring in vSphere Web Client” on page 167.

For more information on HCA for vC Ops, see *HCA for vC Ops Administration Manual*.

Health monitoring

Health monitoring indicators enable you to monitor the status of different aspects of each component. By monitoring component health, UCP Director is able to detect warning or error conditions that can lead to failure.

The overall health of a component is displayed as its monitoring state.

The monitoring state of a component includes health and performance data. As a result, degraded performance can contribute to a downgrade of the monitoring state. For example, a steady or severe decline in the performance of a component could indicate a concern regarding the health of that component.

Component monitoring state is also presented to UCP DOC. This enables UCP DOC to aggregate and display the health status of multiple UCP sites. For more information on UCP DOC, see Chapter 4, “UCP DOC and UCP Disaster Recovery,” on page 69.

For more information on monitoring states, see “System status” on page 80.

For UCP Director to be able to monitor the health of switches in UCP Director, SNMP monitoring and reporting needs to be enabled. Server health information is received from HCSM and storage health information is received from HDvM.

Management monitoring

When using vCenter, the servers that compose the management block and the VMs hosted on it are visible when you are logged in with UCP system administrator access.

When using SCVMM, the health of the clustered servers that compose the management block can be viewed using Windows Failover Cluster Monitor on an external server or workstation.

vCenter alarms

If you are using vCenter as your hypervisor manager, events can also trigger a vCenter alarm. In addition to the default vCenter alarms, UCP Director has incorporated alarms for physical switches, the storage system, servers, and the chassis.

Note: UCP alarms that are added to vCenter are prefaced with **Hitachi**.

For more information on events, see "Events" on page 62.

Alarms can be triggered by SNMP events, or by events received from an element manager. An alarm can also be triggered by the monitoring state of a component.

When an alarm is triggered, an email is sent to the notification email address that corresponds to the component triggering the alarm. These email addresses were setup when UCP was fist installed, and can be updated by modifying the corresponding alarm.

Some alarms have multiple editable triggers, depending on the status of the element being monitored. For example, a notification can be sent when the status is set to warning, and again when it is set to alert. Another email may be sent when the component is back to normal.

For more information on UCP alarms, see Appendix C, "VMware alarms," on page 329.

Jobs, events, and reporting

UCP Director tracks user-initiated actions as jobs. These jobs are then reported to the hypervisor manager. This section contains information on:

- Jobs
- Events
- Reporting and syslogs

Jobs

For each job, the following information is tracked:

- **Name** — The name of the job.
- **Target Type** — The resource type that the job is performed against.
- **Target ID** — The UCP ID of the resource that the job is performed against.
- **Status** — The status of the job.
- **User** — The user who initiated the job.
- **Date Time** — The date and time that the job started.

For a list of all jobs that can be generated by UCP, see Appendix A, “Jobs,” on page 255.

Note: UCP Director jobs are reported ask tasks in vCenter.

With the exception of performing more than one storage operation on a server, only one job can be performed on an element at a time. To perform a second job against an element, the first job must finish.

UCP Director purges jobs from its database according to the data retention policy of the hypervisor manager you use. For example, if you are using SCVMM with the default retention policy of 90 days, UCP Director will internally delete records of jobs that are 90 days old.

Events

UCP Director tracks events that are initiated by both scheduled and user-initiated jobs, as well as SNMP traps that are sent from hardware components.

When an event is initiated by:

- A job, UCP Director records the event and associates it with the corresponding job and target resource. Each job is associated with one or more events, depending on the complexity of the job.

- An SNMP trap, UCP Director records the event and associates it with the target resource.

After recording an event, UCP Director then forwards it to your hypervisor manager. For each event, the following information is tracked:

- **Description** — A description of the event.
- **Severity** — The severity of the event. Possible values are:
  - **Info** — Informational only. No action needs to be taken.
  - **Warning** — Abnormal but non-critical behavior has occurred. Actions may need to be taken to identify and correct the issue.
  - **Error** — The hardware is not functioning correctly. Action likely needs to be taken to correct the issue.
- **Date Time** — The date and time that the event occurred.
- **User** — The user who initiated the action that triggered the event.
- **Target Type** — The resource type that the event is associated with.
- **Target ID** — The UCP ID of the resource that the event is associated with.

For more information on UCP events, see Appendix B, “Events,” on page 265.

UCP Director uses the data retention policy of the hypervisor manager you use to determine how long events should be retained.

Reporting and syslogs

Syslogs are collected and consolidated in the /logs folder of the UCPUtility VM. Syslog files are organized into sub folders based on the IP address of source.

An audit log is maintained in the syslog for the related component or device. Audit log records can be found by filtering for entries that begin with *AUDIT:*.

Tip: Configure individual hosts to report the syslog to the UCPUtility VM to consolidate host syslogs.

Firmware update management in vSphere Web Client

When using vSphere Web Client, UCP Director is able to facilitate firmware updates on switches, chassis, and servers. This simplifies the process of updating firmware and helps to ensure system compatibility as updates are applied.

All firmware updates are distributed in a bundled firmware update file, which is tested and approved by HDS prior to distribution. When an update has been approved, HDS support will contact you to let you know that the update is available.

Before updating component firmware, you will first need to update the available firmware in UCP Director. To do this, retrieve the firmware update file from HDS and copy it to the update repository in UCP. For information on how to copy the bundled firmware update file, see "Updating available firmware in vSphere Web Client" on page 85.

Only one firmware update file can be present at a time. Each time a firmware update file is copied to the update repository, it will replace the previous firmware update file.

After updating the available firmware in UCP Director you can apply the available updates to individual components. Only users with UCP administrator privileges are able to update element firmware. For instructions on updating:

- Switches, see "Updating Ethernet and Fibre Channel switch firmware in vSphere Web Client" on page 144.
- Chassis, see "Updating chassis firmware in vSphere Web Client" on page 201.
- Servers, see "Updating server firmware in vSphere Web Client" on page 202.

To ensure system stability, no operations that change the configuration of a component will be possible in UCP Director when updating firmware, such as changing the VLANs on an Ethernet switch. Any component being updated will also be temporarily non-responsive, and redundant components will be used to ensure that the process does not disrupt system operations.

For example:

- Switches are updated one at a time to ensure that redundant access to is available.
- Chassis updates are staged across redundant SVP controllers to ensure that the chassis never loses management access.
- When updating all server firmware, servers in an ESXi cluster will be updated one at a time so that virtual machines can be gracefully migrated during firmware updates. If the server is a standalone server, updates should be scheduled during a maintenance window.

In the event of a failure when updating multiple components, the update process will cease and no further components will be updated. After the issue is fixed, the remaining components will be able to be updated.

Security

UCP can function as a part of its own domain, or it can be integrated into an existing domain.

When using the AD1 VM, a trust relationship may be configured between UCP and the production domain, but this is not required.

When integrated into an existing domain, the AD1 VM is not used and the organizational units (OU) and users that UCP Director uses must be added to the production domain. These accounts are configured in UCP Director and your hypervisor manager when UCP Director is deployed.

In addition to the AD accounts, UCP Director also uses some local accounts to access and administer internal components. This includes chassis, switches, and the element managers (HCSM and HDvM).

User authentication

To administer resources in UCP Director, you must have an account in AD and sufficient permissions in your hypervisor manager. Access to individual resources is role-based. To administer components in UCP, you need to be added to the AD group that corresponds to the appropriate role. The role that you need access to is different, depending on the hypervisor manager that you use.

AD accounts

UCP requires the following service accounts when accessing its supporting services and software: svc_sql, svc_ucp, svc_vcntr, and ucp_wdsdeploy. For security compliance, their passwords can also be changed at regular intervals. These service accounts should not be disabled or deleted.

When using the AD1 VM, UCP includes the ucpadmin account that comes pre-configured with access to resources in UCP. In addition, when using vCenter, the following pre-configured accounts are also included:

- ucpNetworkAdmin
- ucpServerAdmin
- ucpStorageAdmin

Each of these accounts are added to their own AD group and can be edited as needed.

vCenter security

All access to vCenter is authorized by SSO (Single Sign On) whether using the integrated domain model or stand-alone UCP. Authorization from multiple sources into vCenter is aggregated through SSO.

All user access in UCP Director is managed through AD and authorized by SSO (single sign on). To administer components in UCP, your account needs to be added to the AD group that corresponds to the appropriate vCenter role, as follows:

- UCP System Administrator — Is able to administer all portions of UCP. In addition, service template management, firmware upgrades, and performance monitoring are only available to the UCP system administrator.
- UCP Network Administrator — Is able to administer all Ethernet switches in UCP.
- UCP Server Administrator — Is able to administer all servers and server images in UCP.
- UCP Storage Administrator — Is able to administer the storage system and all Fibre Channel switches in UCP.

For a list of the privileges that these roles are configured to have, see Appendix D, “VMware privileges,” on page 333.

The following is an overview of each privilege added by UCP Director:

- UCP View — Enables read-only viewing access to UCP Director.
- UCP.SystemAdministration — Enables full UCP Director orchestration access.
- UCP.ServerAdministration — Enables server orchestration access.
- UCP.StorageAdministration — Enables storage system orchestration access.
- UCP.NetworkAdministration — Enables access network orchestration access.
- UCP.ServerConsole — Able to use the console feature to access HCSM, servers, and chassis.
- UCP.StorageConsole — Able to use the console feature to access HDvM.
- UCP.NetworkConsole — Able to use the console feature to access Ethernet switches.
- UCP.Service — Used internally by the svc_ucpdcntr account.

UCP Director enables the management of hardware elements in vCenter that vCenter does not natively support, such as Fibre Channel and Ethernet switches. Because vCenter does not natively support them, they are not able to be managed like other elements at the folder or cluster level. To manage these elements, UCP Director requires credentials with administrative access to the element to be added to it.

Tips:

- When customizing roles, consider cloning an existing role instead of modifying it directly.
- Simplify user role management by assigning vCenter roles to Active Directory groups instead of individual users.

To have view-only access to objects in UCP, you need to:

1. Create a new role in vCenter.
2. Assign the UCPView privilege.
3. Grant an AD user or group access to the role.

SCVMM security

In SCVMM, UCP uses the built-in Administrator role to administer access to all UCP resources. As a result, to be able to view or perform any operation in UCP, your account will need to be added to the Administrator role. To manage hardware elements, like switches, that are not natively supported by SCVMM, UCP Director requires credentials with administrative access to the elements that are added to it.

4

UCP DOC and UCP Disaster Recovery

UCP Director Operations Center (DOC) is a powerful tool that enables you to monitor and review the status of one or more UCP installations, or sites, from a single window. By integrating it with UCP Disaster Recovery, it also enables the administration and automation of volume replication between sites.

This chapter contains an overview of UCP DOC and UCP Disaster Recovery.

About UCP DOC and UCP Disaster Recovery

When you have more than one UCP site that you monitor, you can use UCP DOC to view the status of all of your installation from a single window. If you have also worked with HDS personnel to configure your sites for disaster recovery, then you can also use UCP DOC to manage UCP Disaster Recovery.

For more information on UCP DOC and UCP Disaster Recovery, see *UCP DOC Administration Manual*.

UCP Disaster Recovery storage considerations

When using UCP Disaster Recovery, one site will be designated as the protected site, and one will be designated as the recovery site. Volumes are replicated from the protected site to the recovery site. Depending on the configuration, UCP Disaster Recovery can take up significant storage resources at each site to accommodate:

- Journal volumes if using asynchronous replication to record changes.
- Test volumes at the recovery site to accommodate testing recovery volumes without interrupting replication.

For more information on replication and UCP Disaster Recovery, see *UCP DOC Administration Manual*.

Part II: Using UCP Director

This part contains the following chapter:

5

UCP Director Console

UCP Director Console is integrated into your hypervisor manager. This enables it to function as a seamless interface between the hypervisor manager, UCP Director, and the UCP system components.

Because each hypervisor and each hypervisor client functions differently, UCP Director Console also functions differently depending on the available feature set and the interface used.

This chapter explains how to use UCP Director Console to administer UCP Director.

UCP Director Console permissions

To access UCP Director Console, you must be logged in with an AD account that has sufficient permissions to UCP Director. For more information on access requirements, see "Security" on page 65.

Connecting to UCP Director Console

Because UCP Director Console is tightly integrated into your hypervisor manager, it is accessed differently depending on the hypervisor manager that you use.

Depending on the hypervisor and interface you use, however, certain features may or may not be available. The following table lists the features that are available by hypervisor and interface:

Feature	vCenter		SCVMM	Brocade Ethernet and Cisco Ethernet	Cisco converged
	vSphere Client	vSphere Web Client			
Status Monitor page	X	X	X	X	X
Servers table	X	X	X	X	X
Images table	X	X	X	X	X
Storage System page	X		X	X	X
Storage System table		X		X	X
Ethernet Switches table	X	X	X	X	
Fibre Channel Switches table	X	X	X	X	
Converged Switches table					X
Service Templates table	X	X	X	X	X
Server Profiles table	X	X	X	X	X
Identity Types page	X	X	X	X	X
Chassis page		X		X	X
Firmware updates		X		X	

Accessing UCP Director Console in vCenter

When using vCenter, you can access UCP Director Console through both vSphere Client and vSphere Web Client. To access UCP Director Console from either interface, from the **Home** screen, click on the **UCP Director** icon.

When using vSphere Web Client, certain pages may require you to have accepted a security certificate. To accept the security certificate, navigate to the following page in a web browser, where <UCPManagement> is the IP address of the management VM, and accept the indicated certificate:

```
https://<UCPManagement>/ui
```

Accessing UCP Director Console in SCVMM

When using SCVMM, you need to first import UCP Director Console as an SCVMM add-in. You can import UCP Director Console on any workstation that can access UCP Director. If UCP has been setup without remote access, you can import UCP Director Console on the workstation VM.

To import UCP Director Console as an SCVMM add-in:

1. Download the UCP Director Console installer by navigating to the following URL in a web browser, where <UCPManagement> is the IP address of the UCPManagement VM:

   ```
   https://<UCPManagement>/ui/extension/
   get?Platform=SCVMM&Client=UiConsole&Version=V2012R2
   ```

2. Save the HitachiUCPDirectorSCVMMPlugin.zip file.

3. Open SCVMM and connect to the SCVMM VM using an account that has been added to the SCVMM administrator role.

4. Use the SCVMM **Import Console Add-in** function to import the *HitachiUCPDirectorSCVMMPlugin.zip* file as an SCVMM.

After importing, restart SCVMM and access UCP Director Console using the **UCP Director** icon.

When using SCVMM, certain pages may require you to have accepted a security certificate. To accept the security certificate, navigate to the following page in a web browser, where <UCPManagement> is the IP address of the management VM, and accept the indicated certificate:

```
https://<UCPManagement>/ui
```

Using UCP Director Console

Depending on the hypervisor manager and client that you use, UCP Director Console has different pages and tables, as follows:

- **Status Monitor** page, as explained in "System status" on page 80.
- **Ethernet Switches**, **Fibre Channel Switches**, and **Converged Switches** tables, as explained in "Viewing switch inventory" on page 131.
- **Storage System** page or table, as follows:
  - In vSphere Web Client, the storage system is displayed on the **Storage System** table.
  - In SCVMM and vSphere Client, the storage system is displayed on the **Storage System** page.

  For more information on the storage system, see "Viewing the storage system" on page 163.
- **Servers** table, as explained in "Viewing server inventory" on page 193.
- **Chassis** table, when using vSphere Web Client, as explained in "Chassis" on page 196.
- **Server Profiles** table, as explained in "Viewing server profile inventory" on page 210.
- **Identity Types** page, as explained in "Identity types" on page 214.
- **Images** table, as explained in "ESXi image packages in vCenter" on page 121.
- **Service Templates** table, as explained in "Viewing service template inventory" on page 225.

All information in UCP Director Console can be accessed through these tables and pages.

Note: The hypervisor search box is not able to search UCP Director inventory.

At the top of UCP Director Console are the following bars:

- Information bar — A black bar at the top of some pages that contains the **Inventory** and **Help** menus.
  - The **Inventory** menu can be used to access different pages in UCP Director Console.
  - The **Help** menu contains links to view information about UCP and download the UCP Director CLI installer. It also contains links to the following product books:
    - *UCP Administration Manual*
    - *UCP Pre-Installation Requirements and Configuration*
    - *UCP Director CLI Reference*
    - *UCP Director API Reference*
    - *UCP Director Third-Party Copyrights and Licences*

    In addition, when using vCenter as your hypervisor manager, the following product books are available:
    - *HCA for vC Ops Administration Manual*
    - *HCA for vC Ops Third-Party Copyrights and Licenses*

    For more information on downloading the UCP Director CLI installer, see "Downloading the CLI" on page 78. For more information on viewing about and support information, see "Viewing about and support information" on page 78.
- Navigation bar — When using vSphere Client or SCVMM, a gray bar that appears under the information bar. It contains icons that are used to navigate among the major tables and pages in UCP Director Console, as follows:
  - **Status Monitor** icon () — Used to display the **Status Monitor** page.
  - **Servers** icon () — Used to display the **Servers** and **Images** tables.

- **Storage System** icon () — Used to display the **Storage System** page or table.
- **Ethernet Switches** icon () — Used to display the **Ethernet Switches** table.
- **Fibre Channel Switches** icon () — Used to display the **Fibre Channel Switches** table.
- **Converged Switches** icon () — Used to display the **Converged Switches** table.
- **Provisioning** icon () — Used to display the **Service Templates** and **Server Profiles** tables and the **Identity Types** page.
- **Settings** icon () — Used to display configure UCP Director settings. Only visible when viewing the **Status Monitor** page. For more information on the **Status Monitor** page, see "UCP Director settings" on page 82.

The icons on the navigation bar change color to reflect the aggregate of the monitoring state for each element of the indicated type. If any component of a particular site is different from the others, UCP Director will display the most severe value, such as error or warning.

Downloading the CLI

To access the UCP Director CLI, first download the UCP Director CLI installer. To download the UCP Director CLI installer, from the **Help** menu on the information bar, click on the **Download CLI** link. For more information on the UCP Director CLI, see the *UCP Director CLI Reference* book.

Viewing about and support information

The **About** dialogue is used to display the UCP version, serial number, and support information. To display the **About** dialogue, from the **Help** menu on the information bar, click on the **About** button.

Working with data in tables

Tables in UCP Director Console work like other tables in your hypervisor manager. They display information related to the corresponding managed resources.

Resources that are displayed on each table are grouped by default criteria. Depending on the resource, some data columns may be hidden.

To hide or show columns on a table in:

- vSphere Web Client:

  1. Right-click on a column header.
  2. Click on the **Show / Hide Columns** link.
  3. Select the columns that should be displayed.
  4. Click on the **OK** button.

- vSphere Client and SCVMM, right-click on a column header and select the columns that should be displayed.

You can also change the way records are filtered, grouped, and sorted as follows:

- To filter the records in a table, in the **Filter** field, begin typing the criteria that you want to filter the records by. As you type, the records in the table will automatically be filtered to only display those records that contain the string of text that you are typing.

- To change the way records in a table are grouped, select the criteria that you want the records to be grouped by from the **Group By** field. For example, to have all of the servers on the **Servers** panel grouped by the cluster that they are a member of, select the name of the cluster from the **Group By** field.

- To change the way that records are sorted in a table, click on the column that you want to sort the records by. Records will automatically be sorted in ascending order based on the criteria that the records are being grouped by. Clicking on the column again will sort the records in descending order.

You can perform actions against resources in UCP Director Console, such as a server, by right-clicking on the resource and then clicking on the action link. Depending on the type of resource being managed, different options will be available. For example, to open a console connection to a server, right click on the server, and then click on the **Console** link.

Some tables also have buttons at the top of the table that perform an associated action, such as to add an Ethernet switch, or to launch an element manager, such as HDvM. Clicking on one of these buttons performs the indicated action.

Refreshing UCP Director Console pages

When using vSphere Client or SCVMM, UCP Director Console does not refresh pages automatically. As a result, the status of inventory can change after a page is loaded without those changes being reflected in UCP Director Console. For example:

- The state of the hardware could change due to a power failure
- A server could be set to maintenance mode

To make sure that you are viewing the most current information, click on the **Refresh** button on the information bar.

System status

The **Status Monitor** page graphically displays the monitoring state of each hardware element managed by UCP. It also is used to display storage system usage and SNMP events.

To display the **Status Monitor** page, in:

- vSphere Web Client and SCVMM, from the navigation bar, click on the **Status Monitor** icon. For more information on the navigation bar, see "Using UCP Director Console" on page 76.
- vSphere Web Client, in the **Monitoring** section of the **Home** page, click on the **UCP Director** icon.

Individual monitoring state

The following elements are represented by a colored shape on the **Status Monitor** page: Ethernet switches, Fibre Channel switches, converged switches, servers, chassis, and storage pools. The monitoring state of the element is indicated by the color, as follows:

- OK — 
- Error — 
- Warning — 
- Unknown — 

For more information on monitoring state, see "Monitoring indicators and monitoring state" on page 54.

Moving the cursor over the square will display information related to the element. To view element summary information, when using:

- vSphere Client or SCVMM, click on the **View Summary** link.
- vSphere Web Client, click on the element icon.

For more information on a:

- Servers, see Chapter 12, "Server administration," on page 189.
- Chassis, see "Chassis" on page 196.
- Switches, see Chapter 9, "Physical network administration," on page 129.
- The storage system and storage pools, see Chapter 11, "Storage system administration," on page 161.

Storage system use

The physical and virtual storage system use are displayed in the **Storage System Utilization** section of the **Status Monitor** page. The:

- Physical use of the storage system is displayed on the **Physical Utilization** bar, which is broken into **Reserved** and **Free** space.

- Virtual use of the storage system is displayed on the **Logical Utilization** bar, which is broken into **Allocated** and **Unallocated** space.
- Actual use is displayed next to the legend below each bar.

For more information on the storage system use and the properties shown, see "Viewing the storage system" on page 163.

Events

The events shown on the **Status Monitor** page are only those events that are triggered by an SNMP trap. All SNMP events are reported on the **All Events** tab, while each of the hardware-specific event tabs only display the SNMP events that are related to the corresponding hardware object.

For each event shown on the status monitor page, the following properties are shown: **Description**, **Severity**, **Date Time**, **User**, **Target Type**, and **Target ID**.

To see events that are triggered by a scheduled or user-initiated job, from:

- vSphere Client, in the **Management** section, click on the **Events** link.
- vSphere Web Client, in the **Monitoring** section, click on the **Event Console** link.
- SCVMM, click on the **Jobs** link.

For more information on events, see "Events" on page 62. For a listing of each event generated by UCP Director, see Appendix B, "Events," on page 265.

UCP Director settings

The settings menu is used to configure universal settings that enable UCP Director to function. To access the settings menu, from:

- vSphere Client and SCVMM, click on the **Settings** icon on the **Status Monitor** page.
- vSphere Web Client, click on the **UCP Director Settings** button on the **Status Monitor** page.

Configuring SNMP settings

To configure SNMP settings:

1. From the settings menu, click on the link that corresponds to the type of SNMP settings that you want to modify.

   – For switches, click on **SNMP Settings: Ethernet**, **SNMP Settings: Converged Network**, or **SNMP Settings: Fibre Channel**.

     The top of the dialog displays the following read-only informational fields:

     • **Version** — The SNMP version of the protocol that is being sent to UCP Director for SNMP monitoring.

     • **Monitor IP Address** — The UCP Director IP address that listens to SNMP traps.

     After the **Version** and **Monitor IP Address** fields, the SNMP settings dialogs display the fields you use to configure SNMP settings. To configure SNMP settings, perform the following:

     • In **Authentication** section:

       – Select the protocol to use from the **Protocol** list

       – Type the username in the **Username** field

       – Type the password in both the **Password** and **Confirm Password** fields

     Note: If you select **NoAuth** as the authentication protocol, then you will not be able to enter a password.

     • In **Privacy** section:

       – Select the protocol to use from the **Protocol** list

       – Type the password in both the **Password** and **Confirm Password** fields

   – For the storage system or servers, on the corresponding **SNMP Settings: Storage** or **SNMP Settings: Compute** dialog:

The top of the dialog displays the following read-only informational fields:

- **Version** — The SNMP version of the protocol that is being sent to UCP Director for SNMP monitoring.
- **Monitor IP Address** — The UCP Director IP address that listens to SNMP traps.

After the **Version** and **Monitor IP Address** fields, the SNMP settings dialogs display the fields you use to configure SNMP settings. To configure SNMP settings, perform the following:

- In the **Community String** field, type the community string used to authenticate with the storage system.
- In the **Confirm Community String** field, type the community string again.

Important: Before setting the community string for storage or server SNMP settings, the SNMP settings need to be configured in HDvM or HCSM, respectively. The corresponding element manager also needs to be configured in UCP Director. For more information on configuring:

- HDvM, see "Configuring Hitachi Device Manager (HDvM)" on page 162.
- HCSM, see "Configuring Hitachi Compute Systems Manager (HCSM)" on page 190.

2. Click on the **OK** button.

Configuring monitoring mode

Before monitoring can be enabled, the corresponding SNMP settings need to be configured first. To configure SNMP settings, see "Configuring SNMP settings" on page 83.

To configure the monitoring mode:

1. From the settings menu, click on the **Monitoring Mode** link.
2. On the **Monitoring Mode** dialog, for each category of hardware element in inventory, select the monitoring mode as follows:

- To disable monitoring and reporting, select the **Off** option.
- To enable monitoring but disable reporting, select the **Monitoring Only** option.
- To enable both monitoring and reporting, select the **Monitoring and Reporting** option.

3. Click on the **OK** button.

Configuring AMQP credentials

Advanced Message Queuing Protocol (AMQP) is used to organize the jobs and messages generated by UCP Director. For security reasons, the credentials used to connect to it can be changed.

To configure AMQP credentials, after they have been configured on the AMQP server:

1. From the settings menu, click on the **AMQP Credentials** link.
2. On the **AMQP Credentials** dialog:
   - In the **Username** field, type the username with administrative access to the AMQP server.
   - In the **Password** field, type the password that corresponds to the specified account in the **Username** field.
3. Click on the **OK** button.

Updating available firmware in vSphere Web Client

Ethernet and Fibre Channel switch, as well as server and chassis firmware are distributed via a zip file from Hitachi Data Systems. This zip file is then uploaded to UCP Director, which updates the available firmware versions.

To update the available firmware:

1. From the settings menu, click on the **Firmware Update** link.
2. On the **Firmware Update** dialog, in the **Firmware Update Package** field, type the path of the firmware update file.
3. Click on the **OK** button.

After uploading the firmware bundle you will be able to manually update the firmware on each individual component.

For more information on firmware management in UCP Director, see "Firmware update management in vSphere Web Client" on page 64.

Configuring WDS & UCP IP addresses

The **WDS & UCP IP Addresses** dialog is used to configure the IP addresses of the WDS and UCP IP addresses. This should only be edited if the actual IP addresses of these VMs have changed. The:

- WDS IP address is used by the WDS server for the deployment of Windows and Linux images.
- UCP IP address is the IP address of the UCPManagement VM on the management network.

To update the WDS and UCP IP addresses:

1. From the settings menu, click on the **WDS & UCP IP Addresses** link.
2. On the **WDS & UCP IP Addresses** dialog:
   - In the **WDS IP Address** field, type the IP address of the WDS server.
   - In the **UCP IP Address** field, type the IP address of the UCP server.
3. Click on the **OK** button.

Configuring SCP server credentials

The **SCP Server Credentials** dialogue is used to configure the SCP server connection information. The SCP server is used by UCP Director to store firmware update packages and is accessed internally through the firmware update feature. For more information on the firmware update feature, see "Updating available firmware in vSphere Web Client" on page 85.

To update the SCP server credentials:

1. From the settings menu, click on the **SCP Server Credentials** link.
2. On the **SCP Server Credentials** dialog:
   - In the **IP Address** field, type the IP address of the SCP server.

- In the **Username** field, type the username with administrative access to the SCP server.

- In the **Password** field, type the password that corresponds to the specified account in the **Username** field.

3. Click on the **OK** button.

Part III: Image management

Management of Windows and Linux images in UCP is facilitated through a Windows Deployment Server (WDS) that is included in the UCP management stack. Management of ESXi images is handled through UCP which, in turn, utilizes vSphere tools. Automated deployment of images is initiated through service templates.

This part contains the following chapters.

6

Images overview

Operating system images are a foundational part of server deployment in UCP. The compute servers in UCP need to be deployed as hosts before they can accommodate production workloads. Service templates are used for deploying a variety of image types.

This chapter covers the following image-related concepts:

Hypervisor managers

If the hypervisor manager is SCVMM, all image deployment is executed by the WDS server. When it is vCenter, the deployment server will be WDS for Windows or Linux images, but ESXi images are deployed by vSphere's Auto Deploy. Non-hypervisor hosts are never included in the hypervisor manager's inventory, but they are managed through UCP's server inventory.

The following table explains the deployment types that are possible with each hypervisor manager:

Hypervisor manager	Hypervisor hosts	Non-Hypervisor hosts
vCenter	ESXi stateless only	Windows / Linux
SCVMM	Windows 2012 R2 SP1 with Hyper-V loaded	Windows / Linux

Windows Deployment Server

UCP includes a dedicated VM for hosting a Windows Deployment Server (WDS) server. This VM handles deployments of Windows and Linux images to non-hypervisor hosts. In SCVMM environments, WDS is also used when deploying Windows hypervisor hosts. The WDS service performs unattended installations with the help of answer files that you customize for your images.

UCP Director

The following section explains important details necessary for you to understand how images are managed using UCP Director.

Image permissions

To administer host images, your Active Directory account or group must:

- When using vCenter, be added to the UCP System Administrator role.
- When using SCVMM, be added to the SCVMM administrator role.

For more information on access requirements, see “Security” on page 65.

Image properties

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director records the following properties of each image.

Image name

For ESXi images, the image name is set when editing or cloning an image. For non-ESXi images the image name is obtained from WDS or from the image file.

Note: Never rename an ESXi image with any method other than UCP or vSphere's power CLI. If it was renamed with Windows file management, for example, UCP will not be able to detect and manage the image.

Image description

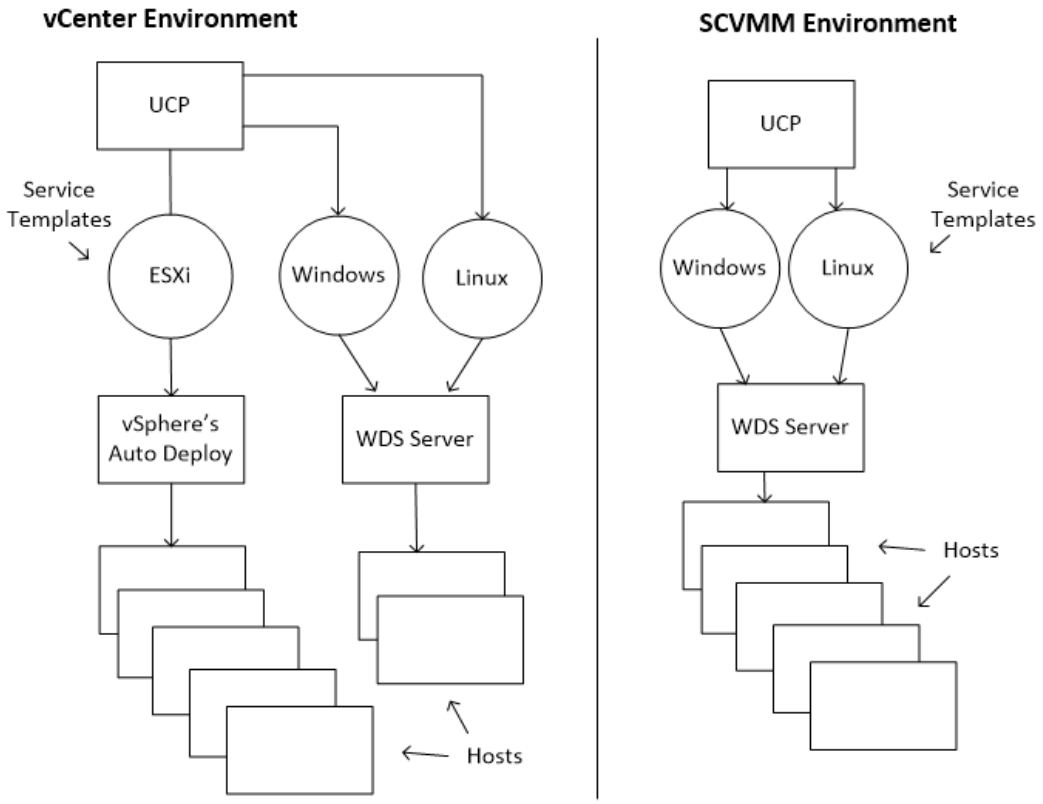
For ESXi images, the description is set when editing an image or when the image is cloned. Cloned ESXi images have the same description as the source image by default. For non-ESXi images the description is obtained from WDS or from the image file.

Image type

In UCP image inventory, the Image Type properties may be any of the following values:

Type	Description
Custom	A generic designator used by Custom service templates. This type is deployed to hosts that will receive an OS image by some means outside of UCP. For example, perhaps you wish to enable LPAR (Logical Partitioning) on the blade.
EsxiStateless	ESXi stateless images are deployed to system memory - not on a hard disk. The image loads over the network each time the server boots. In vCenter, ESXi images normally would be managed with power shell cmdlets. But UCP provides a graphical interface for executing those commands.
Linux	A Linux image that will be deployed by the WDS VM. The service template type will be Linux and the host will always be non-hypervisor.
Windows	A Windows image that will be deployed by the WDS VM. In SCVMM environments, this may be a hypervisor deployment if using a hypervisor service template.

The following diagram illustrates the various image types along with their deployment method. Images deployed through the WDS server will need to be added and configured manually.



ESXi images

ESXi images are the hypervisor image type used when using vCenter. UCP Director tracks ESXi images in both local and remote repositories in UCP inventory. ESXi images are divided into two types:

- UCP images, which are located in local inventory.
- Non-UCP images, which are located in external repositories.

Only UCP images can be deployed to a server. Non-UCP images can be cloned to local inventory. The cloned image in local inventory is then a UCP image that can be deployed to a server.

Images that have been deployed to a server can not be edited while they are applied to a server. To edit an image that is currently applied to a server, clone it and then edit the cloned image. When you have finished editing the cloned image, you can then deploy it to a server by individually assigning it to a server or making it the default image for a server type.

When booting an ESXi image, UCP Director uses Auto Deploy to deploy the image to the server. UCP Director does not attach a boot LUN when deploying an ESXi image. Instead, the stateless image is deployed each time the server boots.

UCP comes with an ESXi image that is designed for your servers. It has the HBA and CNA drivers, as well as the MPIO software for the HBA preloaded.

Default images

When using vCenter as the hypervisor manager, each server type used has a default image associated with it. By default, when a server boots, UCP Director automatically deploys the default image that is assigned to it. Only a local, ESXi UCP image can be used as a default image. The default image can be overridden for an individual server by deploying a specific ESXi, Windows, or Linux image to the server.

When a server is reset, if an ESXi image has been configured for that individual server, then vCenter will automatically deploy that image to the server. If an image has not specifically been configured for that server, then vCenter will deploy the default image for the server type.

ESXi image updates

All updates to ESXi images must either come from another ESXi image or from a VMware depot file in a repository. As a result, to add a custom driver, agent, or other package, it must be added to an image or a VMware depot. Images and VMware depots can then be added to a custom repository, which can be accessed as a URL or file share. Refer to VMware documentation for information regarding how to create VMware images, depot files, and repositories.

New ESXi images that include critical driver updates are distributed through an official Hitachi Data Systems external repository. Additional updates and patches can also be downloaded from VMware and added to ESXi images.

Each time UCP Director refreshes image inventory, it scans the contents of all images in external image repositories that have been added to UCP Director. When an updated version of any package in an active image is found, UCP Director will first clone the active image and apply the updated package to the cloned ESXi image.

After the images have been updated, UCP Director can then send an email describing the image or images that were cloned, the update that was found, and the new image names. Images that have been updated can then be reviewed before they are applied to one or more servers.

ESXi image properties

To see a list of typical ESXi image properties that UCP Director tracks, see Chapter 7, “Review commonly used image properties,” on page 111.

7

Prepare images for deployment

This chapter steps you through the procedure of adding your Windows images to the WDS server and adding the drivers that are necessary through the boot and installation phases of deployment

A sample CentOS image (version 6.4) is provided in the WDS VM. A script is also provided that configures WDS to deploy it. If you copy a Red Hat image to the WDS server, the same script can be used to configure it for deployment.

A default ESXi image is provided in UCP installations that use vCenter. Altering the ESXi images is only necessary when patches or updates are released by VMware.

This chapter covers:

Windows and Linux images

The section explains how to prepare Windows and Linux images for deployment. For a list of supported Windows and Linux operating systems versions, see the UCP Release Notes.

Add Windows images

If the image is Windows Server 2012 R2 SP1, it can be used for either hypervisor or non-hypervisor deployments. Other supported Windows versions are used only in non-hypervisor deployments. The template type dictates how the image will be deployed.

WDS handles Windows deployments with WIM files (Windows Imaging Format). For any Windows deployment, there are two WIM files, and the drivers must be added to **both**:

- boot.wim - Loads a WinPE environment from which the OS deployment is launched
- install.wim- Installs the operating system.

Note: If you plan to deploy both Windows Server 2012 R2 SP1 and Windows Server 2008 R2 SP1, be sure that you only have one boot.wim in WDS. Confirm that it is the boot.wim derived from Windows Server 2012 R2 SP1.

For a reliable installation, testing has shown that it's best to add the boot-critical drivers to *both* WIM files. This ensures that the drivers are available during all phases of deployment.

DISM (Deployment Imaging Servicing Management) is included in any system running Windows 8.1 or higher. This document assumes you will use the WDS VM to launch DISM.

For more information regarding DISM, see: http://technet.microsoft.com/en-us/library/hh824821.aspx. Alternatively the DISM cmdlets can be executed from PowerShell. For instructions, see: http://technet.microsoft.com/en-us/library/hh852126.aspx.

Determine which drivers to use

The following drivers are included on your service VM in the UCP management stack. Please review the following list to know what drivers are needed for your particular Windows image.

Windows 2008 R2 SP1

When the blades use separate FC and NIC devices:

- Hitachi Fibre Channel driver version 4.2.6.880 or above
- Emulex network driver version 4.1.334.25 or above

When the blades use the CNA device in a single-rack converged model of UCP, use:

- The STORPORT Miniport driver 2.74.014.001
- Emulex OneConnect NIC driver version 4.6.142.8

Windows Server 2012 R2 SP1

When the blades have a separate Fibre Channel HBA devices, use:

- Hitachi Fibre Channel driver version 4.4.8.1500 or higher
- Emulex network driver version 10.0.835.0

When the blades use the CNA device in a single-rack converged model of UCP, use:

- Emulex SCSI driver 2.76.2.1
- The Storport Miniport driver 2.44.3.1
- Emulex network driver version 10.0.835.0

To find these drivers, log into the UCP Service VM and open **E:\InstallMedia\WDS\CB500_Windows_Drivers**. Copy the necessary drivers to the WDS VM where you plan to use DISM.

Determine the driver injection method

Usually DISM is used for adding drivers to the install.wim and WDS is used for adding drivers to the boot.wim. But, in one type of environment, as explained in the following table, DISM must be used for both wim files because the /forceunsigned argument is required for the Hitachi FC driver.

Depending on your environment, indicated by columns in the table below, follow only the procedures that have a check mark in that column.

Procedure	UCP upgraded from 3.02 to 3.5 - Switch model is NOT converged		UCP 3.5 (no upgrade) - All switch models
	Image type - 2012 R2 SP1 or newer	Image type = Older than 2012 R2 SP1	Image type = Any supported Windows image
"Share your Windows images with the WDS VM" on page 101	✓	✓	✓
"Add drivers to install.wim (DISM)" on page 102	✓ **w/forceunsigned**	✓	✓
"Add drivers to boot.wim (DISM)" on page 102	✓ **w/forceunsigned**		
"Add the drivers to the boot image with WDS" on page 104		✓	✓
Chapter 8, "Refresh image inventory." on page 119	✓	✓	✓

Share your Windows images with the WDS VM

1. Place the Windows image so it can be accessed from the WDS VM, such as a network share.
2. Move the Hitachi Fibre Channel and Emulex network drivers from the UCP Service VM to the WDS VM, if they are not already there.
3. On the WDS VM, mount your Windows ISO by right-clicking the ISO and clicking **Mount**
4. Browse to view the contents of the mounted ISO
5. Copy the entire contents of the ISO onto a disk location where the files can be modified.
6. Open a cmd window and change directory to C:\Windows\System32. This is where DISM will be executed from.

Add drivers to install.wim (DISM)

1. Use the following command to get the 'Index' number of the version of Windows you wish to modify and use. The following case uses Windows Server 2008 R2 SERVERDATACENTER, which is cataloged as Index 5.

   dism /get-wiminfo /wimfile:C:\temp\sources\install.wim

2. Next, create a folder on the C: drive called 'mount'

3. Use the following DISM command to mount Index 5 (or other desired version of Windows) into the C:\mount directory.

   dism /mount-wim:C:\temp\sources\install.wim /MountDir:C:\mount /wimfile:C:\temp\sources\install.wim /Index:5

4. In the following commands, supply the location where you copied the drivers to. This example adds the Emulex (NIC) driver:

   dism /image:C:\mount /Add-Driver:C:\Drivers\Emulex\be2nd62.inf

   This example adds the Hitachi FC driver:

   dism /image:C:\mount /Add-Driver:C:\Drivers\HitachiHBA\hfcwdd.inf

   If the UCP system is an upgrade from 3.0.2 to 3.5, and the image is Windows 2012 R2SP1, use:

   dism /image:C:\mount /Add-Driver:C:\Drivers\Win2K2012R2\HitachiHBA\hfcwdd.inf /forceunsigned

5. Save the install image by running the following command:

   dism /unmount-wim /MountDir:C:\Mount /commit

6. The result is an install.wim file located in C:\temp\sources (or equivalent directory where you copied the Windows source files. This file will be added to WDS in section 3.

Add drivers to boot.wim (DISM)

This is only needed when the UCP system was **upgraded** from v3.0.2 to v3.5 **and** the installation image is **Windows 2012 R2 SP1** and the switch model is not converged. The WDS server (on a Windows 2012 system) will not add unsigned drivers to the boot.wim and the Hitachi FC driver is unsigned. The NIC driver is signed, but, to save time, you could add the NIC driver with DISM too.

In the following steps, you will use the same drivers that you added to the install.wim.

1. Use the following command to get the 'Index' number of the version of Windows you wish to modify and use. If you want a permanent installation of Windows (not Windows PE), select the index value corresponding to Microsoft Windows Setup (x64).

   dism /get-wiminfo /wimfile:C:\temp\sources\boot.wim

2. Use the following DISM command to mount Index 2 (or other desired version) into the C:\mount directory. Make sure you have permissions to access this file as Microsoft often marks boot.wim files as read-only by default.

   dism /mount-wim:C:\temp\sources\boot.wim /MountDir:C:\mount /wimfile:C:\temp\sources\boot.wim /Index:2

3. In the following commands, supply the location where you copied the drivers on the WDS VM. Example 1 is the Emulex (NIC) driver. Example 2 is the HBA (Fibre Channel) driver.

   dism /image:C:\mount /Add-Driver:C:\Drivers\latest\WS2k12R2\Emulex\ocnd64.inf

   dism /image:C:\mount /Add-Driver:C:\Drivers\latest\WS2k12R2\FC\hfcwdd.inf /forceunsigned

4. Save the boot image by running the following command:

   dism /unmount-wim /MountDir:C:\Mount /commit

   The result is a boot.wim file located in C:\temp\sources (or equivalent directory where you copied the Windows source files). Proceed with steps for adding Windows images to WDS. Then create boot and image unattend files and refresh UCP image inventory. You can skip the procedure **Add the drivers to the boot image with WDS** as this process was already done through DISM.

Add the modified Windows image to WDS

Two procedures in this section show how to add the install.wim and boot.wim files to WDS.

Add the install.wim

1. On the WDS VM, launch Windows Deployment Services. Right click **Install Images** and click **Add Install Image**.

2. Select **Create an image group named**, enter an appropriate name, and then click **Next**.

3. Click **Browse** and navigate to the **install.wim** file that you customized in c:\temp\sources.

4. Click on **install.wim**, click **Open**, and then click **Next**.

5. In the **Available Images** screen, choose the version of Windows that corresponds with the Index number you chose to mount and modify.

6. In the **Summary** screen, click **Next**. Progress is shown while the image is added to WDS.

7. When the image is successfully added, click **Finish**. The install image has now been added to WDS.

Add the boot.wim

1. Right click **Boot Images**, and then click **Add Boot Image**...

2. Click **Browse** and navigate to the **boot.wim** file.

3. Select the **boot.wim** file, click **Open**, and then click **Next**

4. Type a descriptive image name and click **Next**.

5. In the **Summary** screen, click **Next**.

6. When the image is added, click **Finish**. The image is now added under **Boot Images**

Add the drivers to the boot image with WDS

Drivers can be added to the Boot.wim in WDS with the following steps. The exception, as explained earlier, is if the WDS server operating system is older than Windows Server 2012 R2 SP1 and the image being modified is Windows Server 2012 R2 SP1.

1. In Windows Deployment Services, locate **Boot Images**. Right click the previously added boot image discussed earlier and choose **Add Driver Packages to Image**...

2. Click **Next**, and then click **Add**.

3. In the **Add Attribute** dialog box, change **Attribute Type** to **Driver Group Name**.

4. Select the driver name appropriate to the version of Windows you are provisioning, and then click **OK**.

5. Click **Search for Packages**, the two drivers are automatically selected, and then click **Next**.

6. Click **Next** in the **Summary** page. Progress will be displayed as drivers are added to the boot image. When it is complete, click **Finish**.

Create boot unattend and image unattend files

On the WDS server there are template copies of the boot unattend and image unattend files. In this section, you will make copies of these templates and customize them for your image. When making UCP service templates, you will choose the image unattend and boot unattend files that were edited for your particular Windows image.

If the passwords in the unattend files have to be encrypted, use the SIM tool (System Image Manager) which comes in the ADK from Microsoft. (Windows® Assessment and Deployment Kit – a free download).

Boot unattend files

Boot unattend files are located in the following folder on the WDS server:

D:\RemoteInstall\Boot\x64\Windows\BootUnattendFiles

For Windows 2012 boot unattend

1. Make a copy of **Windows2012DatacenterBootUnattend.xml** and place it in the folder specified above. Make the filename unique, like Windows2012DatacenterBootUnattend_ActiveCopy.xml.

2. Right click your copy and choose **Edit**.

3. Find the section **<component name="Microsoft-Windows-Setup"**

4. Edit your domain and the password for the built-in user named **ucp_wdsdeploy**.

```
<WindowsDeploymentServices>
    <Login>
        <Credentials>
        <Domain>_Edit.Your.Domain_</Domain>
        <Password>_AddPassword_</Password>
        <Username>ucp_wdsdeploy</Username>
```

5. Find the section **<ImageSelection>**

6. Edit the **ImageGroup** and **ImageName** values to match the names exactly as you created them in WDS.

```
<InstallImage>
    <ImageGroup>_EditGroupName_</ImageGroup>
    <ImageName>_EditImageName_</ImageName>
```

7. Find the section **<UserData>**

8. Enter the product key value for your Windows 2012 image.

```
<ProductKey>
    <Key>_Your_key_here_</Key>
```

For Windows 2008 R2 boot unattend

1. Make a copy of **Windows2008R2DatacenterBootUnattend.xml** and place it in the folder specified above. Make the filename unique, like Windows2008R2DatacenterBootUnattend_ActiveCopy.xml.

2. Find the section **<ImageSelection>**

3. Edit the **ImageGroup** and **ImageName** values to match the names exactly as you created them in WDS.

```
<InstallImage>
    <ImageGroup>_EditGroupName_</ImageGroup>
    <ImageName>_EditImageName_</ImageName>
```

Image unattend files

Templates of image unattend files are located in the following folder on the WDS server:

D:\RemoteInstall\Boot\x64\Windows\ImageUnattendFiles

For Windows 2012 image unattend

1. Make a copy of **TemplateWindows2012DatacenterImageUnattend.xml**, and place it in the folder specified above. Make the filename unique.

2. Right click your copy and click **Edit**.

3. Find the section **<settings pass="specialize"> <component name="Microsoft-Windows-Shell-Setup"**

4. Add the product key for your Windows 2012 image. It should match the key you entered in the boot unattend file earlier.
<ProductKey>_**Your_key_here**_</ProductKey>

5. In the same section, also modify:

```
<UserAccounts>
   <AdministratorPassword>
   <Value>_Add.Password.Here_</Value>
   <PlainText>false</PlainText>
</UserAccounts>
  <TimeZone>_Your.Time.Zone_</TimeZone>
  <RegisteredOrganization>_Your.Org_</RegisteredOrganization>
  <RegisteredOwner>_Your.Name_</RegisteredOwner>
```

   To save the password with encryption, use Microsoft System Image Manager (included in the Windows Assessment and Deployment Kit, or ADK). See http://technet.microsoft.com/en-us/library/cc766409%28v=ws.10%29.aspx.

6. Save and close the file.

For Windows 2008 R2 image unattend

1. Make a copy of **TemplateWindows2008R2DatacenterImageUnattend.xml** and place it in the folder specified above. Make the filename unique.

2. Edit the same values as listed in the previous section for Windows Server 2012.

3. Save and close the file.

Refresh UCP image inventory

After finishing the preceding steps, refresh the image inventory in UCP Director so that the Windows image is made available for use.

For more information, see "Refresh image inventory" on page 119.

Add Linux images

A CentOS image is provided in the WDS VM. A script is also provided that configures the CentOS image for deployment. The script is: D:\ ucpbaremetaltools \Add-LinuxIsoToWDS.ps1. Simply right-click the file and choose Open with PowerShell and answer the prompts. This prepares the default CentOS image for deployment. Afterwards, perform a manual refresh of UCP image inventory.

If you have your own distribution of Red Hat, a few extra steps are necessary. The following sections explain how to introduce your installation ISO to the WDS VM and get the proper drivers added.

Copy your Linux image file to the WDS server

Through a remote desktop session to the WDS server, copy your Linux ISO directly to the D drive of the WDS server. The script will later ask for its location.

Verify the latest Linux drivers are on the WDS server

1. On the WDS server, navigate to the **D:\RemoteInstall\Boot\x64\ Linux\Drivers** directory

2. You will see the folders: **RHEL6.2**, **RHEL6.4-HB1**, and **RHEL6.4-HB2**

3. Depending on your blade type, choose either the “HB1” or “HB2” folder and copy its ISO out of the folder and into **D:\RemoteInstall\Boot\x64\ Linux\Drivers**. The script expects the ISO to be in this location.

Note: If UCP has experienced an upgrade, a new service VM was provided. The new service VM contains the latest drivers for Linux. They should have been copied from the new service VM to the WDS server. If you don’t find them on the D drive of the WDS server, please check the service VM’s drive at E:\UCPAppliance\InstallMedia\WDS.

Edit and run the Linux configuration script

Now that your Linux ISO is accessible to WDS and the existence of the driver folders has been verified, the configuration script may be edited and launched.

1. On the WDS VM, go to **D:\ucpbaremetaltools** and edit the script named **Add-LinuxIsoToWDS.ps1**

2. Find the string **$FILE_NAME_CB500_DRIVER_ISO = "C50-DUX-0620-05.iso"** and replace the name of the .iso file for your blade type. The driver package ISO needs to be at **D:\RemoteInstall\Boot\x64\Linux\Drivers**

3. Launch the following script which will ask for the location of your Linux ISO. Launch it by right-clicking it and selecting **Run with PowerShell**.

   D:\ucpbaremetaltools\AddLinuxToWDS.ps1

4. Press **Enter** when prompted and this opens a file explorer

5. Navigate to the Linux installation ISO, click on it, and click **Open**

6. The script asks for the Linux distribution name. Type it and press **Enter**. For example: RedHat

7. The next question asks for the version, for example, type 6.4 and press **Enter**

8. The script continues by adding the drivers to your copy of Linux

9. The script finishes with a line of text like:

   Finished copying syslinux binary files to D:\RemoteInstall\Boot\x64\Linux\Images\RedHat6.4

Note: The WDS VM also includes template kickstart files, which can be customized as needed. These files are located on the WDS VM in the following location:

D:\remoteinstall\boot\x64\linux\<OS Name>\kickstartfiles

Refresh UCP image inventory

After finishing the preceding steps, refresh the image inventory in UCP Director so that the new Linux image is made available for use.

For more information, see "Refresh image inventory" on page 119.

ESXi images

This section describes how you can prepare ESXi images for deployment and will give you an overview for how:

- vCenter's Auto Deploy rules work

- UCP manages Auto Deploy rules
- ESXi image repositories and image updates work in UCP

In UCP environments, the compute blades use ESXi stateless images. The image is about 35MB and loads via the network into host memory every time the server boots.

As a high-level explanation, the ESXi image gets deployed through a series of communications between:

- the PXE request from the server,
- the DHCP server that answers the PXE call,
- a TFTP server that passes the image to the host,
- and the Auto Deploy service that controls what image loads to which blade

Auto Deploy rules

Auto Deploy rules are used for mapping images to specific servers. Normally the administrator needs to create auto deploy rules by hand through power CLI. But UCP handles this for you. Servers that are requesting an image are examined for a defining attribute that matches the rule.

When a booting server matches the pattern in an Auto Deploy rule, the image associated with the rule is loaded on that server. UCP has chosen the following two patterns upon which to base Auto Deploy rules:

1. The server vendor and model
2. Or a single server's UUID

When UCP is first deployed, it has a default rule and a default ESXi image for the B1 blade model and the B2 blade model.

UCP does not support the creation or deletion of Auto Deploy rules by any means other than UCP.

Host Profiles

Host profiles are used by vCenter to reconfigure the stateless ESXi host details after each reboot. Every UCP cluster service template must be configured to use the basic default host profile that was prepared for you when UCP was first deployed.

If the host profile needs to be re-created for any reason, see the instructions in "Preparing VMware host profiles in vCenter" on page 237.

After UCP deploys a cluster, you will find that a new host profile has been created for that cluster. Customize this copy with specific settings related to the cluster, for example, the root password.

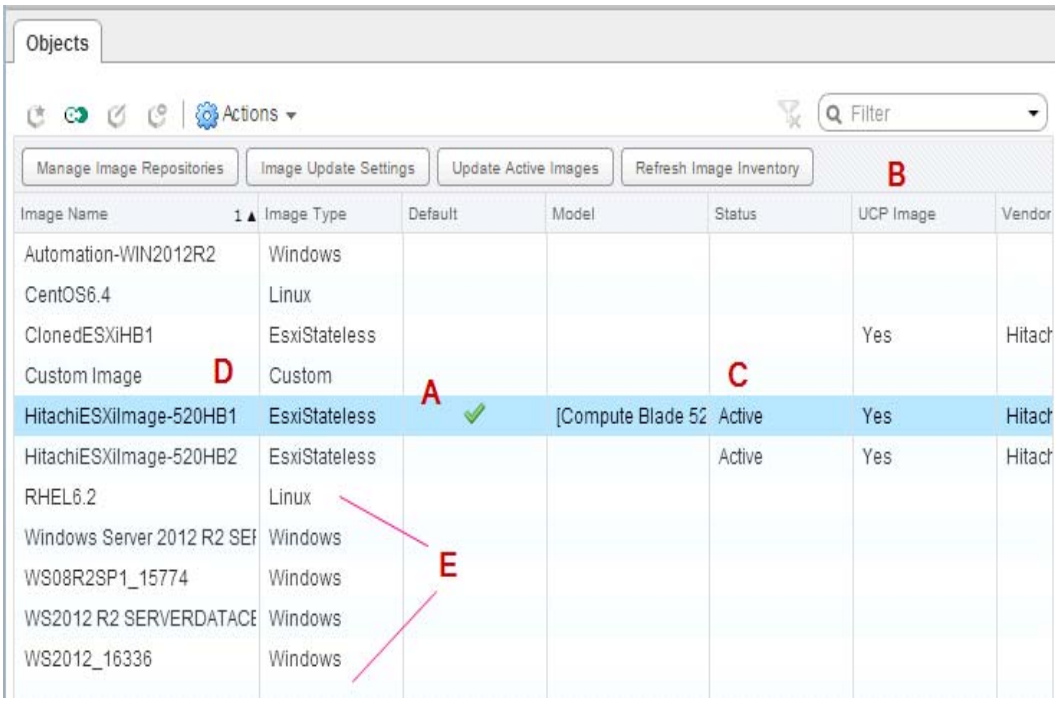
Repositories

UCP has an internal repository where ESXi images are stored. These images can be deployed to hosts. UCP can also examine the contents of external repositories in search of updates. However, UCP cannot *deploy* an image unless it resides within the UCP internal repository. Cloning an image transfers it from an external repository to the internal one.

The following sections are intended to help you become familiar with how image repositories are managed in the vSphere web client.

Review commonly used image properties

Here you will find an explanation of important properties to monitor in your vSphere web client.



A. **Default** - In the screenshot above, the default image is indicated by a green checkmark. In this particular environment, we have only B1 blades. If there were also B2 blades, a checkmark would also appear next to the image for B1 blades.

B. **UCP Image** - Indicates the ESXi image was created by UCP and is deployable to servers. After we add an external repository containing a newer ESXi image, UCP will depict the image here, but it will not be marked as Yes under UCP Image. This means it can be cloned but not deployed. It also may contain newer VIBs (driver packages) that can be donated to older ESXi images.

C. **Active Status** - Indicates there is an auto deploy rule that associates the image to a server. For ESXi images only. Active ESXi images cannot be edited but they can be cloned and can be applied to additional servers. Notice that the ConedESXiHB1 image in the print screen is not active.

D. **Custom Image** - Indicates a logical object associated with custom service templates. Custom templates are deployed when the administrator intends to load an operating system manually.

E. **Linux and Windows images** - Linux and Windows images are kept and managed within the WDS server. They cannot be copied or edited through the UCP Image Inventory view. If Windows and Linux images aren't showing up in your inventory, it is because WDS has not yet been configured.

External image repositories

An external repository is added to UCP when you need to add new ESXi images.

Note: As with any update to a production system, you should test a patched image on one server before applying it to all production servers.

The provided default ESXi image in UCP contains necessary drivers for the Fibre Channel and network devices. UCP enables you to clone the default image and then add patches to the cloned image.

Updates to ESXi images are released on VMware's website at: https://www.vmware.com/patchmgr/findPatch.portal.

Manually adding ESXi updates to UCP

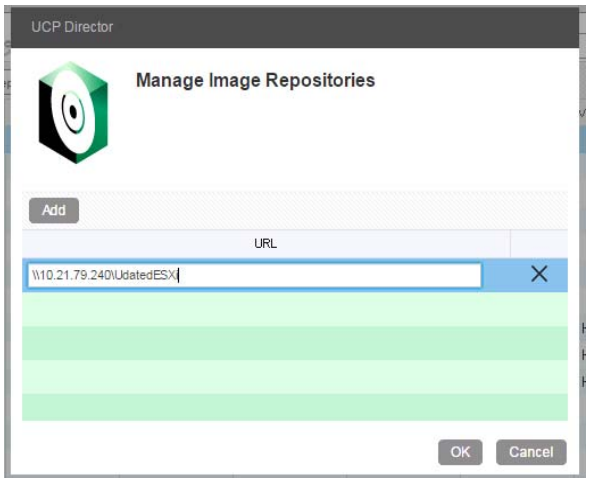
1. On the above website, locate the updates you require and then download them. For example, in the screenshot below, we have selected the "Critical" bug fix (656.6 MB file).

2. Place the updates onto a network share that is accessible to UCP.

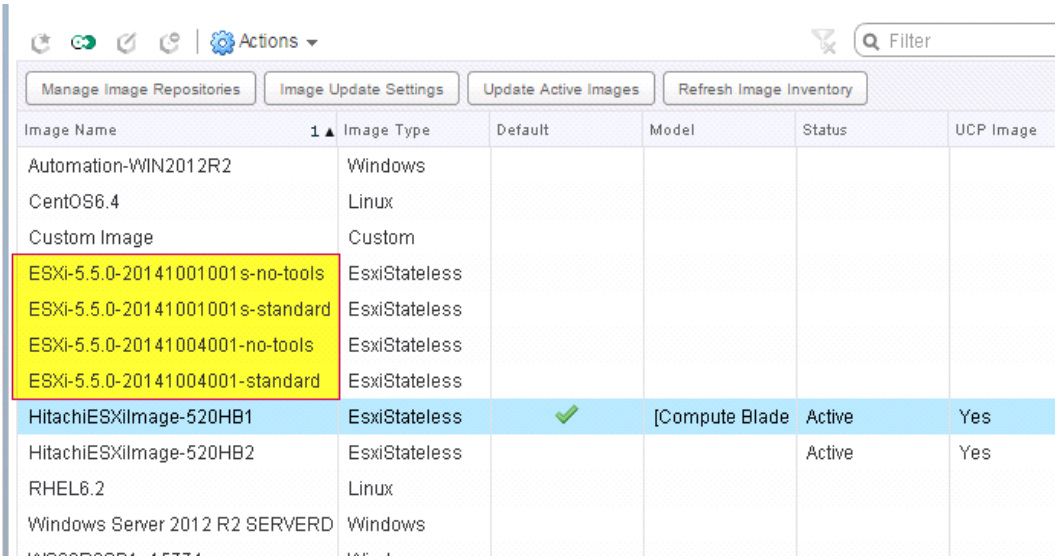
3. When sharing the network location, give Read privileges to the Ucpadmin and ucp_svc accounts

4. In the **UCP image inventory** screen, click the **Manage Repositories** button

5. Click the **Add** button, type the network share, click **OK**



6. Click **Refresh Image Inventory**. The new image will then appear in the list. For example, in the screenshot below, the highlighted text below indicates the name of recently added images that were copied from the network folder shown in the previous screenshot.



Cloning the default ESXi image

The default ESXi image cannot be edited because it is marked as **Active**. It, therefore, must be cloned before updates can be added. Later, the cloned and updated copy will be configured for deployment.

1. Right-click the default image and choose **Clone**. Give the clone a name

2. Right click the image and choose **Edit Image**

3. The pop up lists all the drivers and packages in the current image as well as potential updates. Some items are flagged with a yellow bang to indicate that updates are available from the newer image found in the external repository.

4. Select the packages that you would like to update, and then click OK.

8

Deploy images in UCP Director

To administer the image deployment process, UCP Director monitors the Windows Deployment Server (WDS) image inventory on the WDS VM that Hyper-V, Windows and Linux images are deployed from.

This chapter covers:

About deploying images

Hyper-V, Windows, and Linux images are deployed through service templates. You will need to prepare a service template to administer the deployment.

For more information on service templates, see Chapter 14, “Service template administration,” on page 221.

When deploying an image to a server, UCP Director creates and attaches a boot volume to the server and installs the image to the boot volume. That boot volume is then used each time the server boots.

Important:

- VMware depot files are a special zip file format used by VMware. Using Windows zip files will not work. Renaming a VMware depot file in Windows after it has been created will prevent it from working.

For a list of supported OS versions, see the release notes.

View image inventory

The images that UCP Director can deploy are displayed on the **Images** table. To view the **Images** table, in:

- vSphere Web Client and SCVMM, from the navigation bar, click on the **Images** icon. For more information on the navigation bar, see “Using UCP Director Console” on page 76.

- vSphere Client, from the **Home** page, click on the **vCenter** link, and then click on the **Images** link in the **Inventory Lists** section.

When using vCenter, the **Images** table displays a list of all images in local inventory and remote repositories. For each image, the following properties are shown: **Image Name**, **Image Type**, **Default**, **Model**, **Status**, **UCP Image**, **Vendor**, **Description**, **Last Modified**, **ID**, and **Global ID**.

When using SCVMM, the **Images** table displays a list of all images in inventory. For each image, the following properties are shown: **Image Name**, **Image Type**, **Description**, **ID**, and **Global ID**.

Refresh image inventory

UCP Director periodically scans the WDS server and, when using vCenter, ESXi image repositories for new or updated images. To manually initiate an inventory refresh:

1. From the **Images** table, click on the **Refresh Image Inventory** button.

2. In response to the confirmation message, click on the **Yes** button. UCP service templates can now be created to deploy your image.

Note: When using UCP Director Console in vSphere Client, the **Images** table will not refresh until you manually refresh the page. For information on refreshing the page, see "Refreshing UCP Director Console pages" on page 80.

Deploy a cloned ESXi image

In the previous chapter, we walked through the steps to clone the default image for the B1 blades and update it with patches from VMware. Here we will walk through the steps to deploy it to a host.

Test the cloned and edited image on a host

It's important to first test any new image to a single host with your production workload. If tests are successful, this image can be more widely deployed. This can be achieved by making it the new default ESXi image and by configuring it as the Pending image for clusters that are already deployed.

1. Right-click the target host and choose **Change Image** under the **All Hitachi Compute Platform Actions** menu.

2. Choose the newly updated cloned image, and then click **OK**. Behind the scenes, UCP will create a new Auto Deploy rule for the server. If you want to verify this for yourself, open a vSphere Power CLI window, connect to vCenter, and then run the command **get-deployrule**. The UUID of this ESXi host will be tied to the cloned image.

3. Reboot the host to load the new image in UCP Server Inventory

4. If tests are successful, you can configure the image to be the default, using the next procedure.

Set the cloned image as default

In vCenter, a default ESXi image can be assigned for each server model. The default image for that model will then be loaded each time a server of that type reboots unless an individualized auto deploy rule exists for the blade.

For example, all clustered blades have auto deploy rules based on their UUID. For this reason, clustered hosts need to be configured with the Hitachi UCP option for Change Cluster Image.

To change the ESXi image that is applied to a server type by default:

1. In UCP Image Inventory, find your successfully tested cloned image in the list of images.
2. Right-click it and click **Set As Default**
3. In the pop up window, choose the blade model it will be the 'default' image for, and then click **OK**.
4. UCP will now display the cloned image as the default.

Post-deployment tasks for ESXi images

UCP Director automates much of the work involved in adding, updating, and removing ESXi images.

Viewing an ESXi image summary in vCenter

When using vCenter, additional information about an image is available on the image summary. To view the summary of an individual image, from the **Images** table:

- In vSphere Client, right-click on the image, and then click on the **Image Summary** link.
- In vSphere Web Client, click on the name of the image in the vCenter menu on the left.

The top of the summary view contains the following properties: **Image Type**, **ID**, and **Description**. In addition, for ESXi images, the top of the summary view also contains the following properties: **Default**, **Model**, **Status**, **UCP Image**, **Vendor**, and **Last Modified**.

Note: The name of the image is shown at the top of the summary.

For ESXi images, the **Packages** table is displayed at the bottom of the image summary. The **Packages** table is used to display the packages that make up the ESXi image. For more information on ESXi packages, see "ESXi image packages in vCenter" on page 121.

In vSphere Web Client, the following:

- Views are displayed on the **Monitor** tab:
  - **Tasks** — Displays jobs related to the image. For more information on image jobs, see "ESXi image packages in vCenter" on page 121.
  - **Events** — Displays events related to the image.
- Tables are displayed on the **Related Objects** tab:
  - **Servers** — Displays a list of all servers that the image is applied to. For more information on servers, see Chapter 12, "Server administration," on page 189.

ESXi image packages in vCenter

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director monitors and reports the following properties of each ESXi image package:

- **Name** — The name of the package.
- **Vendor** — The vendor of the package.
- **Version** — The version of the package.
- **Release Date** — The date that the package was released.
- **Stateless** — Whether or not the package has been designed to run with an ESXi image that boots over the network and loads the hypervisor from a network location.

- **Summary** — A brief description of the package.
- **Acceptance Level** — The level of support for the package from VMware.
- **Description** — The description of the package. This is defined in the package.

Managing ESXi image repositories

To add, remove, or edit ESXi image repositories:

1. From the **Images** table, click on the **Manage Image Repositories** button.
2. On the **Manage Image Repositories** dialog:
   - To add an ESXi image repository, click on the **Add** button, and type the URL of the remote location or network share in the text box.
   - To edit an ESXi image repository, type the correct URL of the remote location or network share for the image repository in the text box where the old location is.
   - To remove an ESXi image repository, click on the **Delete** icon ( ) next to the repository you want to delete in the **Repositories** section.
3. Click on the **OK** button.

Notes:

- Before adding an ESXi image repository, it is important to ensure that UCP Director can communicate with it. UCP Director uses PowerCLI to communicate with ESXi image repositories, which relies on the Internet Explorer proxy settings on the UCP VM.
- To ensure that your ESXi images are current, either add the official VMware repository or manually add a network share to UCP Director and copy select images to it from the repository. The VMware repository is located at:

  https://hostupdate.VMware.com/software/VUM/PRODUCTION/main/vmw-depot-index.xml

Configuring ESXi image update settings

UCP looks for updates in repository locations that you have added to UCP. The **Image Update Settings** window is used to set the update schedule and determine who is notified of updates. To configure image update settings:

1. On the **Images** table, click on the **Image Update Settings** button.

2. On the **Image Update Settings** window:

   – Select the appropriate interval to check for updates from the **Schedule Image Updates** section.

   – Type the email address for ESXi image update notifications to be sent to in the **Notification Emails** field. If typing more than one email address, email addresses should be comma-separated.

Note: Sending ESXi image update notification emails requires the SMTP and sender account to be configured in vCenter. When these settings are entered into vCenter, UCP Director will send an email and issue an event in vSphere Client. To configure email settings, in vSphere Client:

1. From the **Administration** section of the **Home** page, click on the **vCenter Server Settings** button.

2. Click on the **Mail** link and configure the SMTP server and sender account.

3. Click on the **OK** button when done.

Manually checking external repositories

After you manually copy a newer ESXi image to a UCP external repository, clicking the Update Active Images button causes UCP to:

- Check all active images to see if they could benefit from an update found in the repository

- Copy active images and add the newer packages from the repository

- Send notification if email recipients had been configured

To manually check external repositories for updates:

1. On the **Images** table, click on the **Update Active Images** button.

2. In response to the confirmation message, click on the **Yes** button.

Editing an ESXi image

Editing an ESXi image enables you to rename the image, update its description, or change the packages that it includes. Only UCP images that are not actively applied to a server or set as the default image for a server type can be edited. To edit an active or default image, first clone the image and edit the clone instead.

To edit an ESXi image:

1. On the **Images** table, right-click on the ESXi images that you want to edit, and then click on the **Edit Image** link.

2. In the **Edit Image** window:

   – To rename the image, type a new name in the **Image Name** field. The current name of the image is shown next to the **Edit Image** window title.

   – To change the description of the image, type a new description In the **Description** field.

   – Use the **Packages** table to change the packages assigned to the image.

     The **Packages** table lists each package that is included in the image.

     • To change the version of a package, select the alternative version of the package. For each package that has been added to the image, all available versions of that package are shown.

       In vSphere Client, Packages that are out of date are marked with an update icon (). For more information on packages, see "ESXi image packages in vCenter" on page 121.

- To add a new package, click on the **Add Packages** button. When the **Add Packages** dialog appears, select the packages to add, and then click on the **OK** button.

  The **Add Packages** dialog lists all packages that are included image repositories or inventory that have not been added to the current image.

- To delete a package, click on the delete icon ( ) to the right of the package.

  If no repositories have been added that contain images with updated packages, then only one version of each package will be included in inventory.

3. Click on the **OK** button.

Removing an ESXi image

Only UCP ESXi images that are not actively applied to a server or configured as the default image for a server type can be removed. If an active image needs to be removed, change the image applied to the server or server type, and then remove the image.

To remove an image:

1. On the **Images** table, right-click on the image that you want to remove, and then click on the **Remove** link.

2. Click on the **Yes** button when prompted.

Part IV: Resource administration

This part contains these chapters:

9

Physical network administration

This chapter explains how to administer Ethernet, Fibre Channel, and converged network switches. Before administering switches, it is important to understand the components involved. For more information on switches, see “Networking and switches” on page 24.

Switch permissions

To administer a switch, your Active Directory account or group must:

- When using vCenter, either:
  - Be added to the UCP System Administrator or, for:
    - Ethernet and converged switches, the UCP Network Administrator role.
    - Fibre Channel switches, the UCP Storage Administrator role.
  - Be added to a custom role that has the UCPView privilege or, for:
    - Ethernet and converged switches, the UCP Network Administration privilege.
    - Fibre Channel switches, the UCP Storage Administration privilege.

  Using a custom role that has the UCPView privilege will enable you to see switches, but you will not be able to administer them.
- When using SCVMM, be added to the SCVMM administrator role.

For more information on access requirements, see "Security" on page 65.

Switch properties

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director monitors and reports the following properties of each switch in inventory:

- **Switch Name** — The name that has been assigned in the switch. This is dynamically retrieved from the switch after it has been added to inventory. If the switch name has not been defined, the IP address of the switch will be used.
- **Status** — The state of the switch. Possible values are:
  - **Active** — UCP Director is able to communicate with the switch.

  - **Unreachable** — UCP Director is unable to connect to the switch. Switches will also show up as **Unreachable** when in maintenance mode.

  - **Unsupported** — UCP Director is able to connect to the switch but the hardware or firmware is unsupported.

  - **Initializing** — UCP Director is in the process of adding the switch to inventory. After the switch has been added to inventory, it will stay in the **Initializing** status until the prerequisites for **Active** status have been met and an inventory refresh has taken place.

  - **Inconsistent** — The switch is returning a different model, make, or serial number than what was detected when it was added to inventory.

- **Serial Number** — The serial number of the switch. This is dynamically retrieved from the switch after it has been added to inventory.

- **Type** — The switch type. For:

  - Ethernet switches: either Access or Aggregate.

  - Fibre Channel switches: either edge or core.

  - Converged switches: access.

- **Make and Model** — The make and model of the switch. This is dynamically retrieved from the switch after it has been added to inventory.

- **IP Address** — The IP address that is used to connect to the switch. This is provided when adding the switch to inventory.

- **Fabric ID** — For Fibre Channel switches, the Fibre Channel fabric that the switch is part of.

Viewing switch inventory

The switches that UCUCP Director administers are displayed on the corresponding inventory tables, as follows:

- Ethernet switches are displayed on the **Ethernet Switches** table.

- Fibre Channel switches are displayed on the **Fibre Channel Switches** table.
- Converged switches are displayed on the **Converged Switches** table.

To view the **Ethernet Switches** table, in:

- vSphere Web Client and SCVMM, from the navigation bar, click on the **Ethernet Switches** icon.
- vSphere Client, from the **Home** page, click on the **vCenter** link, and then click on the **Ethernet Switches** link in the **Inventory Lists** section.

To view the **Fibre Channel Switches** table, in:

- vSphere Web Client and SCVMM, from the navigation bar, click on the **Fibre Channel Switches** icon.
- vSphere Client, from the **Home** page, click on the **vCenter** link, and then click on the **Fibre Channel Switches** link in the **Inventory Lists** section.

To view the **Converged Switches** table, in:

- vSphere Web Client and SCVMM, from the navigation bar, click on the **Converged Switches** icon.
- vSphere Client, from the **Home** page, click on the **vCenter** link, and then click on the **Converged Switches** link in the **Inventory Lists** section.

For more information on the navigation bar, see "Using UCP Director Console" on page 76.

The switches tables display a list of all switches of the corresponding type in inventory. For each switch, the following properties are shown: **Switch Name**, **Status**, **Monitoring State**, **Serial Number**, **Type**, **Make and Model**, **Firmware**, **IP Address**, **ID**, and **Global ID**. **Available Firmware** is shown when viewing the **Ethernet Switches** or **Fibre Channel Switches** tables in vSphere Web Client.

Adding and removing switches

The following sections describe the procedures for, and technical processes that UCP Director engages in, when adding or removing switches.

Adding a switch

When a switch is added to inventory, if SNMP monitoring is enabled, UCP Director configures the SNMP settings and adds the account that is used to communicate with the switch to receive SNMP traps. For more information on SNMP settings, see "SNMP monitoring" on page 55.

In addition, when an Ethernet or Converged switch is added to inventory, UCP Director makes the following changes:

- On Cisco Ethernet and Converged switches, UCP Director enables Cisco discovery protocol (CDP).
- On Brocade and Ethernet switches, UCP Director enables all ports and makes a backup of the Ethernet and Converged switch configuration. For more information, see "Ethernet and Converged switch backups" on page 145.
- On Brocade Ethernet switches, UCP Director enables link layer discovery protocol (LLDP).

For more information on switch configuration, see "Switches" on page 29.

To add one or more switches:

1. On the switches table, click on the **Add Switch** button.
2. In the **Add Switch** window, for each switch that you want to add, click on the **Add** button and then:
   - In the **IP Address** field, type the management IP address of the switch.
   - In the **Username** field, type the username of an account with administrative access to the switch.
   - In the **Password** field, type the password that corresponds to the specified account in the **Username** field.

Important: To ensure system security, UCP Director does not support switches without a password set. A password must be configured on a switch before it can be added to UCP Director inventory.

3. Click on the **OK** button.

Note: Only add switches that are part of UCP. Adding switches from outside UCP can result in unpredictable behavior.

Removing a switch

When a switch is removed from inventory, UCP Director removes all SNMP settings, and account that is used to communicate with the switch to receive SNMP traps. For more information on SNMP settings, see "SNMP monitoring" on page 55.

Important: Removing a switch only removes it from inventory and UCP Director will be unable to interact with it. Network connectivity will still be active until the switch is physically disconnected.

In addition, when an Ethernet or Converged switch is removed, all Ethernet and Converged switch backups will also be removed. Because all backups are removed, they can not later be restored if the Ethernet or Converged switch is added back to inventory at a later time.

To remove a switch:

1. On the switch table, right-click on the switch that you want to remove, and then click on the **Remove** link.

2. In response to the confirmation message, click on the **Yes** button.

Viewing a switch summary

Additional information about a switch is available on the switch summary. To view the summary of an individual switch, from the appropriate switches table:

- In vSphere Client or SCVMM, right-click on the switch, and then click on switch summary link for the type of switch you want to view the summary of.

- In vSphere Web Client, click on the name of the switch in the vCenter menu on the left.

The top of the switch summary displays the following properties: **Status**, **Monitoring State**, **Serial Number**, **Type**, **Firmware**, **IP Address**, and **ID**. **Fabric ID** is shown when viewing a Fibre Channel switch summary. **Available Firmware** is shown when viewing an Ethernet or Fibre Channel switch summary in vSphere Web Client.

Note: The name of the switch is shown at the top of the switch summary.

Switch summaries also include the ports diagram, which contains the make and model of the switch and a visual representation of the port layout. Moving the cursor over a port will display detailed information regarding the port. For more information on switch ports, see "Switch ports" on page 140.

In vSphere Client and SCVMM, the following tables are displayed at the bottom of the switch summary:

- **Ports** — Used to display a list of switch ports.
- **Connection Settings** — Used to display the settings used to connect to the switch. For more information on switch connection settings, see "Configuring switch connection settings" on page 143.
- **Events** — Used to display events related to the switch. For more information on switch events, see "Switch events" on page 140.
- **Backups** — When viewing the summary of an Ethernet and a Converged switch, displays the list of all Ethernet or Converged switch backups associated with the selected switch. For more information on Ethernet switch backups, see "Ethernet and Converged switch backups" on page 145.

In vSphere Web Client, the following:

- Tables are displayed at the bottom of the switch summary:
  - **Ports** — Used to display a list of switch ports.
  - **Monitoring Indicators** — Used to display switch monitoring information. For more information on switch monitoring, see "Switch monitoring in vSphere Web Client" on page 137.

- Views are displayed on the **Monitor** tab:
  - **Performance** — Displays performance monitoring information related to the switch. For more information on switch performance monitoring, see "Switch performance monitoring in vSphere Web Client" on page 137.
  - **Tasks** — Displays jobs related to the switch. For more information on switch jobs, see "Switch jobs in vSphere Web Client" on page 139.
  - **Events** — Displays events related to the switch. For more information on switch events, see "Switch events" on page 140.
- Tables are displayed on the **Related Objects** tab:
  - **Hosts** — Displays a list of VMware hosts that are connected to the selected switch.
  - **Servers** — Displays a list of all servers that are connected to the selected switch. For more information on servers, see "Server administration" on page 189.
  - **Ethernet Switches** — When viewing the summary of an Ethernet switch, displays a list of Ethernet switches connected to the selected switch.
  - **Backups** — When viewing the summary of an Ethernet switch, displays the list of all Ethernet switch backups associated with the selected switch. For more information on Ethernet switch backups, see "Ethernet and Converged switch backups" on page 145.
  - **Storage System** — When viewing the summary of a Fibre Channel or converged switch, displays the storage system that is connected to the switch. For more information on the storage system, see Chapter 11, "Storage system administration," on page 161.
  - **Fibre Channel Switches** — When viewing the summary of a Fibre Channel switch, displays a list of Fibre Channel switches connected to the selected switch.
  - **Converged Switches** — When viewing the summary of a converged switch, displays a list of Fibre Channel switches connected to the selected switch.

Switch monitoring in vSphere Web Client

In vSphere Web Client, the monitoring indicators for a switch are displayed in the **Monitoring Indicators** table at the bottom of the switch summary. Depending on the model, UCP Director monitors the following indicators for each switch:

Indicator	Type	Description
Temperature	Health	Health indicator for Temperature
Fan	Health	Health indicator for Fan
Power Supply	Health	Health indicator for Power Supply

For more information on monitoring, see "Monitoring" on page 54.

Switch performance monitoring in vSphere Web Client

When using vSphere Web Client you can view graphs that show the historical values of performance monitoring indicators. To view performance monitoring for a switch:

1. From the switch summary, click on the **Monitor** tab.
2. Click on the **Performance** tab.

From the **Performance** tab, you can select to display graphs related to the switch as a whole, or an individual port. To view performance graphs:

1. Select the component that you want to view performance graphs for from the **View** field.
2. Select the corresponding element from the **Element ID** field.
3. Select how you want the data aggregated from the **Aggregation Frequency** field.
4. Select the time frame that you want data from in the **From** and **To** sections.
5. Click on the **Apply** button.

Depending on the switch model, graphs for following performance monitoring indicators may be shown:

Component	Performance monitoring counter
Ethernet switch or Converged switch	Memory Usage (%)
	CPU Usage (%)
Ethernet switch port or Converged switch Ethernet port or Converged switch FCoE port	Unknown Protocol Packets (counts)
	Packet Transmit Errors (counts)
	Transmit Packets Dropped (counts)
	Packet Receive Errors (counts)
	Multicast Transmits (counts)
	Data Receive Rate (Mbps)
	Data Transmit Rate (Mbps)
	Unicast Transmits (counts)
	Broadcast Transmits (counts)
	Packets Transmitted (counts)
	Receive Packets Dropped (counts)
	Broadcast Receives (counts)
	Unicast Receives (counts)
	Multicast Receives (counts)
	Packets Received (counts)

Component	Performance monitoring counter
Fibre Channel switch port or Converged switch Fibre Channel port	Invalid Transmitted Words (counts)
	Received Link Reset (counts)
	CRC Errors (counts)
	Too Long Frames (counts)
	Multicast Transmits (counts)
	Loss of Synchronization Errors (counts)
	Transmitted Link Reset (counts)
	Primitive Sequence Protocol Errors (counts)
	Data Receive Rate (Mbps)
	Data Transmit Rate (Mbps)
	Frame Transmit Rate (FPS)
	Invalid Ordered Sets (counts)
	Frame Receive Rate (FPS)
	Received Offline Sequence (counts)
	Address Errors (counts)
	Delimiter Errors (counts)
	Encoding Disparity Count (counts)
	Loss of Signal Errors (counts)
	Transmitted Offline Sequence (counts)
	Buffer Credit Zero state Count (counts)
	Multicast Receives (counts)
	Link Failures (counts)

For more information on performance monitoring, see "Performance monitoring" on page 59.

Switch jobs in vSphere Web Client

When using vSphere Web Client, to view jobs related to a switch:

1. From the switch summary, click on the **Monitor** tab
2. Click on the **Tasks** tab.

For more information on jobs, see "Jobs" on page 62.

Switch events

To view events related to a switch, from the switch summary in:

- vSphere Client or SCVMM, click on the **Events** tab.
- vSphere Web Client, click on the **Monitor** tab, and then click on the **Events** tab.

Events shown on this tab are filtered to only show those events related to the selected switch. For more information on events, see "Events" on page 62.

Switch ports

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director monitors and reports the appropriate properties for each port, as follows:

- Switch port attributes
  - **Port ID** — The ID of the port, as it is stored in the switch.
  - **Port Channel ID** — The ID of the port channel that the port is a member of.
  - **VLAN IDs** — The IDs of the VLANs that have been configured on port.
  - **Native VLAN ID** — The native VLAN ID that is assigned to the port.
  - **Unmanaged** — Used to indicate if the port should be unmanaged by UCP Director. UCP Director will not modify the VLANs of unmanaged ports except when applying service templates and server profiles.
  - **State** — The state of the port, as reported by the switch. Some common values are:
    - **Online** — A device is connected and registered to the port.
    - **No Light** — No device is connected to the port.
    - **No Sync** — A device is connected to the port but it is not registering.

For more information on port state information, see the appropriate switch documentation.

  - **Status** — The status of the Fibre Channel switch port. Possible values are:
    - **F-Port** — A device is connected and has performed a fabric login.
    - **E-Port** — The type of device connected to the port is a Fibre Channel switch and the port is acting as an inter-switch link (ISL).
    - **L-Port** — A device is connected and has performed a loop login (FC-AL).
    - **U-Port** — A device is connected but is not registering.
    - **Disabled** — The port has been disabled.
  - **Type** — The port type.

- Connected device attributes
  - **Port ID** — The ID of the port that is connected to the switch.
  - **Device Type** — The type of device that is connected to the switch, such as a server or Ethernet switch.
  - **WWPN** — The WWPN of the device that the port is connected to.
  - **Device** — The name or IP address of the device that the port is connected to.

Note: Additional properties may be associated with a switch that are not displayed through UCP. For more information, see the corresponding user manual.

Viewing a switch port configuration

To view the port configuration of a switch, from the switch summary:

- In vSphere Client or SCVMM, from the switch summary, click on the **Ports** tab.
- In vSphere Web Client, refer to the **Ports** table.

Setting unmanaged ports on an Ethernet or Converged switch

UCP Director will not configure VLANs on unmanaged ports, except when applying a service template or server profile. To mark an unmanaged port on an Ethernet or converged switch:

1. When using:
   - vSphere Client or SCVMM, from the summary of the switch you want to mark unmanaged ports on, click on the **Ports** tab.
   - vSphere Web Client, from the **Ethernet Switches** table, right-click on the switch that you want to mark unmanaged ports on, and then click on the **Set Unmanaged Ports** link.
2. Make sure that the appropriate ports are marked in the **Unmanaged** column.
3. Click on the **OK** button.

Refreshing switch inventory

UCP Director periodically scans the switches in inventory. This is done to determine the relationship between switches and other components. When refreshing inventory, UCP Director also makes sure that the following are properly configured:

- On Brocade and Cisco Ethernet switches:
  - Link layer discovery protocol (LLDP)
  - Rapid spanning tree protocol (RSTP)
  - SNMP settings
  - VLAN configuration
- On Cisco Ethernet switches only:
  - Cisco discovery protocol (CDP)
  - Virtual port channel configuration (vPC)
- On Brocade Ethernet switches only:
  - Port channel groups

Refreshing inventory also detects and reports:

- Unreachable and unsupported switches
- On Ethernet switches, mismatching VLANs between access switch ports and the hosts that they are connected to

For more information on inventory refresh, see “Refreshing inventory” on page 52.

To manually initiate a switch inventory refresh:

1. From the switches table, click on the **Refresh Switch Inventory** button.
2. Click on the **Yes** button when prompted.

Note: When using UCP Director Console in vSphere Client, switch tables will not refresh until you manually refresh the page. For information on refreshing the page, see “Refreshing UCP Director Console pages” on page 80.

Configuring switch connection settings

To view or change switch connection settings:

1. When using:
   - vSphere Client or SCVMM, from the summary of the switch you want to view or change connection settings for, click on the **Connection Settings** tab.
   - vSphere Web Client, from the switches table, right-click on the switch that you want to view or change connection settings for, and then click on the **Update Connection Settings** link to display the **Connection Settings** dialog.
2. Review and make necessary changes to the following fields:
   - **Username** — The name of the account with administrative rights to log into the switch.
   - **Password** — The password that corresponds to the specified username.

- **IP Address** — The management IP address used to connect to the switch.

3. Click on the **OK** button.

Accessing a switch

To facilitate switch administration, UCP Director Console provides a link to an SSH console to administer the switch.

To remotely connect to the switch through the SSH console, from the switches table, right-click on the switch, and then click on the **Command Line** link.

For information relating to the command line interface requirements, see the release notes.

Updating Ethernet and Fibre Channel switch firmware in vSphere Web Client

When using vSphere Web Client, you can update Ethernet and Fibre Channel switch firmware. To ensure compatibility, Ethernet and Fibre Channel switch firmware should be updated before updating chassis, or server firmware. For more information on updating firmware, see "Firmware update management in vSphere Web Client" on page 64.

Before updating firmware on an Ethernet or Fibre Channel switch, UCP Director will check to ensure that the **Monitoring State** is **OK**. It will also confirm that there is network redundancy for each ESXi server.

To update firmware on an individual Ethernet or Fibre Channel switch:

1. On the switches table, right-click on the switch that you want to update firmware on, and then click on the **Update Firmware** link.

2. In response to the confirmation message, click on the **Yes** button.

To update firmware on all Ethernet or Fibre Channel switches:

1. On the switches table, click on the **Update All Firmware** button.

2. In response to the confirmation message, click on the **Yes** button.

When updating firmware on more than one Ethernet or Fibre Channel switch, UCP Director will first update switches one by one on one path before updating the switches on the other path. This ensures that all hosts that have been configured for redundant network access do not lose connectivity.

Ethernet and Converged switch backups

Before making changes to an Ethernet or Converged switch, UCP Director enables you to backup and restore the configuration of the switch. This includes all of the port group, VLAN ID, and SNMP settings on the Ethernet or Converged switch. By backing up the Ethernet or Converged switch, you can easily manage and protect the access network from disruptive changes.

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director records the following properties of each Ethernet Switch backup:

- **Description** — The description of the backup.
- **Pinned** — Whether or not the backup has been pinned. Pinned backups are excluded from the regular retention policy and will not be deleted.
- **Firmware** — The OS version of the Ethernet or Converged switch when it was taken.
- **User** — The user ID that recorded the Ethernet or Converged switch backup.
- **Date Time** — The date and time that the backup was recorded.
- **Switch ID** — The UCP Director ID number assigned to the Ethernet or Converged switch that the port is part of.

Backing up an Ethernet and Converged switch

Before backing up an Ethernet or Converged switch, it needs to be active in inventory. To do this, follow the steps below that are applicable to your switch type.

To backup an Ethernet switch:

1. On the **Ethernet Switches** table, right-click on the Ethernet switch that you want to backup, and then click on the **Backup** link.

2. On the **Backup Ethernet Switch** dialog, type a description of the backup in the **Description** field.

3. To keep the backup past the retention policy, select the **Pinned** option.

4. Click on the **OK** button.

To backup a Converged switch:

1. On the **Converged Switches** table, right-click on the Converged switch that you want to backup, and then click on the **Backup** link.

2. On the **Backup Converged Switch** dialog, type a description of the backup in the **Description** field.

3. To keep the backup past the retention policy, select the **Pinned** option.

4. Click on the **OK** button.

Viewing Ethernet and Converged switch backups

Ethernet and Converged switch backups are shown on the **Backups** table. To view the **Backups** table, in:

- vSphere Client or SCVMM, from the Ethernet switch summary, click on the **Backups** tab.

- vSphere Web Client, when viewing the related objects of an Ethernet switch, click on the **Backups** button.

For more information on the Ethernet and Converged switch summary, see "Viewing a switch summary" on page 134.

For each backup, the following properties are shown: **Description**, **Pinned**, **Firmware**, **User**, **Date Time**, and **ID**. The **Global ID** column is shown in vSphere Web Client.

Viewing an Ethernet and Converged switch backup summary

To view the summary of an individual Ethernet switch backup in:

- vSphere Client or SCVMM, right-click on the Ethernet or Converged switch backup on the **Backups** table, and then click on the **Backup Details** link.

- vSphere Web Client, click on the description of the Ethernet or Converged switch backup in the vCenter menu on the left when viewing an Ethernet or Converged switch summary.

The top of the Ethernet or Converged switch backup summary displays the following properties: **Pinned**, **Firmware**, **User**, **Date Time**, **Switch ID**, and **ID**, fields.

Note: The description of the Ethernet switch is shown at the top when viewing the Ethernet switch backup summary.

The bottom of the Ethernet or Converged switch summary view displays the raw configuration data in the backup.

Ethernet and Converged switch backup jobs in vSphere Web Client

When using vSphere Web Client, to view jobs related to an Ethernet or Converged switch backup:

1. From the Ethernet or Converged switch backup summary, click on the **Monitor** tab
2. Click on the **Tasks** tab.

For more information on jobs, see "Jobs" on page 62.

Ethernet or Converged switch backup events in vSphere Web Client

When using vSphere Web Client, to view events related to an Ethernet or Converged switch backup, click on the **Monitor** tab while viewing the Ethernet or Converged switch backup summary. Events shown on this tab are filtered to only show those events that relate to the selected Ethernet or Converged switch backup. For more information on events, see "Events" on page 62.

Editing Ethernet and Converged switch backups

To edit an Ethernet or Converged switch backup:

1. On the **Backups** table, right-click on the Ethernet or Converged switch backup that you want to edit, and then click on the **Edit** link.
2. On the **Edit Backup** window:
   - To update the description, enter an updated description of the backup in the **Description** field.

– To keep the backup past the retention policy, select the **Pinned** option.

3. Click on the **OK** button.

Restoring Ethernet switch backups

To restore an Ethernet switch backup:

1. On the **Backups** table, right-click on the Ethernet switch backup that you want to restore, and then click on the **Restore Backup** link.

2. Click on the **Yes** button when prompted.

Removing Ethernet and Converged switch backups

To remove an Ethernet switch backup:

1. On the **Backups** table, right-click on the Ethernet or Converged switch backup that you want to remove, and then click on the **Remove** link.

2. Click on the **Yes** button when prompted.

Setting the backup retention policy

You can define how many backups to keep by configuring the Ethernet or Converged switch backup retention policy. Older, unpinned backups in excesses of the number of retained backups will be purged. If a backup has been pinned, it it will be kept regardless of age. The number of pinned backups to be kept is set apart from the total number of backups kept. The number of pinned backups that are kept count toward the total number of backups kept.

To set the Ethernet or Converged switch backup retention policy:

1. On the **Ethernet Switches** or **Converged Switches** table, click on the **Backup Retention Policy** button to display the **Backup Retention Policy** dialog.

2. Enter the total number of backups to be kept for each Ethernet or Converged switch in the **Total Kept** field.

3. Enter the number of pinned backups that will be kept in the **Pinned Kept** field. Because pinned backups count against the total number of backups kept, the number of pinned backups kept must be lower than the total number of total kept.

4. Click on the **OK** button.

Backing up all Ethernet and Converged switches

To backup all Ethernet switches:

1. On the **Ethernet Switches** table, click on the **Backup All** button to display the **Backup All Ethernet Switches** dialog.

2. Enter a description of the backups in the **Description** field.

3. Click on the **OK** button.

To backup all Converged switches:

1. On the **Converged Switches** table, click on the **Backup All** button to display the **Backup All Ethernet Switches** dialog.

2. Enter a description of the backups in the **Description** field.

3. Click on the **OK** button

10

Logical network administration

This chapter explains how to administer the logical networks that run on the UCP network switches. Before administering logical networks, it is important to understand the components involved. For more information on network components, see “Networking and switches” on page 24.

VLANs

You can apply VLANs to ports on a switch from either an individual host or all hosts in a cluster. When applying VLANs, the VLANs that are configured on a port on a host are appended to the corresponding port on the access Ethernet switch.

Appending VLANs from a host or cluster is not a destructive process as new VLANs are added to current VLANs.

Note: To ensure that you see the latest VLAN configuration when configuring VLANs by host or cluster, make sure to refresh Ethernet inventory before applying VLANs. For more information on refreshing Ethernet inventory, see "Refreshing switch inventory" on page 142.

Configuring VLANs by hypervisor host

For ESXi and Hyper-V hosts, you can automatically apply the VLANs that are configured on the hosts to the switch ports that they are connected to.

Configuring VLANs by a host requires that both NICs in the host are connected to the virtual or logical switch. If only one NIC is attached to a virtual or logical switch, the other NIC will need to be manually attached before configuring VLANs by host.

To apply the VLANs from a host to the connected switches:

1. From the **Servers** table, right-click on the host that you want to apply the VLANs from and, if using vSphere Web Client, move the mouse over the **All Hitachi Unified Compute Platform Director Actions** menu. For more information on the **Servers** table, see "Viewing server inventory" on page 193.

2. Click on the **Configure Host Network** link.

3. On the **Configure Host Network** screen, review the changes that will be made, as follows:

   – **Host Port Configuration: Current**

   - **Uplink Port** — The port on the host that the VLANs will be applied to the switch from. Only two ports should be listed for the host.

   - **VLAN IDs** — The VLAN IDs that are configured on the host and will be appended to the switch.

- **Switch Port Configuration: Current**
  - **Switch Name** — The name of the switch.
  - **Port** — The name of the port on the switch.
  - **VLAN IDs** — The VLAN IDs that are configured on the switch.
- **Switch Port Configuration: Final**
  - **VLAN IDs** — The combination of VLAN IDs from the ports on the host and switch that will be applied to the switch.

4. Click on the **OK** button.

Configuring VLANs by hosts in a cluster

The VLANs specified in a service template are automatically configured by UCP onto each blade's attached ports on the physical Ethernet switches. If afterwards, more VLAN IDs are added to the host configuration, this UCP feature will add the additional VLAN IDs to the physical ports.

When using vCenter, you will need to manually add the new VLAN to the VDS uplink before executing the following steps. A prerequisite is that both NICs in the hosts are connected to the virtual or logical switch. If only one NIC on a host is attached to a virtual or logical switch, the other NIC will need to be manually attached before configuring VLANs.

To apply the VLANs from all hosts in a cluster to the switches that they are connected to:

1. When using:
   - vSphere Client or SCVMM:
     1. From the navigation bar, click on the **Servers** icon to view the **Servers** table. For more information on the navigation bar, see “Using UCP Director Console” on page 76.
     2. Right-click on the host that is part of the cluster that you want to apply the VLANs from and click on the **Configure Cluster Network** link.
   - vSphere Web Client:
     1. From the vCenter **Clusters** table, right-click on the on the vCenter **Clusters** table.

2. Right-click on the cluster that contains the hosts you want to apply VLANs from, move the mouse over **All Hitachi Unified Compute Platform Director Actions**, and then click on the **Configure Cluster Network** link.

2. On the **Configure Cluster Network** screen, review the changes that will be made, as follows:

   – **Host Port Configuration: Current**

     • **Uplink Port** — The port on the host that the VLANs will be appended to the switch from. Only two ports should be listed for each host. VLANs should be the same on both ports and should be assigned by the virtual switch or virtual distributed switch.

     • **VLAN IDs** — The VLAN IDs that are configured on the host and will be appended to the switch.

   – **Switch Port Configuration: Current**

     • **Switch Name** — The name of the switch.

     • **Port** — The name of the port on the switch.

     • **VLAN IDs** — The VLAN IDs that are configured on the switch.

   – **Switch Port Configuration: Final**

     • **VLAN IDs** — The combination of VLAN IDs from the ports on the host and switch that will be applied to the switch.

3. Click on the **OK** button.

The same feature exists for stand alone ESXi hosts. First ensure that the host has both NICs attached to a VDS and that the new VLAN ID is in the uplink port group of the VDS. Then follow the same steps as for Configure Cluster Network, but choose Configure Host Network instead.

Configuring VLANs by non-hypervisor hosts

VLANs on a Windows, Linux, or custom host are configured when the server profile is applied to the host. After a server profile is applied, additional VLANs that might manually be added on the host side can be configured to attached physical Enternet switch ports by UCP.

To apply the VLANs from a host to the connected switches:

1. From the **Servers** table, right-click on the host that you want to apply the VLANs from and, if using vSphere Web Client, move the mouse over the **All Hitachi Unified Compute Platform Director Actions** menu. For more information on the **Servers** table, see "Viewing server inventory" on page 193.

2. Click on the **Configure Host Network** link.

3. On the **Configure Host Network** screen, for each uplink port under the **Host Port Configuration** section, type the VLAN IDs that are associated with that port in the corresponding field under the **VLAN IDs** column.

4. After the appropriate VLAN IDs have been entered, review the changes that will be made, as follows:

   – **Host Port Configuration: Current**

     • **Uplink Port** — The port on the host that you will enter VLAN IDs for in the corresponding VLAN IDs field. Only two ports should be listed for the host.

     • **VLAN IDs** — Enter the VLAN IDs that will be applied for the corresponding **Uplink Port** here.

   – **Switch Port Configuration: Current**

     • **Switch Name** — The name of the switch.

     • **Port** — The name of the port on the switch.

     • **VLAN IDs** — The VLAN IDs that are configured on the switch.

5. Click on the **OK** button.

Configuring automatic VLAN and port channel group creation

Depending on your environment, you may not want UCP to modify the host VLAN configuration or automatically create port channel groups. If port channel groups and host VLAN configuration are disabled, UCP Director will not configure the port channel groups when performing an inventory refresh. You will also not be able to manually configure VLANs by host or cluster and they will not be configured when applying a service template.

To enable or disable host or cluster VLAN configuration and automatic port channel group creation:

1. On the switches table, click on the **Ethernet Features** button.
2. To:
   - Disable Ethernet features, deselect the **Port Channel Groups and Host VLAN Configuration** option.
   - Enable Ethernet features, select the **Port Channel Groups and Host VLAN Configuration** option.
3. Click on the **OK** button.

Important: Deploying service templates requires Ethernet features to be enabled. Disabling Ethernet features disables service template deployment.

SCVMM host networking

For Hyper-V hosts to have access to network resources, SCVMM networking needs to be configured. The following sections explain the networking configurations that need to be set in SCVMM.

Logical network

Logical networks are used in SCVMM to segment and enable network traffic. At least one logical network needs to be created for network traffic. When creating a logical network:

- To ensure network reliability, UCP is designed to use VLAN-based independent networks.

- For each network site, add VLAN 0 for management and one or more IP subnet and VLANs for VM networks.

  If you will be creating Hyper-V clusters, also add an IP subnet and VLAN for the cluster and live migration networks.

SCVMM IP pools

With the exception of the management network, IP pools will need to be defined for each IP subnet that you added to the logical networks created. This is done to statically assign IP addresses to the virtual network adapters (vNICs) configured on the host, and the VMs that will use those vNICs. When creating an IP pool:

- Cluster and Live Migration — Because these networks are internal networks, do not define gateway, DNS, or WINS settings.

- VM networks — For the VM networks to have external access, configure the appropriate gateway, DNS, and WINS settings.

SCVMM VM networks

SCVMM VM networks need to be defined for each IP subnet in a logical network to enable connectivity on that IP subnet and to assign a name.

Port profiles

Port profiles can be used to enable NIC teaming, bandwidth management, and security settings, as follows:

- NIC teaming — At least one uplink port profile needs to be created for each logical network. When creating a port profile, to ensure optimal performance, it is a UCP best practice to use dynamic load balancing and switch independent teaming.

- Bandwidth management and security settings — If you want to manage bandwidth and security settings, at least one virtual port profile needs to be created for each configuration.

Logical switches

Logical switches are used as a template for creating virtual switches. When creating a logical switch, to enable NIC teaming, select the **Team** uplink mode and add the port profile that you want to apply to virtual switches based off this logical switch.

vCenter cluster networking

Cluster networking in vCenter requires a VDS. You can use an existing VDS or create one when creating a service template. If you will use an existing VDS when creating the cluster, make sure that the VDS is configured as follows:

- The service template should have at least two port groups configured, one for management and one for vMotion. Additional port groups can be used for VM networks.
- The management port group should not have any VLAN IDs applied to it. Management traffic should be untagged and use the UCP management VLAN ID.
- If the vMotion port group will not use the management VLAN ID, apply a VLAN ID to the vMotion port group.

Configuring Fibre Channel zones on a hypervisor host

You can manually configure the Fibre Channel zones of hypervisor hosts. UCP Director monitors the following properties regarding each Fibre Channel zone:

- **Zone Name** — The name of the Fibre Channel zone.
- **Initiator Port** — The name of the host bust adapter (HBA) port on the initiating host.
- **Initiator WWPN** — The WWPN of the initiator port.
- **Storage System Name** — The name of the target storage system that the host is connected to.
- **Target** — The port on the target storage system that the host is connected to.
- **Target WWPN** — The WWPN of the port on the target storage system that the host is connected to.

Viewing Fibre Channel zones

To view and administer Fibre Channel zones on a hypervisor host, you use the **Configure Fibre Channel Zones** window.

To display the **Configure Fibre Channel Zones** window:

1. From the **Servers** table, right-click on the host that you want to configure Fibre Channel zones for and, if using vSphere Web Client, move the mouse over the **All Hitachi Unified Compute Platform Director Actions** menu. For more information on the **Servers** table, see "Viewing server inventory" on page 193.

2. Click on the **Configure Fibre Channel Zones** link.

The **Configure Fibre Channel Zones** window displays the two Fibre Channel fabrics that are associated with the selected host.

For each fabric, the **Initiator Port** and **Initiator WWN** for all zones within it are displayed, followed by a list of each Fibre Channel zone. To view the details of an individual Fibre Channel zone, click on the name of the Fibre Channel zone.

From the **Configure Fibre Channel Zones** window, you can also add, edit, and delete Fibre Channel zones. Changes made to Fibre Channel zones on the **Configure Fibre Channel Zones** window are not saved until you click on the **OK** button.

Add a Fibre Channel zone

To add a Fibre Channel zone:

1. Click on the **Add** button under the fabric that you want to add the Fibre Channel zone to.

2. On the **Add Fibre Channel Zone** dialog:

   – In the **Zone Name** field, type a name for the Fibre Channel zone.

   – In the **Target** field, select the target port.

3. Click on the **OK** button.

Edit a Fibre Channel zone

To edit a Fibre Channel zone:

1. Click on the **Edit** link beside the Fibre Channel zone you want to edit to display the **Edit Fibre Channel Zone** dialog.

2. Select the new target port on the storage system from the **Target** field.

3. Click on the **OK** button.

Delete a Fibre Channel zone

To delete a Fibre Channel zone, click on the **Delete** link.

11

Storage system administration

This chapter explains how to administer the storage system and storage resources in UCP. Before administering the storage system, it is important to understand the components involved. For more information on the storage system, see “Storage system” on page 34.

Storage system permissions

To administer the storage system, your Active Directory account or group must:

- When using vCenter, either:
  - Be added to the UCP System Administrator or UCP Storage Administrator role.
  - Be added to a custom role that has the UCP Storage Administration or UCPView privileges.

  Using a custom role that has the UCPView privilege will enable you to see the storage system, but you will not be able to administer it.
- When using SCVMM, be added to the SCVMM administrator role.

For more information on access requirements, see “Security” on page 65.

Configuring Hitachi Device Manager (HDvM)

To change the HDvM configuration, from the **Storage System** page or table:

1. Click on the **HDvM Settings** button to open the **HDvM Settings** dialog.
2. On the **HDvM Settings** dialog:
   - In the **XML Service URL** field, type the URL that is used to connect to the HDvM XML API.
   - In the **Web Console URL** field, type the URL that is used to launch the HDvM web console.
   - In the **Username** field, type the name of the account that will be used to log into HDvM. This account must have Modify and View rights in HDvM.
   - In the **Password** field, type the password that corresponds to the specified username.
3. Click on the **OK** button.

For more information on the **Storage System** page or table, see “Viewing the storage system” on page 163.

After HDvM has been configured, you can access HDvM by clicking on the **Open HDvM** button when viewing the storage system.

Storage system properties

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director monitors and reports the following properties of the storage system:

- **Storage Name** — The name of the storage system.
- **Serial Number** — The serial number of the storage system.
- **Type** — The type of storage array.
- **Allocated** — The total capacity of the storage system that has been assigned to volumes that have been attached to hosts.
- **Unallocated** — The total capacity of the storage system that has been assigned to volumes that have not been attached to hosts.
- **Reserved** — The total storage system capacity that has been reserved for storage pools.
- **Free** — The total amount of unused space in the storage system.
- **Physical** — The total physical capacity of the storage system.

In addition to the previously indicated storage system properties, UCP Director also monitors the storage system pools, and volumes.

Viewing the storage system

Depending on the hypervisor manager and client that you are using, the storage system is displayed on either the **Storage System** page or **Storage System** table. To view the **Storage System** page or table, in:

- vSphere Client and SCVMM, from the navigation bar, click on the **Storage System** icon. For more information on the navigation bar, see "Using UCP Director Console" on page 76.
- vSphere Web Client, from the **Home** page, click on the **vCenter** link, and then click on the **Storage System** link in the **Inventory Lists** section.

About the Storage System page in vSphere Client or SCVMM

The top of the **Storage System** page displays the following properties: **Serial Number**, **Firmware**, **Physical**, **ID**, **Monitoring State**, and **Type**.

Note: The name of the storage system is shown at the top of the **Storage System** page in vSphere Client.

Below these properties are the ports diagram and storage system utilization bars.

The ports diagram lists the name of the storage system and provides a visual representation of the ports layout. Moving the mouse cursor over a port will display detailed information regarding the port. For more information regarding ports, see "Storage system ports" on page 170.

The storage system utilization bars display storage system use as follows:

- **Physical Utilization** — Shows the physical utilization of the storage system in terms of **Reserved** and **Free** space.
- **Logical Utilization** — Shows the virtual utilization of the storage system in terms of the **Allocated** and **Unallocated** space.

  Moving the cursor over the shaded area on one of the bars will show the actual usage numbers.

The following tables are displayed at the bottom of the **Storage System** page:

- **Pools** — Used to display the pools inventory. For more information on pools, see "Pools" on page 171.
- **Volumes** — Used to display the volumes inventory. For more information on volumes, see "Volumes" on page 176.
- **Ports** — Used to display the storage system ports inventory. For more information on storage system ports, see "Storage system ports" on page 170.
- **Events** — Used to display events related to the storage system. For more information on storage system events, see "Storage system events" on page 170.

About the Storage System table in vSphere Web Client

The **Storage System** table displays the following storage system properties: **Name**, **Serial Number**, **Monitoring State**, **Type**, **Firmware**, **Allocated**, **Unallocated**, **Reserved**, **Free**, **Physical**, **ID**, and **Global ID**.

Additional storage system information is available on the storage system summary. To view the storage system summary, click on the name of the storage system in the vCenter menu on the left when viewing the **Storage System** table.

The top of the storage summary displays the following properties: **Serial Number**, **Monitoring State**, **Type**, **Firmware**, **Allocated**, **Unallocated**, **Reserved**, **Free**, and **ID**.

Note: The name of the storage system is shown at the top of the storage system summary.

Beside the storage system properties is the ports diagram. The ports diagram lists the name of the storage system and provides a visual representation of the ports layout. Moving the mouse cursor over a port will display detailed information regarding the port. For more information regarding ports, see "Storage system ports" on page 170.

The following:

- Tables are displayed at the bottom of the storage system summary:
  - **Ports** — Used to display information on the storage system ports. For more information on ports, see "Storage system ports" on page 170.
  - **Monitoring Indicators** — Used to display storage system monitoring information. For more information on storage system monitoring, see "Storage system monitoring in vSphere Web Client" on page 166.
- Views are displayed on the **Monitor** tab:
  - **Performance** — Displays performance monitoring information related to the storage system. For more information on storage system performance monitoring, see "Storage system performance monitoring in vSphere Web Client" on page 167.

  - **Tasks** — Displays jobs related to the storage system. For more information on storage system jobs, see "Storage system jobs in vSphere Web Client" on page 170.

  - **Events** — Displays events related to the storage system. For more information on storage system events, see "Storage system events" on page 170.

- Tables are displayed on the **Related Objects** tab:

  - **Pools** — Displays pools related to the storage system. For more information on pools, see "Pools" on page 171.

  - **Volumes** — Displays volumes related to the storage system. For more information on volumes, see "Volumes" on page 176.

  - **Fibre Channel Switches** — In a Cisco Ethernet or Brocade Ethernet configuration, displays Fibre Channel switches related to the storage system.

  - **Converged Switches** — In a Cisco converged configuration, displays converged switches related to the storage system.

For more information on switches, see Chapter 9, "Physical network administration," on page 129.

Storage system monitoring in vSphere Web Client

In vSphere Web Client, the monitoring indicators for the storage system are displayed in the **Monitoring Indicators** table at the bottom of the storage system summary. Depending on the model, UCP Director monitors the following indicators:

Indicator	Type	Description
DKC Battery	Health	Health indicator for DKC Battery
DKC Cache	Health	Health indicator for DKC Cache
DKC Cache Switch	Health	Health indicator for DKC Cache Switch
DKC Environment	Health	Health indicator for DKC Environment
DKC Fan	Health	Health indicator for DKC Fan
DKC Power Supply	Health	Health indicator for DKC Power Supply
DKC Processor	Health	Health indicator for DKC Processor
DKC Shared Memory	Health	Health indicator for DKC Shared Memory

Indicator	Type	Description
DKU Drive	Health	Health indicator for DKU Drive
DKU Environment	Health	Health indicator for DKU Environment
DKU Fan	Health	Health indicator for DKU Fan
DKU PowerSupply	Health	Health indicator for DKU PowerSupply
Cache Performance	Performance	Performance indicator for Cache
Processors	Composite	Composite indicator for processors
Pools	Composite	Composite indicator for Pools
Connection	Health	Health indicator for Connection
Cache	Health	Health indicator for Cache
Power Supply	Health	Health indicator for Power Supply
AC	Health	Health indicator for AC
Battery	Health	Health indicator for Battery
Backup Battery	Health	Health indicator for Backup Battery
Controller	Health	Health indicator for Controller
Enclosure	Health	Health indicator for Enclosure
Loop	Health	Health indicator for Loop
CTL Connector	Health	Health indicator for CTL Connector
Additional Battery	Health	Health indicator for Additional Battery
I/F Board	Health	Health indicator for I/F Board
CTL Fan	Health	Health indicator for CTL Fan
IOM	Health	Health indicator for IOM

For more information on monitoring, see "Monitoring" on page 54.

Storage system performance monitoring in vSphere Web Client

When using vSphere Web Client you can view graphs that show the historical values of performance monitoring indicators. To view performance monitoring for the storage system:

1. From the storage system summary, click on the **Monitor** tab
2. Click on the **Performance** tab.

From the **Performance** tab, you can select to display graphs related to the storage system as a whole, or an individual component of the storage system. To view performance graphs:

1. Select the component that you want to view performance graphs for from the **View** field.

2. Select the corresponding element from the **Element ID** field.

3. Select how you want the data aggregated from the **Aggregation Frequency** field.

4. Select the time frame that you want data from in the **From** and **To** sections.

5. Click on the **Apply** button.

Depending on the storage system model, graphs for following performance monitoring indicators may be shown:

Component	Performance monitoring counter
Storage system	Cache Write Pending Percentage (%)
	Cache Memory Usage Percentage (%)
	Cache Memory Usage (MB)
	Physical Space (B)
	Cache Write Pending (MB)
	Reserved Space (B)
	Allocated Space (B)
	Free Space (B)
	Unallocated Space (B)
Storage system port	Average I/O Rate (IOPS)
	Average Transfer Rate (MBps)
Storage system processor	Processor Busy Percentage (%)

Component	Performance monitoring counter
Storage system parity group	Random Write Transfer Percentage (%)
	Busy Percentage (%)
	Read Transfer Rate (MBps)
	Random Read Transfer Percentage (%)
	Random Read I/O Rate (IOPS)
	Read Hit Percentage (%)
	Random Write I/O Rate (IOPS)
	Sequential Read I/O Rate (IOPS)
	Write Hit Percentage (%)
	Read I/O Rate (IOPS)
	Sequential Write I/O Percentage (%)
	Read I/O Percentage (%)
	Sequential Read Transfer Rate (MBps)
	Write Transfer Rate (MBps)
	Random Read Transfer Rate (MBps)
	Random Write Transfer Rate (MBps)
	Write I/O Rate (IOPS)
	Sequential Write Transfer Rate (MBps)
	Sequential Write Transfer Percentage (%)
	Sequential Read I/O Percentage (%)
	Sequential Total I/O Rate (IOPS)
	Sequential Total Transfer Rate (MBps)
	Write I/O Percentage (%)
	Read Transfer Percentage (%)
	Sequential Read Transfer Percentage (%)
	Random Total Transfer Rate (MBps)
	Random Read I/O Percentage (%)
	Random Write I/O Percentage (%)
	Write Transfer Percentage (%)
	Random Total I/O Rate (IOPS)

For more information on performance monitoring, see "Performance monitoring" on page 59.

Storage system jobs in vSphere Web Client

When using vSphere Web Client, to view jobs related to the storage system:

1. From the storage system summary, click on the **Monitor** tab
2. Click on the **Tasks** tab.

For more information on jobs, see "Jobs" on page 62.

Storage system events

To view events related to the storage system, in:

- vSphere Client or SCVMM, from the **Storage System** page, click on the **Events** tab.
- vSphere Web Client, from the storage system summary, click on the **Monitor** tab, and then click on the **Events** tab.

Events shown on this tab are filtered to only show those events related to the storage system. For more information on events, see "Events" on page 62.

Storage system ports

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director monitors and reports the following properties of each port on the storage system:

- **Port Name** — The friendly name of the storage system port.
- **WWPN** — The World Wide Port Name (WWPN) of the port.
- **Speed** — The speed at which the port is configured to operate.
- **Type** — The type of the port connection.
- **Attributes** — The role of the port. Possible values are:
  - **Target** — A standard port used for host connectivity.

  - **Initiator** — A remote replication port that is used to communicate with an RCU target port.
  - **RCU Target** — A remote replication port used to communicate with an initiator port.
  - **External** — A port that has been configured to virtualize a storage system through universal volume manager (UVM).

Viewing the storage system port configuration

To view the port configuration of the storage system, in:

- vSphere Client and SCVMM, from the **Storage System** page, click on the **Ports** tab.
- vSphere Web Client, from the storage system summary, refer to the **Ports** table.

Pools

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director monitors and reports the following properties of each pool in the storage system:

- **Type** — The type of pool. Possible values are:
  - **HDP** — Hitachi Dynamic Provisioning
  - **HDT** — Hitachi Dynamic Tiering
  - **HTI** — Hitachi Thin Provisioning
- **Capacity** — The total physical capacity of the pool.
- **Used** — The used physical capacity of the pool.
- **Free** — The unused physical capacity of the pool.
- **Physical Utilization** — A graphical representation of the percent of total physical capacity of the pool that has been used.

- **Limit** — Also known as the over subscription amount, the limit is the percentage of the physical capacity of the pool that can be used to create volumes.

Note: You can change the limit in HDvM. If you use HDvM to increase the subscription limit of a storage pool, it will not be reflected until storage inventory has been refreshed. For more information on refreshing storage inventory, see "Refreshing storage inventory" on page 180.

- **Subscribed** — The total capacity of all volumes that have been created in the pool.
- **Available** — The available capacity of the pool to create volumes in.
- **Storage System ID** — The ID of the associated storage system.

Viewing pool inventory

The storage pools that UCP Director administers are displayed on the **Pools** table. To display the **Pools** table in:

- vSphere Client and SCVMM, from the **Storage System** page, click on the **Storage Pools** tab.
- vSphere Web Client, from the storage system summary, click on the **Related Objects** tab, and then click on the **Pools** button.

The **Pools** table displays a list of all pools in inventory.

Viewing a pool summary

The pool summary view is used to display information about a storage pool. To view a storage pool summary in:

- vSphere Client or SCVMM, from the **Pools** table, right-click on the the pool you want to view the summary of, and then click on the **Storage Pool Summary** link.
- vSphere Web Client, from the **Storage System** table, in the vCenter menu:

  1. Click on the name of the storage system.
  2. Click on the **Pools** link.

3. Click on the ID of the storage pool.

The top of the pool summary displays the following properties: **Type**, **Monitoring State**, **Storage System ID**, **Capacity**, and **Limit**.

Note: The ID of the storage pool is shown at the top of the summary view.

The pool summary also includes the pool bars. The pool utilization bars display pool use as follows:

- **Physical Utilization** — Shows the physical utilization of the pool in terms of **Used** and **Free** space.

- **Subscription Utilization** — Shows the subscription utilization of the pool in terms of the **Subscribed** and **Available** space.

  Moving the cursor over the shaded area on one of the bars displays the actual usage numbers.

In vSphere Client and SCVMM, the following tables are displayed at the bottom of the pool summary:

- **Drives** — Used to display the drives that comprise the pool. For more information on drives, see "Drives" on page 176.

- **Volumes** — Used to display volumes created from the pool. For more information on volumes, see "Volumes" on page 176.

- **Events** — Used to display events related to the pool. For more information on pool events, see "Storage system events" on page 170.

In vSphere Web Client, the following:

- Table is displayed at the bottom of the pool summary:

  – **Drives** — Used to display the drives that comprise the pool. For more information on drives, see "Drives" on page 176.

- Views are displayed on the **Monitor** tab:

  – **Performance** — Displays performance monitoring information related to the pool. For more information on pool performance monitoring, see "Pool performance monitoring in vSphere Web Client" on page 174.

  - **Tasks** — Displays jobs related to the pool. For more information on pool jobs, see “Pool jobs in vSphere Web Client” on page 175.

  - **Events** — Displays events related to the pool. For more information on pool events, see “Pool events in vSphere Web Client” on page 175.

- Tables are displayed on the **Related Objects** tab:

  - **Storage System** — Displays the storage system that the pool is contained in. For more information regarding the storage system, see “Viewing the storage system” on page 163.

  - **Volumes** — Used to display volumes created from the pool. For more information on volumes, see “Volumes” on page 176.

Pool performance monitoring in vSphere Web Client

When using vSphere Web Client you can view graphs that show the historical values of performance monitoring indicators. To view performance monitoring for a pool:

1. From the pool summary, click on the **Monitor** tab.
2. Click on the **Performance** tab.

To select how to display the performance graphs for the pool, from the **Performance** tab:

1. Select how you want the data aggregated from the **Aggregation Frequency** field.
2. Select the time frame that you want data from in the **From** and **To** sections.
3. Click on the **Apply** button.

Depending on the storage system model, graphs for following performance monitoring indicators may be shown:

Component	Performance monitoring counter
Pool	Subscription Limit Percentage (%)
	Subscribed Capacity (B)
	Used Capacity (B)
	Capacity (B)
	Read I/O Rate (IOPS)
	Current Subscription Percentage (%)
	Write Response Rate (µsec)
	Write I/O Rate (IOPS)
	Used Percentage (%)
	Read Response Rate (µsec)

For more information on performance monitoring, see "Performance monitoring" on page 59.

Pool jobs in vSphere Web Client

When using vSphere Web Client, to view jobs related to a storage pool:

1. From the pool summary, click on the **Monitor** tab
2. Click on the **Tasks** tab.

For more information on jobs, see "Jobs" on page 62.

Pool events in vSphere Web Client

When using vSphere Web Client, to view events related to a storage pool, click on the **Monitor** tab while viewing the pool summary.

Events shown on this tab are filtered to only show those events that relate to the selected storage pool. For more information on events, see "Events" on page 62.

Drives

For each drive that is part of a pool, UCP Director monitors and reports the following information:

- **Type** — The drive type.
- **Capacity** — The total amount of available hard drive space across all hard drives of the indicated type.
- **Percentage Allocated** — The total percent of allocated hard drive space across all hard drives of the indicated type.

The **Drives** table lists the drives that are combined to create a pool. To view the **Drives** table in:

- vSphere Client or SCVMM, from the pool summary, click on the **Drives** table.
- vSphere Web Client, from the pool summary, refer to the **Drives** table.

Volumes

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director monitors and reports the following information of each volume:

- **Volume Name** — The name of the associated datastore in vCenter.
- **Volume Type** — The volume type, either HDP or HDT.
- **Boot Volume** — Whether or not the volume is a boot volume for a non-hypervisor or Hyper-V host.
- **Replicated Volume** — Whether or not the volume is being replicated through UCP Disaster Recovery.
- **LDEV** — The LDEV number of the volume. When assigning LDEV numbers, UCP Director uses the next available LDEV number.
- **Pool ID** — The ID of the pool that the volume is part of.
- **Capacity** — The total physical capacity of the volume.
- **Used** — The used physical capacity of the volume.

- **Attached Servers** — The hosts that the volume are attached to.
- **Physical Utilization** — The percentage of physical space used in the volume.

Viewing volumes inventory

The storage volumes that UCP Director administers are displayed on the **Volumes** table. To view the **Volumes** table, in:

- vSphere Client or SCVMM, from the **Storage System** page, click on the **Volumes** tab.
- vSphere Web Client, from the storage system summary, click on the **Related Objects** tab, and then click on the **Volumes** button.

The **Volumes** table displays a list of all volumes in inventory.

Viewing a volume summary in vSphere Web Client

When using vSphere Web Client, you can view additional information about a volume on the volume summary. To view the volume summary:

1. From the **Storage System** table, in the vCenter menu, click on the name of the storage system.
2. Click on the **Volumes** link.
3. Click on the ID of the volume.

The top of the volume summary displays the following properties: **ID**, **Storage System ID**, **Volume Type**, **Pool ID**, **LDEV**, **Capacity**, **Used**, and **Physical Utilization**.

Note: The ID of the volume is shown at the top of the volume summary.

The following views are displayed on the **Monitor** tab:

- **Performance** — Displays performance monitoring information related to the volume. For more information on volume performance monitoring, see “Volume performance monitoring in vSphere Web Client” on page 178.

- **Tasks** — Displays jobs related to the volume. For more information on volume jobs, see "Volume jobs in vSphere Web Client" on page 179.

- **Events** — Displays events related to the volume. For more information on volume events, see "Volume events in vSphere Web Client" on page 179.

The following tables are displayed on the **Related Objects** tab:

- **Storage System** — Displays the storage system that the volume is contained in. For more information regarding the storage system, see "Viewing the storage system" on page 163.

- **Hosts** — Displays a list of VMware hosts that are connected to the selected volume.

- **Servers** — Displays a list of all servers that are connected to the selected volume. For more information on servers, see Chapter 12, "Server administration," on page 189.

Volume performance monitoring in vSphere Web Client

When using vSphere Web Client you can view graphs that show the historical values of performance monitoring indicators. To view performance monitoring for a volume:

1. From the volume summary, click on the **Monitor** tab.

2. Click on the **Performance** tab.

To select how to display the performance graphs for the volume, from the **Performance** tab:

1. Select how you want the data aggregated from the **Aggregation Frequency** field.

2. Select the time frame that you want data from in the **From** and **To** sections.

3. Click on the **Apply** button.

Depending on the storage system model, graphs for following performance monitoring indicators may be shown:

Component	Performance monitoring counter
Volume	Read Transfer Rate (MBps)
	Used Capacity (B)
	Write Transfer Rate (MBps)
	Read Hit Percentage (%)
	Write Response Rate (µsec)
	Write I/O Rate (IOPS)
	Total Response Rate (µsec)
	Write Hit Percentage (%)
	Sequential Total I/O Rate (IOPS)
	Sequential Total Transfer Rate (MBps)
	Read I/O Rate (IOPS)
	Random Total Transfer Rate (MBps)
	Total Capacity (B)
	Used Percentage (%)
	Read Response Rate (µsec)
	Random Total I/O Rate (IOPS)

For more information on performance monitoring, see "Performance monitoring" on page 59.

Volume jobs in vSphere Web Client

When using vSphere Web Client, to view jobs related to a volume:

1. From the volume summary, click on the **Monitor** tab
2. Click on the **Tasks** tab.

For more information on jobs, see "Jobs" on page 62.

Volume events in vSphere Web Client

When using vSphere Web Client, to view events related to a volume, click on the **Monitor** tab while viewing the volume summary.

Events shown on this tab are filtered to only show those events that relate to the selected volume. For more information on events, see "Events" on page 62.

Creating and attaching a volume

For instructions on:

- Creating a new host volume, see "Creating a new host volume" on page 181.
- Creating a new cluster volume, see "Creating a new cluster volume" on page 184.
- Attaching an existing volume to a host, see "Attaching an existing volume to a host" on page 182.
- Attaching an existing volume to all hosts in a cluster, see "Attaching an existing volume to a cluster" on page 185.

Refreshing storage inventory

UCP Director periodically scans the storage system to determine the relationship between it and other hardware components. For more information on inventory refresh, see "Refreshing inventory" on page 52.

To manually initiate a storage system inventory refresh:

1. When viewing storage inventory, click on the **Refresh Storage Inventory** button.
2. In response to the confirmation message, click on the **Yes** button.

Note: When using UCP Director Console in vSphere Client, the **Storage System** page will not refresh until you manually refresh the page. For information on refreshing the page, see "Refreshing UCP Director Console pages" on page 80.

Configuring host storage

Configuring host storage enables you to create and attach new volumes, attach existing volumes, and configure existing volumes.

Important: Do not detach volumes in the hypervisor manager outside of UCP Director. The hypervisor manager does not clean up HSDs and Fibre Channel zones.

To access the **Configure Host Storage** dialog:

1. From the **Servers** table, right-click on the host that you want to manage storage on and, if using vSphere Web Client, move the mouse over the **All Hitachi Unified Compute Platform Director Actions** menu. For more information on the **Servers** table, see "Viewing server inventory" on page 193.

2. Click on the **Configure Host Storage** link.

Creating a new host volume

To create a new volume and add it to a host, from the **Configure Host Storage** dialog:

1. Select the **Create New Volume** option.

2. Click on the **Next** button.

3. On the **Create New Volume** step:

   – In the **Disk Size** field, type the total amount of space to use to create the volume in GB.

   – To manually select the storage system ports to use, select the **Manually Select Storage System Ports** option, and then select the appropriate ports for each fabric.

   – If creating and attaching a volume to a hypervisor OS:

      • In the **Name** field, type the name that will be assigned to the volume.

      • To format the volume, select the **Format** option, and the volume will be formatted as follows:

- In SCVMM, the volume will be formatted using NTFS.
- In vCenter, the volume will be formatted as a datastore.

If this option is not selected, the volume will be created and attached as a raw volume.

- In the **Pools** table, select the pool to create the volume from. For information on the **Pools** table, see "Viewing pool inventory" on page 172.

4. Click on the **OK** button.

Attaching an existing volume to a host

To add an existing volume to a host, from the **Configure Host Storage** dialog:

1. Select the **Attach Existing Volume** option.
2. Click on the **Next** button.
3. On the **Attach Existing Volume** step:
   - To manually select the storage system ports to use, select the **Manually Select Storage System Ports** option, and then select the appropriate ports for each fabric.
   - In the **Volumes** table, select the volume or volumes to attach to the host. The **Volumes** table is filtered to not display volumes that are attached to other OS types. For information on the **Volumes** table, see "Viewing volumes inventory" on page 177.
4. Click on the **OK** button.

Configuring an existing host volume

To configure an existing volume on a host, from the **Configure Host Storage** dialog:

1. Select the **Configure Existing Volumes** option.
2. Click on the **Next** button.

3. On the **Configure Host Storage** step:

   – To detach a volume:

      1. Right-click on the volume then click on the **Detach Volume** link.

      2. In response to the confirmation message, click on the **Yes** button.

Notes:

- When using:

  – vCenter, before detaching a datastore from an ESXi host, unmount it in vCenter before detaching it.

  – SCVMM, before detaching a formatted volume, log into the host and unmount it before detaching it.

- To detach a boot volume:

  – The host must be powered on.

  – When using SCVMM, the host should be removed from SCVMM before the boot volume is detached.

   – To expand a volume:

      1. Right-click on the volume then click on the **Expand Volume** link.

      2. When prompted to enter the new capacity of the volume, enter a value that is larger than the current volume size in the **Volume Size** field.

Note: The minimum volume expansion is 1.2 GB.

      3. Click on the **OK** button.

      For non-ESXi hosts, after expanding the logical size of a volume, you may need to log into the host and expand the formatted size of the volume.

4. Click on the **Close** button.

Configuring hypervisor cluster storage

Configuring cluster storage enables you to create and attach new volumes, attach existing volumes, and configure existing volumes on all hosts in a cluster.

Important: Do not detach volumes in the hypervisor manager outside of UCP Director. The hypervisor manager does not clean up HSDs and Fibre Channel zones.

To access the **Configure Cluster Storage** dialog, in:

- vSphere Client and SCVMM, from the **Servers** table, right-click on a host that is part of the cluster that you want to manage storage on, and then click on the **Configure Cluster Storage** link.
- vSphere Web Client, from the VMware **Clusters** table, right-click on the cluster that you want to manage storage on, and then click on the **Configure Cluster Storage** link.

Creating a new cluster volume

To create a new volume and add it to all hosts in a cluster, from the **Configure Cluster Storage** dialog:

1. Select the **Create New Volume** option.
2. Click on the **Next** button.
3. On the **Create New Volume** step:
   - In the **Name** field, type a name to assign to the volume.
   - In the **Disk Size** field, type the total amount of space to use to create the volume in GB.
   - To format the volume, select the **Format** option, and the volume will be formatted as follows:
     - In SCVMM, the volume will be formatted using CSVFS.
     - In vCenter, the volume will be formatted as a datastore.

     If this option is not selected, the created volume will be created and attached as a raw volume.

- To manually select the storage system ports to use, select the **Manually Select Storage System Ports** option, and then select the appropriate ports for each fabric.

- In the **Pools** table, select the pool to create the volume from. For information on the **Pools** table, see "Viewing pool inventory" on page 172.

4. Click on the **OK** button.

5. When using SCVMM, validate the cluster to ensure that storage was correctly configured to all hosts in the cluster.

Attaching an existing volume to a cluster

To add an existing volume to a cluster, from the **Configure Cluster Storage** dialog:

1. Select the **Attach Existing Volume** option.

2. Click on the **Next** button.

3. On the **Attach Existing Volume** step:

   - To manually select the storage system ports to use, select the **Manually Select Storage System Ports** option, and then select the appropriate ports for each fabric.

   - In the **Volumes** table, select the volume or volumes to attach to all hosts in the cluster. The **Volumes** table is filtered to not display volumes that are attached to other OS types. For information on the **Volumes** table, see "Viewing volumes inventory" on page 177.

4. Click on the **OK** button.

5. When using SCVMM, validate the cluster to ensure that storage was correctly configured to all hosts in the cluster.

Configuring an existing cluster volume

To configure an existing volume on a cluster, from the **Configure Cluster Storage** dialog:

1. Select the **Configure Existing Volumes** option.

2. Click on the **Next** button.

3. On the **Configure Cluster Storage** step:

   – To detach a volume:

      1. Right-click on the volume then click on the **Detach Volume** link.

      2. In response to the confirmation message, click on the **Yes** button.

Notes:

- When using:

  – vCenter, before detaching a datastore from an ESXi host, unmount it in vCenter before detaching it.

  – SCVMM, before detaching a formatted volume, log into the host and unmount it before detaching it.

- To detach a boot volume:

  – The host must be powered on.

  – When using SCVMM, the host should be removed from SCVMM before the boot volume is detached.

   – To expand a volume:

      1. Right-click on the volume then click on the **Expand Volume** link.

      2. When prompted to enter the new capacity of the volume, enter a value that is larger than the current volume size in the **Volume Size** field.

Note: The minimum volume expansion is 1.2 GB.

      3. Click on the **OK** button.

      For non-ESXi hosts, after expanding the logical size of a volume, you may need to log into the host and expand the formatted size of the volume.

4. Click on the **Close** button.

5. When using SCVMM, validate the cluster to ensure that storage was correctly configured to all hosts in the cluster.

Detaching and deleting volumes

Before deleting a volume, that volume must first be detached from all hosts/clusters it is attached to. Unlike when a volume is detached by UCP Director, detaching volumes in a hypervisor manager does not clean up the associated HSDs and Fibre Channel zones. Using UCP Director ensures that the LDEV ID is removed from the host storage domain (HSD).

If the removed LDEV is the last in the HSD, UCP Director will also remove the HSD and associated Fibre Channel zones.If other volumes still reside in the HSD, the HSD will be retained as to not disrupt the data paths.

After the volume has been detached, UCP Director rescans the volumes attached to the host to validate that the host is no longer able to see the detached volume.

Note: If a volume is detached through the hypervisor manager, and the HSDs and Fibre Channel zones are not cleaned up, the volume will still be presented to the server.

When using vCenter, if the volume is a datastore, the volume will also need to be manually unmounted first. Unmounting a volume in vCenter ensures that:

- No virtual machines (VM) reside on the datastore
- The datastore is not part of a datastore cluster
- The datastore is not managed by storage dynamic resource scheduling (DRS)
- Storage input/output control (SIOC) is disabled for the datastore
- The datastore is not being used by vSphere heartbeat

For more information on detaching a volume from a:

- Host, see “Configuring an existing host volume” on page 182.
- Cluster, see “Configuring an existing cluster volume” on page 185.

After unmounting and detaching the volume, UCP Director is able to delete the volume. Deleting a volume is a one-way, destructive process and any data that was contained in the volume will be lost.

Important: When using SCVMM:

- To detach a data volume from a Hyper-V host, the host must be powered on.
- To detach a boot volume from a Hyper-V host, manually remove the host from SCVMM inventory, power off the server, and then use UCP to detach the volume.

To delete a volume, from the **Volumes** table:

1. Right-click on the volume that you want to delete then click on the **Delete Volume** link.
2. In response to the confirmation message, click on the **Yes** button.

12

Server administration

This chapter explains how to administer servers and server inventory in UCP. Before administering servers, it is important to understand how they are used. For more information on servers, see “Chassis and servers” on page 19.

Note: Because host deployment involves servers, images, server profiles, and service templates, the procedures involved are covered in Chapter 15, “Host deployment,” on page 241.

Servers administration permissions

To administer servers, your Active Directory account or group must:

- When using vCenter, either:
  - Be added to the UCP System Administrator or UCP Server Administrator role.
  - Be added to a custom role that has the UCP Server Administration or UCPView privileges.

  Using a custom role that has the UCPView privilege will enable you to see servers, but you will not be able to administer them.
- When using SCVMM, be added to the SCVMM administrator role.

For more information on access requirements, see “Security” on page 65.

Configuring Hitachi Compute Systems Manager (HCSM)

To change the HCSM configuration, from the **Servers** table:

1. Click on the **HCSM Settings** button to open the **HCSM Settings** dialog.
2. On the **HCSM Settings** dialog:
   - In the **XML Service URL** field, type the URL that is used to connect to the HCSM XML API.
   - In the **Web Console URL** field, type the URL that is used to launch the HCSM web console.
   - In the **Username** field, type the name of the account that will be used to log into HCSM. This account must have Modify and View rights in HCSM.
   - In the **Password** field, type the password that corresponds to the specified username.
3. Click on the **OK** button.

For more information on the **Servers** table, see “Viewing server inventory” on page 193.

After HCSM has been configured, you can open HCSM by clicking on the **Open HCSM** button on the **Servers** table.

Server properties

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director monitors and reports the following properties of each server in inventory:

- **Host Name**
  - ESXi hosts — The host name that is used in vCenter if one has been assigned.
  - Hyper-V hosts - The host name that is used in SCVMM if one has been assigned.
  - For Windows, Linux, or custom hosts — A dynamically assigned name made from the host type and IP address or the host name that you manually set when setting the host name. For more information on setting the host name, see "Setting a non-hypervisor host name" on page 205.

  If no host name has been assigned, the **Host Name** field will display the IP address of the server. If UCP Director is not able to determine the IP address, then the **Host Name** field will display **Not Configured**.
- **Power** — The power state of the server.
- **Maintenance Mode** — Whether or not the host is in maintenance mode, as reported from hypervisor manager.
- **LID** — The power state of the LID (location indication diode) on the server.
- **Serial Number** — The serial number of the server.
- **Slot** — If the server is in a chassis, the slot number that the server is located in.
- **Server Profile ID** — The UCP Director ID number assigned to the server profile.
- **LOM IP Addresses** — The lights-out management (LOM) IP address of the server.

- **Chassis Serial Number** — The serial number of the chassis that the server is located in.
- **Cluster Name** — If the host is a member of a cluster, the name of the cluster, as shown in the hypervisor manager.
- **Current Image** — The current host image that the server is running.
- **Pending Image** — The host image that the server will boot next time it is reset.
- **OS Type** — The type of OS that the server is configured for. Valid options are **ESXiStateless**, **Windows**, **Linux**, or **Custom**.
- **CPU Type** — The quantity and model of the CPUs in the server.
- **NIC** — The model name of the NIC card in the server, as obtained from HCSM.
- **HBA** — The model name of the HBA card in the server, as obtained from HCSM.
- **Hardware Details** — The server model, number of CPU cores, CPU model, and amount of onboard memory.
- **LOM Firmware** — The version of the management software on the server.
- **EFI Firmware** — The version of the EFI on the motherboard of the server.
- **Cores Per CPU** — The number of CPU cores in the server.
- **RAM** — The amount of physical memory in the server.
- **Make and Model** — The name of the manufacturer and the model of the server.

Viewing server inventory

The servers that UCP Director administers are displayed on the **Servers** table. To view the **Servers** table, in:

- vSphere Client and SCVMM, from the navigation bar, click on the **Servers** icon. For more information on the navigation bar, see "Using UCP Director Console" on page 76.
- vSphere Web Client, from the **Home** page, click on the **vCenter** link, and then click on the **Servers** link in the **Inventory Lists** section.

The **Servers** table displays a list of all servers in inventory.

Viewing a server summary

Additional information about a server is available on the server summary. To view the summary of a server, from the **Servers** table:

- In vSphere Client or SCVMM, right-click on the server, and then click on the **Server Summary** link.
- In vSphere Web Client, click on the name of the server in the vCenter menu on the left.

The top of the server summary displays the following properties: **Monitoring State**, **LOM IP Address**, **Current Image**, **Pending Image**, **OS Type**, and **ID**. **Maintenance Mode** is shown in vSphere Web Client.

Note: The **Host Name** property is shown at the top of the server summary.

The server power status indicator is shown near the properties at the top of the server summary. The serve power status indicator is used to display the power status of the server and LID, as follows:

- When the server or LID is active, the corresponding **Power** or **LID** field is green.
- When the server or LID is inactive, the corresponding **Power** or **LID** field is gray.

The **Make and Model** property of the server is displayed at the top of the server summary.

When using vSphere Client or SCVMM, you can display additional information about the server by moving the cursor over the info icon () in the power status indicator. When using vSphere Web Client, this information is displayed on the **Server Information** table.

In vSphere Client and SCVMM, the following tables are displayed at the bottom of the server summary:

- **Volumes** — Used to display the volumes that are attached to the server. For more information on volumes, see "Volumes" on page 176.
- **Ethernet Switches** — Used to display the Ethernet switches that are attached to the server.
- **Fibre Channel Switches** — Used to display the Fibre Channel switches that are attached to the server.
- **Converged Switches** — Used to display the converged switches that are attached to the server.
- **Events** — Used to display events related to the server. For more information on server events, see "Server events" on page 195.

For more information on switches, see Chapter 9, "Physical network administration".

In vSphere Web Client, the following:

- Table is displayed at the bottom of the server summary:
  - **Server Information** — Displays the server properties.
- Views are displayed on the **Monitor** tab:
  - **Tasks** — Displays jobs related to the server. For more information on server jobs, see "Server jobs" on page 195.
  - **Events** — Displays events related to the server. For more information on server events, see "Server events" on page 195.
- Tables are displayed on the **Related Objects** tab:
  - **Chassis** — Displays the chassis that the server is located in. For more information on chassis, see "Chassis" on page 196.

- **Hosts** — Displays a list of VMware hosts that are hosted on the server.
- **Ethernet Switches** — In a Brocade Ethernet or Cisco Ethernet configuration, displays a list of Ethernet switches that are attached to the server.
- **Fibre Channel Switches** — In a Brocade Ethernet or Cisco Ethernet configuration, displays a list of Fibre Channel switches that are attached to the server.
- **Converged Switches** — In a Cisco converged configuration, displays a list of converged switches that are attached to the server.
- **Volumes** — Displays a list of the volumes that are attached to the server. For more information on volumes, see "Volumes" on page 176.

For more information on switches, see Chapter 9, "Physical network administration".

Server jobs

When using vSphere Web Client, to view jobs related to a server:

1. From the server summary, click on the **Monitor** tab
2. Click on the **Tasks** tab.

For more information on jobs, see "Jobs" on page 62.

Server events

To view events related to a server, as well as the switches connected to the server, from the server summary in:

- vSphere Client or SCVMM, click on the **Events** tab.
- vSphere Web Client, click on the **Monitor** tab, and then click on the **Events** tab.

Events shown on this tab are filtered to only show those events that relate to the selected server. For more information on events, see "Events" on page 62.

Chassis

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director monitors and reports the following properties of each chassis:

- **SVP IP address** — Service Processor address for the chassis. Used to open a browser or SSH session.
- **Chassis Name** — The chassis name, as reported by HCSM.
- **Power** — The power state of the chassis.
- **Serial Number** — The serial number of the chassis.
- **Dictionary** — The dictionary version currently installed on the chassis SVP.
- **Parameter** — The equipment parameter currently used by the chassis SVP.
- **Available Dictionary** — The version of the chassis dictionary that is available. This version will be applied if the firmware is updated.
- **Available Parameter** — The version of the chassis equipment parameter that is available. This version will be applied if the firmware is updated.

Viewing chassis inventory in vSphere Web Client

When using vSphere Web Client, the chassis that UCP Director administers are displayed on the **Chassis** table. To view the **Chassis** table, from the **Home** page:

1. Click on the **vCenter** link.
2. Click on the **Chassis** link in the **Inventory Lists** section.

The **Chassis** table displays a list of all chassis that are being managed by UCP Director. For each chassis, the following properties are shown: **SVP IP Address**, **Chassis Name**, **Power**, **Monitoring State**, **Serial Number**, **ID**, **Global ID**, **Firmware**, **Dictionary**, **Parameter**, **Available Firmware**, **Available Dictionary**, and **Available Parameter**.

Viewing a chassis summary

Information about a chassis is available on the chassis summary. To view the summary of an individual chassis in:

- vSphere Client or SCVMM, from the **Servers** table, right-click on the name of the server that is located in the chassis you want to view details for, and then click on the **Chassis Summary** link.
- vSphere Web Client, from the **Chassis** table, click on the name of the chassis in the vCenter menu on the left.

The top of the chassis summary displays the following properties: **Monitoring State**, **Serial Number**, **Power**, and **ID**.

Note: The IP address of the chassis is shown at the top of the chassis summary.

The chassis power status indicator is shown near the properties at the top of the chassis summary. The chassis power status indicator is used to display the power status of each server and server LID, as follows:

- When the server or LID is active, the corresponding **Power** or **LID** field is green.
- When the server or LID is inactive, the corresponding **Power** or **LID** field is gray.

The **Make and Model** property of the chassis is displayed at the top of the chassis power status indicator.

The following tables are available at the bottom of the chassis summary:

- **Fan Modules** — Used to display the fan modules in the chassis. For more information on fan modules, see "Fan modules" on page 199.
- **Switch Modules** — Used to display the switch modules in the chassis. For more information on switch modules, see "Switch modules" on page 199.
- **Power Modules** — Used to display the power modules in the chassis. For more information on power modules, see "Power modules" on page 200.

- **Management Modules** — Used to display the management modules in the chassis. For more information on management modules, see "Management modules" on page 200.

In vSphere Client and SCVMM, the following tables are displayed in addition to the previous tables at the bottom of the chassis summary:

- **Servers** — Used to display the servers that are in the chassis. For more information on servers, see "Viewing server inventory" on page 193.

- **Events** — Used to display events related to the chassis. For more information on chassis events, see "Chassis events" on page 199.

In vSphere Web Client, the following:

- Views are displayed on the **Monitor** tab:
  - **Tasks** — Displays jobs related to the chassis. For more information on chassis jobs, see "Chassis events" on page 199.
  - **Events** — Displays events related to the chassis. For more information on chassis events, see "Chassis events" on page 199.
- Tables are displayed on the **Related Objects** tab:
  - **Hosts** — Displays a list of VMware hosts that are connected to the selected chassis.
  - **Servers** — Displays a list of all servers that are connected to the selected chassis. For more information on servers, see "Viewing server inventory" on page 193.

Chassis jobs in vSphere Web Client

When using vSphere Web Client, to view jobs related to a chassis:

1. From the chassis summary, click on the **Monitor** tab
2. Click on the **Tasks** tab.

For more information on jobs, see "Jobs" on page 62.

Chassis events

To view events related to a chassis, from the chassis summary in:

- vSphere Client or SCVMM, click on the **Events** tab.
- vSphere Web Client, click on the **Monitor** tab, and then click on the **Events** tab.

Events shown on this tab are filtered to only show those events related to the selected chassis. For more information on events, see "Events" on page 62.

Fan modules

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director monitors and reports the following properties of each fan module in the chassis:

- **Slot** — The slot that the fan module is installed in.
- **Health** — The health status of the fan module.
- **Power** — Whether the fan module is on or off.

To view fan modules that are located in a chassis, from the chassis summary, click on the **Fan Modules** tab.

Switch modules

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director monitors and reports the following properties of each switch module in the chassis:

- **Slot** — The slot that the switch module is installed in.
- **IP Address** — The management IP address of the switch module.
- **Health** — The health status of the switch module, as reported in HCSM.
- **Power** — The power status of the switch module.
- **Maintenance Mode** — Whether or not the switch module is in maintenance mode.

- **Serial Number** — The serial number of the switch module, as retrieved from HCSM.

The switch modules, both Ethernet and Fibre Channel, located in a chassis are listed even if they have not been added to inventory. To view additional details related to a switch, the switch will first need to be added to inventory.

To view the switch modules that are located in a chassis, from the chassis summary, click on the **Switch Modules** tab. For more information on switches, see Chapter 9, "Physical network administration".

Power modules

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director monitors and reports the following properties of each power module in the chassis:

- **Slot** — The slot that the power module is installed in.
- **Health** — The health status of the power module.
- **Power** — Whether the power module is on or off.

To view power modules that are located in a chassis, from the chassis summary, click on the **Power Modules** tab.

Management modules

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director monitors and reports the following properties of each management module in the chassis:

- **Slot** — The slot that the management module is installed in.
- **SVP IP Address** — The management IP address of the management module. Because one management module functions as the primary management module, and the second management module is in standby in the event that the primary management module fails, both management modules should show the same **SVP IP Address**.
- **Health** — The health status of the management module.
- **Power** — Whether the management module is on or off.
- **Active** — Whether or not the management module is actively in use.

- **Firmware** — The firmware version of the management module.
- **Dictionary** — The dictionary version of the management module.
- **Parameter** — The equipment parameter version of the management module.

To view management modules that are located in a chassis, from the chassis summary, click on the **Management Modules** tab.

Accessing a chassis

To facilitate administering a chassis, UCP Director Console provides links to administer the chassis through the SVP by either a Web or SSH interface.

To remotely connect to the SVP through:

- The Web interface:
  - In vSphere Client or SCVMM, from the chassis summary view, click on the **Chassis Actions** list, and then click on the **Console** link.
  - In vSphere Web Client, from the **Chassis** table, right-click on the chassis, and then click on the **Console** link.
- The SSH interface:
  - In vSphere Client or SCVMM, from the chassis summary view, click on the **Chassis Actions** list, and then click on the **Command Line** link.
  - In vSphere Web Client, from the **Chassis** table, right-click on the chassis, and then click on the **Command Line** link.

For information relating to the command line interface, see the release notes

Note: UCP components are configured with optimal settings before being deployed. Consult with HDS personnel before modifying them.

Updating chassis firmware in vSphere Web Client

When using vSphere Web Client, you can update chassis firmware. To ensure compatibility, switch firmware should be updated before updating chassis firmware. For more information on updating firmware, see "Firmware update management in vSphere Web Client" on page 64.

Before updating firmware on a chassis, UCP Director will check to ensure that the **Monitoring State** is OK.

To update the firmware on one chassis:

1. On the **Chassis** table, right-click on the name of the chassis that you want to update firmware on, and then click on the **Update Chassis Firmware** link.

2. In response to the confirmation message, click on the **Yes** button.

To update the firmware on a chassis and all servers in that chassis:

1. On the **Chassis** table, right-click on the name of the chassis that you want to update firmware on, and then click on the **Update Chassis and Server Firmware** link.

2. In response to the confirmation message, click on the **Yes** button.

When updating the firmware on a chassis and all servers in the chassis, the chassis will be updated first, then each server in the chassis will be updated. When this happens:

- Updates will be applied to servers sequentially.

- In vCenter, ESXi hosts will be put into maintenance mode as the updates are applied.

- If there is a failure at any stage in the process, the update will stop. When this happens, correct the failure and run the update again.

Updating server firmware in vSphere Web Client

When using vSphere Web Client, you can update server firmware. To ensure compatibility, chassis firmware should be updated before updating server firmware. For more information on updating firmware, see "Firmware update management in vSphere Web Client" on page 64.

To update the firmware on a server:

1. On the **Servers** table, right-click on the server that you want to update firmware on, and then click on the **Update Firmware** link.

2. In response to the confirmation message, click on the **Yes** button.

Refreshing server inventory

UCP Director periodically scans the servers in inventory. This is done to determine the relationship between servers and other components. For more information on inventory refresh, see “Refreshing inventory” on page 52.

To manually initiate an inventory refresh:

1. From the **Servers** table, click on the **Refresh Server Inventory** button.

2. In response to the confirmation message, click on the **Yes** button.

Note: When using UCP Director Console in vSphere Client, the page that you are viewing to display inventory will not refresh until you refresh the page as well. For information on refreshing the list of elements, see “Refreshing UCP Director Console pages” on page 80.

Power management

Under normal operating conditions, servers managed by UCP Director should not need to be powered off. From time to time, however, a server may need to be powered off or reset, such as to move it, deploy a different service template, or address a failure. You will not be able to power off, on, or reset a server when a template is being applied. This section contains instructions for:

- Powering off a server
- Powering on a server
- Resetting a server

Powering off a server

When powering off a server, UCP Director abruptly cuts power to the server. As a result, powering off a server is disruptive as the hypervisor manager will be unable to perform any operations on the server, such as moving VMs. When a server that is part of a cluster is powered off, however, the VMs will be migrated like they normally would. To gracefully shut down a:

- Standalone ESXi host in vCenter, put the server in maintenance mode before powering it off.

- Windows, Linux, or custom host, log into the OS and shutdown the server before powering it off.

To power off a server:

1. From the Servers table, right-click on the server you want to power off, and then click on the **Power Off** link.

2. If prompted to confirm powering off the server, click on the **Yes** button.

Powering on a server

Because server identity information is stored in server profiles, for a server to receive an IP address from the DHCP server and be accessible when it is powered on, a server profile will need to be applied.

To power on a server:

1. From the **Servers** table, right-click on the server you want to power on, and then click on the **Power On** link.

2. In response to the confirmation message, click on the **Yes** button.

Resetting a server

Resetting a server powers off the server before powering it back on.

To reset a server:

1. From the **Servers** table, right-click on the server you want to reset, and then click on the **Reset** link.

2. In response to the confirmation message, click on the **Yes** button.

Locating a server

To assist in locating a physical server in a large datacenter environment, the front indicator light can be turned on.

To activate the LID on a server, from the **Servers** table, right-click on the server, and then click on the **Turn LID On** link.

After a server has been located, to turn off the front indicator light, from the **Servers** table, right-click on the server, and then click on the **Turn LID Off** link.

Setting a non-hypervisor host name

You can manually set the host name that is reported for non-hypervisor Windows, Linux, and custom hosts. This can be used to manually track the host name that the system administrator configures on the server, or it can be used for inventory purposes.

To set the host name on a non-hypervisor host:

1. From the **Servers** table, right-click on the server you want to set the host name of, and then click on the **Set Host Name** link.

2. Type the name of the host in the **Host Name** field.

3. Click on the **OK** button.

Accessing a server

To facilitate administering a server, UCP Director Console provides a link to a console that can be used to administer the server.

To remotely connect to a server through the console, from the **Servers** table, right-click on the server, and then click on the **Console** link.

For information relating to console requirements, see the release notes.

13

Server profile administration

This chapter explains how to administer server profiles and server profile inventory in UCP. Before administering server profile inventory, it is important to understand how server profiles are used. For more information on server profiles, see “Service templates” on page 50.

Note: Because host deployment involves servers, images, server profiles, and service templates, the procedures involved are covered in Chapter 15, “Host deployment,” on page 241.

Server profile permissions

To administer host server profiles, your Active Directory account or group must:

- When using vCenter, be added to the UCP System Administrator role.
- When using SCVMM, be added to the SCVMM administrator role.

For more information on access requirements, see “Security” on page 65.

Server profile properties

In addition to the applicable standard properties listed in “Standard component properties” on page 53, UCP Director records the following properties of each server profile:

- **Server Profile Name** — The name that has been assigned to the server profile.
- **Server Name** — The value of the host name variable of the server that the server profile is associated with, if applicable.
- **IP Address** — The IP address assigned to the server profile.
- **OS Type** — The OS type associated with the server, either **Hypervisor** or **Non-Hypervisor**.
- **Server Model** — The server type that the server profile can be associated with.
- **Server Serial Number** — The serial number of the server that the server profile is associated with, if applicable.
- **UUID** — The UUID associated with the server profile.
- **Description** — The description of the server profile.
- **Subnet** — The subnet associated with the profile.
- **Gateway** — The gateway used for network communication by servers with the server profile applied.

- **DNS** — The DNS server used for domain resolution by servers with the server profile applied.

- **NIC Port**

  – **MAC Address** — The MAC Address associated with the NIC port in the server profile.

  – **VLAN** — The management VLAN ID associated with the NIC port in the server profile.

- **HBA Port**

  – **WWNN** — The WWNN associated with the HBA port in the server profile.

  – **WWPN** — The WWPN associated with the HBA port in the server profile.

EFI settings

UCP Director records the following EFI settings in each server profile:

- **Processor Turbo Mode** — Whether or not Intel processor turbo mode is enabled. The default is **Enabled**.

- **Processor Hyper-Threading** — Whether or not processor hyper-threading is enabled. The default is **Enabled**.

- **Processor Hardware Prefetcher** — Whether or not the processor instruction prefetcher is enabled. The default is **Enabled**.

- **Memory Mode** — The memory mode associated with the server profile. The optimal memory mode is dependent on the physical layout of the DIMMs. Valid options are **Existing**, **Independent**, **Mirroring**, and **Sparing**. The default is **Independent**.

- **Memory Speed** — The speed that the memory in the server has been configured to run at. Valid options are **Auto**, **Force DDR3 800**, **Force DDR3 1333**, and **Force DDR3 1600**. The default for B2 server models is **Auto**, and the default for A1/B1 server models is **Force DDR3 1600**.

- **Node Interleaving** — Whether or not NUMA node (CPU socket and corresponding memory banks) interleaving is enabled. The default mode is **NUMA**.

- **RAS Deconfigured Mode** — Whether or not RAS (reliability, availability, and serviceability) memory correction technology is enabled. The default is **Enabled**.

- **DDR Voltage** — The voltage of the memory in the server. Valid options are **Auto**, **Force to 1.50V**, and **Force to 1.35V**. The default is **Force to 1.5V**.

Viewing server profile inventory

The server profiles that UCP Director administers are displayed on the **Server Profiles** table. To view the **Server Profiles** table, in:

- vSphere Client and SCVMM, from the navigation bar, click on the **Provision** icon, and then click on the **Server Profiles** tab. For more information on the navigation bar, see "Using UCP Director Console" on page 76.

- vSphere Web Client, from the **Home** page, click on the **vCenter** link, and then click on the **Server Profiles** link in the **Inventory Lists** section.

The **Server Profiles** table displays a list of all server profiles in inventory.

Creating, editing, and removing server profiles

The following sections describe the processes that need to be completed when adding, editing, or removing a server profile. This section contains instructions for:

- Creating a server profile

- Editing a server profile

- Deleting a server profile

Creating a server profile

To create a server profile:

1. From the **Server Profiles** table, from:

   – vSphere Client or SCVMM, click on the **Create Server Profile** button

   – vSphere Web Client, click on the create icon ( ).

2. Click on the **Next** button then, on the **Create Server Profile** window:

   – In the **Server Profile Name** field, type the name of the server profile.

   – In the **Description** field, type a description of the server profile.

   – In the **OS Type** field, select either Hypervisor or Non-Hypervisor. Hypervisor server profiles will automatically use the management VLAN. You can specify the management VLAN ID for non-hypervisor server profiles.

   – In the **Network Adapter Ports** field, select the number of adapter ports to designate for the server.

   – In the **Server Model** field, select the model of the server.

3. Click on the **Next** button then, on the **Identity Settings** window:

   – In the **UUID** section, to enable UCP Director to automatically assign the UUID, select the **From UUID Pool** option.

     To manually specify the UUID, select the **Manual** option, and then type the UUID in the **UUID** field.

   – In the **Management IP Address** section, to enable UCP Director to automatically assign the IP address, select the **From IP Pool** option, and then select the pool from the **IP Address Pool** and the range from the **Range** field.

     To manually specify the IP address, select the **Manual** option, and then type the IP address in the **IP Address** field. Manually specified IP addresses are used to deploy the OS only and will not be used after the OS is deployed.

   – If this is a Cisco Ethernet or Brocade Ethernet configuration:

     • In the **Network Adapter MAC Address** section, to enable UCP Director to automatically assign the MAC address, select the **From MAC Pool** option, and then select the pool from the **MAC Address Pool** and the range from the **Range** field.

       To manually specify the MAC address, select the **Manual** option, and then type the MAC address to be assigned to each NIC port in the corresponding **NIC Port** field.

- In the **WWNN and WWPN** section, to enable UCP Director to automatically assign the WWNN and WWPNs, select the **From WWN Pool** option, and then select the pool from the **WWN Pool** and the range from the **Range** field.

  To manually specify the WWNN and WWPNs, select the **Manual** option, and then type the WWNN and WWPN to be assigned to each HBA port in the corresponding **HBA Port** fields.

– If this is a Cisco converged configuration, in the **Converged Network Adapter Settings** section, to enable UCP Director to automatically assign the MAC address, WWNN, and WWPNs, select the **From Pool** option. Then, for each ID, select the pools from the **MAC Address Pool** and **WWN Pool** fields, and the ranges from the **Range** fields.

  To manually specify the MAC address, WWNN, and WWPNs, select the **Manual** option, and then, for each physical port:

  - In the **MAC Address** column, type the MAC address that will be used for Ethernet traffic in the first field and for Fibre Channel traffic in the second field.

  - In the **WWNN** and **WWPN** columns, type the WWNN and WWPN to be used for Fibre Channel traffic.

– If you are creating a non-hypervisor server profile, in the **Native VLAN ID** field, type the VLAN ID that you will use for host management.

To be able to create a server profile, there needs to be enough IDs in the identity pools. For more information on ID pools, see "Identity types" on page 214.

4. Click on the **Next** button then, on the **EFI Settings** window:

   – To use default EFI settings, select the **EFI Default Settings** option.

   – To manually specify the EFI settings, deselect the **EFI Default Settings** option and, for each setting, select the option that you want to specify. Selecting **Existing** will leave the value that is currently set unchanged.

5. Review the server profile that will be created, and then click on the **Submit** button.

Editing a server profile

By editing a server profile, you can change the name, description, native VLAN ID, and EFI settings of that server profile.

To edit a server profile, from the **Server Profiles** table:

1. Right-click on the server profile that you want to edit, and then click on the **Edit** link.

2. Follow the appropriate procedures detailed in "Creating a server profile" on page 210. You are only able to edit the native VLAN ID on non-hypervisor server profiles.

When using vSphere Client or SCVMM, to edit a server profile, from the **Servers** table:

1. Right-click on the server that you want to edit, and then click on the **Edit Server Profile** link.

2. Follow the appropriate procedures detailed in "Creating a server profile" on page 210. You are only able to edit the native VLAN ID on non-hypervisor server profiles.

If the server profile is currently applied to a server, the server will need to be restarted to re-apply the server profile before the changes will take effect.

Deleting a server profile

To be able to delete a server profile, that server profile can not be applied to a server. To delete a server profile:

1. On the **Server Profiles** table, right-click on the name of the server profile that you want to remove, and then click on the **Delete** link.

2. In response to the confirmation message, click on the **Yes** button.

Viewing a server profile summary

Additional information about a server profile is available on the server profile summary. To view the summary of an individual server profile, from the **Server Profiles** table:

- In vSphere Client or SCVMM, right-click on the server profile, and then click on the **Server Profile Summary** link.
- In vSphere Web Client, click on the name of the server profile in the vCenter menu on the left.

The server profile summary view is divided into several sections that each contain different properties.

Note: The name of the server profile is shown at the top of the summary.

Identity types

In addition to being able to generate UUIDs, UCP Director maintains IP address, MAC address, and WWN pools. UCP Director also supports manually entered identities. To view an identity:

1. In:
   - vSphere Web Client and SCVMM, from the navigation bar, click on the **Provision** icon, then click on the **Identity Types** tab. For more information on the navigation bar, see "Using UCP Director Console" on page 76.
   - vSphere Client, from the **Home** page, click on the **vCenter** link, and then click on the **Identity Types** link in the **Inventory Lists** section.
2. Click on the link that corresponds to the type of identity that you want to see, as follows:
   - **Pools** — Used to display the pools and each range within each pool.
   - **Manual** — Used to display the IDs that have been manually allocated.

     The **Pools** link is used to display UUIDs that are automatically generated.

Managing IP ranges

All identity pool ranges are created when UCP is first deployed or upgraded to version 3.5.1. In an upgrade scenario, UCP examines the production servers and extracts the identity numbers from them. A server profile is generated for each blade and contains the exact identity numbers for the blade that it is assigned to. Assigned identities are viewable in the section for each identity type. If the identity number falls within one of the ranges, it will be found in the Allocated ID list under the Pool of that type. Otherwise, it is listed under the heading Manual.

The ranges of MAC, WWN, and UID contain enough identities to accommodate the maximum supported quantity of blades in UCP. Therefore, new ranges of these types are not needed.

More IP ranges, however, may be needed for a variety of reasons. The CLI or API must be used to create a new IP range. Care is needed when deciding the starting and ending IP address as well as the DNS server. These IP addresses are used during the deployment of the blade operating system, whether through Auto Deploy or through WDS. After deployment, the blade may continue to use the address if it also uses the UCP native VLAN ID. These blades will also get a host name from the DNS server.

If UCP was upgraded from version 3.0.2, the blades should access the UCPUtility VM for domain name resolution. If upgraded from v3.5, the blades use the AD VM for DNS.

New IP ranges can be made using the following CLI commands:

```
1. $IdentityPoolId = (Get-UcpIpAddressIdentityPool).IdentityPoolId

2. New-UcpIpAddressIdentityPoolRange -IdentityPoolId $IdentityPoolId -
   StartAddress <StartAddress> -EndAddress <EndAddress> -DefaultGateway
   <GatewayAddress> -Dns <AD-Or-UCPUtility-IP> -SubnetMask <SubnetMask>
```

Or by using the following API:

Request Header

```
POST https://ucpmanagement.ucp.local/api/identitypools/ipaddress/
<IPAddressPoolID>/identitypoolranges

HTTP/1.1

Content-Type: application/json; charset=utf-8
```

Request body

```
{

"StartAddress":"<IPAddress>",

"EndAddress":"<IPAddress>",

"SubnetMask":"<SubnetMask>",

"DefaultGateway":"<GatewayAddress>",

"DnsAddress":"<AD-Or-UCPUtility-IP>"

}
```

IDs allocated from a pool

For each identity type, the **Pools** link displays the IDs in the pool. These IDs are broken into two sections, **ID Ranges** and **Allocated IDs**. The **ID Ranges** section displays the available addresses in the pool. For each pool, the **ID Ranges** section displays the following:

- **ID** — The UCP Director ID number assigned to the pool. This number is dynamically assigned by UCP Director to the pool.
- **Start** — The first ID included in the pool.
- **End** — The last ID included in the pool.
- **Available** — The total number of identities in the pool that are available to be assigned.
- **Total** — The total number of identities in the pool.

Below the **ID Ranges** section is the **Allocated IDs** section. The **Allocated IDs** section displays the addresses of that type that have been allocated to server profiles. For each address, the **Allocated IDs** section displays:

- **Address** — The identity that is assigned to the profile.
- **Date Reserved** — The date the identity was assigned.
- **Server Profile ID** — The ID of the server profile that the identity is assigned to.

Manually entered IDs

For each identity type, the **Manual** link displays the IDs that have been manually entered. These IDs are shown in an **Allocated IDs** section. The **Allocated IDs** section lists each manually entered ID that is allocated to a server profile. For each address, the **Allocated IDs** section displays:

- **Address** — The identity that is assigned to the profile.
- **Date Reserved** — The date the identity was assigned.
- **Server Profile ID** — The ID of the server profile that the identity is assigned to.

Note: For UUIDs, both manually entered and dynamically assigned IDs are shown.

Applying a server profile

Applying a server profile to a server assigns the identity and EFI settings from the server profile to the server. When a server profile is applied to a server, the selected server will reboot and:

- The EFI settings on the server will be configured according to the server profile.
- The identities assigned to the server will be set according to the server profile.
- The DHCP server in UCP will be configured with the IP address and MAC address from the server profile.
- The native VLAN ID will be applied to the ports on the attached Ethernet switch.

To be able to apply a server profile to a server, the server must:

- Be powered off
- Not be part of a cluster
- Not have any storage attached
- Not currently have another server profile associated

- Be the same server model as specified in the server profile

To apply a server profile from the **Server Profiles** table:

1. On the **Server Profiles** table, right-click on the server profile that you want to assign, and then click on the **Apply** link.
2. On the **Apply Server Profile** window, select the server that you want to apply the server profile to.
3. Click on the **OK** button.

If using vSphere Client and SCVMM, you can also apply a server profile from the **Servers** table. To apply a server profile from the **Servers** table:

1. On the **Servers** table, right-click on the server that you want to assign a server profile to, and then click on the **Apply Server Profile** link.
2. On the **Apply Server Profile** window, select the server profile that you want to apply to the server.
3. Click on the **OK** button.

Move a server profile

Moving a server profile will power off the server that the server profile is applied to and apply the server profile to the selected server. Because of this, the server that the server profile is applied to must meet the same requirements when applying a server profile. For more information on the requirements to apply a server profile, see "Applying a server profile" on page 217.

To move a server profile from the **Server Profiles** table:

1. On the **Server Profiles** table, right-click on the server profile that you want to move, and then click on the **Move** link.
2. On the **Move Server Profile** window, select the server that you want to move the server profile to.
3. Click on the **OK** button.

If using vSphere Client and SCVMM, you can also move a server profile from the **Servers** table. To move a server profile from the **Servers** table:

1. On the **Servers** table, right-click on the server that you want to move the server profile from, and then click on the **Move Server Profile** link.
2. On the **Move Server Profile** window, select the server profile that you want to move the server to.
3. Click on the **OK** button.

Extract server profile

To extract a server profile:

1. From the **Servers** table, click on the **Extract Server Profile** button.
2. Select the server or servers to extract server profiles from.
3. Click on the **Next** button, and on the **Extract Server Profile** window:
   - In the **Server Profile Name** field, type a name for the server profile.
   - In the **Description** field, type a description for the server profile.
4. Click on the **Submit** button.

The server will be rebooted and the new profile will automatically be associated with the server. The server continues to use all of the same ID numbers except for UUID.

Remove server profile

Removing a server profile will disassociate it from the server but will not delete it. Before a server profile can be removed, the associated server must be powered off.

To remove a server profile from a server:

1. On the **Server Profiles** table, right-click on the server profile that you want to remove, and then click on the **Remove From Server** link.
2. Click on the **Yes** button when prompted.

14

Service template administration

This chapter explains how to administer service templates and service template inventory in UCP. Before administering service template inventory, it is important to understand how service templates are used. For more information on service templates, see “Service templates” on page 50.

Note: Because host deployment involves servers, images, server profiles, and service templates, the procedures involved are covered in Chapter 15, “Host deployment,” on page 241.

Service template permissions

To administer service templates, your Active Directory account or group must:

- When using vCenter, be added to the UCP System Administrator role.
- When using SCVMM, be added to the SCVMM administrator role.

For more information on access requirements, see "Security" on page 65.

Service template properties

In addition to the applicable standard properties listed in "Standard component properties" on page 53, UCP Director records the following properties of each service template:

- **Service Template Name** — The name that has been assigned in the service template.
- **Service Template Type** — The configuration and type of image that the service template has been configured to apply. Valid values are: **EsxiStateless**, **EsxiStatelessCluster**, **WindowsHyperV**, **Windows**, **Linux**, or **Custom**.
- **Boot Image** — The name of the boot image that is assigned to the service template.
- **Boot Image Type** — The type of image applied by the service template. Valid values are: **EsxiStateless**, **Windows**, **Linux**, or **Custom**.
- **Cluster Template** — When using vCenter, whether or not the service template is an ESXi cluster service template.

ESXi host service templates

In addition to the properties that UCP Director records for all service template types, UCP Director also records the following properties for ESXi host service templates:

- **VM Network VLAN IDs** — The VLAN IDs that will be configured on Ethernet or converged switch ports connected to servers that this service template will be attached to. These VLAN IDs will also be applied to the virtual distributed switches that the servers are connected to.

- **Management VLAN ID** — The management VLAN that will be used for hosts based on this service template.

ESXi cluster service templates

In addition to the properties that UCP Director records for all service template types, UCP Director also records the following properties for ESXi host service templates:

- **VM Network VLAN IDs** — The VLAN IDs that will be configured on Ethernet or converged switch ports connected to servers that this service template will be attached to. These VLAN IDs will also be applied to the virtual distributed switches that the servers are connected to.
- **Management VLAN ID** — The management VLAN that will be used for hosts based on this service template.
- **vSphere Host Profile** — The name of the associated vSphere host profile.
- **vMotion VLAN ID** — The VLAN ID that will be used for vMotion.
- **Enable High Availability** — Whether or not the service template is for a high availability ESXi cluster.
- **Failover CPU Percentage** — For high availability ESXi cluster service templates, the reserve CPU percentage to maintain in case a host experiences a failure or needs to be powered off.
- **Failover RAM Percentage** — For high availability ESXi cluster service templates, the reserve RAM percentage to maintain in case a host experiences a failure or needs to be powered off.
- **Enable vSphere DRS** — Whether or not vSphere Distributed Resource Scheduler is enabled on the hosts in the cluster.
- **Create Storage Cluster** — Whether or not the cluster is configured as a vSphere storage cluster.
- **Enable Storage DRS** — For clusters that are configured as a storage cluster, whether or not DRS is enabled.
- **Automate Storage DRS** — For clusters that are configured as a storage cluster, whether or not the movement of VMs is automated between volumes.

- **Enable Storage DRS I/O Metric** — For clusters that are configured as a storage cluster, whether or not to use I/O metrics in the storage DRS recommendations.

Hyper-V and Windows service templates

In addition to the properties that UCP Director records for all service template types, UCP Director also records the following properties for Hyper-V and Windows service templates:

- **Boot Volume Pool** — The pool ID that the boot volume is located in.
- **Boot Volume Size** — The size of the boot volume.
- **Boot Unattend Location** — The location of the Windows boot unattend file.
- **Image Unattend Location** — The location of the Windows image unattend file.
- **Management VLAN ID** — The management VLAN that will be used for hosts based on this service template.
- **Storage System ID** — The ID of the storage system that the boot volume is part of.
- **Trunk VLAN IDs** — The VLAN IDs that will be configured on Ethernet or converged switch ports connected to servers that this service template will be attached to.

Linux host service templates

In addition to the properties that UCP Director records for all service template types, UCP Director also records the following properties for Linux service templates:

- **Boot Volume Pool** — The pool ID that the boot volume is located in.
- **Boot Volume Size** — The size of the boot volume.
- **Kickstart Location** — The location of the Linux kickstart file.
- **Storage System ID** — The ID of the storage system that the boot volume is part of.

- **Trunk VLAN IDs** — The VLAN IDs that will be configured on Ethernet or converged switch ports connected to servers that this service template will be attached to.

Custom host service templates

In addition to the properties that UCP Director records for all service template types, UCP Director also records the following properties for custom host service templates:

- **Trunk VLAN IDs** — The VLAN IDs that will be configured on Ethernet or converged switch ports connected to servers that this service template will be attached to.

Viewing service template inventory

The service templates that UCP Director administers are displayed on the **Service Templates** table. To view the **Service Templates** table, in:

- vSphere Client and SCVMM, from the navigation bar, click on the **Provision** icon, and then click on the **Service Templates** tab. For more information on the navigation bar, see "Using UCP Director Console" on page 76.

- vSphere Web Client, from the **Home** page, click on the **vCenter** link, and then click on the **Service Templates** link in the **Inventory Lists** section.

The **Service Templates** table displays a list of all service templates in inventory.

Creating, cloning, editing, and removing service templates

The following sections describe the processes that need to be completed when adding, editing, or removing a service template. This section contains instructions for:

- Creating a service template
- Cloning a service template
- Deleting a service template

Creating a service template

This section contains instructions for:

- Creating an ESXi standalone service template
- Creating an ESXi cluster service template
- Creating a Hyper-V, Windows, or Linux service template
- Creating a custom host service template

Creating an ESXi standalone service template

To create an ESXi standalone service template:

1. From the **Service Templates** table, from:
   - vSphere Client or SCVMM, click on the **Create Service Template** button
   - vSphere Web Client, click on the create icon ().
2. On the **Create Service Template** window:
   - In the **Service Template Name** field, type the name of the service template.
   - In the **Type** field, select **ESXi Standalone**.
3. Click on the **Next** button then, on the next window:
   - In the **Boot Image** field, select the name of the image to be applied to servers based on the service template.
4. Click on the **Next** button then, on the next window:
   - The **Management VLAN ID** field is read only and is used to show you the management VLAN ID that ESXi hosts use.
   - In the **VM Network VLAN IDs** field, type the VM network VLANs that will be applied to ports on the Ethernet or converged switches connected to hosts based on this service template.

VLANs should be entered by range or individual VLAN ID in a comma separated format. To enter a range of VLANs, enter X-Y, where X is the first VLAN ID and Y is the last VLAN ID. For example, entering *5, 10-12, 20* would set the VLANs to 5, 10, 11, 12, and 20.

5. Click on the **Next** button then, on the next window, to associate storage with the service template:

   – To indicate that a volume should be created and attached to hosts based on the service template when it is deployed:

      1. Click on the **Create** button.

      2. In the **Disk Size** field, type the size of the volume to be created.

      3. To configure the volume as a datastore, select the **Format** option, and then type the name of the datastore in the **Name** field.

      Important: When deploying an ESXi service template to more than one host or cluster, the datastore name will need to be edited between each deployment because datastore names must be unique to the datastore.

      4. To configure a raw, non-datastore volume, select the **Raw Volume** option, and then select the way the volume should be optimized from the **Intended Use** field. Possible options include **Default**, **Windows**, and **Linux**.

         Note: You may need to unselect the Format checkbox to see the Raw Volume option.

      5. To manually select the storage system ports to use, select the **Manually Select Storage System Ports** option, and then select the appropriate ports for each fabric.

      6. Select the pool to create the volume in from the **Storage Pools** table. For more information on storage pools, see "Pools" on page 171.

      7. Click on the **OK** button.

   – To attach an existing volume or volumes:

      1. Click on the **Attach** button.

      2. Select the volume or volumes to attach from the **Volumes** table.

3. Click on the **OK** button.

Note: If creating an ESXi cluster service template with storage DRS enabled, at least two datastores must be attached or created. Attaching additional datastores can increase performance.

6. Click on the **Next** button.

7. Review the service template that will be created, and then click on the **Submit** button.

Creating an ESXi cluster service template

Before creating an ESXi cluster service template you will need to prepare the VMware host profile that will be applied by the ESXi cluster service template. For more information on VMware host profiles, see "Preparing VMware host profiles in vCenter" on page 237.

To create an ESXi cluster service template:

1. From the **Service Templates** table, from:
   - vSphere Client or SCVMM, click on the **Create Service Template** button
   - vSphere Web Client, click on the create icon ().
2. On the **Create Service Template** window:
   - In the **Service Template Name** field, type the name of the service template.
   - In the **Type** field, select **ESXi Cluster**.
3. Click on the **Next** button then, on the next window:
   - In the **Boot Image** field, select the name of the image to be applied to servers based on the service template.
   - In the **vSphere Host Profile** field, select the vSphere host profile to apply to hosts in the cluster created by the service template. For more information on preparing a vSphere host profile, see "Preparing VMware host profiles in vCenter" on page 237.

4. Click on the **Next** button then, on the next window:

   – To configure the service template for VMware high availability, select the **Enable High Availability** option, then:

     • In the **Failover CPU Percentage** field, type the reserve CPU percentage. This is the reserve CPU percentage to maintain before migrating VMs to another host.

     • In the **Failover RAM Percentage** field, type the reserve RAM percentage. This is the reserve RAM percentage to maintain before migrating VMs to another host.

   Note: Applying a service template that is configured for High Availability requires a minimum of 3 servers.

   – To enable vSphere DRS, select the **Enable vSphere DRS** option.

5. Click on the **Next** button then, on the next window:

   – If creating an ESXi cluster service template with a new VDS, select the **Create New VDS** option, and then:

     • The **Management VLAN ID** field is read only and is used to show you the management VLAN ID that ESXi hosts use.

     • In the **VM Network VLAN IDs** field, type the VLANs that will be applied to ports on the Ethernet or converged switches connected to hosts based on this service template.

       VLANs should be entered by range or individual VLAN ID in a comma separated format. To enter a range of VLANs, enter X-Y, where X is the first VLAN ID and Y is the last VLAN ID. For example, entering *5, 10-12, 20* would set the VLANs to 5, 10, 11, 12, and 20.

       UCP Director creates a separate port group on the VDS for each data network VLAN ID when the service template is deployed. If you want the VLAN IDs to share a single port group, only specify one VLAN ID in the service template. Then, after deploying the template, you can add additional VLAN IDs to the VDS and configure the cluster network to apply the VLAN IDs to the connected Ethernet or converged switches. For more information on configuring the cluster network, see "Configuring VLANs by hosts in a cluster" on page 153.

- In the **vMotion VLAN ID** field, type the vMotion VLAN ID that will be applied to ports on the Ethernet or converged switches connected to hosts based on this service template.

– If creating an ESXi cluster using an existing VDS, select the **Use Existing VDS** option, and then:

- In the **Distributed Switch** field, select the name of the VDS that you want to use.
- In the **Management Port Group Name**, select the associated management port group that you want to use for the UCP management network.
- In the **vMotion Port Group Name**, select the associated port group that will be used for vMotion.

6. Click on the **Next** button then, on the next window, to associate storage with the service template:

– If creating an ESXi storage cluster template, select the **Create Storage Cluster** option. Then, to enable storage DRS for the storage cluster, select the **Enable Storage DRS** option and:

- To fully automate the I/O metric for storage DRS recommendations, select the **Automate Storage DRS** option.

Note: If the I/O metric for storage DRS recommendations is fully automated, you will not be able to use volumes in HDT pools.

- To enable the vSphere I/O metric for storage DRS recommendations setting, select the **Enable Storage DRS I/O Metric** option.

Note: If creating a storage cluster, all existing or new datastores based on the template will be added to the storage cluster.

If creating an storage DRS cluster, VMs will be able to be dynamically moved from one volume to another for load balancing. As a result, at least two volumes will be required to create the storage DRS cluster.

– To indicate that a volume should be created and attached to hosts based on the service template when it is deployed:

1. Click on the **Create** button.
2. In the **Disk Size** field, type the size of the volume to be created.
3. To configure the volume as a datastore, select the **Format** option, and then type the name of the datastore in the **Name** field.

Important: When deploying an ESXi service template to more than one host or cluster, the datastore name will need to be edited between each deployment because datastore names must be unique to the datastore.

4. To configure a raw, non-datastore volume, select the **Raw Volume** option, and then select the way the volume should be optimized from the **Intended Use** field. Possible options include **Default**, **Windows**, and **Linux**.

   Note: You may need to unselect the Format checkbox to see the Raw Volume option.

5. To manually select the storage system ports to use, select the **Manually Select Storage System Ports** option, and then select the appropriate ports for each fabric.
6. Select the pool to create the volume in from the **Storage Pools** table. For more information on storage pools, see "Pools" on page 171.
7. Click on the **OK** button.

– To attach an existing volume or volumes:

1. Click on the **Attach** button.
2. Select the volume or volumes to attach from the **Volumes** table.
3. Click on the **OK** button.

Note: If creating an ESXi cluster service template with storage DRS enabled, at least two datastores must be attached or created. Attaching additional datastores can increase performance.

7. Click on the **Next** button.

8. Review the service template that will be created, and then click on the **Submit** button.

Creating a Hyper-V, Windows, or Linux service template

To create a Hyper-V, Windows or Linux service template:

1. From the **Service Templates** table, from:

   – vSphere Client or SCVMM, click on the **Create Service Template** button

   – vSphere Web Client, click on the create icon ().

2. On the **Create Service Template** window:

   – In the **Service Template Name** field, type the name of the service template.

   – In the **Type** field, select either the **Hyper-V Standalone**, **Windows**, or **Linux** options..

3. Click on the **Next** button then, on the next window, define the boot volume that will be created by the service template:

   – If creating a Hyper-V or Windows service template:

   • In the **Boot Image** field, select the name of the image to be applied to servers based on the service template.

   • In the **Boot Unattend Location** field, select the location of the boot unattend file.

   • In the **Image Unattend Location** field, select the location of the image unattend file.

   • In the **Boot Volume Size** field, type the size of the boot volume to create.

Note: The minimum boot volume size for Windows images is 44 GB and the maximum size is 2 TB.

- Select the pool to create the volume in from the **Boot Volume Pool** table. For more information on storage pools, see "Pools" on page 171.

– If creating a Linux service template:

- In the **Boot Image** field, select the name of the image to be applied to servers based on the service template.
- In the **Kickstart Location** field, select the location of the kickstart file.
- In the **Boot Volume Size** field, type the size of the boot volume to create.

Note: The minimum boot volume size for Linux images is 8.5 GB and the maximum size is 16 TB.

- Select the pool to create the volume in from the **Boot Volume Pool** table. For more information on storage pools, see "Pools" on page 171.

4. Click on the **Next** button then, on the next window:

– If creating a Hyper-V service template, the **Management VLAN ID** field is read only and is used to show you the management VLAN ID that Hyper-V hosts use.

– The **Trunk VLAN IDs** field, type the trunk VLANs that will be applied to ports on the Ethernet or converged switches connected to hosts based on this service template.

VLANs should be entered by range or individual VLAN ID in a comma separated format. To enter a range of VLANs, enter X-Y, where X is the first VLAN ID and Y is the last VLAN ID. For example, entering *5, 10-12, 20* would set the VLANs to 5, 10, 11, 12, and 20.

5. Click on the **Next** button then, on the next window, to associate additional storage with the service template:

– To indicate that a volume should be created and attached to hosts based on the service template when it is deployed:

1. Click on the **Create** button.
2. In the **Disk Size** field, type the size of the volume to be created.

3. To manually select the storage system ports to use, select the **Manually Select Storage System Ports** option, and then select the appropriate ports for each fabric.

4. Select the pool to create the volume in from the **Storage Pools** table. For more information on storage pools, see "Pools" on page 171.

5. Click on the **OK** button.

– To attach an existing volume or volumes:

1. Click on the **Attach** button.

2. Select the volume or volumes to attach from the **Volumes** table.

3. Click on the **OK** button.

6. Click on the **Next** button.

7. Review the service template that will be created, and then click on the **Submit** button.

Creating a custom host service template

To create a custom host service template:

1. From the **Service Templates** table, from:

– vSphere Client or SCVMM, click on the **Create Service Template** button

– vSphere Web Client, click on the create icon ().

2. On the **Create Service Template** window:

– In the **Service Template Name** field, type the name of the service template.

– In the **Type** field, select the **Custom** option.

3. Click on the **Next** button then, on the next window:

– In the **Boot Image** field, select the **Custom Image** option.

4. Click on the **Next** button then, on the next window:

   – The **Trunk VLAN IDs** field, type the trunk VLANs that will be applied to ports on the Ethernet or converged switches connected to hosts based on this service template.

     VLANs should be entered by range or individual VLAN ID in a comma separated format. To enter a range of VLANs, enter X-Y, where X is the first VLAN ID and Y is the last VLAN ID. For example, entering *5, 10-12, 20* would set the VLANs to 5, 10, 11, 12, and 20.

5. Review the service template that will be created, and then click on the **Submit** button.

Cloning a service template

To clone a service template:

1. On the **Service Templates** table, right-click on the name of the service template that you want to clone, and then click on the **Clone** link.

2. Type the name of the cloned service template in the **Service Template Name** field.

3. Click on the **OK** button.

Editing a service template

By editing a service template, you can change the name of that service template. To edit a service template:

1. From the **Service Templates** table, right-click on the service template that you want to edit, and then click on the **Edit** link.

2. Follow the appropriate procedures detailed in "Creating a service template" on page 226. When editing a service template, the **Boot Image** field will be filtered to show only the images of the selected image type.

Deleting a service template

Because service templates are only used when deploying a server, deleting a service template will not affect any server that has already been deployed using it.

To delete a service template:

1. On the **Service Templates** table, right-click on the name of the service template that you want to remove, and then click on the **Delete** link.

2. In response to the confirmation message, click on the **Yes** button.

Viewing a service template summary

Additional information about a service template is available on the service template summary. To view the summary of an individual service template, from the **Service Templates** table:

- In vSphere Client or SCVMM, right-click on the service template, and then click on the **Service Template Summary** link.

- In vSphere Web Client, click on the name of the service template in the vCenter menu on the left.

Note: The name of the service template is shown at the top of the summary.

The **Volumes** table is displayed at the bottom of the service template summary. The **Volumes** table is used to display the volumes associated with the service template that will be attached to hosts that are deployed using it.

Service template jobs in vSphere Web Client

When using vSphere Web Client, to view jobs related to a service template, while viewing the service template summary, click on the **Monitor** tab, and then click on the **Tasks** tab. For more information related to the jobs shown on the **Tasks** tab, see "Jobs" on page 62.

Service template events in vSphere Web Client

When using vSphere Web Client, you can view the events related to a service template. To view events related to a service template, while viewing a service template summary, click on the **Monitor** tab, and then click on the **Events** tab.

Events shown on this tab are filtered to only show those events that relate to the selected service template. For more information related to the events shown on the **Events** tab, see "Events" on page 62.

Preparing VMware host profiles in vCenter

When creating an ESXi cluster service template, UCP Director uses VMware host profiles to define some of the host settings. A sample profile is included with UCP. This host profile, and subsequent copies, can be used when creating an ESXi cluster service template.

Instead of using the sample host profile, you can manually create a host profile for use with UCP Director. To manually create and configure a host profile:

1. Configure an ESXi reference host as follows:

   – A standalone host that is not part of a cluster.

   – Have two NICs attached to a standard vSwitch.

   – Not using a virtual distributed switch (VDS).

   – Send syslogs to the syslog server on the UCPUtility VM on port 514. This can be configured by using SSH to connect to the host and issuing the following commands:

     ```
     esxcli system syslog config set --loghost='udp://
     UCPUTILITYVMIP:514'

     esxcli system syslog config set –logdir-unique=true

     esxcli system syslog reload
     ```

     Where UCPUTILITYVMIP is the IP address of the UCPUtility VM.

   – Send the coredump to the vCenter VM on port 6500. This can be configured by using SSH to connect to the host and issuing the following commands:

     ```
     esxcli system coredump network set --interface-name vmk0 --server-
     ipv4 VCENTERIP --server-port 6500

     esxcli system coredump network set --enable true

     esxcli system coredump network get

     exit
     ```

     Where VCENTERIP is the IP address of the vCenter VM.

- Be deployed using the same image that will be used by the cluster.

2. Create a host profile from the reference host
3. Edit the host profile and configure it as follows:
   - Firewall security — In the **Firewall configuration > Ruleset Configuration** section, enable the following rulesets:
     - activeDirectoryAll
     - ntpClient
     - syslog
   - Storage — In the **Storage configuration > Native Multi-Pathing > Storage Array Type Plugin (SATP) configuration > SATP default PSP configuration > VMW_SATA_DEFAULT_AA** section, change the **PSP name** to *VMW_PSP_RR*.

Part V: Host deployment

This part contains the following chapter:

15

Host deployment

This chapter explains how to prepare, deploy, and configure hosts in UCP. Deploying servers in UCP requires a firm understanding of UCP architecture as well as how UCP Director functions.

For more information on:

- UCP architecture, see Chapter 2, “UCP hardware components,” on page 11.
- How UCP Director functions, see Chapter 3, “UCP software components,” on page 41.

Overview

While UCP Director automates many of the processes required to deploy hosts and clusters, there are several manual procedures that need to be performed. Specifically, to deploy a host or cluster, you will need to:

- Preparing UCP and the hypervisor manager
- Preparing the server or servers
- Deploying the service template
- Configuring the host or cluster

Preparing UCP and the hypervisor manager

Before deploying a host, you will need to ensure that the appropriate configurations have been made in UCP Director, as follows:

- For ESXi clusters in vCenter:
  - You will need to prepare a VMware host profile. For more information on host profiles, see "Preparing VMware host profiles in vCenter" on page 237.
  - If you will use an existing VDS instead of creating a new one, you will need to prepare the VDS. For more information on preparing the VDS, see "vCenter cluster networking" on page 158.
- When using SCVMM, you will need to prepare the networking configuration for the hosts. For more information on preparing host networking, see "SCVMM host networking" on page 156.
- You will need to prepare a server profile for each host. For more information on server profiles, see Chapter 13, "Server profile administration," on page 207.
- You will need to prepare a service template to administer the deployment. For more information on service templates, see Chapter 14, "Service template administration," on page 221.

Preparing the server or servers

After preparing UCP for host deployment, before you can deploy a host you will need to ensure that the server is properly configured, as follows:

- The server must be powered off or, when using vCenter, in maintenance mode.
- No volumes are attached to the server. This includes ensuring that no storage connections are configured on the HBA ports in the HBA EFI.
- When using vCenter, no VDS applied and not in a cluster.
- Any server profiles that are currently attached to the servers are the server profiles that you intend to deploy.

Deploying the service template

After UCP Director and the server or servers have been properly configured for host deployment, you will need to use the service template that you configured. Depending on the type of host or cluster that you want to deploy, the procedures for deploying a service template will be different. For instructions on deploying:

- An ESXi cluster, see "Deploying an ESXi cluster" on page 244.
- One or more Hyper-V hosts, see "Deploying a Hyper-V service template" on page 247.
- An ESXi standalone, Windows, Linux, or custom host, see "Deploying an ESXi standalone or non-hypervisor Windows, Linux, or custom host from a service template" on page 250.

When deploying an ESXi cluster, or if the Hyper-V hosts will be clustered, it is best practice to use servers from different chassis to increase component redundancy.

Configuring the host or cluster

After deploying the service template, additional changes may need to be made, as follows:

- For an ESXi cluster, you will need to configure settings in the host profile and configure high availability. For more information on configuring an ESXi cluster, see "Configuring an ESXi cluster" on page 245.

- For a Hyper-V standalone host, you will need to configure host networking. For more information on Hyper-V standalone host networking, see “Configuring Hyper-V standalone host networking” on page 248.

- For hosts that will be clustered into a Hyper-V cluster, you will need to configure the hosts and create the cluster. For more information on Hyper-V clustering, see “Configuring a Hyper-V cluster” on page 248.

- For Windows, Linux, and custom hosts, you will need to manually configure networking on the host.

If you have configured networking on the host, you can then use UCP to configure the network settings from the host in UCP Director. For more information on configuring networking in UCP Director, see Chapter 10, “Logical network administration,” on page 151.

Deploying and configuring ESXi clusters in vCenter

After preparing the host profile and server profile for each host in the cluster, the service template, and servers, you are ready to deploy and configure the ESXi cluster. This section contains instructions on:

- Deploying an ESXi cluster

- Configuring an ESXi cluster

Deploying an ESXi cluster

An ESXi cluster service template can be deployed to all servers in an ESXi cluster at the same time. Doing this will automatically create the ESXi cluster.

To deploy an ESXi cluster service template:

1. On the **Service Templates** table, right-click on the ESXi cluster template that you want to use to create the ESXi cluster, and then click on the **Apply** link.

2. On the next window:

   – In the **Cluster Name** field, type a name to assign to the cluster in VMware.

– In the **Servers** field, type the number of servers to assign to the ESXi cluster.

3. Click on the **Next** button then, on the next window, select the servers to add to the ESXi cluster.

4. Click on the **Next** button then, on the next window, for each server:

   – In the **vMotion IP** column, type the vMotion IP address to assign to the server.

   – In the **vMotion Subnet** column, type the subnet to use for vMotion on the server.

   Servers are listed by chassis and slot.

5. Click on the **Next** button then, on the next window, assign an available server profile to each of the selected servers. Each selected server and available server profile is listed, as follows:

   – Selected servers — Listed, by chassis and slot, in the **Selected Servers** section.

   – Available server profiles — Listed in the **Available Server Profiles** section. Each available server profile is listed by both the server profile name and associated IP address.

   To assign an available server profile to a server, click on it in the **Available Server Profiles** column and drag it to the slot that you want to assign it to in the **Selected Servers** column. If one of the servers already has a server profile applied, that same server profile needs to be re-applied to the server.

6. Click on the **Finish** button to deploy the service template.

Configuring an ESXi cluster

After UCP completes the cluster, you will need to use the vSphere Web Client to edit the host profile that is applied to the hosts in the cluster. Not all of these options can be seen when using the thick client.

To do this, configure the following:

- Root password — In the **Security configuration** section, select the **Configure a fixed administrator password** option, and then type the password in the **Password** and **Confirm Password** fields.

- Gateway — In the **Networking configuration > NetStack Instance > defaultTcpipStack > IP route configuration** section, type the gateway in the **Default IPv4 gateway** field.

- Storage — In the **Storage configuration > Native Multi-Pathing (NMP)** section, deselect the **PSP and SATP configuration for NMP devices** option to allow the Hitachi HBA driver to manage the settings.

Because the reference host was removed, add one of the cluster members as the reference host and re-apply the host profile to the cluster. Next, reboot all hosts in the cluster then, from the host profile, check the cluster for compliance.

The following is only needed if the cluster service template was not configured to create a storage cluster or enable HA on the host cluster:

- Configure the vSphere heartbeat datastores. To do this, ensure that the cluster has at least two 10G named datastores. For more information on creating datastores, see "Creating a new cluster volume" on page 184.

- Edit the cluster settings and enable HA and DRS. When enabling HA, select the 10G heartbeat datastores that were created.

Deploying and configuring Hyper-V hosts and clusters in SCVMM

After preparing networking in SCVMM, as well as the server profile, service template, and server, you are ready to deploy and configure a Hyper-V host.

Note: UCP Windows Deployments configure the default page file to be a maximum of 4GB. If your workload requires an alternate page file setting, please see http://support.microsoft.com/kb/2860880 to determine what settings are most appropriate for your workload, and then apply that setting to each host as necessary.

This section contains instructions on:

- Deploying a Hyper-V service template

- Configuring Hyper-V standalone host networking

- Configuring a Hyper-V cluster

Deploying a Hyper-V service template

A Hyper-V service template can be used to create one or more Hyper-V hosts.

To deploy a Hyper-V service template:

1. On the **Service Templates** table, right-click on the Hyper-V service template that you want to use, and then click on the **Apply** link.

2. Select the servers to apply the service template to then click on the **Next** button.

3. Assign an available server profile to each of the selected servers. Each selected server and available server profile is listed, as follows:

   – Selected servers — Listed, by chassis and slot, in the **Selected Servers** section.

   – Available server profiles — Listed in the **Available Server Profiles** section. Each available server profile is listed by both the server profile name and associated IP address.

   To assign an available server profile to a server, click on it in the **Available Server Profiles** column and drag it to the slot that you want to assign it to in the **Selected Servers** column. If one of the servers already has a server profile applied, that same server profile needs to be re-applied to the server.

4. Click on the **Next** button then, on the next window:

   – In the **Username** field, type the username of a user with credentials to add the host to SCVMM.

   – In the **Password** field, type the password that corresponds to the indicated user.

   – In the **Host Groups** field, select the host group that the host will be added to.

5. Click on the **Finish** button to deploy the service template.

Note: UCP Director does not automatically configure NIC teaming in SCVMM. As a result, after deploying a Hyper-V template, you will need to configure NIC teaming for the server to ensure redundant paths.

If creating more than one Hyper-V host for the purpose of creating a Hyper-V cluster, you can manually cluster them after they are deployed. For more information on creating a Hyper-V cluster, see "Configuring a Hyper-V cluster" on page 248.

Configuring Hyper-V standalone host networking

After using a service template to deploy a Hyper-V host, you will need to configure a virtual switch on the host using the logical switch created in SCVMM for network access. When configuring the virtual switch, add a virtual network adapter for the each SCVMM VM network that will be configured on the host. Only the virtual network adapter that supports the management SCVMM VM network should have the **This virtual network adapter inherits settings from the physical management adapter** setting selected.

Configuring a Hyper-V cluster

After using a service template to deploy the Hyper-V hosts that you will add to a cluster, you will need to prepare them for clustering, as follows:

1. Configuring cluster networking
2. Configuring the quorum drive
3. Creating the Hyper-V cluster

Configuring cluster networking

Each Hyper-V host in a cluster needs to have a virtual switch configured on the host using the logical switch created in SCVMM for network access. When configuring the virtual switch, add a virtual network adapter for each SCVMM VM network that will be used on the host, as follows:

- Management — Select the **This virtual network adapter inherits settings from the physical management adapter** setting.
- Cluster and Live Migration— Select and assign a static IP address to the vNIC.

Additional virtual network adapters should be added to each host in the cluster for each VM network that the cluster will use.

Configuring the quorum drive

Review Microsoft's best practices for a quorum drive:

http://technet.microsoft.com/en-us/library/cc770620(v=ws.10).aspx

If a Quorum drive will be required by the cluster:

1. Create and attach a formatted NTFS volume to one of the hosts that will be part of the cluster. For more information on creating and attaching a volume to a host, see "Creating a new host volume" on page 181.

2. After the volume has been created, attach the volume to each additional host that will be part of the cluster. For more information on attaching an existing volume to a host, see "Attaching an existing volume to a host" on page 182.

Creating the Hyper-V cluster

Use SCVMM to create the cluster. When creating the cluster:

- Use a unique IP address that:
  - Is specified in a UCP IP address range that will not be used by a service template.
  - Will not conflict with any IP addresses allocated to UCP IP address ranges.
- When selecting storage, the smallest drive will be selected as the quorum drive. If additional volumes have been attached, ensure that the quorum drive is the smallest volume.
- Because virtual switches were already attached to each host in the cluster, do not specify any additional virtual switches.

Deploying an ESXi standalone or non-hypervisor Windows, Linux, or custom host from a service template

To apply a service template to one or more servers:

1. On the **Service Templates** table, right-click on the service template that you want to apply, and then click on the **Apply** link.

Important: When using vCenter, if the service template specifies a formatted datastore, you can only apply the service template to one server at a time. This is because datastore names must be unique and the name of the datastore will have to be changed between deployments.

2. Select the servers to apply the service template to then click on the **Next** button.

3. Assign an available server profile to each of the selected servers. Each selected server and available server profile is listed, as follows:

   – Selected servers — Listed, by chassis and slot, in the **Selected Servers** section.

   – Available server profiles — Listed in the **Available Server Profiles** section. Each available server profile is listed by both the server profile name and associated IP address.

   To assign an available server profile to a server, click on it in the **Available Server Profiles** column and drag it to the slot that you want to assign it to in the **Selected Servers** column. If one of the servers already has a server profile applied, that same server profile needs to be re-applied to the server.

4. Click on the **Finish** button to deploy the service template.

Changing an ESXi image in vCenter

When using ESXi images in vCenter, you can change the ESXi image that is assigned to a server without applying a service template. This makes it easy to apply an updated or test image to a server. This section contains instructions for:

- Changing the ESXi image assigned to an individual server

- Changing the ESXi image assigned to all servers in a cluster in vSphere Web Client

After changing the image that is assigned to a server, you will need to restart the server to apply the image.

Changing the ESXi image assigned to an individual server

If an ESXi image is assigned to a server, the image that is assigned to that server can be changed without having to apply a service template.

To change the ESXi image that is assigned to a server:

1. From the **Servers** table, right-click on the server that you want to change the assigned image on, and then click on the **Change Image** link. For more information on the **Servers** table, see "Viewing server inventory" on page 193.

2. On the **Change Image** window, select the ESXi image to assign to the server.

3. Click on the **OK** button.

Changing the ESXi image assigned to all servers in a cluster in vSphere Web Client

When using vSphere Web Client, the image that is assigned to all servers in an ESXi cluster can be changed without having to apply a service template.

To change the ESXi image on all servers in a cluster:

1. From the vCenter **Clusters** table, right-click on the cluster that contains the servers that you want to change the assigned image on, move the cursor over the **All Hitachi Unified Compute Platform Actions** menu, and then click on the **Change Cluster Image** link.

2. On the **Cluster Image Update** screen, select the image that you want to apply.

3. Click on the **OK** button.

4. In response to the confirmation message, click on the **Yes** button.

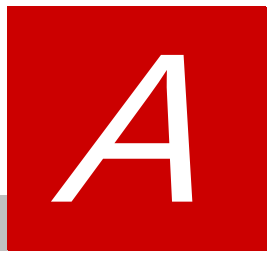
After changing the ESXi cluster image, you can deploy the image to all hosts in a cluster. When this happens, each host in the cluster will be put into maintenance mode and restarted one at a time to retrieve the new image until the image has been applied to all hosts in the cluster. To deploy the ESXi image to all hosts in a cluster:

1. From the vCenter **Clusters** table, right-click on the cluster that contains the servers that you want to change the image assigned on, move the cursor over the **All Hitachi Unified Compute Platform Actions** menu, and then click on the **Deploy Cluster Image** link.

2. Review the current and pending image assigned to the servers in the cluster, and then click on the **OK** button.

Part VI: Appendices

This part contains these appendixes:



Jobs

This appendix lists each of the jobs that are generated by UCP Director. The jobs listed in this appendix are grouped by category. A brief description is included for each job.

UCP Director

The following table lists all of the jobs that are not directly related to the hardware inventory.

Task	Description
Add Disaster Recovery Connection Information	Tracks the progress of adding DR connection information
Add identity pool range	Add identity pool range
Add Paired Devices to replication copy group	Tracks the progress of adding paired devices for replication
Add server profile	Add server profile
Adding journal volumes to a journal	Tracks the progress of expanding a journal by adding journal volumes to an existing journal
Aggregating ConvergedNetwork performance data	Aggregating ConvergedNetwork performance data
Aggregating Ethernet performance data	Aggregating Ethernet performance data
Aggregating Fibre Channel performance data	Aggregating Fibre Channel performance data
Aggregating physical device performance data	Aggregating physical device performance data
Aggregating storage journal performance data	Aggregating storage journal performance data
Aggregating storage parity group performance data	Aggregating storage parity group performance data
Aggregating storage pool performance data	Aggregating storage pool performance data
Aggregating storage port performance data	Aggregating storage port performance data
Aggregating storage processor performance data	Aggregating storage processor performance data
Aggregating storage system performance data	Aggregating storage system performance data
Aggregating storage volume performance data	Aggregating storage volume performance data
Configure UCP Settings	Track the progress of configuring UCP settings
Copy update package to UCP firmware update repository	Track progress of copying updates
Create a copy group	Tracks the progress of creating a copy group

Task	Description
Create a new journal	Tracks the progress of creating a new journal for replication
Delete a journal	Tracks the progress of deleting a journal
Purge UCP Director events that exceed the retention policy	Tracks the progress of removing events from UCP Director that exceed the data retention policy.
Purge UCP Director jobs that exceed the retention policy	Tracks the progress of removing jobs from UCP Director that exceed the data retention policy.
Refresh health information for all elements	Refresh monitor state information for all elements
Refresh performance data for Converged switches	Refresh performance data for Converged switches
Refresh performance data for Ethernet switches	Refresh performance data for Ethernet switches
Refresh performance data for Fibre Channel switches	Refresh performance data for Fibre Channel switches
Refresh performance data for storage system	Refresh performance data for storage system
Refresh performance for a UCP resource type	Refresh performance data for all monitored elements
Remove identity pool range from pool	Remove identity pool range from pool
Remove paired device from replication copy group	Tracks the progress of removing paired devices
Remove server profile	Remove server profile
Removes a copy group and all associated paired devices	Tracks the progress of removing a copy group
Replace the saved Horcm config with the current Horcm file	Tracks the progress of replacing the Horcm file with the last trusted Horcm file.
Resolves CCI Server name	Tracks the progress of resolving the command control interface server name
Restore Horcm configuration with the last trusted configuration	Tracks the progress of reoring Horcm configuration
Set the active image update schedule	Tracks the progress of configuring the run time of a scheduled job in UCP Director.
Update a performance counter	Update a performance counter
Update Disaster Recovery Connection Information	Tracks the progress of updating DR connection information
Update monitor mode	Update the monitor mode for all elements
Update server profile	Update server profile

Task	Description
Update SNMP configurations	Update SNMP configuration for all monitored elements
Update the copy group status	Tracks the progress of pair or split operation on a copy group

Ethernet

The following table lists all of the jobs that are related to Ethernet inventory.

Task	Description
Add Ethernet switch to inventory	Tracks the progress of adding an Ethernet switch to inventory.
Apply global VLANs to all Ethernet switches	Tracks the progress of applying global VLANs to all Ethernet switches in inventory.
Change Ethernet switch SNMP settings	Tracks the progress of changing the SNMP security settings and reporting mode for all Ethernet switches.
Configure Ethernet switch VLAN settings based on a cluster	Tracks the progress of configuring the VLAN settings in an Ethernet switch to match the VLAN settings of the indicated cluster.
Configure Ethernet switch VLAN settings based on a host	Tracks the progress of configuring the VLAN settings in an Ethernet switch to match the VLAN settings of the indicated host.
Create an Ethernet switch backup	Tracks the progress of creating an Ethernet switch backup.
Delete an Ethernet switch backup	Tracks the progress of deleting an Ethernet switch backup.
Refresh Ethernet switch inventory	Tracks the progress of discovering the network topology links between all hosts and Ethernet switches in inventory.
Remove Ethernet switch from inventory	Tracks the progress of removing an Ethernet switch from inventory.
Reset native VLAN for all Ethernet switches	Tracks progress of resetting native VLAN to applicable Ethernet switches in inventory
Restore an Ethernet switch backup	Tracks the progress of restoring an Ethernet switch backup.
Save Ethernet switch unmanaged ports	Tracks the progress of updating the unmanaged ports on the Ethernet switch.
Set the Ethernet switch backup retention policy	Tracks the progress of setting the Ethernet switch backup retention policy.
Turn off SNMP monitoring for Ethernet switches	Tracks the progress of turning off SNMP monitoring for all Ethernet switches. Monitoring and reporting will be disabled.
Turn on SNMP monitoring and reporting for Ethernet switches	Tracks the progress of changing the SNMP mode for all Ethernet switches to monitoring and reporting.

Task	Description
Turn on SNMP monitoring only for Ethernet switches	Tracks the progress of changing the SNMP mode for all Ethernet switches to monitoring only. Reporting will be disabled.
Update an Ethernet switch backup	Tracks the progress of updating one or more details relating to an Ethernet switch backup.
Update Ethernet switch connection information	Tracks the progress of updating the credentials used to access an Ethernet switch.
Update Ethernet switch features	Tracks the progress of updating the selected Ethernet switch features.
Update Ethernet Switch firmware	Tracks the progress of ethernet switch firmware update
Update Ethernet Switches firmware	Tracks the progress of ethernet switches firmware update

Fibre Channel

The following table lists all of the jobs that are related to Fibre Channel inventory.

Task	Description
Add Fibre Channel switch to inventory	Tracks the progresss of adding a Fibre Channel switch to inventory.
Change Fibre Channel switch SNMP settings	Tracks the progress of changing the SNMP security settings and reporting mode for all Fibre Channel switches.
Create Fibre Channel switch zones	Tracks the progress of creating one or more zones on a Fibre Channel switch.
Delete zone on a Fibre Channel switch	Tracks the progress of deleting a zone on a Fibre Channel switch.
Refresh Fibre Channel switch inventory	Tracks the progress of discovering the Fibre Channel topology between the hosts, Fibre Channel switches, and storage system in inventory.
Remove Fibre Channel switch from inventory	Tracks the progress of removing a Fibre Channel switch from inventory.
Turn off SNMP monitoring for Fibre Channel switches	Tracks the progress of turning off SNMP monitoring for all Fibre Channel switches. Monitoring and reporting will be disabled.
Turn on SNMP monitoring and reporting for Fibre Channel switches	Tracks the progress of changing the SNMP mode for all Fibre Channel switches to monitoring and reporting.
Turn on SNMP monitoring only for Fibre Channel switches	Tracks the progress of changing the SNMP mode for all Fibre Channel switches to monitoring only. Reporting will be disabled.

Task	Description
Update Fibre Channel switch connection information	Tracks the progress of updating the credentials used to access a Fibre Channel switch.
Update Fibre Channel switch firmware	Tracks the progress of FC switch firmware update
Update Fibre Channel switches firmware	Tracks the progress of FC switches firmware update
Update zone on a Fibre Channel switch	Tracks the progress of updating a zone on a Fibre Channel switch.

Converged network

The following table lists all of the jobs that are related to Fibre Channel inventory.

Task	Description
Add Converged switch to inventory	Tracks the progress of adding an Converged switch to inventory.
Refresh Converged switch inventory	Tracks the progress of discovering the network topology links between all hosts and Converged switches in inventory.
Remove Converged switch from inventory	Remove Converged switch from inventory
Save Converged switch unmanaged ports	Tracks the progress of updating the unmanaged ports on the Converged switch.
Update Converged network features	Tracks the progress of updating the selected Converged network features.
Update Converged switch connection information	Tracks the progress of updating the credentials used to access a Converged switch.

Server

The following table lists all of the jobs that are related to server inventory.

Task	Description
Apply server profile	Apply server profile
Apply service template	Track progress of apply template
Assign pending image to a server	Tracks the progress of assigning a pending image to a server. A manual reboot is required to apply the image.
Associate server profile	Associate server profile
Change cluster pending ESXi image	Tracks the progress of changing the ESXi image on a cluster

Task	Description
Change image repository	Tracks the progress of adding, updating, or removing an image repository.
Change the SNMP settings for servers	Tracks the progress of changing the SNMP security settings and reporting mode for servers.
Clone service template	Tracks progress of template clone
Create cluster from service template	Track progress of create cluster
Create new image	Tracks the progress of creating a new image.
Create service template	Tracks progress of template creation
Delete images from image repository	Tracks the progress of deleting one or more images from inventory.
Delete service template	Tracks progress of template delete
Deploy ESXi image to a cluster	Tracks progress of deploying pending image to a cluster
Deploy image to server	Tracks the progress of rebooting the server to deploy the pending image.
Edit image	Tracks the progress of editing an image.
Extract server profile	Extract server profile
Move server profile	Move server profile
Power off server	Tracks the progress of powering off a server.
Power on server	Tracks the progress of powering on a server.
Refresh image inventory	Tracks the progress of scanning image repositories for changed content and refreshing image inventory.
Refresh server inventory	Tracks the progress of refreshing the server inventory.
Removing server profile from server	Removing server profile from server
Reset server	Tracks the progress of resetting a server.
Set a default image for a server type	Tracks the progress of setting the default image that will be applied to a server type. This will set the pending image of all servers of the server type unless the server has a unique image applied directly to it. A manual reboot is required to apply the image to servers of the server type.
Set image update notification recipient address	Tracks the progress of updating the recipient address that image update notifications will be sent to.
Turn off server LID	Tracks the progress of turning off the server LID (Location Identifier LED).
Turn off SNMP monitoring for servers	Tracks the progress of turning off SNMP monitoring for all servers. Monitoring and reporting will be disabled.

Task	Description
Turn on server LID	Tracks the progress of turning on the server LID (Location Identifier LED).
Turn on SNMP monitoring and reporting for servers	Tracks the progress of changing the SNMP mode for all servers to monitoring and reporting.
Turn on SNMP monitoring only for servers	Tracks the progress of changing the SNMP mode for all servers to monitoring only. Reporting will be disabled.
Unassociate server profile	Unassociate server profile
Update active images	Tracks the progress of scanning all active images for updates. When updates are found, the active image will be cloned and the cloned image will be updated with the available updates. This task can be run manually or on a user-defined schedule.
Update chassis and server firmware	Tracks the progress of chassis and server firmware update
Update chassis firmware	Tracks the progress of chassis firmware update
Update HCSM connection information	Tracks the progress of updating the HCSM location and credentials.
Update host name	Tracks the progress of updating a host name
Update server boot type	Tracks the progress of updating the server boot type.
Update server firmware	Tracks the progress of server firmware update
Update service template	Tracks progress of template update

Storage

The following table lists all of the jobs that are related to storage inventory.

Task	Description
Attach an existing volume to a cluster	Tracks the progress of attaching an existing volume to all hosts in a cluster.
Attach an existing volume to a host	Tracks the progress of attaching an existing volume to a host.
Change storage system SNMP settings	Tracks the progress of changing the SNMP security settings and reporting mode for storage.
Create a new HTI Volume	Create a new HTI Volume
Create a new volume	Tracks the progress of creating a new volume in a pool. This volume is not attached to a host or a cluster.
Create a new volume and attach it to a cluster	Tracks the progress of creating a new volume and attaching it to all hosts in a cluster.
Create a new volume and attach it to a host	Tracks the progress of creating a new volume and attaching it to a host.

Task	Description
Delete a volume	Tracks the progress of deleting a volume.
Detach a volume from a cluster	Tracks the progress of detaching a volume from all hosts in a cluster.
Detach a volume from a host	Tracks the progress of detaching a volume from a host.
Expand the size of an existing volume	Tracks the progress of expanding the size of an existing volume.
Refresh storage inventory	Tracks the progress of refreshing the storage inventory.
Resync storage element manager inventory for the storage system	Tracks the progress of resyncing the storage inventory with the storage system
Turn off SNMP monitoring for storage	Tracks the progress of turning off SNMP monitoring for storage. Monitoring and reporting will be disabled.
Turn on SNMP monitoring and reporting for storage	Tracks the progress of changing the SNMP mode for storage to monitoring and reporting.
Turn on SNMP monitoring only for storage	Tracks the progress of changing the SNMP mode for storage to monitoring only. Reporting will be disabled.
Update HDvM connection information	Tracks the progress of updating the HDvM location and credentials.

B

Events

This appendix lists each of the events that can be triggered by UCP Director. The events listed in this appendix are grouped by category. A brief description is included for each event.

UCP Director

The following table lists all of the events that are not directly related to the hardware inventory.

Event	Severity	Recommended action
AMQP Server {IpAddress} encounters a nonrecoverable issue.	Error	Contact the system administrator.
An unauthorized access exception occurred while accessing {packagename}.	Error	N/A
An unexpected error has occurred. Please contact system administrator and report exception: {id}.	Error	N/A
An unexpected error occurred while copying the update package: {errormessage}	Error	N/A
Cannot access UCP database.	Error	Contact the system administrator.
Cannot authenticate with {element}. Please verify the credentials.	Error	Contact the system administrator.
Cannot connect to the AMQP service at {ipAddress} using provided credentials. Make sure user {username} exists and has been granted the appropriate permissions.	Error	Please check the AMQP service and verify the credentials.
Cannot find event: {eventId}.	Error	Contact the system administrator.
Cannot find job: {jobId}.	Error	Contact the system administrator.
Cannot find Virtual Manager: {virtualManagerId}.	Error	Contact the system administrator.
Connected successfully to the AMQP service at IP Address: {ipAddress}.	Info	N/A
Contacting {elementType} with IP address: {switchIP} to configure SNMP.	Info	N/A
Corrupted event record. Target: {targetType}:{targetId}. Message: {messageId}{arguments}. Error: {exceptionType}:{exceptionMessage}.	Error	N/A
Could not register {elementType} for SNMP monitoring as IP address: {ipAddress} is already registered for {elementType}	Error	N/A
Could not register {elementType} for SNMP monitoring.	Error	N/A
Could not register {elementType} for SNMP monitoring.	Warning	N/A
Could not resolve host name: {HostName} as DNS resolution failed.	Error	N/A

Event	Severity	Recommended action
Could not unregister element for SNMP monitoring	Error	N/A
Could not unregister element for SNMP monitoring	Warning	N/A
Failed to communicate with the AMQP service at IP Address: {ipAddress}. {ErrorMessage}.	Error	Please check the AMQP service and verify the credentials.
Failed to configure SNMP for {elementType} with IP address: {switchIP}.	Error	Check UCP inventory settings for the failed switch or switches.
Failed to configure SNMP on {numberFailed} out of total {totalNumber} of {resourceType} devices. The list of failed device Ids is {failedDeviceIds}	Error	Contact the system administrator.
Failed to remove SNMP configuration from {elementType} with IP address: {switchIP}	Error	N/A
Failed to send/receive test message to AMQP.	Error	Please check the AMQP service and verify the credentials.
Formatted volume {volumeid} is still mounted on host {hostname}.	Error	Unmount the formatted volume in the hypervisor manager and retry detach operation.
Monitor service fails to discover inventory from Orchestrator service: {resourceUrl}	Error	Contact the system administrator.
Monitor service fails to gather performance data from replication manager: {resourceUrl}	Error	N/A
Monitor service fails to refresh performance: {resourceUrl}	Error	Contact the system administrator.
Monitoring service is not responding	Error	Contact the system administrator.
New resource created: Id='{id}', Resource type: '{resourceType}', global id='{globalId}'.	Info	N/A
No such element manager: {elementmanagerid}.	Error	N/A
Path '{remotepath}' not found.	Error	N/A
Performance data aggregation failed for {resourceType} due to alreadying running aggregation thread	Warning	N/A
Performance data aggregation failed for {resourceType} SQL Message: {message}	Error	Contact the system administrator.
Platform is not supported: Product={product} Version={version} Build={build}	Error	Contact the system administrator.
Registration of Hitachi Unified Compute Platform (UCP) extension at {uri} succeeded.	Info	N/A
Remove SNMP configuration from {elementType} for switch with IP address: {switchIP}.	Info	N/A

Event	Severity	Recommended action
Requested resource not found: {resource}.	Error	N/A
Resource created with Id: {resourceId}.	Info	N/A
ResourceType {resourceType}, GlobalId {globalId}, Metric {metricName} at {metricCurrentValue} is within the threshold limits: TooHighError={tooHighError}, TooHighWarning={tooHighWarning}, TooLowError={tooLowError}, TooLowWarning={tooLowWarning}; Damping is {dampingSetting}.	Info	Contact the system administrator.
ResourceType {resourceType}, GlobalId {globalId}, Metric {metricName} at {metricCurrentValue} violates the defined error thresholds: TooHighError={tooHighError}, TooHighWarning={tooHighWarning}, TooLowError={tooLowError}, TooLowWarning={tooLowWarning}; Damping is {dampingSetting}.	Error	Contact the system administrator.
ResourceType {resourceType}, GlobalId {globalId}, Metric {metricName} at {metricCurrentValue} violates the defined warning thresholds: TooHighError={tooHighError}, TooHighWarning={tooHighWarning}, TooLowError={tooLowError}, TooLowWarning={tooLowWarning}; Damping is {dampingSetting}.	Warning	Contact the system administrator.
SNMP data collection authentication failed for switch {ipAddress}, authentication protocol use: {authenticationProtocol}	Error	Contact the system administrator.
Snmp data collection error: Switch {ipAddress} doesn't recognize oids: [{oids}].	Error	Contact the system administrator.
SNMP data collection failed for switch {ipAddress}. Failed to retrieve Oids: {oids}	Error	Contact the system administrator.
SNMP data collection privacy validation failed for switch {ipAddress}, privacy protocol used is {privacyProtocol}	Error	Contact the system administrator.
Specified resource cannot be found. Resource Type: '{element}', Resource Id: '{IdOrName}'.	Error	N/A
Starting now, no configuration changing tasks will be allowed on UCP for the duration of the update.	Info	N/A
Starting update for UCP settings	Info	N/A
Succeeded in configuring SNMP on {elementType} with IP address: {switchIP}.	Info	N/A

Event	Severity	Recommended action
Succeeded in removing SNMP configuration from {elementType} for switch with IP address: {switchIP}.	Info	N/A
System error has occurred.	Error	Contact the system administrator.
The state of monitoring for this element is already set to the desired state.	Info	N/A
UCP Inventory information is inconsistent with actual inventory.	Error	Please wait for all relevant tasks to finish, perform a refresh and then retry the operation.
UCP is waiting for jobs with job IDs: {jobids} to finish before starting the update.	Info	N/A
UCP Monitoring Service failed to start.	Error	Please verify UCP Director and SQL Server database are working then retry.
UCP Monitoring Service started.	Info	N/A
UCP restarted; task aborted.	Error	N/A
UCP Scheduled Job: {jobType} has been updated to run {dayOfWeek} of every week at {time}.	Info	N/A
UCP Scheduled Job: {jobType} has been updated to run daily at {time}.	Info	N/A
UCP Scheduled Job: {jobType} not found.	Error	Please check the job type.
UCP Scheduled Job: {jobType} updated to run with an interval type of {intervalType} and interval value of {intervalValue}.	Info	N/A
UCP Scheduled Job:{jobType} has been updated to run day {dayOfMonth} of every month at {time}.	Info	N/A
UCP Scheduler Service fail to start scheduled job: {jobName}.	Error	Please verify UCP Director and SQL Server database are working then retry.
UCP Scheduler Service failed to start.	Error	Please verify UCP Director and SQL Server database are working then retry.
UCP Scheduler Service started.	Info	N/A
UCP Scheduler Service stopping.	Warning	N/A
Unable to delete resource {resourceId} from UCP database.	Error	Please retry the task. If it fails again, contact the system administrator.

Event	Severity	Recommended action
Unable to update record for {nameOrId} from UCP database.	Error	Please retry the task. If it fails again, contact the system administrator.
Unknown event: {eventname} found.	Error	N/A
Update has finished, UCP can now be used to perform configuration changing operation.	Info	N/A
Update job timed out while waiting for following UCP jobs: {jobIds} to finish.	Error	Please wait for all tasks to finish and try to run updates again.
Update of AMQP settings has failed as the settings are invalid. Please check the settings and try again.	Error	N/A
Update of UCP settings has failed.	Error	N/A
Update of UCP settings successfully completed.	Info	N/A
Update to the account used by Hitachi Unified Compute Platform (UCP) extension at {uri} succeeded.	Info	N/A
Virtual platform manager (id={virtualManagerId}) is updated.	Info	N/A
Waiting for host to deploy after successful firmware update of the server {serverid}.	Info	N/A

Ethernet

The following table lists all of the events that are related to Ethernet inventory.

Event	Severity	Recommended action
{Count} blowers for Ethernet Switch ({IpAddress}) are failed or missing. Replace failed or missing blower assemblies immediately.	Error	Contact the System Administrator to replace the affected Hardware.
{Count} fan Field Replaceable Unit(s) (FRU) for Ethernet Switch ({IpAddress}) are missing. Install fan FRUs immediately.	Error	Contact the System Administrator to install the affected Hardware.
A feature license is expired on Ethernet switch with IP address {IpAddress}.	Error	Contact the system administrator.
A feature license of Ethernet switch with IP address {IpAddress} will expire on {expiryDate}.	Warning	Contact the system administrator.
A software crash occurred on Ethernet switch with IP address {IpAddress}.	Error	Contact the system administrator.
Add Ethernet switch to inventory failed.	Error	N/A

Event	Severity	Recommended action
An Ethernet switch with the following IP address already exists in inventory: {ipAddress}.	Error	N/A
An operation is already in progress for Ethernet switch {IpAddress}	Error	N/A
An operation is already in progress for Ethernet switch {IpAddress}	Error	N/A
Authentication failure occurred for Ethernet switch with IP address {IpAddress}.	Error	Contact the system administrator.
Cannot access on-boarded switch with IP address: {ipAddress}. Stored credentials are no longer valid.	Error	N/A
Cannot configure VLAN on the Ethernet Switch with IP Address: {ipaddress} as the port {portID} connected to host {hostname} is marked unmanaged	Error	N/A
Cannot find backup {backupId} of Ethernet switch {switchid}.	Error	N/A
Cannot on-board switch with IP address: {ipAddress}. Provided credentials are invalid.	Error	N/A
Cannot on-board switch with IP Address: {ipAddress}. Switch is Unsupported.	Error	N/A
Cannot perform this action when Host/Cluster Network Configuration feature is disabled.	Error	N/A
Cannot update SNMP user: {user} for Ethernet switch: {ipAddress} as the user is a ssh user for the switch.	Error	N/A
Cannot upgrade aggregate switch {aggregateIpAddress}, because access switch {accessIpAddress} does not have a redundant ethernet path.	Error	N/A
Cannot upgrade aggregate switch {aggregateIpAddress}, because access switch {accessIpAddress} does not have Port Association Feature enabled. Please enable the Port Association Feature on the following interfaces: {portList}.	Error	N/A
Cold recovery failed for Ethernet switch ({IpAddress}). Error code: {ReturnCode}	Warning	N/A
Converged Switch with IP address: {ipAddress} is in Initializing state.	Error	Please wait for all relevant tasks to finish, perform a refresh and then retry the operation.
Current temperature: {MeasuredTemperature} (C) for Ethernet Switch ({IpAddress}) is below shutdown threshold. System shutdown cancelled.	Warning	Contact the system administrator.

Event	Severity	Recommended action
Discovery protocol was enabled on Ethernet switch {IpAddress}.	Info	N/A
Discovery protocol was not enabled on Ethernet switch {IpAddress}.	Error	Contact the system administrator.
Ethernet switch ({IpAddress}) Field Replaceable Unit (FRU): {FRUId} failed to power on.	Error	Contact the system administrator.
Ethernet switch ({IpAddress}) Field Replaceable Unit (FRU): {FRUId} failed transition to {state} state.	Error	Contact the system administrator.
Ethernet switch ({IpAddress}) Field Replaceable Unit (FRU): {FRUId} has faulted. Sensors are above maximum limits.	Error	Contact the system administrator.
Ethernet switch ({IpAddress}) Field Replaceable Unit (FRU): {FRUId} has faulted. Sensors are below minimum limits.	Error	Contact the system administrator.
Ethernet switch ({IpAddress}) Field Replaceable Unit (FRU): {FRUId} has unknown hardware identifier. FRU faulted.	Error	Contact the system administrator.
Ethernet switch ({IpAddress}) Field Replaceable Unit (FRU): {FRUId} is overheating. The unit is shutting down.	Error	Contact the system administrator.
Ethernet switch ({IpAddress}) Field Replaceable Unit (FRU): {FRUId} powered down unexpectedly.	Error	Contact the system administrator.
Ethernet switch ({IpAddress}) Field Replaceable Unit (FRU): {FRUId} set to faulty. Return code: {ReturnCode}	Error	Contact the system administrator.
Ethernet switch {IpAddress} added to inventory.	Info	N/A
Ethernet switch {IpAddress} configured successfully with Global VLAN range: {GlobalVlanRange}.	Info	N/A
Ethernet switch {IpAddress} configured successfully with native VLAN range: {NativeVlan}.	Info	N/A
Ethernet switch {IpAddress} does not exist in inventory.	Error	N/A
Ethernet switch {IpAddress} failed to configure VLANs as the switch is in Initializing state.	Error	N/A
Ethernet switch {IpAddress} is unreachable.	Error	N/A
Ethernet switch {IpAddress} removed from inventory.	Info	N/A
Ethernet switch {IpAddress} state changed to unreachable.	Error	N/A

Event	Severity	Recommended action
Ethernet switch {switchId} had more unpinned backups than the retention policy allowed ({totalNumberOfBackupPerSwitch}). The following unpinned backups have been removed: {backupIds}.	Info	N/A
Ethernet switch {var1} was restarted.	Warning	N/A
Ethernet switch VLAN settings for cluster: {clusterName} updated.	Info	N/A
Ethernet switch with IP address {IpAddress} is going to shutdown. The shutdown reason is {shutdownReason}.	Info	N/A
Ethernet switch with IP address {IpAddress} was warm restarted with no configuration changes.	Info	N/A
Ethernet Switch with IP address: {ipAddress} is in Initializing state.	Error	Please wait for all relevant tasks to finish, perform a refresh and then retry the operation.
Ethernet Switch with IP address: {ipAddress} is not healthy.	Error	N/A
Ethernet switch with IP address: {targetIpAddress} was detected when trying to update switch information for switch with IP address: {ipAddress}.	Error	N/A
Failed backup Ethernet switch {switchId}. This switch has reached the maximum number of pinned backups {maxNumberOfPinnedBackup}.	Error	N/A
Failed to backup Ethernet switch {switchId}.	Error	N/A
Failed to read SFP transceiver for interface {InterfaceName} of the Ethernet Switch ({IpAddress}).	Warning	N/A
Failed to refresh Ethernet switch inventory details for connected host(s) on retry refresh operation.	Error	N/A
Failed to refresh Ethernet switch inventory details for connected host(s).	Warning	N/A
Failed to refresh Ethernet switch inventory on a retry refresh operation.	Error	N/A
Failed to refresh Ethernet switch inventory.	Warning	N/A
Failed to remove backup {backupId} of Ethernet switch {switchid}.	Error	N/A
Failed to remove port channel interface: {PortChannelInterface} for Ethernet switch {IpAddress}.	Warning	N/A

Event	Severity	Recommended action
Failed to restore backup {backupId} on Ethernet switch {switchid}.	Error	N/A
Failed to update backup {configurationId} of Ethernet switch {switchid}.	Error	N/A
Failed to update Ethernet features.	Error	N/A
Failed to update Ethernet switch ({IpAddress}) Field Replaceable Unit (FRU) {FRUId} information.	Warning	N/A
Failed to update the Ethernet switch backup retention policy as some Ethernet switches have more number of pinned backups. The current maximum number of pinned backups allowed is ({maxNumberOfPinnedBackup}):. The following Ethernet switches meet the current maximum: {listOfSwitchIds}.	Error	N/A
Failed to update the Ethernet switch backup retention policy to {totalNumberOfBackupPerSwitch} unpinned and {maxNumberOfPinnedBackup} pinned backups per Ethernet switch.	Error	N/A
Failed to update the Ethernet switch backup retention policy. The following Ethernet switches have more backups than {totalNumberOfBackupPerSwitch}.List of switches - {listOfSwitchIds}.	Error	N/A
Failed to update the Ethernet switch backup retention policy. The total number of backups per Ethernet switch must be less than or equal to {ucpMaxtotalNumberOfBackupPerSwitch}.	Error	N/A
Failures while resetting Global VLAN range.	Error	N/A
Failures while resetting native VLAN.	Error	N/A
Field Replacable Unit {FRUId} for the Ethernet Switch ({IpAddress}) is being powered off (based on the user configuration) upon receiving a hardware ASIC error. Reason: {FaultReason}	Error	Contact the system administrator.
Field Replaceable Unit (FRU) or Switch {FRUId} with interface module {InterfaceModuleId} may not be supported on the Ethernet Switch ({IpAddress}). Check firmware version as a possible cause.	Error	Contact the system administrator.
Firmware update failed for Ethernet Switch with IP Address: {ipAddress}. Detailed error message: {errormessage}.	Error	Manual intervention is required. Please contact system administrator to troubleshoot the component update failure and update it manually if required.

Event	Severity	Recommended action
Firmware update started for Ethernet Switch with IP Address: {ipAddress}. Switch will be rebooted after the firmware download.	Info	N/A
Firmware update will not be started for Ethernet Switch with IP Address: {ipAddress} as the switch failed validation checks.	Error	N/A
Interface {InterfaceName} IP of the Ethernet Switch ({IpAddress}) overlap with management IP {managementIp}.	Error	Contact the system administrator.
Interface {InterfaceName} of the Ethernet Switch ({IpAddress}) is auto-enabled by edge loop detection (ELD).	Info	N/A
Interface {InterfaceName} of the Ethernet Switch ({IpAddress}) is shut down by edge loop detection (ELD) for loop in VLAN {VlanId}.	Error	Contact the system administrator.
Interface module on slot {SlotIdentifier} for Ethernet Switch ({IpAddress}) is shutting down.	Error	Contact the system administrator.
Invalid port name: {portName}.	Error	N/A
Invalid VLAN range is provided to configure for Ethernet switch {IpAddress}. VLAN range should be between {ValidVlanRange}.	Error	N/A
Invalid VLAN(s) found for host: {host}. Only trunk VLANs in range {vlanrange} are allowed. Please go to vCenter and fix the VLAN configuration.	Error	N/A
inventory updated for Ethernet switch {IpAddress}	Info	N/A
Link down command issued for down links on Ethernet Switch with IP Address: {ipAddress}	Info	N/A
Link down failed for down links on Ethernet Switch with IP Address: {ipAddress}	Error	N/A
Link up command issued for the down links on Ethernet Switch with IP Address: {ipAddress}	Info	N/A
Link up failed for down links on Ethernet Switch with IP Address: {ipAddress}	Error	N/A
LinkDown event received from Ethernet switch {var1} on port {ifIndex}. The desired admin status for this port is {ifAdminStatus} and operational status is {ifOperStatus}. The following device(s) will experience connectivity issues: {var2}.	Error	Ensure that the desired administration status of the port and the operation status are the same.

Event	Severity	Recommended action
LinkDown event received from Ethernet switch {var1} on port {ifIndex}. The desired admin status for this port is {ifAdminStatus} and operational status is {ifOperStatus}. There are no devices connected to the port.	Info	N/A
LinkUp event received from Ethernet switch {var1} on port {ifIndex}. The desired admin status for this port is {ifAdminStatus} and operational status is {ifOperStatus}. Connectivity will be reestablished with the following devices(s): {var2}.	Info	N/A
LinkUp event received from Ethernet switch {var1} on port {ifIndex}. The desired admin status for this port is {ifAdminStatus} and operational status is {ifOperStatus}. There are no devices connected to the port.	Info	N/A
Measured temperature: {MeasuredTemperature} (C) for Ethernet Switch ({IpAddress}) exceeds environmental specifications.	Warning	Contact the system administrator.
Measured Temperature: {MeasuredTemperature} (C) for Ethernet Switch ({IpAddress}) exceeds system temperature limit. System will be shutting down in 2 minutes.	Warning	Contact the system administrator.
Network subsystem is initializing	Error	Contact the system administrator.
No such switch: {switchid}.	Error	N/A
No switch found for SNMP configuration	Warning	N/A
No VLANs configured for host: {hostName}.	Info	N/A
On-boarded switch with IP Address: {ipAddress} become unresponsive or is now Unsupported.	Error	N/A
One of the Blower for Ethernet Switch ({IpAddress}) has either failed or is missing. Replace failed or missing blower assembly immediately.	Error	Contact the System Administrator to replace the affected Hardware.
Port {portNumber} Chip of the Ethernet Switch ({IpAddress}) faulted due to internal error.	Error	Contact the system administrator.
Port {portNumber} of the Ethernet Switch ({IpAddress}) has faulted because of many link failures.	Error	Contact the system administrator.
Port channel configuration {PortChannelInterface} defined on Ethernet switch {IpAddress}.	Info	N/A
Port channel configuration failed on Ethernet switch {IpAddress}.	Error	Contact the system administrator.

Event	Severity	Recommended action
Port channel interface: {portChannelInterface} updated for Ethernet switch {IpAddress}	Info	N/A
Port: {PortNumber} for Ethernet Switch ({IpAddress}) has timed out due to incompatible inactivity. Timeout value: {DeadTimeout}, correct value: {Value}.	Warning	Contact the system administrator.
Received unexpected power down for Ethernet switch ({IpAddress}) Field Replaceable Unit (FRU): {FRUId}. But cannot determine if it has power.	Warning	N/A
Received unexpected power down for Ethernet switch ({IpAddress}) Field Replaceable Unit (FRU): {FRUId}. But FRU still has power.	Warning	N/A
Running configuration of Ethernet switch with IP address {IpAddress} is changed from CLI (TerminalType: {terminalType}).	Info	N/A
Server:{serverid} does not have a redundant ethernet path.	Error	Please check the Ethernet switches in the UCP inventory and make sure that they are all healthy and reachable.
SNMP configuration updated for Ethernet switch {IpAddress}.	Info	N/A
Snmp Password is not strong enough for Ethernet switch {IpAddress}. Password should contain characters from at least three of the following classes: lower case letters, upper case letters, digits and special characters.	Warning	N/A
Spanning tree protocol (STP) was enabled and configured for the Ethernet switch {IpAddress}.	Info	N/A
Speed for Ethernet Switch ({IpAddress}) Blower: {BlowerNumber} is below threshold. Measured speed: {MeasuredSpeed} (RPM)	Warning	Contact the system administrator.
Status of a port with Port Number: {portNumber} on Ethernet switch {IpAddress} was changed to {portStatus}.	Warning	Contact the system administrator.
Successfully created backup {backupId} of Ethernet switch {switchId}. This backup is pinned.	Info	N/A
Successfully created backup id {backupId} of Ethernet switch {switchId}. This backup is unpinned.	Info	N/A
Successfully disabled Host Network Configuration feature.	Info	N/A

Event	Severity	Recommended action
Successfully enabled Host Network Configuration feature.	Info	N/A
Successfully marked backup {backupId} of Ethernet switch {switchid} as pinned.	Info	N/A
Successfully marked backup {backupId} of Ethernet switch {switchid} as unpinned.	Info	N/A
Successfully obtained host(s) information.	Info	N/A
Successfully refreshed Ethernet switch inventory.	Info	N/A
Successfully removed pinned backup {backupId} of Ethernet switch {switchid}.	Info	N/A
Successfully removed the SNMP configuration from Ethernet switch {IpAddress}.	Info	N/A
Successfully removed unpinned backup {backupId} of Ethernet switch {switchid}.	Info	N/A
Successfully reset global VLAN range: {GlobalVlanRange}.	Info	N/A
Successfully reset native VLAN : {NativeVlan}.	Info	N/A
Successfully restored backup {backupId} on Ethernet switch {switchid}.	Info	N/A
Successfully updated firmware for Ethernet Switch with IP Address: {ipAddress}	Info	N/A
Successfully updated the description of backup {backupId} of Ethernet switch {switchId}.	Info	N/A
Successfully updated the Ethernet switch backup retention policy. The total number of backups per Ethernet switch is {totalNumberOfBackupPerSwitch} and the maximum number of pinned backups per Ethernet switch is {maxNumberOfPinnedBackup}.	Info	N/A
Successfully updated unmanaged ports for Ethernet switch {IpAddress}.	Info	N/A
Switch port {PortNumber} of the Ethernet Switch ({IpAddress}) is disabled. Reason: {DisableReason}	Warning	Contact the system administrator.
Temperature of interface module on slot {SlotIdentifier} for Ethernet Switch ({IpAddress}) is high. Measured Temperature: {MeasuredTemperature} (C). Unit will be shut down in 2 minutes if temperature remains high.	Warning	Contact the system administrator.

Event	Severity	Recommended action
The following Ethernet switches have more unpinned backups than the updated retention policy allows ({totalNumberOfBackupPerSwitch}): {switchId}. Unpinned backups in excess of the retention policy will be removed.	Info	N/A
The following host(s)/device(s): {devices} might lose connectivity due to deletion of the switch.	Warning	N/A
The host: {host} has invalid number of uplinks. UCP requires atleast two uplinks for each host attached to the same virtual switch or virtual distributed switch.	Error	N/A
The overall status of UCP's Ethernet resources is now Critical. View UCP's Status Monitor for more information.	Error	Contact the Network Administrator.
The overall status of UCP's Ethernet resources is now Not Applicable. View UCP's Status Monitor for more information.	Info	N/A
The overall status of UCP's Ethernet resources is now Ok.	Info	N/A
The overall status of UCP's Ethernet resources is now Unknown. View UCP's Status Monitor for more information.	Warning	Contact the Network Administrator.
The overall status of UCP's Ethernet resources is now Warning. View UCP's Status Monitor for more information.	Warning	Contact the Network Administrator.
The VLAN configuration for host: {host} on uplinks do not match with each other. {vlanMismatchMessage}. Please go to vCenter and fix the VLAN configuration.	Error	N/A
There is no firmware update available for Ethernet switch with IP Address: {ipAddress}	Info	N/A
Turning off Fan {fanNumber} of the Ethernet Switch ({IpAddress}) because of airflow direction mismatch.	Error	Contact the system administrator.
UCP requires that there should be an access switch connected to the aggregate switch with IP address: {IpAddress}.	Error	N/A
UCP requires that there should be an aggregate switch connected to the access switch(s) with IP address: {IpAddress}.	Error	N/A
UCP requires that two access switches in active state should be connected to the host: {hostName}	Error	N/A
Unable to configure spanning tree protocol (STP) for Ethernet switch {IpAddress}	Error	N/A

Event	Severity	Recommended action
Unable to remove SNMP configuration for Ethernet switch {IpAddress}. Please remove the SNMP configuration manully from the Ethernet switch.	Error	N/A
Unable to retrieve Ethernet switch details from UCP database. Please contact UCP system administrator.	Error	N/A
Unable to retrieve platform information	Warning	N/A
Unable to update Ethernet switch VLAN settings for Cluster: {clusterName}.	Error	N/A
Unable to update the SNMP configuration for Ethernet switch {IpAddress}.	Error	N/A
Unit in the Slot number or Ethernet Switch {UnitId} with Field Replaceable Unit (FRU) {FRUID} is faulted. It is incompatible with the {incompatibilityType} configuration. Check firmware version as a possible cause.	Error	Contact the system administrator.
Update started for the Ethernet switch path rooted at switch with IP Address: {ipAddress}	Info	N/A
VLANs for Ethernet Switch with IP address: {IpAddress}, port: {PortNumber} were configured to match the VLANs {vlans} on the host: {HostName}.	Info	N/A
VLANs: {uplinkVlans} on host: {hostName} uplink port: {uplink} vlans do not match the connected Ethernet switch {IpAddress}. Switch port: {portId} has VLANs: {portVlans}. Host will not be able to communicate on mismatched VLANs	Warning	N/A
Warm recovery failed for Ethernet switch ({IpAddress}). Return code: {ReturnCode}	Warning	N/A

Fibre Channel

The following table lists all of the events that are related to Fibre Channel inventory.

Event	Severity	Recommended action
{Count} blowers are failed or missing. Replace failed or missing blower assemblies immediately.	Error	Contact the System Administrator to replace the affected Hardware.
{Count} fan Field Replaceable Unit(s) (FRU) are missing. Install fan FRUs immediately.	Error	Contact the System Administrator to install the affected Hardware.
{Count} fan FRUs failed. Replace failed fan FRUs immediately.	Error	Contact the System Administrator to replace the affected Hardware.

Event	Severity	Recommended action
{Count} fans are faulty.	Error	Contact the system administrator.
{FailureCount} fans are out of service. System is going to shut down immediately.	Error	Contact the system administrator.
A Fibre Channel switch with IP address: {ipAddress} already exists in the inventory.	Error	Please ensure that the switch IP address and credentials are correct.
All fan Field Replaceable Unit(s) FRUs missing. Install fan FRUs immediately.	Error	Contact the System Administrator to install the affected Hardware.
All fans failed. Replace failed fan FRUs immediately.	Error	Contact the System Administrator to replace the affected Hardware.
All Fibre Channel switch ports are offline.	Error	Contact the system administrator.
An unknown error occurred at Fibre Channel Switch with IP address: {ipaddress}	Error	Unknown error. Please check the configuration then try again.
An unknown error occurred for Fibre Channel zone: {zoneid}.	Error	Unknown error. Please check the configuration then try again.
Authentication and privacy username for Fibre Channel Switch must be between 2 and 32 characters long.	Error	N/A
Authentication password for Fibre Channel Switch must be between 1 and 20 characters.	Error	N/A
Authentication protocol: {TypeAuth} and privacy protocol: {TypePrivacy} are an unsupported combination.	Error	N/A
Commit zone database size: {ZoneDbSize} is larger than supported size: {MaxZoneDbSize}.	Warning	Contact the system administrator.
Created/reused the following Fibre channel zone(s): {ZoneName} for the following fabric: {FabricName}.	Info	N/A
Current temperature: {MeasuredTemperature} (C) is below shutdown threshold. System shutdown cancelled.	Warning	Contact the system administrator.
Domain: {DomainNumber} has a maximum zone database size of {MaxZoneDbSize}.	Warning	Contact the system administrator.
Domain: {DomainNumber} has lowest memory available for the zone database in the fabric.	Warning	Contact the system administrator.
Failed to access monitoring service at Fibre Channel switch. Confirm that monitoring service is running.	Error	N/A
Failed to add or configure SNMP for one or more Fibre Channel switches.	Error	N/A

Event	Severity	Recommended action
Failed to remove the Fibre Channel zone or Host Storage Domains.	Warning	N/A
Failed to update firmware for Fibre Channel Switch with IP Address: {ipAddress}. Detailed error message: {errormessage}.	Error	Contact the system administrator.
Fan {FanNumber} is faulty.	Warning	Contact the system administrator.
Fan is not faulty.	Info	N/A
Fan: {FanNumber} has faulted. Measure speed: {MeasuredSpeed} (RPM) is above threshold.	Warning	Contact the system administrator.
Feature Management Information Base (MIB): {Mibname} on Fibre Channel switch with IP address: {switchipaddress} was disabled. UCP has restored the MIB capabilities.	Info	N/A
Fibre Channel Switch blower: {BlowerNumber} has faulted. Measured voltage: {MeasuredVoltage} is above threshold. Nominal Voltage: {NominalVoltage}.	Warning	Contact the system administrator.
Fibre Channel Switch blower: {BlowerNumber} has faulted. Measured voltage: {MeasuredVoltage} is below threshold. Nominal Voltage: {NominalVoltage}.	Warning	Contact the system administrator.
Fibre Channel switch cold recovery failed. Error code: {ReturnCode}.	Error	Contact the system administrator.
Fibre Channel switch Field Replaceable Unit (FRU): {FRUId} has faulted. Sensors are below minimum limits.	Error	Contact the system administrator.
Fibre Channel switch Field Replaceable Unit (FRU): {FRUId} powered down unexpectedly.	Error	Contact the system administrator.
Fibre Channel switch Field Replaceable Unit (FRU): {FRUId} set to faulty. Return code: {ReturnCode}.	Warning	Contact the system administrator.
Fibre Channel switch Field Replaceable Unit (FRU): {FRUId} failed to power on.	Error	Contact the system administrator.
Fibre Channel switch Field Replaceable Unit (FRU): {FRUId} has faulted. Sensors are above maximum limits.	Error	Contact the system administrator.
Fibre Channel switch Field Replaceable Unit (FRU): {FRUId} sensors have exceeded the maximum limit. The unit is being reset.	Error	Contact the system administrator.
Fibre Channel switch Field Replaceable Unit (FRU): {FRUId} failed transition to {state} state.	Error	Contact the system administrator.
Fibre Channel switch Field Replaceable Unit (FRU): {FRUId} is overheating. The unit is shutting down.	Error	Contact the system administrator.

Event	Severity	Recommended action
Fibre Channel Switch with IP Address : {ipAddress} is not healthy.	Error	N/A
Fibre Channel Switch with IP address: {ipAddress} added to inventory.	Info	N/A
Fibre Channel Switch with IP Address: {IPAddress} could not be removed from inventory.	Error	Contact the system administrator.
Fibre Channel Switch with IP address: {IPAddress} has been removed from inventory.	Info	N/A
Fibre Channel switch with IP address: {ipAddress} has been updated.	Info	N/A
Fibre Channel Switch with IP address: {ipaddress} is invalid.	Error	N/A
Fibre Channel Switch with IP address: {ipaddress} was found to be in an inconsistent state (i.e. The make/model/serial number of the switch is inconsistent with UCP records).	Error	Verify the IP address and retry the operation. If that does not work, remove the switch from inventory then add the switch back to inventory.
Fibre Channel zone(s): {zonename} could not be created, edited, or deleted.	Error	N/A
Fibre Channel zone(s): {zonename} have been created, updated, or removed successfully.	Info	N/A
Field Replaceable Unit: {FRUId} is no longer faulted.	Info	N/A
Firmware update started for Fibre Channel Switch with IP Address: {ipAddress}.	Info	N/A
Firmware update will not be started for Fibre Channel Switch with IP Address: {ipAddress} as it failed the validation checks.	Error	N/A
High temperature warning time has expired. System is preparing to shutdown.	Error	Contact the system administrator.
High temperature warning time has expired. System preparing for shutdown. Measured Temperature: {MeasuredTemperature} (C).	Error	Contact the system administrator.
Measured temperature: {MeasuredTemperature} (C) exceeds environmental specifications.	Warning	Contact the system administrator.
Measured Temperature: {MeasuredTemperature} (C) exceeds system temperature limit. System will be shutting down in 2 minutes.	Warning	Contact the system administrator.
Merged zone database exceeds limit.	Warning	Contact the system administrator.

Event	Severity	Recommended action
Mismatch in Power Supply Unit (PSU) fan air flow direction. Replace PSU with fan air flows in same direction. System will be shut down in 2 minutes.	Warning	Contact the system administrator.
Mismatch in Power Supply Unit(PSU) fan air flow direction. System is shutting down.	Error	Contact the system administrator.
No fans are faulty.	Info	N/A
No such fabric: {fabricid}.	Error	N/A
No such zone: {zone} present in fabric.	Error	N/A
No such zone: {zone}.	Error	N/A
One fan Field Replaceable Unit(s) FRU missing. Install fan FRU immediately.	Warning	Contact the System Administrator to install the affected Hardware.
One fan has failed. Replace failed fan Field Replaceable Unit (FRU)immediately.	Warning	Contact the System Administrator to replace the affected Hardware.
One of the blower has either failed or is missing. Replace failed or missing blower assembly immediately.	Error	Contact the System Administrator to replace the affected Hardware.
One or more Fibre Channel zones are of an unsupported configuration and cannot be managed by UCP.	Error	Create or delete zones manually through Fibre Channel switch tool or SSH/Telnet interface.
One or more Fibre Channel zones for server: {serverid} are of an unsupported configuration and cannot be managed by UCP.	Error	Create or delete zones manually through Fibre Channel switch tool or SSH/Telnet interface.
One or more zones could not be created on the Fibre Channel Fabric.	Error	Create or delete zones manually through Fibre Channel switch tool or SSH/Telnet interface.
One or two fans have failed. Replace failed fan Field Replaceable Unit(s) (FRU) immediately.	Warning	Contact the System Administrator to replace the affected Hardware.
Port fault occurred for port: {portNumber}.	Error	Contact the system administrator.
Port selection does not meet UCP requirements.	Error	Please input ports that meet UCP requirements. You must select at least one even numbered and one odd numbered port for each fabric.
Port: {portNumber} has faulted because of many link failures	Error	Contact the system administrator.
Port: {PortNumber} has timed out due to incompatible inactivity. Timeout value: {DeadTimeout}, correct value: {Value}.	Warning	Contact the system administrator.

Event	Severity	Recommended action
Power and fan speeds are not available from the Power supply/Fan unit: {CombofanAndpowersupplyunitnumber}. Please ensure that the unit has power and the switch is powered on.	Error	Contact the system administrator.
Power Supply Unit (PSU) fan Field Replaceable Units (FRU) air flow matched. System shutdown canceled.	Info	N/A
Privacy password for Fibre Channel Switch must be between 1 and 20 characters	Error	N/A
Received unexpected power down for Fibre Channel Switch Field Replaceable Unit: {FRUId} but {FRUId} still has power.	Warning	Contact the system administrator.
Received unexpected power down for Field Replaceable Unit: {FRUId}, but cannot determine if it has power.	Warning	Contact the system administrator.
Required license: {LicenseName} is missing.	Error	Contact the system administrator.
Rescan failed for Fibre Channel switch with IP Address: {ipAddress}.	Error	N/A
Rescan of storage topology failed.	Error	N/A
Rescan retry failed for Fibre Channel switch with IP Address: {ipAddress}.	Error	Please check switch inventory and retry operation.
Rescan succeeded for Fibre Channel switch with IP Address: {ipAddress}.	Info	N/A
Server:{serverid} does not have a redundant Fibre Channel path. Each Fibre Channel path should be in a separate fabric.	Error	N/A
Slot: {SlotNumber} has faulted. Voltage is above threshold. Nominal Voltage: {NominalVoltage}. Measured Voltage: {MeasuredVoltage}.	Warning	Contact the system administrator.
Slot: {SlotNumber} has faulted. Voltage is below threshold. Nominal Voltage: {NominalVoltage}. Measured Voltage: {MeasuredVoltage}.	Warning	Contact the system administrator.
Slot: {SlotNumber} has high measured temperature: {MeasuredTemperature}.	Warning	Contact the system administrator.
Slot: {SlotNumber} is shutting down.	Error	Contact the system administrator.
SNMP configuration for switch or switches with IP address(s): {IpAddress} failed.	Error	N/A
SNMP configuration for switch with IP address: {IpAddress} updated.	Info	N/A

Event	Severity	Recommended action
SNMP not configured properly on Fibre Channel switches: {ipAddress2}.	Error	N/A
Speed for fan: {FanNumber} with sensor: {SensorNumber} is below threshold. Measured speed: {MeasuredSpeed} (RPM).	Warning	Contact the system administrator.
Speed for Fibre Channel switch blower: {BlowerNumber} is above threshold. Measured speed: {MeasuredSpeed} (RPM).	Warning	Contact the system administrator.
Speed for Fibre Channel switch blower: {BlowerNumber} is below threshold. Measured speed: {MeasuredSpeed} (RPM)	Warning	Contact the system administrator.
Status of a port with Port Number: {portNumber} on Fibre Channel switch with IP address: {switchipaddress} was changed to {portStatus}.	Warning	Contact the system administrator.
Successfully updated firmware for Fibre Channel Switch with IP Address: {ipAddress}.	Info	N/A
Switch name for Fibre Channel Switch with IP address: {ipAddress} changed to switch name: {switchName}	Info	N/A
Switch port: {PortNumber} disabled. Reason for disabling: {DisableReason}.	Warning	Contact the system administrator.
System is within normal temperature specifications. Measured Temperature: {MeasuredTemperature} (C).	Info	N/A
Temperature sensors failed. Service immediately.	Warning	Contact the system administrator.
The Default Zone access mode is set to All Access.	Info	N/A
The Default Zone access mode is set to No Access.	Warning	Contact the system administrator.
The effective configuration has been disabled: {ADId}.	Warning	Contact the system administrator.
The IP address of Fibre Channel switch or switches that were not added to inventory are: {ipAddress1}.	Error	Please check switch inventory and retry operation.
The overall status of UCP's Fibre Channel resources is now Critical. View UCP's Status Monitor for more information.	Error	Contact the Storage Administrator.
The overall status of UCP's Fibre Channel resources is now Not Applicable. View UCP's Status Monitor for more information.	Info	N/A
The overall status of UCP's Fibre Channel resources is now Ok.	Info	N/A

Event	Severity	Recommended action
The overall status of UCP's Fibre Channel resources is now Unknown. View UCP's Status Monitor for more information.	Warning	Contact the Storage Administrator.
The overall status of UCP's Fibre Channel resources is now Warning. View UCP's Status Monitor for more information.	Warning	Contact the Storage Administrator.
The specified initiator World Wide Name (WWN): {initiatorwwn} and target WWN: {targetwwn} are not in the same fabric.	Error	Please check that the specified initiator WWN and target WWN reside in the same fabric.
The specified World Wide Name(s) (WWN): ({wwn}) could not be found in the fabric ID(s): ({fabricIds})	Error	N/A
The specified zone name(s): {zonenames} within the fabric(s): {fabricname} is not unique.	Error	Please provide a unique identifier and retry the operation.
The warning time for faulty fan has expired. System is now preparing to shutdown.	Error	Contact the system administrator.
There is no firmware update available for Fibre Channel switch with IP Address: {ipAddress}	Info	N/A
Transaction Commit failed. Reason code: {ReasonCode} {ApplicationReason} - {ReasonString}.	Warning	Contact the system administrator.
Two circuit paired power supplies are faulty. Please check the {SwitchSide} AC main switch/circuit to see if it has power.	Warning	Contact the system administrator.
Two fan FRUs missing. Install fan FRUs immediately.	Warning	Contact the System Administrator to install the affected Hardware.
Two fans failed. Replace failed fan Field Replaceable Unit(s) (FRU) immediately.	Warning	Contact the System Administrator to replace the affected Hardware.
UCP could not connect to Fibre Channel switch with IP address: {ipAddresss}.	Error	Contact the system administrator.
UCP Director requires exactly two Fibre Channel fabrics to perform zoning operations. Number of fabric(s): {numberOfFabrics}, fabric information: {fabricInfo}.	Error	Please check the UCP Fibre Channel switch inventory to ensure that all switches have been added to inventory.
UCP identified Fibre channel fabrics with the same ID: {fabricId} with fabric information: {fabricInfo}. UCP requires exactly two fabrics with distinct IDs to properly perform zoning operations.	Error	Please check the UCP Fibre Channel switch inventory to ensure that all switches have been added to inventory.
UCP identified that Zone ID: {zonedid} may be a zone for an existing path and cannot be modified or deleted. Please detach volume before deleting this path.	Error	N/A

Event	Severity	Recommended action
UCP inventory details have expired for Fibre Channel switches as the cache refresh failed.	Error	Check UCP inventory settings for the failed switch or switches.
UCP requires that there should be an core switch connected to the edge switch(s) with IP address: {IpAddress}.	Error	N/A
UCP requires that there should be edge switch(s) connected to the core switch with IP address: {IpAddress}.	Error	N/A
UCP requires that two edge switches in active state should be connected to the host: {hostName}	Error	N/A
Unable to allocate memory for configuration file {ConfigFileName}. Error message {SystemErrorMessage}.	Error	Contact the system administrator.
Unable to connect to Fibre Channel Switch with IP address: {ipAddress}. Please validate the following - 1)IP address is correct. 2)Credentials are correct. 3) Fibre Channel switches have been on-boarded. 4) Network connectivity is available.	Error	Please ensure that the switch IP address and credentials are correct.
Unable to create a zone for at least one of the hosts in the Cluster.	Error	N/A
Unable to create configuration file: {ConfigFileName}. Error message: {SystemErrorMessage}.	Error	Contact the system administrator.
Unable to discover host port adapter(s): ({portIds}) on UCP fabric.	Error	Please check that the specified initiator WWN is a UCP host and that the host is online and has active operating system. Perform fiber channel switch refresh if host is online and operation still fails with this error.
Unable to examine configuration file: {ConfigFileName}. Error message {SystemErrorMessage}.	Error	Contact the system administrator.
Unable to read contents of configuration file: {ConfigFileName}. Error message: {SystemErrorMessage}.	Error	Contact the system administrator.
Unable to update SNMP configuration for Fibre Channel switch with IP Address: {IpAddress}. Error Message: {ErrorFromSwitch}	Error	N/A
Unable to update SNMP configuration for switch with IP address: {IpAddress}.	Warning	N/A
Unstable link detected during merge at port: {PortNumber}.	Warning	Contact the system administrator.

Event	Severity	Recommended action
Update started for the Fibre channel switch path rooted at switch with IP Address: {ipAddress} in fabric: {fabricName}	Info	N/A
Using backup temperature sensor. Service immediately.	Warning	Contact the system administrator.
Warm recovery failed. Return code: {ReturnCode}.	Error	Contact the system administrator.
Zone member(s): ({wwns}) do not exist in the fabric: {fabricId}. UCP requires that all zone members exist in the fabric to complete the operation.	Error	Create or delete zones manually through Fibre Channel switch tool or SSH/Telnet interface.

Converged network

The following table lists all of the events that are related to Fibre Channel inventory.

Event	Severity	Recommended action
A Converged switch with the following IP address already exists in inventory: {ipAddress}.	Error	N/A
A feature license is expired on Converged switch with IP address {IpAddress}.	Error	Contact the system administrator.
A feature license of Converged switch with IP address {IpAddress} will expire on {expiryDate}.	Warning	Contact the system administrator.
A software crash has occurred on the Converged switch with IP address {IpAddress}.	Error	Contact the system administrator.
Add Converged switch to inventory failed.	Error	N/A
An operation is already in progress for Converged switch {IpAddress}	Error	N/A
An operation is already in progress for the Converged switch {IpAddress}	Error	N/A
Authentication failure occurred for Converged switch with IP address {IpAddress}.	Error	Contact the system administrator.
Cannot access on-boarded switch with IP address: {ipAddress}. Stored credentials are no longer valid.	Error	N/A
Cannot on-board switch with IP address: {ipAddress}. Provided credentials are invalid.	Error	N/A
Cannot on-board switch with IP Address: {ipAddress}. Switch is Unsupported.	Error	N/A

Event	Severity	Recommended action
Cannot update SNMP user: {user} for Converged switch: {ipAddress} as the user is a ssh user for the switch.	Error	N/A
Converged Network subsystem is initializing	Error	Contact the system administrator.
Converged switch ({IpAddress}) Field Replaceable Unit (FRU): {FRUId} failed to power on.	Error	Contact the system administrator.
Converged switch ({IpAddress}) Field Replaceable Unit (FRU): {FRUId} has unknown hardware identifier. FRU faulted.	Error	Contact the system administrator.
Converged switch ({IpAddress}) Field Replaceable Unit (FRU): {FRUId} is overheating. The unit is shutting down.	Error	Contact the system administrator.
Converged switch {IpAddress} added to inventory.	Info	N/A
Converged switch {IpAddress} does not exist in inventory.	Error	N/A
Converged switch {IpAddress} failed to configure VLANs as the switch is in Initializing state.	Error	N/A
Converged switch {IpAddress} is unreachable.	Error	N/A
Converged switch {IpAddress} removed from inventory.	Info	N/A
Converged switch {IpAddress} state changed to unreachable.	Error	N/A
Converged switch {var1} was restarted.	Warning	N/A
Converged switch VLAN settings for cluster: {clusterName} updated.	Info	N/A
Converged switch with IP address {IpAddress} is going to shutdown. The shutdown reason is {shutdownReason}.	Info	N/A
Converged switch with IP address {IpAddress} was warm restarted with no configuration changes.	Info	N/A
Converged switch with IP address: {targetIpAddress} was detected when trying to update switch information for switch with IP address: {ipAddress}.	Error	N/A
Discovery protocol was enabled on Converged switch {IpAddress}.	Info	N/A
Discovery protocol was not enabled on Converged switch {IpAddress}.	Error	Contact the system administrator.
Failed to refresh Converged switch inventory details for connected host(s) on retry refresh operation.	Error	N/A

Event	Severity	Recommended action
Failed to refresh Converged switch inventory details for connected host(s).	Warning	N/A
Failed to refresh Converged switch inventory on a retry refresh operation.	Error	N/A
Failed to refresh Converged switch inventory.	Warning	N/A
Failed to remove port channel interface: {PortChannelInterface} for Converged switch {IpAddress}.	Warning	N/A
Failed to update Converged network features.	Error	N/A
Invalid port name: {portName}.	Error	N/A
inventory updated for Converged switch {IpAddress}	Info	N/A
LinkDown event received from Converged switch {var1} on port {ifIndex}. The desired admin status for this port is {ifAdminStatus} and operational status is {ifOperStatus}. The following host(s) will experience connectivity issues: {var2}.	Error	Ensure that the desired administration status of the port and the operation status are the same.
LinkDown event received from Converged switch {var1} on port {ifIndex}. The desired admin status for this port is {ifAdminStatus} and operational status is {ifOperStatus}. There are no hosts connected to the port.	Info	N/A
LinkUp event received from Converged switch {var1} on port {ifIndex}. The desired admin status for this port is {ifAdminStatus} and operational status is {ifOperStatus}. Connectivity will be reestablished with the following host(s): {var2}.	Info	N/A
LinkUp event received from Converged switch {var1} on port {ifIndex}. The desired admin status for this port is {ifAdminStatus} and operational status is {ifOperStatus}. There are no hosts connected to the port.	Info	N/A
No switch found for SNMP configuration	Warning	N/A
On-boarded switch with IP Address: {ipAddress} become unresponsive or is now Unsupported.	Error	N/A
Port channel configuration {PortChannelInterface} defined on Converged switch {IpAddress}.	Info	N/A
Port channel configuration failed on Converged switch {IpAddress}.	Error	Contact the system administrator.
Port channel interface: {portChannelInterface} updated for Converged switch {IpAddress}	Info	N/A

Event	Severity	Recommended action
Running configuration of Converged switch with IP address {IpAddress} is changed from CLI (TerminalType: {terminalType}).	Info	N/A
SNMP configuration updated for Converged switch {IpAddress}.	Info	N/A
Snmp Password is not strong enough for the Converged switch {IpAddress}. Password should contain characters from at least three of the following classes: lower case letters, upper case letters, digits and special characters.	Warning	N/A
Spanning tree protocol (STP) was enabled and configured for the Converged switch {IpAddress}.	Info	N/A
Status of a port with Port Number: {portNumber} on Converged switch {IpAddress} was changed to {portStatus}.	Warning	Contact the system administrator.
Successfully obtained host(s) information.	Info	N/A
Successfully refreshed Converged switch inventory.	Info	N/A
Successfully removed the SNMP configuration from Converged switch {IpAddress}.	Info	N/A
Successfully updated unmanaged ports for Converged switch {IpAddress}.	Info	N/A
The following host(s)/device(s): {devices} might lose connectivity due to deletion of the switch.	Warning	N/A
The overall status of UCP's ConvergedNetwork resources is now Critical. View UCP's Status Monitor for more information.	Error	Contact the Network Administrator.
The overall status of UCP's ConvergedNetwork resources is now Not Applicable. View UCP's Status Monitor for more information.	Info	N/A
The overall status of UCP's ConvergedNetwork resources is now Ok.	Info	N/A
The overall status of UCP's ConvergedNetwork resources is now Unknown. View UCP's Status Monitor for more information.	Warning	Contact the Network Administrator.
The overall status of UCP's ConvergedNetwork resources is now Warning. View UCP's Status Monitor for more information.	Warning	Contact the Network Administrator.
UCP requires that there should be an access switch connected to the aggregate switch with IP address: {IpAddress}.	Error	N/A

Event	Severity	Recommended action
UCP requires that there should be an aggregate switch connected to the access switch(s) with IP address: {IpAddress}.	Error	N/A
Unable to configure spanning tree protocol (STP) for Converged switch {IpAddress}	Error	N/A
Unable to remove SNMP configuration for Converged switch {IpAddress}. Please remove the SNMP configuration manully from the Converged switch.	Error	N/A
Unable to retrieve Converged switch details from UCP database. Please contact UCP system administrator.	Error	N/A
Unable to retrieve platform information	Warning	N/A
Unable to update Converged switch VLAN settings for Cluster: {clusterName}.	Error	N/A
Unable to update the SNMP configuration for Converged switch {IpAddress}.	Error	N/A

Server

The following table lists all of the events that are related to server inventory.

Event	Severity	Recommended action
{HCSM} cannot be reached. No Server actions can be executed at this time.	Error	Contact the system administrator.
{hostname} has boot volume already attached.	Error	Please detach and delete attached volumes and try again.
A {trapAlertLocation} has failed to power off.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
A {trapAlertLocation} has failed to power on.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
A {trapAlertLocation} has failed to power reset.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
A {trapAlertLocation} has powered off.	Info	Check Hitachi Compute System Manager (HCSM) for more details.
A {trapAlertLocation} has powered on.	Info	Check Hitachi Compute System Manager (HCSM) for more details.
A {trapAlertLocation} power off request issued.	Info	N/A
A {trapAlertLocation} power on request issued.	Info	N/A

Event	Severity	Recommended action
A {trapAlertLocation} power reset request issued.	Info	N/A
A {trapAlertLocation} reset power request issued.	Info	Check Hitachi Compute System Manager (HCSM) for more details.
A CPU temperature alert occurred in a {trapAlertLocation}. Message: {trapAlertContent}.	Error	The CPU may need replacement.
A CPU temperature warning occurred in a {trapAlertLocation}. Message: {trapAlertContent}.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
A driver could not be injected while applying service template {templateName} to server {serverId} because the driver package was inaccessible.	Warning	N/A
A server blade partition for a {trapAlertLocation} has experienced a critical event. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
A server blade partition for a {trapAlertLocation} has experienced a warning event. Event text: {trapAlertContent}.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
A server blade partition for a {trapAlertLocation} has recovered from an error. Event text: {trapAlertContent}.	Info	N/A
A system configuration error is detected in a {trapAlertLocation}, serial number {serverSerialNumber} (UUID = {serverUuid}).	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Added new image repository location(s) '{repositoryName}'. However, the location(s) could not be accessed at this time. Ensure the location(s) are specified correctly and are accessible.	Error	N/A
Adding a reference host to virtual switch failed in vCenter.	Error	N/A
Applied image {imageName} to server {serverId} for OS deployment.	Info	N/A
Apply service template failed to apply network settings.	Error	Please resolve the issue and try to apply template again.
Apply service template failed to deploy operating system.	Error	Please resolve the issue and try to apply template again.
Applying host profile failed in vCenter.	Error	N/A
Applying serverprofile {serverprofileid} to server {serverid} failed	Error	N/A
Applying serverprofile {serverprofileid} to server {serverid} started	Info	N/A

Event	Severity	Recommended action
Applying serverprofile {serverprofileid} to server {serverid} succeeded	Info	N/A
Applying service template failed.	Error	N/A
Applying service template(s) succeeded.	Info	N/A
Applying service template: {servicetemplateid} failed.	Error	N/A
Applying service template: {servicetemplateid} started	Info	N/A
Applying service template: {servicetemplateid} succeeded	Info	N/A
Associated Server Profile {serverprofileid} with server {serverid}	Info	N/A
Associating Server Profile {serverprofileid} from server {serverid} failed	Error	N/A
At least 2 datastore volumes should be provided to SDRS enabled cluster.	Error	N/A
At least two virtual machines have the same UUID: {uuid}. Name of one of the virtual machines is {vmname}.	Error	Please consult VMware documentation to resolve the conflict and then try the operation again.
Attaching some volume(s) failed during cluster creation.	Warning	N/A
Attempting to validate identities applied by server profile to server {serverid}.	Info	N/A
Auto deploy did not load the expected image: {imageName}.	Error	N/A
Autodeploy rule for server(s) {serverId} could not be created.	Error	N/A
Boot image is missing or empty.	Error	N/A
Boot mode change failed for server {serverId} because at least one volume is attached.	Error	Ensure there are no volumes attached to the server and try again
Boot type could not be changed for the following servers {serverUuid}.	Error	N/A
Boot unattend file validation failed.	Error	Please resolve the issue and try to apply template again.
Cannot access Image Unattend or kickstart files.	Error	Place file in Temp folder with appropriate privileges.

Event	Severity	Recommended action
Cannot create image: {imageName}.	Error	Please retry the task. If it fails again, contact the system administrator.
Cannot delete image: {imageName}.	Error	Please retry the task. If it fails again, contact the system administrator.
Cannot edit image: {imageName}.	Error	Please retry the task. If it fails again, contact the system administrator.
Cannot find image name in boot unattend file '{filepath}' for server {serveruuid}.	Error	N/A
Cannot perform image operation as image inventory is out of sync. Please wait for all image jobs to finish, refresh the page and try again.	Error	N/A
Cannot reserve boot lun for server {serveruuid}.	Error	N/A
Cannot retrieve value from database.	Error	N/A
Cannot trigger refresh for server inventory as a refresh is already in progress.	Error	N/A
Cannot update host name for server: {ipAddress} as the name provided for the server is not unique.	Error	N/A
Cannot use Formatted Volume name {name} as the provided name is already in use.	Error	Please provide a unique identifier and retry the operation.
Chassis {chassisId} has stabilized after a warning or error. Event text: {trapAlertContent}	Info	N/A
Chassis {chassisId} reported a power supply warning from a {trapAlertLocation}. Event text: {trapAlertContent}.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported a rotational speed issue with the cooling fan in slot {trapSlotNumber}. Event text: {trapAlertContent}.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported a temperature alert event. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported a temperature warning event. Event text: {trapAlertContent}.	Warning	Check chassis ventilation and the lab air conditioning.
Chassis {chassisId} reported a voltage alert event. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported a voltage warning event. Event text: {trapAlertContent}.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.

Event	Severity	Recommended action
Chassis {chassisId} reported a warning event from module {trapModuleIdentifier} in slot {trapSlotNumber}. Event text: {trapAlertContent}.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported a warning event from the cooling fan in slot {trapSlotNumber}. Event text: {trapAlertContent}.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported a warning event from the management module in slot {trapSlotNumber}. Event text: {trapAlertContent}.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported a warning event. Event text: {trapAlertContent}	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported an alert from module {trapModuleIdentifier} in slot {trapSlotNumber}. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported an alert from the cooling fan in slot {trapSlotNumber}. Event text: {trapAlertContent}.	Error	The component may need to be replaced. Contact hardware support.
Chassis {chassisId} reported an alert from the management module in slot {trapSlotNumber}. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported an error event. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported that a cooling fan in slot {trapSlotNumber} has failed to power on. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported that a power supply has stabilized. Event text: {trapAlertContent}.	Info	N/A
Chassis {chassisId} reported that module {trapModuleIdentifier} in slot {trapSlotNumber} has been installed. Event text: {trapAlertContent}.	Info	N/A
Chassis {chassisId} reported that module {trapModuleIdentifier} in slot {trapSlotNumber} has been removed. Event text: {trapAlertContent}.	Error	N/A
Chassis {chassisId} reported that module {trapModuleIdentifier} in slot {trapSlotNumber} has restored redundancy. Event text: {trapAlertContent}.	Info	N/A
Chassis {chassisId} reported that module {trapModuleIdentifier} in slot {trapSlotNumber} has stabilized after a warning or error. Event text: {trapAlertContent}.	Info	N/A

Event	Severity	Recommended action
Chassis {chassisId} reported that module {trapModuleIdentifier} in slot {trapSlotNumber} lacks redundancy. Event text: {trapAlertContent}.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported that power supply capacity is insufficient. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported that the cooling fan in slot {trapSlotNumber} has stabilized. Event text: {trapAlertContent}.	Info	N/A
Chassis {chassisId} reported that the management module in slot {trapSlotNumber} has failed to power on. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported that the management module in slot {trapSlotNumber} has stabilized. Event text: {trapAlertContent}.	Info	N/A
Chassis {chassisId} reported that the power supply module in slot {trapSlotNumber} failed to power on. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported that the switch module in slot {trapSlotNumber} has experienced a warning event. Event text: {trapAlertContent}.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported that the switch module in slot {trapSlotNumber} has failed to power on. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported that the switch module in slot {trapSlotNumber} has powered off. Event text: {trapAlertContent}.	Error	N/A
Chassis {chassisId} reported that the switch module in slot {trapSlotNumber} has reset. Event text: {trapAlertContent}.	Info	N/A
Chassis {chassisId} reported that the temperature has stabilized. Event text: {trapAlertContent}.	Info	N/A
Chassis {chassisId} reported that the total number of cooling fans is insufficient. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported that the total number of power supply modules is insufficient. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reported that voltage has stabilized. Event text: {trapAlertContent}.	Info	N/A

Event	Severity	Recommended action
Chassis {chassisId} reported the rotational speed of the cooling fan in slot {trapSlotNumber} has normalized. Event text: {trapAlertContent}.	Info	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reports a power supply alert from a {trapAlertLocation}. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reports AC input has stabilized. Event text: {trapAlertContent}.	Info	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reports an AC input error. Event text: {trapAlertContent}.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reports an AC loss error. Event text: {trapAlertContent}.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reports that a switch module has experienced a critical error. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Chassis {chassisId} reports that the switch module in slot {trapSlotNumber} has stabilized. Event text: {trapAlertContent}.	Info	N/A
Chassis firmware update has timed out for server: {chassisId}.	Error	Please make sure the firmware update is complete before launching other operations.
Cluster {clusterId} with virtual manager at {platformUrl} cannot be managed by UCP	Error	N/A
Cluster creation failed because virtual distributed switch could not be created.	Error	N/A
Cluster HA and/or DRS configuration was not successful.	Error	Please refer to the hypervisor manager messages for more info.
Cluster HA and/or DRS configuration was successful.	Info	N/A
Completed applying service template {templateName} to server {serverId}.	Info	N/A
Compliance failed for created host profile.	Warning	N/A
Configuring Ethernet switch port failed.	Warning	N/A
Configuring Ethernet switch port was successful.	Info	N/A
Copying service template: {servicetemplateid} failed	Error	N/A
Copying service template: {servicetemplateid} started	Info	N/A
Copying service template: {servicetemplateid} succeeded	Info	N/A
Could not add auto deploy rule.	Error	N/A

Event	Severity	Recommended action
Could not create auto deploy rule for servertype: {servertype}	Error	N/A
Could not create auto deploy rule.	Error	N/A
Could not delete auto deploy rule for image: {imageName}	Error	N/A
Could not find provided image when applying service template.	Error	Please resolve the issue and try to apply template again.
Couldn't change boot type for server {serverId} because the SAN and server have inconsistent volume connections.	Error	Some zones on the fibre channel switchs, or HSDs (Host Storage Domains) in the SAN may have been changed or deleted. Please remove all zones and HSDs associated with this server, and try again.
CPU temperature has stabilized in a {trapAlertLocation}. Message: {trapAlertContent}.	Info	N/A
Creating and attaching some volume(s) failed during cluster creation.	Warning	N/A
Creating server profile started	Info	N/A
Creating service template failed	Error	N/A
Creating service template started	Info	N/A
Creation of cluster {clusterName} failed.	Error	N/A
Error accessing {serverUuid} HBA BIOS information from HCSM.	Error	Please resolve the issue and try to apply template again.
Error trying to add host with IP Address: {ipAddress} to System Center.	Error	N/A
Error updating UCP database with new boot type for server {serverId}.	Error	Contact the system administrator.
Extract server profile failed since switch has invalid native vlan value: {nativevlan} for port: {portvalue}	Error	N/A
Extracting server profile failed since native VLANs are not the same for the chosen CNA physical port configuration: {message}	Error	N/A
Extracting server profile failed since switch connectivity is unavailable	Error	N/A
Extracting server profiles failed	Error	N/A
Extracting server profiles failed since switch does not have native VLAN stored for few of the physical ports: {message}	Error	N/A

Event	Severity	Recommended action
Extracting server profiles started	Info	N/A
Extracting server profiles succeeded	Info	N/A
Failed to acquire lock to set image unattend file.	Error	Please try applying template again later.
Failed to add OS deploymentrecord to database.	Error	N/A
Failed to backup Dhcp Configuration.	Error	N/A
Failed to change server LID state. Response from HCSM: {hcsmLidStateChangeResult}.	Error	Contact the system administrator.
Failed to configure native VLAN for host(s) {hostsUuid}	Error	Contact the system administrator.
Failed to configure WDS for server(s) {serverUuids}.	Error	Please resolve the issue and try to apply template again.
Failed to create and attach boot volume to server: {serverId}	Error	N/A
Failed to create auto deploy rule for server {serverid}	Warning	N/A
Failed to create server profile.	Error	N/A
Failed to execute server profile deployment steps successfully for server: {serverid}	Error	N/A
Failed to get Vlan information for Windows hyper-V host {hostName} (ID ={hostId})	Error	N/A
Failed to obtain 4 WWNs required for boot volume.	Error	Please resolve the issue and try to apply template again.
Failed to Power on the server after Profile was applied.	Error	N/A
Failed to put host: {hostname} in maintenance mode.	Error	Check to see if settings on the host allow for the VMs to be migrated to a different host. Alternately, shutdown the VMs and migrate them to a separate host.
Failed to read corresponding IP address for given MAC addresses: {addresses} from DHCP config	Error	N/A
Failed to read or write to boot menu service template file.	Error	Please resolve the issue and try to apply template again.
Failed to receive postbacks from server(s) {severUuids}.	Error	Please resolve the issue and try to apply template again.
Failed to remove auto deploy rule for server {serverid}.	Warning	N/A

Event	Severity	Recommended action
Failed to remove server {serverUuid} from WDS prestaged device list.	Error	N/A
Failed to send image update notification email as SMTP configuration is missing.	Error	N/A
Failed to send image update notification regarding image: {imageName} to one or more recipients: {recipientEmails}.	Error	N/A
Failed to send image update notification regarding image: {imageName} to recipient: {recipientEmails}.	Error	N/A
Failed to update file: {filename}	Error	N/A
Failed to update firmware for chassis: {chassisid}. Detailed error message: {errormessage}.	Error	Manual intervention is required. Please contact system administrator to troubleshoot the component update failure and update it manually if required.
Failed to update firmware for server: {serverId}. Detailed error message: {errormessage}.	Error	Manual intervention is required. Please contact system administrator to troubleshoot the component update failure and update it manually if required.
Failed to update host name for server: {serverUuid} to {name}.	Error	N/A
Failed to update host: {hostName} cache.	Warning	N/A
Failed to update host: {hostName} information in server cache.	Warning	N/A
Failed to update hosts' caches.	Error	N/A
Failed to update Server inventory information.	Error	N/A
Failed to update server's cache.	Error	N/A
Fatal error received from Windows Deployment Services when applying service template {templateName} to server {serverId}.	Error	N/A
Firmware update started for chassis: {chassisid}.	Info	N/A
Firmware update started for file: {filename}.	Info	N/A
Firmware update started for server: {serverid}. Server may be rebooted after the firmware download.	Info	N/A
Health monitor failed to start.	Error	Please check UCP logs for more info.
Health Monitor successfully started.	Info	N/A

Event	Severity	Recommended action
Host {hostId} cannot be found with virtual manager at {platformUrl}	Error	N/A
Host {hostId} with virtual manager at {platformUrl} cannot be managed by UCP	Error	N/A
Host name for server: {serverUuid} was successfully updated to {name}.	Info	N/A
Host was added to platform but UCP does not expect it to be added to platform. Remove host from platform and utilize service templates to deploy platform operating system.	Warning	N/A
Host with IP Address {ipAddress} successfully added to System Center.	Info	N/A
Host(s): {hostName} do not see the volume is formatted.	Error	N/A
Identity {identityValue} is already in use by server profile {serverprofileName}.	Error	Please remove server profile and try the operation again.
Identity pool range {identityPoolRangeId} is in use as one or more identities from it are referenced in server profile.	Error	N/A
Image {imageName} transferred to server {serverId} for OS deployment.	Info	N/A
Image name must be unique	Error	N/A
Image post-apply actions completed for server {serverId}.	Info	N/A
Image unattend file validation failed.	Error	Please resolve the issue and try to apply template again.
Image Unattend or kickstart file is malformed.	Error	Please refer to documentation for format guidelines.
Image(s) added to UCP inventory: {imageName}	Info	N/A
Image(s) removed from UCP inventory: {imageName}	Info	N/A
Image: {imageName} removed successfully.	Info	N/A
Image: {imageName} saved successfully.	Info	N/A
Invalid configuration. Current image cannot be null for host: {hostname}.	Error	Please wait for all relevant tasks to finish, perform a refresh and then retry the operation.
Invalid management vlanid was specified. Please provide valid integer value.	Error	N/A

Event	Severity	Recommended action
Invalid media URL from kickstart file {kickstartfile}: The provided URL is not in the correct format. Expected absolute URL.	Error	Please check that provided media URL is valid and uses either http or https protocol.
Invalid media URL scheme from kickstart file {kickstartfile}: The provided URI scheme '{scheme}' is invalid; expected 'http' or 'https'.	Error	N/A
Invalid service template type	Error	N/A
Invalid user credentials were provided for server {serveruuid} in boot unattend file '{filepath}'.	Error	Please ensure that the provided credentials are correct.
Ip address {ipAddress} is already in use.	Error	N/A
Kickstart file validation failed.	Error	Please resolve the issue and try to apply template again.
LID state change request has been sent to Server Id: {serverUuid} with serial number: {serverSerialNumber}.	Info	N/A
Mac address {macAddress} is already in use.	Error	N/A
MAC settings in server profile do not match with the MAC settings in server to apply the server profile	Error	N/A
Missing media URL from kickstart file {kickstartfile}.	Error	N/A
Missing native vlan Id while extracting server profile	Error	N/A
Missing native vlan Id while extracting server profile {serverprofileid}	Error	N/A
Moving serverprofile {serverprofileid} to server {serverid} failed	Error	N/A
Moving serverprofile {serverprofileid} to server {serverid} started. Source server wont boot till the profile is unassociated.	Info	N/A
Moving serverprofile {serverprofileid} to server {serverid} succeeded	Info	N/A
Multiple Ip addresses found for server: {serverid} in DHCP config	Warning	N/A
New image: {newImageName} created based on original image: {originalImageName}.	Info	N/A
New service template {templatename} was successfully created.	Info	N/A
New service template {templatename} was successfully created.	Info	N/A
No such cluster: {clusterid}.	Error	Please select a valid cluster and retry.

Event	Severity	Recommended action
Number of CNA ports in Server Profile does not match with the number of CNA ports in server to apply the server profile	Error	N/A
Only images made by UCP can be set as default.	Error	N/A
Operation is not allowed on server(s) {serverUuids} as it has storage volume(s) attached to it.	Error	Ensure there are no volumes attached to the server and try again
OS deployment failed and rollback was performed.	Error	N/A
OS deployment failed for {serverUuid} or completion was not reported correctly.	Error	Please login to server and verify if operating system is installed. If operating system is not installed then try to apply template again.
OS deployment of image {imageId} failed for the following servers {serverUuids}.	Error	N/A
OS deployment of image {imageName} successfully completed.	Info	N/A
Postback script section in kickstart file {kickstartfile} does not match as per requirement at line number {linenumber}.	Error	N/A
Power CLI error event occurred. Power CLI Error Message: {powerCliErrorMessage}.	Error	N/A
Power control has failed on a {trapAlertLocation}.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
PowerCli error event occurred.	Error	Please check logs for more details.
Provided identity {identityValue} is already in use by other server profile.	Error	N/A
Provided IP Address is either already in use or IP Addresses in pool range are not enough to satisfy this request.	Error	N/A
Provided MAC Address is either already in use or MAC Addresses in pool range are not enough to satisfy this request.	Error	N/A
Provided media URL {url} is not accessible. Please ensure that is it correct and is accessible.	Error	N/A
Provided WWN Address is either already in use or WWN Addresses in pool range are not enough to satisfy this request.	Error	N/A
Putting host: {hostname} in vCenter maintenance mode.	Info	N/A

Event	Severity	Recommended action
Raw Volume(s) cannot be added to SDRS enabled cluster.	Error	N/A
Removal of server profile {serverprofileid} failed with errormessage: {errormessage}	Error	N/A
Removed server profile {serverprofileid}	Info	N/A
Removing server profile {serverprofileid} started	Error	N/A
Removing server profile from server {serverid} failed.	Error	N/A
Removing server profile from server {serverid} started	Info	N/A
Removing server profile from server {serverid} succeeded	Info	N/A
Removing service template: {servicetemplateid} failed	Error	N/A
Removing service template: {servicetemplateid} started	Info	N/A
Removing service template: {servicetemplateid} succeeded	Info	N/A
Request to change the LID state for Server Id: {serverUuid} with serial number: {serverSerialNumber} timed-out.	Error	N/A
Request to change the power state of server Id: {serverUuid} with serial number: {serverSerialNumber} timed-out.	Error	N/A
Request to change the power state of server with serial number: {serverSerialNumber} (UUID = {serverUuid}) failed. The resulting status from HCSM is: {hcsmPowerStateChangeResult}	Error	Contact the system administrator.
Required postback section was not found in kickstart file {kickstartfile}.	Error	N/A
SCP Management IP Address is missing.	Error	N/A
Sent a request to power {PowerAction} server Id: {serverUuid} with serial number: {serverSerialNumber}.	Info	N/A
Server {serverId} boot type changed to {bootType}.	Info	N/A
Server {serverId} boot type changed to Custom.	Info	N/A
Server {serverId} could not download the boot program from the TFTP server while applying service template {templateName}.	Error	N/A

Event	Severity	Recommended action
Server {serverid} is already undergoing deployment. Please try once the deployment is finished	Error	N/A
Server {serverId} is not updated with settings from profile.	Error	N/A
Server firmware update has timed out for server: {serverId}.	Error	Please make sure the firmware update is complete before launching other operations.
Server Id: {serverUuid} with serial number: {serverSerialNumber} CPU has been disabled in a {trapAlertLocation}. Event text: {trapAlertContent}.	Warning	The component may need to be replaced. Contact hardware support.
Server Id: {serverUuid} with serial number: {serverSerialNumber} experienced a correctable CPU error in a {trapAlertLocation}. Event text: {trapAlertContent}.	Info	N/A
Server Id: {serverUuid} with serial number: {serverSerialNumber} experienced a critical error on {trapAlertLocation}. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Server Id: {serverUuid} with serial number: {serverSerialNumber} has a memory DIMM disabled in a {trapAlertLocation}. Event text: {trapAlertContent}.	Warning	The component may need to be replaced. Contact hardware support.
Server Id: {serverUuid} with serial number: {serverSerialNumber} has a non maskable interrupt on {trapAlertLocation}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Server Id: {serverUuid} with serial number: {serverSerialNumber} has a number of correctable CPU errors which surpassed a warning threshold in a {trapAlertLocation}. Event text: {trapAlertContent}.	Error	The component may need to be replaced. Contact hardware support.
Server Id: {serverUuid} with serial number: {serverSerialNumber} has a number of correctable memory errors which surpassed a warning threshold in a {trapAlertLocation}. Event text: {trapAlertContent}.	Warning	The component may need to be replaced. Contact hardware support.
Server Id: {serverUuid} with serial number: {serverSerialNumber} has a warning event on {trapAlertLocation}. Event text: {trapAlertContent}.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
Server Id: {serverUuid} with serial number: {serverSerialNumber} has a watchdog timer expired on {trapAlertLocation}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Server Id: {serverUuid} with serial number: {serverSerialNumber} has an uncorrectable CPU error in a {trapAlertLocation}. Event text: {trapAlertContent}.	Error	The component may need to be replaced. Contact hardware support.

Event	Severity	Recommended action
Server Id: {serverUuid} with serial number: {serverSerialNumber} has detected a link down error. Event text: {trapAlertContent}.	Error	Check Hitachi Compute System Manager (HCSM) for more details.
Server Id: {serverUuid} with serial number: {serverSerialNumber} has detected a link down warning. Event text: {trapAlertContent}.	Warning	Check Hitachi Compute System Manager (HCSM) for more details.
Server Id: {serverUuid} with serial number: {serverSerialNumber} has detected a link has reconnected. Event text: {trapAlertContent}.	Info	Check Hitachi Compute System Manager (HCSM) for more details.
Server Id: {serverUuid} with serial number: {serverSerialNumber} has experienced a correctable memory error in a {trapAlertLocation}. Event text: {trapAlertContent}.	Info	N/A
Server Id: {serverUuid} with serial number: {serverSerialNumber} has experienced an uncorrectable error in a {trapAlertLocation}. Event text: {trapAlertContent}.	Error	The component may need to be replaced. Contact hardware support.
Server Id: {serverUuid} with serial number: {serverSerialNumber} has normal status reported by {trapAlertLocation}. Event text: {trapAlertContent}.	Info	N/A
Server must be powered off to perform detach operation on boot volume.	Error	N/A
Server profile {serverProfileName}'s {identityType} identity is in use by other server {serverId}.	Error	Please apply other profile to server or remove profile from server and then try the operation again.
Server profile: {serverprofileid} has multiple native VLANs found	Error	N/A
Server(s) {serveruuid} are already in use by other service template.	Error	N/A
Server(s) {serveruuid} are already in use by other service template.	Error	N/A
Service template {templateid} deletion failed.	Error	N/A
Service template {templatename} already exists.	Error	Please check template inventory and provide unique template name.
Service template {templatename} creation failed.	Error	N/A
Service template {templatename} update failed.	Error	N/A
Specified EsxiStateless image {imageid} cannot be found.	Error	Please check that provided image exists and is of type EsxiStateless.

Event	Severity	Recommended action
Specified locale(s) is not supported. Locale(s):{locales}	Error	Please check input parameters and correct them appropriately.
Started applying service template {templateName} to server {serverId}.	Info	N/A
Started OS deployment of image {imageName} for {serverUuid}	Info	N/A
Started to apply service template {templatename} to cluster {clustername}.	Info	N/A
Started using Virtual Distributed Switch {vdsName} for cluster.	Info	N/A
Storage cluster creation failed.	Warning	N/A
Storage cluster creation was successful.	Info	N/A
Storage Configuration was successful.	Info	N/A
Storage operations are not supported for host {hostuuid}. Ensure host is turned on and visible to Vcenter.	Error	N/A
Succeeded in changing the power state of server Id: {serverUuid} with serial number: {serverSerialNumber}. HCSM status: {hcsmPowerStateChangeResult}.	Info	N/A
Successfully added IP address pool range	Info	N/A
Successfully added reference host to vSphere Distributed Switch.	Info	N/A
Successfully applied host profile to all hosts in the cluster.	Info	N/A
Successfully changed server LID state. HCSM response: {hcsmLidStateChangeResult}.	Info	N/A
Successfully cloned service template {templatename1} and created new service template {templatename2}.	Info	N/A
Successfully configured image {imageid} for cluster.	Info	N/A
Successfully configured network on a server(s) {serverUuids}.	Info	N/A
Successfully created base host profile {hostProfile} for cluster.	Info	N/A
Successfully created cluster{clustername}.	Info	N/A
Successfully created server profile.	Info	N/A

Event	Severity	Recommended action
Successfully created Virtual Distributed Switch {vdsName} for cluster.	Info	N/A
Successfully deleted service template {templatename}.	Info	N/A
Successfully removed IP Address pool range	Info	N/A
Successfully removed server profile.	Info	N/A
Successfully removed server profile.	Info	N/A
Successfully update Dhcp Config.	Info	N/A
Successfully updated file: {filename}.	Info	N/A
Successfully updated firmware for chassis: {chassisid}.	Info	N/A
Successfully updated firmware for server: {serverId}	Info	N/A
Successfully updated HCSM information.	Info	N/A
Successfully updated server profile.	Info	N/A
Successfully updated service template {templatename} information.	Info	N/A
Successfully updated service template {templatename} information.	Info	N/A
Successfully validated identities applied to server {serverid} from profile {profilename}.	Info	N/A
Switch connectivity unavailable for server: {serverid}	Error	N/A
The credentials passed in are not valid. Please pass valid domain credential.	Error	N/A
The host: {host} has non-redundant configuration settings for one or more virtual switch/virtual distributed switch. UCP requires atleast two uplinks for each host attached to the same virtual switch/ virtual distributed switch.	Error	N/A
The overall status of UCP's Compute resources is now Critical. View UCP's Status Monitor for more information.	Error	Contact the Compute Administrator.
The overall status of UCP's Compute resources is now Not Applicable. View UCP's Status Monitor for more information.	Info	N/A
The overall status of UCP's Compute resources is now Ok.	Info	N/A

Event	Severity	Recommended action
The overall status of UCP's Compute resources is now Unknown. View UCP's Status Monitor for more information.	Warning	Contact the Compute Administrator.
The overall status of UCP's Compute resources is now Warning. View UCP's Status Monitor for more information.	Warning	Contact the Compute Administrator.
The raw volume {volumeId} can't be attached to server {serverId} because the server is configured to boot ESXi.	Error	N/A
The request restful API is not implemented yet.	Error	N/A
The selected image is already scheduled to be loaded upon next reboot.	Error	N/A
The selected image is already the default for server type: {serverType}.	Error	N/A
The selected server must be in Maintenance Mode before executing the specified power operation.	Error	N/A
The server {serverId} was not able to be removed from vCenter host inventory.	Error	N/A
The supplied server type: {serverType} could not be found. Supported server type(s) include {expectServerTypes}.	Error	N/A
The UUID of a hyper-V host retrieved from SCVMM (name = {name}, id ={id}) is not set.	Warning	N/A
There are duplicate packages in the request.	Error	N/A
There is a duplicate repository location: {repositoryLocation} in the request.	Info	N/A
There were network connectivity issues detected.	Warning	Contact the Network Administrator.
There were storage connectivity issues detected.	Warning	Contact the Storage Administrator.
To edit or delete an image, the image must be created by UCP.	Error	N/A
To edit or delete an image, the image must not be in use by any servers.	Error	N/A
UCP could not configure WDS to use image unattend file.	Error	Please resolve the issue and try to apply template again.
UCP could not update the inventory details for server.	Warning	N/A
UCP credentials used do not have sufficient permissions to access WDS RemoteInstall folder.	Error	N/A

Event	Severity	Recommended action
UCP did not receive WDS events.	Error	Please resolve the issue and try to apply template again.
UCP failed to backup DHCP configuration file.	Error	N/A
UCP failed to read DHCP configuration file.	Error	N/A
UCP failed to restart DHCP Service.	Error	N/A
UCP failed to start DHCP Service.	Error	N/A
UCP failed to stop DHCP Service.	Error	N/A
UCP failed to update DHCP configuration file.	Error	N/A
UCP has reset server with serial number: {serverSerialNumber} (UUID = {serverUuid}). Auto deploy will now load ESXi. This could take a few minutes.	Info	Please access console via the Servers table to view progress.
UCP has successfully updated the inventory for server.	Info	N/A
UCP inventory details for server have expired.	Error	Please wait for all relevant tasks to finish, perform a refresh and then retry the operation.
UCP Scheduled Job {jobType} has been updated to never run.	Info	N/A
UCP Scheduled Job: {jobType} has been updated to run in every {time} minutes.	Info	N/A
Unable to contact repository or repositories: {repositoryLocation}.	Error	N/A
Unable to create or apply the host profile. Please check that the host profile is not currently attached to any of the targeted hosts and try again.	Error	N/A
Unable to create updates for the following image(s): {imageNames}	Error	N/A
Unable to discover server port adapter(s): ({portIds}) on UCP fabric.	Error	Please check that the specified initiator WWN is a UCP host and that the host is online and has active operating system. Perform fiber channel switch refresh if host is online and operation still fails with this error.
Unable to export the new image: {imageName}.	Error	N/A
Unable to get network connectivy for server.	Error	Please check that provided server has network connectivity on ethernet ports and switch can see this server.

Event	Severity	Recommended action
Unable to obtain unique LUN number for provided server {serverUuid}.	Error	N/A
Unable to read CNA settings from HCSM.	Error	N/A
Unable to read contents of file: {FileName}. Error message: {ErrorMessage}.	Error	N/A
Unable to read contents of file: {FileName}. Error message: {ErrorMessage}.	Error	N/A
Unable to retrieve datacenters from the Platform Manager. Ensure that datacenter(s) exist in the Platform Manager and try again.	Error	N/A
Unable to retrieve Mezzanine card slot number for server {serverid}.	Error	N/A
Unable to update HCSM information. Please validate that the service URL, application URL, username, and password are correct.	Error	N/A
Unassociate server profile started for server {serverid}	Info	N/A
Unassociated Server Profile {serverprofileid} from server {serverid}	Info	N/A
Unassociating Server Profile {serverprofileid} with server {serverid} failed	Error	N/A
Update repository locations are not defined.	Info	N/A
Updating host name is only supported on server with custom boot type. Please check boot type and try again.	Error	N/A
Updating host profile from host failed in vCenter.	Error	N/A
Updating server profile {serverprofileid} failed	Error	N/A
Updating server profile {serverprofileid} started	Info	N/A
Updating server profile {serverprofileid} succeeded	Info	N/A
Updating service template: {servicetemplateid} failed	Error	N/A
Updating service template: {servicetemplateid} started	Info	N/A
URL: {URL} cannot be reached.	Error	Verify the URL to ensure it is accurate and/or check that UCP has network access to the URL.
Volume {volumeId} attached to server {serverId}.	Info	N/A
Volume sharing is not allowed across disparate operating systems	Error	N/A

Event	Severity	Recommended action
Volume(s) {LdevList} cannot be shared across disparate operating systems.	Error	N/A
Windows Deployment Services issued a DDP request warning while applying service template {templateName} to server {serverId}.	Warning	N/A
Windows Deployment Services reported that a driver could not be injected when applying service template {templateName} to server {serverId}.	Warning	N/A
Wwn address {wwnAddress} is already in use.	Error	N/A
Wwn settings in server profile do match with the settings in server inorder to apply the server profile	Error	N/A

Storage

The following table lists all of the events that are related to storage inventory.

Event	Severity	Recommended action
A cache module at location {CacheLocation} in storage array: {StorageArrayName} has experienced a blocking event that reduced the amount of available cache.	Error	Contact Global Hitachi Support.
A micro processor at location MPB: {MpbName} MP#: {MpNumber} in storage array: {StorageArrayName} has failed. Storage operation performance will be degraded.	Warning	Contact Global Hitachi Support.
A pool in storage array: {StorageArrayName} is exceeding the defined pool usage threshold. Please consider performing storage DRS actions for VMs on Formatted Volumes participating in the pool.	Warning	Contact Global Hitachi Support.
At least 2 Formatted Volume should be provided to SDRS enabled cluster.	Error	N/A
Attaching volume {volumeId} to host: {hostname} in this cluster.	Info	N/A
Cannot access Horcm instance {HorcmInstanceNumber}. Ensure that file has appropriate permissions and no other application has the file locked.	Error	N/A
Cannot attach boot volume as a data volume.	Error	N/A

Event	Severity	Recommended action
Cannot configure Horcm instance {HorcmInstanceNumber} since it contains the following unattached volumes: {volumeId}. Check that these volumes exist and are attached to appropriate hosts or remove the volumes from configuration.	Error	N/A
Cannot delete journal {journalID} since the journal is being used for replication	Error	N/A
Cannot expand boot volume : {volumeid} as the volume is currently being used by server: {serverid}	Error	N/A
Cannot proceed since volume {volumeid} belongs to a replication pair.	Error	Please stop volume replication and retry
Cannot resolve cci server: {cciServerName}.	Error	N/A
Cannot use volumes from HDT pool on SDRS enabled cluster with automation levels set to fully automated.	Error	Please edit template to choose manual automation level or use volumes from HDP pool.
Cluster Failed to attach volume {volumeId} to host(s): {hostid} in the cluster.	Error	N/A
Connection error occurred at fibre channel switch: {IpAddress}.	Error	Contact the system administrator.
Could not add paired device(s). There are existing paired device name(s): {pairedDeviceNames} in the request for Horcm instance {horcmInstanceNumber}	Error	N/A
Could not add paired volume(s). There are existing paired volume(s): {pairedVolumes} in the request for Horcm instance {horcmInstanceNumber}	Error	N/A
Could not create new copy group. There is an existing copy group name: {copyGroupName} in the request for Horcm instance {horcmInstanceNumber}	Error	N/A
Could not pair/resync copygroup: {copyGroupId}. Reason: {message}.	Error	N/A
Datastore was created successfully.	Info	N/A
Datastore was created successfully.	Info	N/A
Datastore was created successfully.	Info	N/A
Datastore was created successfully.	Info	N/A
Detaching volume {volumeId} from host: {hostname} in this cluster.	Info	N/A

Event	Severity	Recommended action
Drive {DiskNumber} in storage array: {StorageArrayName} has experienced a drive error. HDD sparing will occur and the drive will need to be replaced.	Error	Contact Global Hitachi Support.
Drive {DiskNumber} in storage array: {StorageArrayName} has experienced a drive failure. HDD sparing will occur and the drive will need to be replaced.	Error	Contact Global Hitachi Support.
Drive {DiskNumber} in storage array: {StorageArrayName} has experienced a drive service notification. HDD sparing will occur and the drive will need to be replaced.	Info	Contact Global Hitachi Support.
Drive: {DiskNumber} in storage system: {StorageArrayName} has experienced a media error. HDD sparing will occur and the drive will need to be replaced.	Error	Contact Global Hitachi Support.
External port connected to channel: {ChannelNumber} and port: {PortNumber} in storage system: {StorageArrayName} has been blocked. This will affect communication with any external storage array(s) on this port.	Warning	Contact Global Hitachi Support.
Failed to attach the volume: {volumeid} to server.	Error	N/A
Failed to attach volume {volumeId} to host: {hostname} in this cluster.	Error	N/A
Failed to attach volume to host: {hostname} in this cluster.	Error	N/A
Failed to attach volume: {volumeId} to the cluster.	Error	N/A
Failed to attach volume: {volumeId} to the cluster.	Error	N/A
Failed to create storage path for host.	Error	N/A
Failed to create storage path for server.	Error	N/A
Failed to detach volume {volumeId} from host: {hostname} in this cluster.	Error	N/A
Failed to detach volume: {volumeid} from server.	Error	N/A
Failed to extract LDEV for volume. Please ensure that only supported storage devices are attached to host.	Error	N/A
Failed to identify an available LUN reservation during pre-check process.	Error	N/A
Failed to identify current LUNs correctly on server during pre-check process.	Error	N/A

Event	Severity	Recommended action
Failed to refresh Fibre Channel SAN topology information.	Error	N/A
Formatted Volume was created successfully.	Info	N/A
Formatted Volume was created successfully.	Info	N/A
Formatted Volume was created successfully.	Info	N/A
Formatted Volume was created successfully.	Info	N/A
HDvM is unable to use storage system {StorageSystem} for UCP Director and is reporting: "{errorMsg}". UCP Director will retry until it is able to use the storage system.	Warning	Please ensure that the array is not held up indefinitely by other users/operations so UCP Director can continue this job.
HDvM is unable to use storage system {StorageSystem} for UCP Director and is reporting: "{errorMsg}". UCP Director will retry until it is able to use the storage system.	Warning	Please ensure that the array is not held up indefinitely by other users/operations so UCP Director can continue this job.
HDVM version is not supported. Supported versions include: {versions}.	Error	Please install a supported version of HDVM.
Horcm instance {HorcmInstanceNumber} contains unsupported configuration. Possible cause - Copy group is paired with multiple horcm instances	Error	Please review any manually added configuration entries and ensure that the configurations are valid
Host(s): {hostName} do not see the datastore on this volume.	Error	Please manually refresh Storage system inventory in UCP Director Console. Reboot the ESXi host if it still does not appear as attached.
Host: {hostname} is out of sync with the storage system: {storageSystemId}. The Logical Unit Number(LUN): {luNumber} for the hosts is used on the following port(s): {listofPortNames}, but the host is not recognizing the LUN.	Error	Confirm the ports are connected to UCP fabrics.Perform the following actions. 1) Confirm zones exist for the host and ports. If zones do not exist create zones. 2) Rescan volumes of the hosts from vCenter and confirm the LUN is shown on vCenter. 3) If the LUN is not shown on vCenter, reboot the host.
HTI Pools are not supported. Please specify a different Pool to create volumes from.	Error	N/A
HTI Volume: {volid} could not be deleted.	Warning	N/A
HTI Volumes are not supported. Please specify different Volume(s) to attach.	Error	N/A
In place journal expansion is only supported for Vsp8 array family	Error	N/A

Event	Severity	Recommended action
Invalid pool(HTI) was selected: {poolid}.	Error	N/A
Journal expansion by adding journalVolumes is not supported for the Vsp8 array family	Error	N/A
Journal Volume {journalVolumeId} is already associated with a journal.	Error	N/A
Licensed capacity exceeded for replication software.	Error	N/A
LUN reservation pre-check failed. The LUN number used for this volume by some hosts in the cluster can not be used by all hosts in the cluster.	Error	Detach the volume from any individual hosts it is connected to. Then re-attach the volume to the entire cluster.
No Horcm instances found in UCP {UcpInstanceIdentifier}	Error	N/A
No such copy group {CopyGroupName} exists on Horcm instance {HorcmInstanceNumber}	Error	N/A
No such disaster recovery manager: {disasterRecoveryManagerId}.	Error	N/A
No such Horcm instance {HorcmInstanceNumber} exists	Error	N/A
No such journal {journalId} exists in the Storage system	Error	N/A
No such journal volume {journalVolumeID} in the storage system	Error	N/A
No such paired device {pairedDeviceName} exists in copy group {copyGroupName} and horcm instance {horcmInstanceNumber}	Error	N/A
No such parity group: {parityGroupId} at storage system: {storageSystemId}.	Error	N/A
No such path group: {pathGroupId} exists at storage system: {StorageSystemId} in UCP {UcpInstanceIdentifier}	Error	N/A
No such pool: {poolid} at storage system: {storageSystemId}.	Error	N/A
No such port: {portid} at storage system: {storageSystemId}.	Error	N/A
No such replicated volume {volumeId} on storage system {storageSystemId} in a Horcm instance.	Error	N/A
No such storage system: {storageSystemId}.	Error	N/A
No such volume: {volumeid} at storage system: {storageSystemId}.	Error	N/A

Event	Severity	Recommended action
No volume is mounted on the server	Warning	N/A
One or more of attached hosts do not see the volume is formatted.	Error	Please wait for all relevant tasks to finish, perform a refresh and then retry the operation.
One or more of the Host Storage Domain(s)(HSD): {hsd} for this host are of an unsupported configuration and cannot be managed by UCP.	Error	Use HDvM or Storage Navigator to delete the unsupported HSDs and then perform the Attach or Detach operation.
One or more of the Host Storage Domain(s)(HSD): {hsd} for this server are of an unsupported configuration and cannot be managed by UCP.	Error	Use HDvM or Storage Navigator to delete the unsupported HSDs and then perform the Attach or Detach operation.
One or more volumes could not be attached to cluster.	Error	Please wait for all relevant tasks to finish, perform a refresh and then retry the operation.
One or more volumes could not be attached to host.	Error	Please wait for all relevant tasks to finish, perform a refresh and then retry the operation.
Out of shared memory space in storage array: {StorageArrayName}.	Warning	Contact Global Hitachi Support.
Pool: {PoolNumber} in storage array: {StorageArrayName} has become full.	Warning	Contact Global Hitachi Support.
Pool: {PoolNumber} in storage array: {StorageArrayName} has detected a failure.	Warning	Contact Global Hitachi Support.
Pool: {PoolNumber} in storage array: {StorageArrayName} has exceeded a pool depletion threshold. Please consider performing storage DRS actions for VMs on Formatted Volumes participating in this pool.	Warning	Contact Global Hitachi Support.
Pool: {PoolNumber} in storage array: {StorageArrayName} has exceeded a pool system threshold. Please consider performing storage DRS actions for VMs on Formatted Volumes participating in this pool.	Error	Contact Global Hitachi Support.
Pool: {PoolNumber} in storage array: {StorageArrayName} has exceeded a pool warning threshold. Please consider performing storage DRS actions for VMs on Formatted Volumes participating in this pool.	Warning	Contact Global Hitachi Support.
Pool: {PoolNumber} in storage array: {StorageArrayName} is blocked.	Warning	Contact Global Hitachi Support.

Event	Severity	Recommended action
Port: {PortNumber} on storage array: {StorageArrayName} has been blocked. This will affect communication with any hosts on this port.	Warning	Contact Global Hitachi Support.
Refresh cannot be performed as the Device manager is busy doing a resync or performing some other operations.	Error	Please wait for all relevant tasks to finish, perform a refresh and then retry the operation.
Removed Fibre Channel zone(s): {ZoneName} from the active zoneset in fabric(s): {FabricName}.	Info	N/A
Removed the storage paths for this host on array ports: {PortName}.	Info	N/A
Removed the storage paths for this server on array ports: {PortName}.	Info	N/A
Replication License has expired.	Error	N/A
Replication software invalidated due to expiration of the prerequisite program license key	Error	N/A
ReplicationManager is unable to access the horcm configuration at: {horcm_configuration_directory}. Please ensure the directory is accessible.	Error	N/A
Response time from an external device attached to channel: {ChannelNumber} and port: {PortNumber} has exceeded the timeout value.	Warning	Contact Global Hitachi Support.
Serialization/deserialization failed for an AMQP message of type {messageType}	Error	Contact the system administrator.
Site Recovery Manager Credentials already exist for this UCP.	Error	N/A
Storage Array {StorageSystem} controllers are down.	Error	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a battery failure.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a cache memory failure.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a drive failure.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a failure of a disk path.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a failure of controller with IP Address : {controllerIP}.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a failure of Drive I/O module	Warning	Contact Global Hitachi Support.

Event	Severity	Recommended action
Storage Array {StorageSystem} detected a failure of ENC (I/O Module).	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a failure of host connector on a port.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a failure of host I/O module.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a failure of interface board.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a failure of management module (LAN).	Error	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a failure of side card failure	Error	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a failure of spare drive.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a fan failure.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a generic warning.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a overcapacity for a Dynamic Provisioning pool	Error	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a power supply failure.	Error	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a recoverable failure of controller.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected a UPS failure.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected an invalid SNMP access.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected depletion warning for a Dynamic Provisioning pool.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected initial warning for a Dynamic Provisioning pool.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected multiple drive failures.	Error	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected over threshold of a pool's subscription.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected temperature is over limit.	Error	Contact Global Hitachi Support.

Event	Severity	Recommended action
Storage Array {StorageSystem} detected that pool's subscription is over limit.	Error	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected that write count for a SSD has reach 100%.	Error	Contact Global Hitachi Support.
Storage Array {StorageSystem} detected that write count for a SSD has reached 90%.	Warning	Contact Global Hitachi Support.
Storage Array {StorageSystem} was powered on and the SNMP agent was started.	Info	N/A
Storage Array's {StorageSystem} management module was re-started or Storage Array's SNMP configuration file was reconfigured.	Info	Contact Global Hitachi Support.
Storage disk not found from powershell cmdlet GetSCStorageDiskInfo	Warning	N/A
Storage path creation for server succeeded.	Info	N/A
Successfully added paired devices with ID: {PairedDeviceId} to Copy Group {copyGroupId}	Info	N/A
Successfully attached volume {volumeId} to host: {hostname} in this cluster.	Info	N/A
Successfully attached volume: {volumeid} to server.	Info	N/A
Successfully created copy group with ID: {copyGroupId}	Info	N/A
Successfully created HTI Volume with VolumeId: {VolumeId}	Info	N/A
Successfully created Journal {journalId} for replication	Info	N/A
Successfully deleted Journal {journalId}	Info	N/A
Successfully detached volume {volumeId} from host: {hostname} in this cluster.	Info	N/A
Successfully detached volume: {volumeid} from server.	Info	N/A
Successfully expanded the journal {journalId}	Info	N/A
Successfully paired and resync copy group: {copyGroupName}	Info	N/A
Successfully refreshed Fibre Channel SAN topology information.	Info	N/A
Successfully removed copy group with ID: {copyGroupId}	Info	N/A

Event	Severity	Recommended action
Successfully removed paired device with ID: {PairedDeviceId} from Copy Group {copyGroupId}	Info	N/A
Successfully resolved cci server: {cciServerName}	Info	N/A
Successfully updated credentials for Site Recovery Manager	Info	N/A
Successfully updated HDvM information.	Info	N/A
The API for retrieving physical devices is not implemented for VSP or HUS VM storage systems.	Error	N/A
The controller unit for storage array: {StorageArrayName} has experienced an acute failure. All storage functions have ceased.	Error	Contact Global Hitachi Support.
The current horcm configuration file for horcm instance: {HorcmInstanceNumber} does not match the last trusted horcm configuration. This file has been modified outside of UCP and may contain unsupported and/or incorrect configuration. To fix this issue, restore the Horcm configuration with the last known good horcm configuration.	Error	N/A
The datastore could not be expanded. Refer to logs and task list for more information.	Warning	Please use VMware vSphere Client to login to one of the hosts the volume is attached to and expand the datastore manually.
The datastore has been expanded successfully.	Info	N/A
The Formatted Volume could not be expanded on SCVMM host. Refer to logs and task list for more information.	Warning	Please use VMM Console to login to one of the hosts the volume is attached to and expand the formatted volume manually.
The Formatted Volumehas been expanded successfully.	Info	N/A
The Horcm instance {HorcmInstanceNumber} is not running.	Error	Please restart the Horcm service and try again.
The operation on volume {volumeId} requires access to storage pool {storagePoolId}, which is not accessible by UCP Director.	Error	If you wish to perform the operation with UCP director, add the storage pool to a resource group accessible by UCP Director.
The overall status of UCP's Storage resources is now Critical. View UCP's Status Monitor for more information.	Error	Contact the Storage Administrator.
The overall status of UCP's Storage resources is now Not Applicable. View UCP's Status Monitor for more information.	Info	N/A

Event	Severity	Recommended action
The overall status of UCP's Storage resources is now Ok.	Info	N/A
The overall status of UCP's Storage resources is now Unknown. View UCP's Status Monitor for more information.	Warning	Contact the Storage Administrator.
The overall status of UCP's Storage resources is now Warning. View UCP's Status Monitor for more information.	Warning	Contact the Storage Administrator.
The requested storage processor {storageProcessorId} does not exist on storage system {storageSystemSerialNumber}.	Error	N/A
The requested volume size will exceed the pool subscription limit for pool: {poolid}.	Error	Please select a different pool with sufficient capacity.
The selected HTI volume: {volumeid} has been deleted.	Info	N/A
The selected volume: {volumeid} has been deleted.	Info	N/A
The selected volume: {volumeId} is already attached to server as LUN #: {LunId}.	Info	N/A
The selected volume: {volumeId} is already attached to server as LUN #: {LunId}.	Info	N/A
The specified initiator World Wide Name (WWN): {initiatorwwn} could not be found.	Error	Please check that the specified initiator WWN is a UCP host and that the host is online and has active operating system. Perform fiber channel switch refresh if host is online and operation still fails with this error.
The specified target World Wide Name (WWN): {targetwwn} could not be validated as a known UCP storage array port.	Error	Please check that the specified target WWN is a UCP array port and that the port is online.
The specified volume: {volumeId} has multiple LUN paths with more than one LUN ID and cannot be managed by UCP.	Error	Use HDvM or Storage Navigator to delete the unsupported HSDs and then perform the Attach or Detach operation.
The username or password is incorrect. Please enter valid credentials.	Error	N/A
The volume {volumeId} is part of a SRM Protection group. Please remove the volume from the SRM Protection Group and retry the operation.	Error	Check and update the DR recovery plan
The volume: {volumeid} could not be expanded. Refer to logs and task list for more information.	Error	N/A

Event	Severity	Recommended action
The volume: {volumeid} has been expanded successfully.	Info	N/A
There is no last trusted horcm configuration for horcm instance: {HorcmInstanceNumber}. The current horcm file will be accepted as the last trusted horcm configuration.	Error	N/A
Timed out trying to lock the horcm configuration after: {timeout} seconds. Please try your request again later.	Error	N/A
UCP cannot find an appropriate set of storage ports for this operation. UCP requires 4 total ports. Two of which must be connected to Fabric A, and two to Fabric B. Of the two ports connected to each fabric, one must be from storage cluster 1, and another one must be from storage cluster 2.	Error	N/A
UCP could not update inventory details for storage array {storageSystemId} and its elements (i.e. Pools, Ports, Volumes).	Error	Please wait for all relevant tasks to finish, perform a refresh and then retry the operation.
UCP could not update inventory details for storage arrays and storage array elements (i.e. Pools, Ports, Volumes).	Warning	N/A
UCP could not update inventory details for storage resources that are connected to host(s).	Warning	N/A
UCP has detected either no array or multiple arrays in the resource group assigned to UCP in the device manager.	Error	Please reconfigure HDvM to manage a single VSP storage array.
UCP has updated inventory details for storage resources that are connected to host(s).	Info	N/A
UCP inventory detail has expired for storage resources that are connected to host(s).	Error	Please wait for all relevant tasks to finish, perform a refresh and then retry the operation.
UCP inventory details for storage arrays and storage array elements (i.e. Pools, Ports, Volumes) successfully refreshed.	Info	N/A
UCP inventory refresh for storage arrays and storage array elements (i.e. Pools, Ports, Volumes) has failed. The current inventory details are invalid.	Error	Please wait for all relevant tasks to finish, perform a refresh and then retry the operation.
UCP management configuration information provided to UCP Director is not correct.	Error	N/A

Event	Severity	Recommended action
Unable to connect to HDvM. Please validate the following: 1) Service and Application URL are correct. 2) Username and Password are correct. 3) HDvM service is available. 4) Network connectivity is available.	Error	N/A
Unable to establish Site Recovery Manager connection	Error	N/A
Unable to update HDvM information. Please validate that the service URL, application URL, username, and password are correct. Also ensure that the HDvM version is supported by UCP Director.	Error	N/A
Unexpected error with error code: {errorcode} occurred on the device manager.	Error	Please check logs for more details.
Volume attach operation failed for the host(s): {hostid} in the cluster.	Error	N/A
Volume attach/detach operation failed as the Logical Unit Numbers (LUNs): {luNumbers} in Host Storage Domains (HSDs): {hsds} are shared by multiple volumes: {volumeIds}.	Error	N/A
Volume detach operation failed for volume: {volumeId} attached to the host(s): {hostid} in the cluster.	Error	N/A
Volume detach operation failed for volume: {volumeId} attached to the host(s): {hostid} in the cluster.	Error	N/A
Volume is still attached to server.	Error	The selected volume must not have any paths to hosts before performing "Delete Volume" operation. Please detach the volume from all hosts and retry. If the operation still fails go to HDvM and unallocate volume from all the hosts.
Volume was attached to cluster but the datastore could not be created.	Warning	Please use the VMware vSphere client to login to one of the hosts in the cluster and create the datastore manually.
Volume was attached to host but could not be formatted.	Warning	N/A
Volume was attached to host but the datastore could not be created.	Warning	Please use the VMware vSphere client to login to the host and create the datastore manually.

Event	Severity	Recommended action
Volume(s) can be expanded only in increments of 1 GB. The supplied value to expand volume from current volume size: {currentVolumeSize} to target volume size: {targetVolumeSize} is not allowed.	Error	N/A
Volume: {volid} could not be deleted.	Warning	N/A
Volume: {volumeid} is not attached to server.	Info	N/A
Volume: {volumeId} is still attached to server.	Error	The selected volume must not have any paths to hosts before performing "Delete Volume" operation. Please detach the volume from all hosts and retry. If the operation still fails go to HDvM and unallocate volume from all the hosts.
Volume: {volumeid} was attached but could not be validated from host as an attached volume.	Warning	Please manually refresh Storage system inventory in UCP Director Console. Reboot the hypervisor host if it still does not appear as attached.
Volume: {volumeid} was attached to cluster but could not be formatted.	Warning	N/A
Volume: {volumeid} was attached to cluster but the datastore could not be created.	Warning	Please use the VMware vSphere client to login to one of the hosts in the cluster and create the datastore manually.
Volume: {volumeid} was attached to host but could not be formatted.	Warning	N/A
Volume: {volumeid} was attached to host but the datastore could not be created.	Warning	Please use the VMware vSphere client to login to the host and create the datastore manually.
Volume: {volumeid} was attached to server and validated successfully.	Info	N/A
Volume: {volumeid} was detached from server but there were errors during verification.	Warning	N/A
Volume: {volumeid} was successfully created in pool: {poolId}.	Info	N/A

C

VMware alarms

The following table lists all of the alarms that are generated by UCP Director.

Alarm	Description
Hitachi - AMQP service startup failed	AMQP service failed to startup. Please refer to vCenter Events for details
Hitachi - Chassis AC voltage problem	A chassis has encountered a problem with the alternating current (AC) voltage.
Hitachi - Chassis cooling fan problem	A chassis cooling fan is experiencing a functionality problem. The fan may be failing and need replacement.
Hitachi - Chassis hardware problem	A chassis hardware event occurred. Check HCSM for more details.
Hitachi - Chassis management module problem	A chassis management module experienced a functionality problem.
Hitachi - Chassis module problem	A hardware event has occurred in a chassis module. Check HCSM for more details.
Hitachi - Chassis passthrough module removed	A chassis passthrough module was removed. Check HCSM for more details.
Hitachi - Chassis power supply problem	A chassis power supply has experienced an issue. The power supply may be failing and need replacement.
Hitachi - Chassis SVP firmware update failed	Chassis firmware update has failed. Please contact system administrator to manually troubleshoot the issue and update firmware.
Hitachi - Chassis switch module problem	A chassis switch module experienced a warning or failure.
Hitachi - Chassis temperature problem	The chassis temperature is too high. Check chassis ventilation and datacenter air conditioning.
Hitachi - Chassis voltage problem	A chassis voltage problem needs attention. Please check HCSM for more details.
Hitachi - Converged switch hardware problem	A converged switch is experiencing hardware issues. Refer to vCenter Events for details.

Alarm	Description
Hitachi - Converged switch license expire issue	Software crashed for an converged switch. Please refer to vCenter Events for details.
Hitachi - Converged switch port issue	A Converged switch port experienced a link issue. Refer to vCenter Events for details.
Hitachi - Converged switch rebooted	A Converged switch has rebooted. Refer to vCenter Events for details.
Hitachi - Converged switch software crash	There is a converged switch license expiration issue. Refer to vCenter Events for switch identity and check the corresponding Ethernet switch for more details.
Hitachi - Converged Switches inventory refresh	There are connection issues with one or more converged switches and converged switch inventory has expired. Check the converged switch connectivity settings.
Hitachi - Ethernet Switch firmware update failed	Ethernet switch firmware update has failed. Please contact system administrator to manually troubleshoot the issue and update firmware.
Hitachi - Ethernet switch configuration problem	An Ethernet switch has a configuration issues. Refer to vCenter Events for details.
Hitachi - Ethernet switch hardware problem	An Ethernet switch is experiencing hardware issues. Refer to vCenter Events for details.
Hitachi - Ethernet switch license expire issue	Software crashed for an ethernet switch. Please refer to vCenter Events for details.
Hitachi - Ethernet switch port issue	An Ethernet switch port experienced a link issue. Refer to vCenter Events for details.
Hitachi - Ethernet switch port problem	An Ethernet switch port experienced a problem. Refer to vCenter events for details.
Hitachi - Ethernet switch rebooted	An Ethernet switch has rebooted. Refer to vCenter Events for details.
Hitachi - Ethernet switch software crash	There is an Ethernet switch license expiration issue. Refer to vCenter Events for switch identity and check the corresponding Ethernet switch for more details.
Hitachi - Ethernet Switches inventory refresh	There are connection issues with one or more Ethernet switches and Ethernet switch inventory has expired. Check Ethernet switch connectivity settings.
Hitachi - Fibre Channel Switch firmware update failed	Fibre Channel switch firmware update has failed. Please contact system administrator to manually troubleshoot the issue and update firmware.
Hitachi - Fibre Channel switch configuration problem	A Fibre Channel switch configuration has issues. Refer to vCenter Events for details.
Hitachi - Fibre Channel switch hardware problem	A Fibre Channel switch is experiencing hardware issues. Refer to vCenter Events for details.

Alarm	Description
Hitachi - Fibre Channel switch port problem	A Fibre Channel switch port experienced a problem. Refer to vCenter events for details.
Hitachi - Fibre Channel switch zoning problem	A Fibre Channel switch zoning operation experienced issues. Refer to vCenter Events for details.
Hitachi - Fibre Channel switches inventory refresh	There are connection issues with one or more Fibre Channel switches and Fibre Channel switch inventory has expired. Check Fibre Channel switch connectivity settings.
Hitachi - Hitachi Unified Storage array connection problem	A Hitachi Unified Storage system is experiencing issues connecting to another storage system. Refer to HDvM for details.
Hitachi - Hitachi Unified Storage array hardware problem	A Hitachi Unified Storage system experienced a hardware issue. Refer to HDvM for details.
Hitachi - Hitachi Unified Storage array pool problem	A Hitachi Unified Storage pool has experienced an issue. Refer to HDvM for details.
Hitachi - Hitachi Unified Storage array resource issue	There is an issue with Hitachi Unified Storage system resources. Refer to HDvM for details.
Hitachi - Image repositories unreachable issue	Update active images failed because a repository is unreachable.
Hitachi - Monitor service startup issue	There is an issue with starting the UCP Monitor service.
Hitachi - Overall Compute Status	UCP's Compute resources are experiencing problems. View UCP's Status Monitor for more information.
Hitachi - Overall Ethernet Status	UCP's Ethernet resources are experiencing problems. View UCP's Status Monitor for more information.
Hitachi - Overall Fibre Channel Status	UCP's Fibre Channel resources are experiencing problems. View UCP's Status Monitor for more information.
Hitachi - Overall Storage Status	UCP's Storage resources are experiencing problems. View UCP's Status Monitor for more information.
Hitachi - Scheduler service startup issue	There is an issue with starting the UCP Scheduler service.
Hitachi - Server firmware update failed	Server firmware update has failed. Please contact system administrator to manually troubleshoot the issue and update firmware.
Hitachi - Server blade partition problem	A blade server has experienced a partition issue.
Hitachi - Server CPU correctable or uncorrectable errors	A server CPU has experienced an error or has been disabled. Check HCSM for more details.
Hitachi - Server CPU temperature problem	The CPU temperature is too high. The CPU may need to be replaced.

Alarm	Description
Hitachi - Server element manager refresh	Server inventory has expired due to connection issues with HCSM.
Hitachi - Server failed a power operation	A server failed to respond to a power operation command.
Hitachi - Server is in a degraded state	A warning or serious event has happened on a blade server. Check HCSM for more details.
Hitachi - Server memory DIMM correctable or uncorrectable errors	A server DIMM has experienced errors. Check HCSM for more details.
Hitachi - Server non-maskable interrupt occurred	A non-maskable interrupt has occurred. Check HCSM for more details.
Hitachi - Server watchdog timer has expired	ESXi was unresponsive long enough to cause a timer to expire. Use vCenter diagnostic tools to investigate.
Hitachi - Storage array connection problem	A storage system is experiencing issues connecting to another storage system. Refer to HDvM for details.
Hitachi - Storage array hardware problem	A storage system experienced a hardware issue. Refer to HDvM for details.
Hitachi - Storage array pool problem	A storage pool has experienced an issue. Refer to HDvM for details.
Hitachi - Storage array resource issue	There is an issue with storage system resources. Refer to HDvM for details.
Hitachi - Storage element manager refresh	Storage inventory has expired due to connection issues with HDvM.

D

VMware privileges

UCP Director roles in VMware are configured to have the following privileges:

vCenter privilege	Description	UCP Director roles			
		UCP system admin	UCP server admin	UCP storage admin	UCP network admin
UCP		***X***	***X***	***X***	***X***
UCP View	Enables read-only viewing access to UCP Director	X	X	X	X
UCP.ServerAdministration	Enables server orchestration access	X	X		
UCP.ServerConsole	Enables access to the server console	X	X		
UCP.StorageAdministration	Enables storage system orchestration access	X		X	
UCP.StorageConsole	Enables access to the storage system console	X		X	
UCP.NetworkAdministration	Enables access network orchestration access	X			X
UCP.NetworkGlobalVlan	Enables access to remove all VLANs and apply specific global VLANs to all managed Ethernet switch ports	X			X
UCP.NetworkConsole	Enables access to the Ethernet switch console	X			X

vCenter privilege	Description	UCP Director roles			
		UCP system admin	UCP server admin	UCP storage admin	UCP network admin
UCP.SystemAdministration	Enables full UCP Director orchestration access	X			
UCP.Service	Used internally by the svc_ucpdcntr account				
Alarms		***X***	***X***	***X***	***X***
Alarm.Acknowledge	Suppresses all alarm actions from triggering actions	X	X	X	X
Alarm.Create	Create alarm				
Alarm.Delete	Remove alarm				
Alarm.DisableActions	Disable alarm action	X	X	X	X
Alarm.Edit	Modify alarm	X	X	X	X
Alarm.SetStatus	Set alarm status	X	X	X	X
Datastore	***Datastore***	***X***		***X***	
Datastore.AllocateSpace	Allocate space				
Datastore.Browse	Browse datastore	X		X	
Datastore.Config	Configure datastore	X		X	
Datastore.Delete	Remove datastore (requires privileges to the parent object as well)	X		X	
Datastore.DeleteFile	Remove file (deprecated)				
Datastore.FileManagement	Low level file operations (read, write, delete)				
Datastore.Move	Move datastore				
Datastore.Rename	Rename datastore				
Datastore.UpdateVirtualMachineFiles	Update virtual machine files				
Host.Config		***X***	***X***		
Host.Config.AdvancedConfig	Advanced settings				

vCenter privilege	Description	UCP Director roles			
		UCP system admin	UCP server admin	UCP storage admin	UCP network admin
Host.Config.AuthenticationStore	Authentication Store				
Host.Config.AutoStart	Virtual machine autostart configuration				
Host.Config.Connection	Connection	X	X		
Host.Config.DateTime	Change date and time settings				
Host.Config.Firmware	Firmware				
Host.Config.HyperThreading	Hyperthreading				
Host.Config.Image	Image configuration				
Host.Config.Maintenance	Maintenance	X	X		
Host.Config.Memory	Memory configuration				
Host.Config.NetService	Security profile and firewall				
Host.Config.Network	Network configuration (network, firewall, DNS, and routing)	X			X
Host.Config.Patch	Query patch				
Host.Config.PciPassthru	Change PciPassthru settings				
Host.Config.Power	Power management (high perf, balanced, low power)				
Host.Config.Resources	System resources				
Host.Config.Settings	Change settings				
Host.Config.Snmp	Change SNMP settings				
Host.Config.Storage	Storage partition configuration	X		X	
Host.Config.SystemManagement	System management				
Host.Inventory		***X***	***X***		

vCenter privilege	Description	UCP Director roles			
		UCP system admin	UCP server admin	UCP storage admin	UCP network admin
Host.Inventory.AddHostToCluster	Add host to cluster	X	X		
Host.Inventory.AddStandaloneHost	Add standalone host	X	X		
Host.Inventory.CreateCluster	Create cluster	X	X		
Host.Inventory.DeleteCluster	Remove cluster	X	X		
Host.Inventory.EditCluster	Modify cluster	X	X		
Host.Inventory.MoveCluster	Move cluster to standalone host	X	X		
Host.Inventory.MoveHost	Move host	X	X		
Host.Inventory.RemoveHostFromCluster	Remove host	X	X		
Host.Inventory.RenameCluster	Rename cluster	X	X		
Host Profile		***X***	***X***		
Profile.Clear	Clear	X	X		
Profile.Create	Create	X	X		
Profile.Delete	Delete	X	X		
Profile.Edit	Edit	X	X		
Profile.Export	Export	X	X		
Profile.View	View	X	X		
DvPort Group		***X***	***X***		
DvPortgroup.Create	Create	X			X
DvPortgroup.Delete	Delete	X			X
DvPortgroup.Modify	Modify	X			X
DvPortgroup.PolicyOp	Policy operation	X			X
DvPortgroup.ScopeOp	Scope operation	X			X
Folder		***X***	***X***	***X***	***X***
Folder.Create	Create folder	X	X	X	X
Folder.Delete	Delete folder	X	X	X	X
Folder.Move	Edit folder	X	X	X	X

vCenter privilege	Description	UCP Director roles			
		UCP system admin	UCP server admin	UCP storage admin	UCP network admin
Folder.Rename	Rename folder	X	X	X	X
vDistributedSwitch		***X***			***X***
DVSwitch.Create	Create	X			X
DVSwitch.Delete	Delete	X			X
DVSwitch.HostOp	Host operation	X			X
DVSwitch.Modify	Modify	X			X
DVSwitch.Move	Move	X			X
DVSwitch.ResourceManagement	Policy operation	X			X
DVSwitch.PolicyOp	Port configuration operation	X			X
DVSwitch.PortConfig	Port setting operation	X			X
DVSwitch.PortSetting	Network IO control operation	X			X
DVSwitch.VSPAN	VSPAN operation	X			X
Storage				***X***	
Configure	Allows changing server configuration such as the reports update interval and database connectivity information				
View	View	X		X	

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2627
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0) 1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-92UCP021-05