HITACHI
Inspire the Next

Unified Compute Platform 3.5.1

UCP DOC Administration Manual

Hitachi Data Systems

MK-92UCP054-01

Contents

Preface

This book explains the function and administration of **Hitachi Unified Compute Platform Director Operations Center (UCP DOC)**. The information contained is intended to help UCP administrators better understand how UCP DOC and Hitachi UCP Disaster Recovery works, including concepts that are needed to configure and administer UCP DOC both with and without UCP Disaster Recovery. It is not a solution guide or a replacement for the release notes.

Intended audience

This book is intended for datacenter administrators who monitor the status of multiple UCP sites and who configure and administer UCP Disaster Recovery. It assumes that they are familiar with UCP, the UCP sites they are administering, and the hardware used at a UCP site.

Product version

This guide applies to UCP version 3.5.1.

Document organization

This book contains four chapters and two appendixes.

Chapter/Appendix	Description
Chapter 1, "Introduction to UCP DOC and UCP Disaster Recovery," on page 1	Contains an overview of UCP DOC and UCP Disaster Recovery.
Chapter 2, "UCP DOC Console," on page 5	Explains how to use and configure UCP DOC Console.
Chapter 3, "UCP Disaster Recovery," on page 15	Describes how to use UCP Disaster Recovery.

(Continued)

Chapter/Appendix	Description
Chapter 4, "Jobs and events," on page 35	Explains how to review the status of jobs and events in UCP DOC.
Appendix A, "Jobs," on page 39	Lists all jobs inUCP DOC.
Appendix B, "Events," on page 43	Lists all UCP DOC events and their severity.

Related documents

The following documents contain information about UCP version 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.)

1

Introduction to UCP DOC and UCP Disaster Recovery

UCP 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.

UCP DOC overview

When a UCP site is registered with UCP DOC, UCP DOC will begin to collect monitoring information on that site. The health information for each site is then aggregated together by component type for each site that is added to UCP DOC.

By aggregating the health information for each component type at a site, UCP DOC is able to track the health of the storage system as well as all of the servers and switches at a site.

UCP DOC is hosted on the UCPDatacenter virtual machine (VM), which is hosted in the management block of one of the sites. Sites that are added to UCP DOC can be from one or more different physical locations. For more information on component health and the management block, see *UCP Administration Manual*.

In addition to UCP DOC, the UCPDatacenter VM contains the following supporting software:

- AMQP server
- SQL express

To function correctly, the UCPDatacenter VM needs to have network access to each site that is added, as well as the Microsoft Active Directory server used by UCP Director at the sites to authenticate users.

UCP DOC can be administered visually through UCP DOC Console, or programmatically through the UCP DOC API and UCP DOC CLI.

For more information on:

- UCP DOC Console, see "UCP DOC Console" on page 5.
- UCP DOC API, see *UCP DOC API Reference*.
- UCP DOC CLI, see *UCP DOC CLI Reference*.

UCP Disaster Recovery overview

UCP Disaster Recovery automates the configuration of volume replication in a resource group between two sites in a site pair. Site pairs are created within UCP Disaster Recovery by pairing two properly configured sites that are registered in UCP DOC.

When two sites have been paired, you can use the site pair to replicate volumes from one site to another. This way, when changes are made to the first site, the protected site, they are automatically copied to the second site, the recovery site.

Because UCP DOC collects health monitoring information on the volumes that you pair, UCP Disaster Recovery will then record and monitor the specific health of the volumes being replicated.

Each UCP site abstracts the individual storage system. As a result, sites do not need to use the same storage system model. Instead, UCP Disaster Recovery only requires each of the sites in a site pair to use a Hitachi enterprise-level storage system.

For more information on UCP Disaster Recovery, see Chapter 3, “UCP Disaster Recovery,” on page 15.

2

UCP DOC Console

UCP DOC Console is the stand-alone web-based graphical interface that you can use to administer UCP DOC and, when installed, UCP Disaster Recovery.

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

Accessing UCP DOC Console

To access UCP DOC Console, while using an account with sufficient privileges, navigate to the following URL:

```
https://UCPDATACENTER/ui
```

Where *UCPDATACENTER* is the IP address of the UCPDatacenter VM.

For more information on UCP DOC permissions and access, see "User and group administration" on page 8.

Navigating UCP DOC Console

UCP DOC Console is divided into three functional areas, as follows:

- Info bar — A black bar at the top of UCP DOC Console that displays the following:
  - The **Help** menu, which contains links to product books, the CLI installer, and the about page. The following product books are included in the **Help** menu:
    - *UCP DOC Administration Manual*
    - *UCP DOC API Reference*
    - *UCP DOC CLI Reference*
    - *UCP Administration Manual*

    For more information on downloading the CLI installer, see "Downloading the UCP DOC CLI" on page 8. For more information on viewing about and support information, see "Viewing about and support information" on page 8.
  - The domain and username of the user that is logged into UCP DOC Console.
  - The date and time the page was loaded.

- Navigation bar — A large bar located at the bottom of UCP DOC Console.

  The navigation bar is divided into the following sections: **Dashboard**, **Configuration**, **Disaster Recovery**, and **Jobs and Events**. These sections contain related information and links, as follows:

  – **Dashboard** — Displays the aggregate monitoring state of all components across all sites administered by UCP DOC. For more information on the monitoring state, see "Monitoring site health" on page 12.

  – **Configuration** — Contains links that enable you to add a UCP site, add a user or group, or edit the AMQP credentials.

  – **Disaster Recovery** — Contains links to create a site pair or refresh site pair inventory.

  – **Jobs and Events** —Displays the most recent jobs and events that have been run by UCP DOC.

  Click on the title of a section to display the corresponding page in the body area.

- Body — Located between the info and navigation bars, the body is used to display the contents of the page that you are viewing. UCP DOC Console has four primary pages, as follows:

  – **Dashboard** — Displays each site monitored by UCP DOC. Each site displays the aggregate monitoring state of all components in the system as well as the aggregate monitoring state of each component type. For more information on aggregate component health and the **Dashboard** page, see "Monitoring site health" on page 12.

  – **Configuration** — Used to add and remove users, groups, and sites. For more information on the **Configuration** page, see "UCP DOC configuration" on page 8.

– **Disaster Recovery** — Used to automate volume replication between two sites. For more information on the **Disaster Recovery** page, see Chapter 3, “UCP Disaster Recovery,” on page 15.

Note: UCP Disaster Recovery is optional. If it is not installed, the **Disaster Recovery** section of the navigation bar will indicate that it is not installed and you will not be able to view the **Disaster Recovery** page.

– **Jobs and Events** — Displays the status of all UCP DOC jobs. For more information on the **Jobs and Events** page, see “Jobs and events” on page 35.

Downloading the UCP DOC CLI

To access the UCP DOC CLI, you will need to download the UCP DOC CLI installer and install it from within UCP Director Console. To download the UCP DOC CLI installer, from the **Help** menu, click on the **Download CLI** link. For more information on the UCP DOC CLI, see *UCP DOC CLI Reference*.

Viewing about and support information

The **About** dialogue is used to display the version and serial number of UCP DOC, along with support information and the end user license agreement. To display the **About** dialogue, from the **Help** menu, click on the **About** button.

UCP DOC configuration

User/group administration and site access is administered on the **Sites** and **Users/Groups** tabs of the **Configuration** page. To access the **Configuration** page, from the navigation bar, click on the **Configuration** link.

User and group administration

Access to UCP DOC is role-based. To connect to UCP DOC Console, your AD account needs to:

- Have an appropriate role applied to it
- Be added to a group that has the role applied to it in UCP DOC.

UCP DOC supports the following roles:

- **Administrator** — Able to administer all portions of UCP DOC and UCP Disaster Recovery.
- **Viewer** — Enables read-only access to UCP DOC.

Viewing users

The **Users/Groups** tab of the **Configuration** page is used to display, add, edit, and remove user accounts and groups in UCP DOC.

To display the **Users/Groups** tab of the **Configuration** page, from the navigation bar:

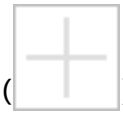
1. Click on the title of the **Configuration** section.
2. Click on the **Users/Groups** tab at the top of the page.

For each user, the following properties are displayed:

- **User/Group** — The domain and user or group ID.
- **Role** — The role that the user or group has been assigned to.

Adding users

To add a user to UCP DOC:

1. From the **Users/Groups** tab on the **Configuration** page, click on the **Add User/Group** icon ().
2. In the **User/Group** field, type the name of the user or group to add to UCP DOC. The username must be entered in the following format:

   Domain\Username

3. As appropriate, select either the **Administrator** or **Viewer** role.
4. Click on the **OK** button.

Editing users

To edit a user with access to UCP DOC:

1. From the **Users/Groups** tab on the **Configuration** page, click on the **Edit** icon ( ) next to the user that you want to edit.
2. Select either **Administrator** or **Viewer** access for the user.
3. Click on the **OK** button.

Removing users

To remove a user from UCP DOC:

1. From the **Users/Groups** tab on the **Configuration** page, click on the **Remove** icon ( ) next to the user that you want to remove.
2. Click on the **Yes** button.

Site administration

Before you can use UCP DOC to monitor a site or use UCP Disaster Recovery to configure a site for disaster recovery, you need to add that site to UCP DOC.

Viewing sites

The **Sites** tab of the **Configuration** page is used to display, add, edit, and remove sites in UCP DOC.

To display the **Sites** tab of the **Configuration** page, from the navigation bar:

1. Click on the title of the **Configuration** section.
2. Click on the **Sites** tab at the top of the page.

For each site, the following properties are displayed:

- **Serial Number** — The serial number of the site.
- **UCPManagement URL** — The URL of the UCPManagement VM at the site.

Adding sites

To add a site to UCP DOC:

1. From the **Sites** tab on the **Configuration** page, click on the **Add UCP Site** icon ().

2. On the **Add UCP Site** window:

   – In the **UCP Site Name** field, type a unique name that will be used to label the site in UCP DOC.

   – In the **UCPManagement URL** field, type the URL of the UCPManagement VM of the site.

   – In the **Username** field, type the username of a user with administrative access to the vCenter and UCPManagement VMs in the following format: *User@Domain*.

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

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

Note: Each site should only be registered in one instance of UCP DOC.

Editing sites

To edit a site in UCP DOC:

1. From the **Sites** tab on the **Configuration** page, click on the **Edit** icon () next to the site that you want to edit.

2. On the **Edit UCP** window, make the appropriate changes as explained in "Adding sites" on page 11.

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

Note: The site name of the site is shown at the top of the edit window.

Removing sites

A site can not be removed if it is part of a site pair.

When a site is removed, all jobs and monitoring information for that site will be retained. If the site is added back to UCP DOC, the saved jobs and monitoring information will be re-associated with the site.

To remove a site from UCP DOC:

1. From the **Sites** tab on the **Configuration** page click on the **Remove** icon ( ) next to the site that you want to remove.
2. Click on the **Yes** button.

Edit AMQP credentials

Advanced Message Queuing Protocol (AMQP) is a service that is run on the UCPManagement VM of each site. UCP DOC subscribes to the AMQP messaging service at each site that is added to UCP DOC to receive disaster recovery-events.

For security reasons, the credentials used to connect to AMQP can be changed, but all sites must use the same credentials.

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

1. In the **Configuration** section of the navigation bar, click on the **AMQP Credentials** button.
2. On the **AMQP Credentials** dialog:
   - In the **Username/Group** field, type the username or group 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.

Monitoring site health

The **Dashboard** page is used to display the status of sites that have been added to UCP DOC.

To display the **Dashboard** page, from the navigation bar, click on the title of the **Dashboard** section.

For each site, in addition to the **Serial Number** and **UCPManagement URL** fields, the following site properties are shown:

- **Monitoring State** — An aggregate of all component monitoring states that is equal to the most concerning monitoring state of any individual component at the site. From most concerning to least concerning, values can be: **Error**, **Warning**, **Unknown**, and **Healthy**. If a site is unreachable, the **Monitoring State** of the site will not be available and will appear as unreachable.

  For example, if all components are **Healthy**, then the monitoring state will be **Healthy**, but if even one component is in a **Warning** or **Error** state, then the entire site will appear as **Warning** or **Error**.

- Component health — Below the overall site properties, the aggregate monitoring state of each component type at the site is shown in a table. For each component type, the table shows the total number in each monitoring state, as follows:

  – Error ( ) — UCP Director is not able to communicate with the indicators or the indicators are not functioning properly.

  – Warning ( ) — UCP Director is able to communicate with the indicators 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.

  – Unknown ( ) — UCP Director is not able to determine the status of the indicator.

  – OK ( ) — UCP Director is able to communicate with the indicators and the indicators are functioning properly.

For more information on administering a site, including UCP monitoring states and component types, see *UCP Administration Manual*.

3

UCP Disaster Recovery

When using vCenter, UCP Disaster Recovery automates the complex task of manually using CCI commands to configure volume replication between two sites in a site pair. This enables volumes from the storage system at one site, the primary site, to be automatically replicated to the storage system at a second site, the recovery site.

This chapter explains how UCP Disaster Recovery functions, and how to use UCP DOC Console to administer UCP Disaster Recovery.

UCP Disaster Recovery volume replication

Because the storage system is abstracted by UCP Director, sites do not need to use the same storage system model. Instead, UCP Disaster Recovery only requires that both sites use one of the following enterprise-class storage systems:

- HUS-VM
- VSP
- VSP G1000

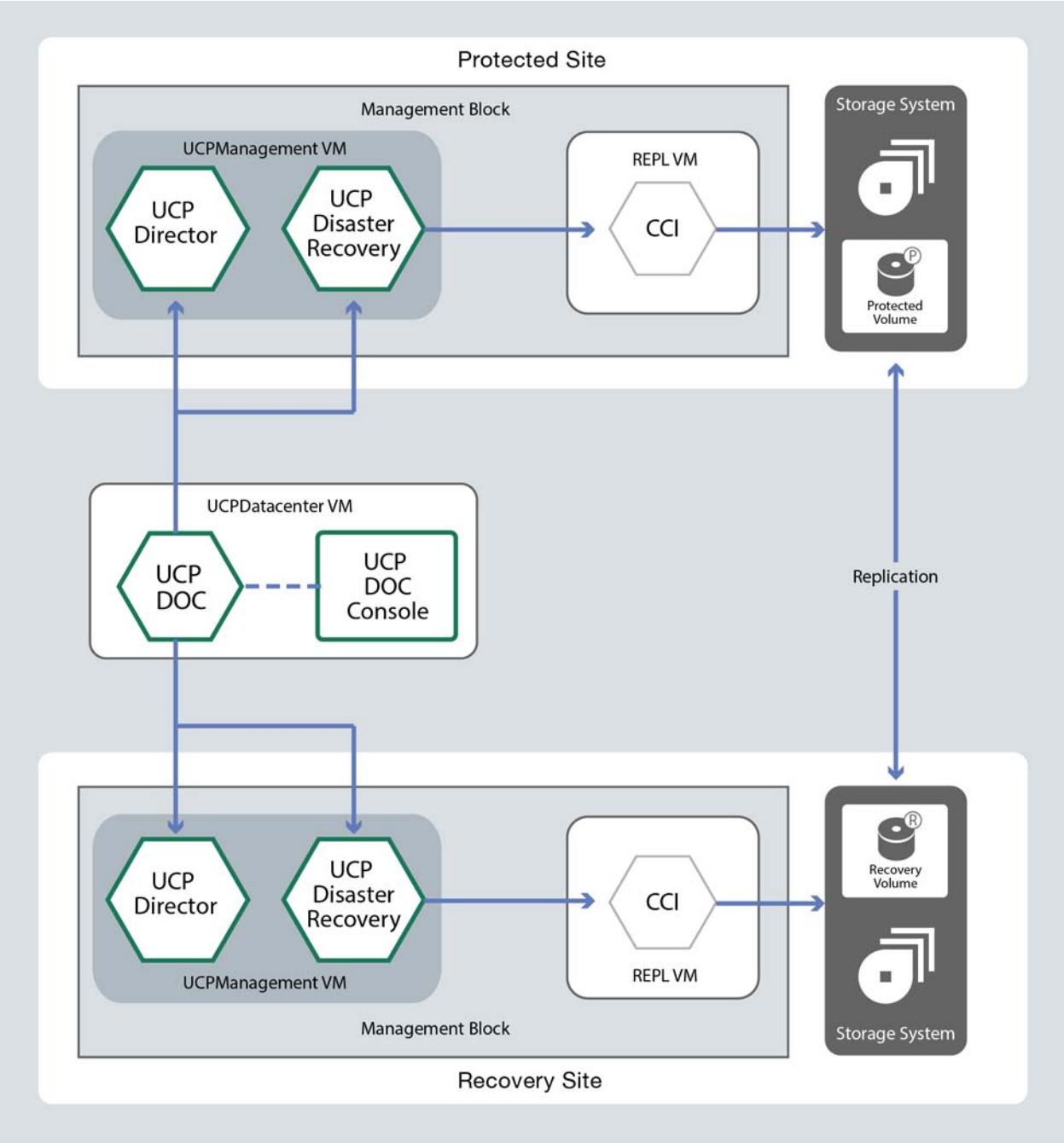
A site pair is a logical construct that is used to pair two sites together. Each site can only be a member of one site pair, and a site pair is only able to contain two sites. After sites have been paired together, replication groups need to be created to contain the volumes that will be replicated.

Replication groups are logical collections of volumes that are replicated from one site to another. It is at the replication group level that the primary and recovery sites are defined. As a result, two sites are able to perform reciprocal backups for each other through the configuration of multiple resource groups.

Because replication can be bi-directional if more than one replication group is added, volumes are identified by their role in the replication group.

- Protected volume — The volume at the protected site. This is the primary data source.
- Recovery volume — A volume at the recovery site that contains the replicated data.
- Test volume — A test volume can be added to recovery groups that contain only ESXi hosts. Test volumes are used to test recovery scripts and processes without affecting the recovery volume. For more information on test volumes, see “Test volumes” on page 23.

When volume replication has been set up, changes to the protected volume are replicated to the recovery volume. The following diagram shows the components and connections involved to replicate volumes between two sites.



After volume replication has been setup, UCP Disaster Recovery protects the volumes that are being replicated. UCP Director does this by blocking any tasks, such as detaching a volume from a host, that might compromise volume replication. This is done to prevent accidentally interrupting volume replication.

Because UCP DOC collects health monitoring information on the volumes that you pair, UCP Disaster Recovery will then record and monitor the specific health of the volumes being replicated.

Replication technology and outage tolerance

UCP Disaster Recovery supports both synchronous and asynchronous replication technology, depending on the needs of the site.

- Synchronous — Hitachi TrueCopy Synchronous Remote Replication

  Synchronous replication is designed for fast, robust, real-time replication within most metropolitan distances. When using synchronous replication, data is written to both sites at the same time and the data that is written at the primary site is not confirmed as successful until the write at the backup site has been confirmed as well.

- Asynchronous — Hitachi Universal Replicator

  Asynchronous replication is designed for scenarios where synchronous replication is not possible, such as when the distance is excessive or when connection latency is a concern. When using asynchronous replication, instead of synchronously writing data to both the primary and recovery volumes, changes to replicated data are tracked in journals until writes can be confirmed.

  UCP uses a single journal stored in a single HDP pool as the journal source. The journal at a site is then used to contain all journal volumes at that site. When a journal volume is used, changes to the protected volume are collected in the journal volume at the protected site. The data is then transfered to the journal volume at the recovery site, where it can be written to the recovery volume.

  For the G1000 storage system, the size of the journal volumes can be variable. For other enterprise Hitachi storage systems, the size of the journal volumes is determined by the maximum outage tolerance between the two sites. The greater the outage tolerance, the larger the journal volumes need to be to accommodate data changes.

The outage tolerance is the number of minutes worth of data changes during an outage that are OK to be held in journal volumes before they are replicated. Because of this, larger journal volumes help prevent the loss of replicated data if two sites are temporarily unable to communicate or if latency causes a backlog of changes.

Synchronization status

UCP Disaster Recovery tracks the status of the volumes that it synchronizes and reports them as follows:

- Paired — Indicates that active replication is taking place between the protected volume and its replicated volume or between the replicated volume and its test volume.

- Simplex — When using copy on write volumes, indicates a failure in replication. This occurs by default before data starts being replicated after volumes have been paired, but can also happen after a failover. When in this state, the test volume will require a pair resynchronization.

  For more information on copy on write volumes, see "Using SRM with a test volume" on page 23.

- Suspended — Indicates that replication between the protected volume and recovery volume or between the recovery volume and a test volume is paused.

Using UCP Disaster Recovery

After configuring volume replication:

- For replication groups that contain non-ESXi hosts, you can configure a separate automated failover solution that makes use of the replicated volumes.

- For replication groups that contain only ESXi hosts, UCP Disaster Recovery can automate the creation of test volumes. You can then use test volumes with VMware Site Recovery Manager (SRM) for the purpose of testing recovery plans.

To enable the creation of test volumes, the REPL VM is added to the management block at each site. The REPL VM hosts the following services:

- VMware Site Recovery Manager (SRM).

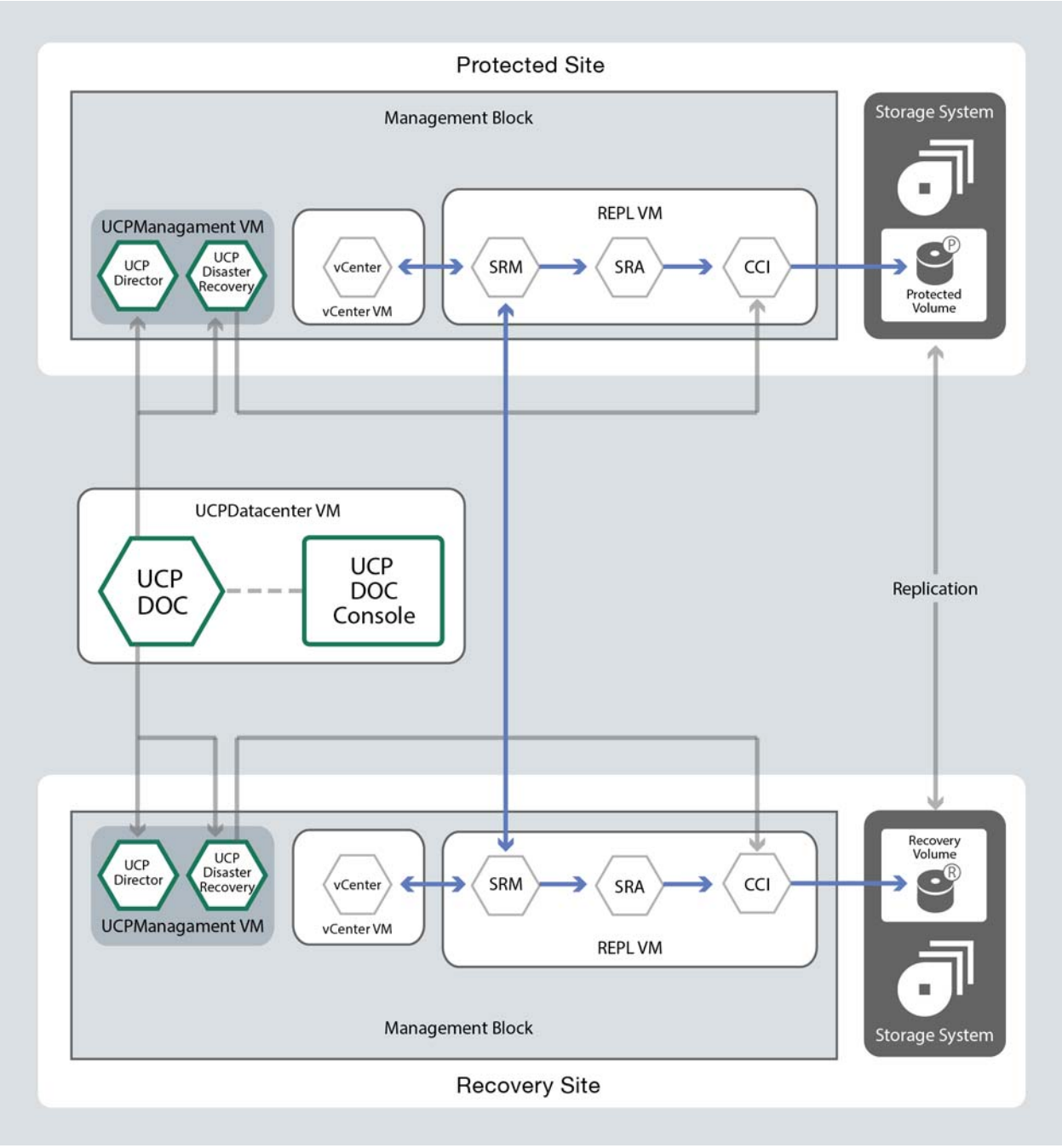
- Hitachi Storage Replication Adapter (SRA) — Integrated with SRM to issue CCI commands to enable the testing of recovery plans.

- Hitachi Command Control Interface (CCI).

An SRM test plan can be configured to use a test volume. If the replication group does not use test volumes, the SRM test plan can be configured to use the replicated volumes for. Executing a test plan enables you to test the automated failover of the primary site. Automated failover enables a backup site to function as a primary site if the primary site becomes unreachable.

When using UCP Disaster Recovery with SRM, SRA is integrated with SRM to bring volume information into SRM and enables it to communicate with the storage system. This facilitates SRM in issuing CCI commands to test recovery plans and enables SRM to execute a failover in the case of a disaster.

The following diagram shows how the components involved in volume recovery are integrated with the components that are involved in volume replication.



Because UCP Disaster Recovery augments SRM instead of replacing it, a firm understanding of SRM is important to properly configure both. Configuration choices in SRM, UCP Disaster Recovery, and UCP Director can affect the settings that you need to specify in the others. For example:

- Creating SRM protection groups that contain the same hosts and volumes as the resource groups that you create in UCP Disaster Recovery.

- According to VMware recommendations, VMs that support a single workload, such as a web server and a database server, should have their volumes protected together. VMware recommends placing their volumes in the same SRM protection group, which means that they should also be in the same replication group.

- Because SRM is able to perform a failover recovery of ESXi hosts, but not hosts running other operating systems, volumes attached to ESXi hosts should not be added to the same replication group as non-ESXi hosts.

- Initiating a failover recovery of non-ESXi servers requires either a manual procedure or a third-party solution.

- All volume pairs in a replication group are synchronized together. Individual pairs are not able to be synchronized apart from the replication group.

- An SRM protection group can be included in more than one protection plan. For example, one protection plan may power up a minimum number of VMs, while another protection plan may power up all VMs. It is important to have enough hosts at the recovery site to support the plan with the most VMs in it to avoid a resource-intensive recovery plan from being executed in SRM without enough hosts at the recovery site to support it.

- After a failover recovery, the recovery site will become the primary site. The original primary site, however, will not automatically convert to being the new recovery site. Manual intervention may be necessary after a failover recovery is performed.

- There should be a corresponding SRM protection group for each UCP DOC replication group.

Test volumes

If a replication group contains volumes that are only attached to ESXi hosts, then a test volume can be created for the replication group. When creating a test volume, you can create either a full test volume or a copy on write test volume.

Synchronization happens at the replication group level. As a result, all test volumes in a replication group must be of the same type. Because of this, when adding new volume pairs to an established replication group, it is important to be aware of what type of test volume the replication group is using because the new volume pair will use the same type.

During replication, both test and recovery volumes are read-only. When the relationship between a test volume and the recovery volume is suspended, the test volume will become read/write until the test is over. Afterward, when the pairing relationship is restored and the test volume is synchronized, it will become read only again. This helps ensure that the test volume is kept in sync with the recovery and protected volumes.

Using SRM without a test volume

When storage system capacity needs to be conserved, and where it is acceptable to perform testing on the actual replicated volume, it is possible to configure a replicated volume to not have a test volume when configuring a replication group.

When a replication group is configured without a test volume, if a test is initiated, then the relationship between the primary and recovery volume is suspended. SRM will then test the recovery plan against the recovery volume. After the test, you will need to manually resynchronize the replication group in UCP Disaster Recovery to re-establish the relationship between the primary and recovery volumes and synchronize any changes that were made after replication was suspended.

Using SRM with a test volume

Sometimes, it is not acceptable to suspend replication to a recovery volume when you want to test a recovery plan in SRM. When this is the case, you can use a test volume.

Because the data in the test volume is a representation of the data in the recovery volume, it can be used for tests instead of the recovery volume. This enables tests to be performed at the same time that replication is being performed. To do this, UCP Disaster Recovery suspends the relationship between the recovery volume and and the test volume to test a recovery plan.

Test volumes are defined when creating and configuring replication groups, and are attached to recovery hosts or clusters along with the recovery volumes as they are defined. Because of this, recovery hosts and clusters will see twice the volumes of a protected host.

There are two types of test volumes that you can use, a full test volume and a copy on write test volume.

Full test volume

A full test volume, also known as a ShadowImage, is an exact replica of the recovery volume and ensures full redundancy at all times. Because it is a full replica, however, the recovery site will need twice the total provisioned space of the primary site, not just the written blocks. As a result, there are three copies of all volumes, providing greater redundancy.

When performing a test against a test volume, SRM will first suspend replication between the recovery volume and the test volume. Because SRM is testing the recovery plan against the test volume, a successful test implies that both the recovery volume and the test volume would be able to function in the case of a failover. Also, after the test is finished, the recovery and test volume will need to be resynchronized.

Copy on write test volume

Where space should be conserved, but a test volume is required, a copy on write test volume can be used. Copy on write test volumes are Hitachi virtual volumes, or v-vols, that are created in a Hitachi Thin Image (HTI) pool.

Copy on write test volumes offer the ability to test SRM without suspending replication between primary volume and recovery volume, while also using a percentage of the size of a full test volume. Instead of being an exact replica of a recovery volume, a copy on write test volume is a virtual representation of the recovery volume that contains pointers to the actual data in the recovery volume. As a result, the host that is connected to both the recovery and test volume sees both volumes as complete copies of the data, even though the actual data is only present in the recovery volume.

Because of this, while you can use a copy on write test volume to test an SRM recovery plan, it is not able to provide the heightened level of data protection that a full test volume provides if something happens to the recovery volume.

UCP Disaster Recovery requires 20% of your HTI pool capacity to be empty when creating new copy on write test volumes to accommodate their variable capacity. This preserves a buffer of space to accommodate the generation of copy on write test volumes for existing volume pairs.

When a copy on write test volume is first created, it is a clean map of all blocks in the volume that it represents and is shown in simplex state.

Changes that are made to the protected volume will be copied to both the recovery volume and the HTI pool that the copy on write test volume is located in, and pointers on the copy on write test volume are updated accordingly. The copy on write test volume will be in paired state when this is taking place.

When an SRM protection plan is tested, it will treat the copy on write test volume as a normal read\write volume. When the relationship between the recovery volume and test volume is suspended, changes to the protected volume will continue to be written to the recovery volume and HTI pool, but the pointers in the copy on write volume are not updated.

When finished testing the SRM recovery plan, you will need to synchronize the replication group in UCP Disaster Recovery to re-establish the relationship between the primary, recovery, and test volumes and synchronize any changes that were made after replication was suspended.

Best practices for setting up replication groups

When setting up your replication groups, we recommend the following best practices:

- Include all data stores and volumes associated with a single workload into the same replication group

- Optimize your disaster recover configuration to stay below 4000 replicated volumes

  Although the UCP DOC software supports all maximum limits and constraints that are driven by the underlying hardware, all software operations such as, refresh, create, delete, etc., are optimized to support 4000 replicated volumes.

UCP Disaster Recovery administration

UCP Disaster Recovery is administered on the **Disaster Recovery** page in UCP DOC Console.

The **Disaster Recovery** page lists each site pair that has been added to UCP Disaster Recovery at the top of a page. When a site pair is selected, the **Disaster Recovery** page will list each replication group that is part of the site pair as well as the volumes that have been added to that replication group.

To display the **Disaster Recovery** page, log into UCP DOC Console and click on the **Disaster Recovery** link in the navigation bar at the bottom of the page.

Site pair administration

In addition to displaying site pairs, the **Disaster Recovery** page is used to add, edit, and remove site pairs in UCP Disaster Recovery.

Creating a site pair

When creating a site pair, UCP Disaster Recovery verifies the:

- Ethernet connectivity between each site.
- Replication path between the storage systems.

To create a site pair:

1. From the **Disaster Recovery** page, click on the **Create Site Pair** icon ().
2. On the **Create Site Pair** screen:
   - In the **Name** field, type a name for the site pair.
   - In the **First Site** field, select the first site of the site pair.
   - In the **Second Site** field, select the second site of the site pair.
   - From the **Replication Technology** section, select the type of replication to perform, either **Synchronous (TC)** or **Asynchronous (HUR)**.
   - If **Asynchronous (HUR)** is selected, in the **Maximum Outage Tolerance** field, enter the maximum outage tolerance.
3. Click on the **OK** button.

Removing a site pair

When you remove a site pair from UCP Disaster Recovery:

- All associated replication groups are removed.

- Replication between the two sites for all volumes is disabled.
- Individual volumes at each site are not removed.

To remove a site pair:

1. From the **Disaster Recovery** page, click on the **Remove Site Pair** icon ().
2. Click on the **Yes** button.

Refreshing site pair inventory

To refresh site pair inventory:

1. In the **Disaster Recovery** section of the navigation bar, click on the **Refresh Site Pair Inventory** button.
2. When prompted, click on the **Yes** button.

Replication group administration

Replication groups contain the volumes that are replicated between sites in a site pair. They are displayed within site pairs on the **Disaster Recovery** page. As a result, the corresponding site pair needs to exist before the replication group can be created.

Befor you set up replication groups, we recommend that you first review "Best practices for setting up replication groups" on page 25.

Setting up replication groups

When setting up a replication group, UCP Disaster Recovery:

1. Creates and adds replicated volume pairs to the replication group.
2. Creates journals at the protected and recovery sites if using asynchronous replication.
3. Sets up replication for the replicated volume pair.

Replication groups are not created independently. Instead, when setting up volume replication, you create a replication group by adding volume replication to a new replication group. For more information on setting up

volume replication, follow the steps in "Setting up volume replication" on page 29 and, in the **Configure Replication Group** section, select the **Create New** option.

Pairing and resynchronizing replication groups

When pairing and resynchronizing a replication group, UCP Disaster Recovery attempts to pair all of the replicated volume pairs in the replication group. This includes:

1. Initiating replication between the protected and recovery volumes.
2. Initiating replication between the recovery and test volumes.
3. Creating the protected and recovery journals if using asynchronous replication in a simplex state.

This can be used to recover a volume in simplex or suspended status after the corresponding failure has been corrected.

To pair and resynchronize a replication group:

1. From the **Disaster Recovery** page, click on the site pair that contains the replication group you want to pair and resynchronize.
2. Click on the **Pair and Resynchronize Replication Group** icon () beside the replication group that you want to pair and resynchronize.
3. Select the protected site from the **Select Protected Site** field if needed.
4. Click on the **Yes** button.

Removing replication groups

When removing a replication group, UCP Disaster Recovery:

1. Stops replication between the recovery and test volumes.
2. Stops replication between the protected and recovery volumes.

3. Removes the journals at the recovery and protected sites if using. asynchronous replication. While the journal will be removed, the journal volume will not be automatically deleted.

Note: Removing a replication group will not detach and delete the test and recovery volumes. To detach and delete the volumes, use UCP Director Console to access the appropriate site.

To remove a replication group:

1. From the **Disaster Recovery** page, click on the site pair that you want to remove the replication group from.
2. Click on the **Remove Replication Group** icon ( ).
3. Click on the **OK** button.

When you remove the last replicated volume from a replication group, UCP Disaster Recovery will automatically remove the corresponding replication group. For more information on removing a volume, see "Removing volume replication" on page 32.

Administering volume replication

Replicated volumes are displayed and administered within replication groups on the **Disaster Recovery** page.

Setting up volume replication

When setting up volume replication, UCP Disaster Recovery:

1. Verifies the replication path between the storage systems.
2. Creates the recovery volume or volumes and attaches them to the recovery host or cluster.
3. Creates the test volume or volumes on the storage system, if applicable.
4. For asynchronous replication:
   - Creates new journals at the protected and recovery sites if creating a new replication group.
   - Expands existing journals, if necessary, for an existing replication group.

5. Initiates replication between the protected and recovery volumes.

6. Initiates replication between the recovery and test volumes.

7. Pairs and resynchronizes all simplex or suspended volumes in the replication group that the volume is added to if adding volume replication to an existing replication group.

To create a new replication group or add volume replication to an existing replication group, follow these steps:

1. On the **Disaster Recovery** page, click on the **Configure as Protected** icon () next to the site that you want to setup replication in.

2. In the **Configure Replication Group** section, select the replication group that you want to add the replicated volume too.

   – To use an existing replication group, select the **Add to Existing** option, and then select the group from the **Select from Existing** field.

   – To create a new replication group, select the **Create New** option, and then type the name of the replication group in the **Enter a Name** field.

3. In the **Protected Resource** section:

   1. In the **Select Source** field, select the host or cluster that is connected to the volume you want to protect.

   2. In the **Select Volume** field, select the volumes in the protected site that you want to protect.

4. In the **Recovery Resource** section:

   – In the **Select Target** field, select the host or cluster that will be connected to the recovery volume.

   – Select the pool that the volume will be created in:

      • To have UCP Disaster Recovery automatically select the pool, click on the **Default** option.

      • To manually select the pool, click on the **Existing** option and select the pool in the **Select from Existing** field.

5. Click on the **Next** button.

6. In the **Test Volume Configuration** section:

    1. Select the test volume type to use, as follows: **Full Copy**, **Copy on Write**, or **None**.

    2. If creating a **Full Copy** or **Copy on Write** test volume, select the pool that the test volume will be created in:

        - To have UCP Disaster Recovery automatically select the pool, click on the **Default** option.

        - To manually select the pool, click on the **Existing** option and select the pool in the **Select from Existing** field.

7. Click on the **Next** button.

8. In the **Summary** section, review the protection configuration, and then click on the **Finish** button.

Expanding volumes

To expand a protected volume, UCP Disaster Recovery will:

1. Verify the replication path between the storage systems.

2. Suspend replication between all protected, recovery, and test volumes in the replication group.

3. Expand the selected protected, recovery, and test volumes.

4. Resume replication between all protected and recovery volumes in the replication group.

Notes:

- When a volume is being expanded, it will not appear in the replication group until the volume is expanded and replication is reestablished or recreated. If this is the only volume in the replication group, the replication group will not appear until the volume is expanded and replication is recreated.

- During volume expansion, no change is made to the journals used for asynchronous replication in either storage system.

To expand a volume:

1. From the **Disaster Recovery** page, click on the replication group to expand the volume in.

2. In the volumes table, click on the **Expand Replicated Volume** icon ( ) next to the volume to expand.

3. Enter the new size of the volume in the **New Volume Size** field.

4. Click on the **OK** button.

Removing volume replication

When removing a volume, UCP Disaster Recovery:

1. Stops replication between the recovery volume and the test volume

2. Stops replication between the protected volume and the recovery volume.

The individual protected, recovery, and test volumes are not detached and deleted. When removing a protected volume from a replication group that contains only one protected volume, UCP Disaster Recovery will also remove the replication group.

To remove replication from a volume:

1. From the **Disaster Recovery** page, click on the replication group to remove volume replication from.

2. In the volumes table, click on the **Remove Replicated Volume** icon ( ) next to the volume to remove.

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

Administering test volumes

All test volumes within a replication group must be of the same type. As a result, test volumes are administered at the replication group level.

Creating test volumes

To add test volumes to a replication group that does not have any test volumes:

1. From the **Disaster Recovery** page, click on the site pair that contains the sites you want to create test volumes in.
2. Click on the site that contains the replication group you want to create test volumes in.
3. Next to the replication group that you want to create test volumes in, click on the **Create Test Volume** icon ( ).
4. In the **Test Volume Pool** section:
    1. Select the test volume type to use, as follows: **Full Copy** or **Copy on Write**.
    2. Select the pool that the test volume will be created in:
        - To have UCP Disaster Recovery automatically select the pool, click on the **Default** option.
        - To manually select the pool, click on the **Existing** option and select the pool in the **Pool** field.
5. Click on the **Next** button.
6. In the **Summary** section, review the protection configuration, and then click on the **Finish** button.

Removing test volumes

To remove test volumes from all protected volumes in a replication group:

1. From the **Disaster Recovery** page, click on the site pair that contains the sites you want to remove test volumes from.
2. Click on the site that contains the replication group you want to remove test volumes from.
3. Next to the replication group that you want to remove test volumes from, click on the remove icon ( ).
4. Click on the **Finish** button.

4

Jobs and events

UCP DOC tracks all actions as jobs. This includes both actions that take place within UCP DOC as well as actions that UCP DOC triggers at a remote site. It also tracks all events that are triggered by jobs or sites that affect UCP DOC or UCP Disaster Recovery.

This chapter describes the jobs and events systems and describes how jobs and events are displayed in UCP DOC Console.

Jobs

Actions performed within UCP DOC are tracked as jobs. Jobs are used to track both actions that take are triggered by UCP DOC, like adding or removing users, as well as actions that take place at remote sites as part of UCP Disaster Recovery functionality, such as resynchronizing storage systems. UCP DOC retains all jobs indefinitely.

The **Jobs** tab of the **Jobs and Events** page is used to display all jobs that are tracked by UCP DOC.

To display the **Jobs** tab of the **Jobs and Events** page, from the navigation bar:

1. Click on the title of the **Jobs and Events** section.
2. Click on the **Jobs** tab at the top of the page.

The **Jobs** tab contains two tables, as follows:

- The top table lists all of the jobs that are tracked by UCP DOC.
- The bottom table is the **Related Events** table. It is used to display all events that are related to a selected job in the top table. If there are no related events, then the **Related Events** table will be blank. For more information on events, see “Events” on page 37.

For each job tracked by UCP DOC, the following properties are displayed:

- status — The status of the job. Job status is indicated as follows:
  - **Success** () — The job completed successfully.
  - **Error** () — The job failed.
  - **Running** () — The job is currently running.
- **Job ID** — The UCP DOC ID of the job.
- **Description** — A plain-text description of the job.
- **User** — The AD domain and user ID of the user who initiated the job.

- **Progress** — The progress of the job is listed in this column, either **Failed**, **Completed**, or a percentage of the current progress.
- **Start Date Time** — The date and time the job started.
- **End Date Time** — The date and time the job finished.
- **Target Type** — The resource type the job was executed against.
- **Target ID** — The ID of the resource the job was executed against.
- **Target Global ID** — The fully qualified ID of the target. This includes the site that the target is associated with.

For a list of all jobs that can be generated by UCP DOC, see Appendix A, “Jobs,” on page 39.

Events

Each job that is run can trigger one or more events, which are then tracked within UCP DOC. UCP DOC retains all events indefinitely.

The **Events** tab of the **Jobs and Events** page is used to display all events that have been triggered by a job. Events related to a specific job are displayed on the **Related Events** table on the Jobs tab when a job is selected.

To display the **Events** tab of the **Jobs and Events** page, from the navigation bar:

1. Click on the title of the **Jobs and Events** section.
2. Click on the **Jobs** tab at the top of the page.

For each event tracked by UCP DOC, the following properties are displayed:

- severity — The severity of the event. Event severity is indicated as follows:
  - **Informational** () — 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 target is not functioning correctly. Action likely needs to be taken to correct the issue.

- **Event ID** — The UCP DOC ID of the event.

- **Description** — A plain-text description of the event. Events that are triggered by a job on a remote site are prefaced with:

  ```
  Remote UCP job name:
  ```

- **User** — The AD domain and user ID of the user who initiated the triggering job.

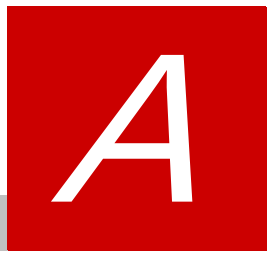
- **Date Time** — The date and time the event was triggered.

- **Target Type** — The resource type the triggering job was executed against.

- **Target ID** — The ID of the resource the triggering job was executed against.

- **Target Global ID** — The fully qualified ID of the target the triggering job was executed against. This includes the site that the target is associated with.

For a list of all events that can be generated by UCP DOC, see Appendix B, “Events,” on page 43.



Jobs

The following is a list of all jobs that are tracked by UCP DOC.

- Add replicated volume pair to replication group
- Add user to UCP Director Operations Center
- Create replication group for site pair
- Create site pair for UCP Director Operations Center
- Create test volume(s) for replication group
- Delete user from UCP Director Operations Center
- Deploying CentOS on all blades
- Deploy management virtual machine
- Expand replicated volume pair
- Register UCP Instance with UCP Director Operations Center
- Unregister UCP Instance from UCP Director Operations Center
- Update UCP Instance registered with UCP Director Operations Center
- Onboard UCP appliance
- Pair and resync a replication group
- Refresh site pair inventory
- Remove replicated volume pair from replication group

- Remove the replication group
- Remove site pair for UCP Director Operations Center
- Remove the test volume pair
- Update Active Directory configuration
- Update blade running configuration
- Update chassis available configuration
- Update chassis running configuration
- Update converged switch running configuration
- Update configuration of UCP Director Operations Center
- Update HUS storage available configuration
- Update HUS 130 storage running configuration
- Update HUSVM storage available configuration
- Update HUS VM storage running configuration
- Update management server network running configuration
- Update management server running configuration
- Update service VM network running configuration
- Update syslog available configuration
- Update user in UCP Director Operations Center
- Update management server switch port group running configuration
- Validate blade
- Validate chassis
- Validate HUS storage
- Validate HUS VM storage

- Validate management server
- Validate management server network
- Validate network Ethernet switch

B

Events

The following table lists all events that are tracked by UCP DOC.

Event	Severity
Unable to connect to the service on {url}. Make sure the service URL is correct, firewall and network settings on this computer and on the server computer are configured properly, and the appropriate services have been started on the server.	Error
Site pair: {sitePairId} for site pair name: {displayName} was created and added to inventory.	Info
Cannot access or read from database.	Error
Destination host unreachable: {host}.	Error
URL: {url} format is invalid.	Error
Unable to connect to the inventory service at {url}.	Error
Site pair: {sitePairId} for site pair: {displayName} was removed from inventory.	Info
Replication group: {replicationGroupId} was not found for site pair: {sitePairId}.	Error
Failed to reach UCP site: {ucpSiteId}.	Error
Site pairs site: {siteIds} already exists in inventory.	Error
Site pair: {sitePairId} was not found.	Error
Failed to connect to UCP instance with IP Address: {ipAddress}.	Error
UCP instance at URL {url} with serial number {serialNumber} is already registered and cannot be registered again.	Error
Cannot unregister UCP instance with IP Address: {ipAddress} as it is part of a DR site pair: {displayName}.	Error
Successfully registered UCP instance with URL: {url}.	Info
Failed to register UCP instance with URL: {url}.	Error
Successfully unregistered UCP instance with URL: {url}.	Info
Failed to unregister UCP instance with URL: {url}.	Error
Failed to update UCP instance with ID: {id}.	Error

Event	Severity
Ucp instace at URL {url} has serial number {newSerialNumber}. This is different that the registered serial number {oldSerialNumber}. This update is not allowed.	Error
Successfully updated UCP instance {id} with URL: {url}.	Info
UCP user: {username} is not a UCP administrator for UCP instance at: {url}.	Error
UCP version {instanceVersion} for UCP instance at {url} is not supported. UCP Director Operations Center supports UCP version {minimumVersion} onwards.	Error
User {user} is not authorized to access orchestrator service at {url}.	Error
Unexpected failure occurred while connecting to server at {url}. Status code: {statusCode}. Please contact your help desk or system administrator.	Error
UCP instance at URL {url} is associate with a site pair, so it cannot be unregistered.	Error
Failed to pair and resync replication group: {replicationGroupId}.	Error
Pair and resync of replication group: {replicationGroupId} was successful.	Info
Primary site: {PrimarySiteId} was not found.	Error
No path exists between sites: {siteIds}.	Error
Successfully added user '{userName}'.	Info
Failed to add user with name '{userName}'.	Error
User with name '{userName}' already exists.	Error
Failed to update user with name '{userName}'.	Error
Failed to delete user with name '{userName}'.	Error
Cannot delete all administrators.	Error
Successfully updated user with name '{userName}'. Assigned to roles: '{roleList}'.	Info
Successfully deleted user with name '{userName}'.	Info
Refresh of site pair inventory was successful.	Info
Test volumes pairs: {volumePairIds} do not belong to the same site and storage system.	Error
The remote job: {jobId} for UCP at site: {siteId} has failed with the following error message: {eventMessage}.	Error
Remote resource not found. url: {url}, response: {responseBody}.	Error
Replicated volume: {volumeId} was successfully added to replication group: {replicationGroupName}.	Info
Failed to reach UCP Site: {ucpSiteId} in site pair: {sitePairId}.	Error
Remote UCP job name: '{jobName}' with id: {jobId} completed at site: {siteId}.	Info
Remote UCP job name: '{jobName}' with id: {jobId} started at site: {siteId}.	Info
Created replication group: {replicationGroupId}.	Info

Event	Severity
Replicated volume pair: {replicatedVolumePairId} was not found.	Error
Replicated volume pair: {replicationVolumePairId} was successfully removed from replication group: {replicationGroupName}.	Info
Expand size: {size} successful for replicated volume pair id: {replicatedVolumePairId}.	Info
Pair state: {state} invalid for expanding replicated volume pair id: {replicatedVolumePairId}.	Error
Expand size: {size} is invalid for replicated volume pair id: {replicatedVolumePairId}.	Error
Remove replication group: {replicationGroupId} is successful.	Info
Failed to connect Monitor State Queue at host {hostName}.	Error
Successfully created journal: {journalId} for replication group: {replicationGroupId}.	Info
Successfully added standard volume pairs for primary volumes: {primaryVolumeIds} into replication group: {replicationGroupId}.	Info
Successfully created test replication group for: {testCopyGroupId} for replication group: {replicationGroupId}.	Info
Successfully added test volume pairs for secondary volumes: {secondaryVolumeIds} into replication group: {replicationGroupId}.	Info
Successfully removed journals from replication group: {replicationGroupId}.	Info
Successfully expanded journals for replication group: {replicationGroupId}.	Info
Successfully refreshed inventory for site pair: {sitePairId}.	Info
Successfully removed standard volume pair {standardvolumePairId} from replication group: {replicationGroupId}.	Info
Successfully removed test volume pair {testVolumePairId} from replication group: {replicationGroupId}.	Info
Successfully updated UCP Datacenter configuration.	Info
Failed to send/receive test message to AMQP.	Error
Failed to update UCP Datacenter configuration.	Error
The remote UCP at site: {siteId} has encountered an error: {eventMessage}	Error
An unexpected error occured while trying to communicate with the remote UCP at site: {siteId}.	Error
The UCP Site: {ucpSiteId} is in use in site pair: {sitePairId}.	Error
Site pair name: {sitePairName} is currently in use at site pair: {sitePairId}. Select a unique site pair name and try again.	Error
Could not find user/group '{userName}' in the directory.	Error
Could not resolve remote Cci server hostname: {cciServername} from site: {siteId}.	Error
The horcm instance: {horcmId} could not be found on site: {siteId}.	Error

Event	Severity
Unable to allocate journal volumes on site: {ucpInstanceId}.	Error
Successfully removed primary configuration from replication group: {replicationGroupName} at sites: {siteIds}.	Info
Successfully removed test configuration from replication group: {replicationGroupName} at site: {siteId}.	Info
Left journal not found for replication group: {replicationGroupId} on site pair: {sitePairId}. Please make sure that free journal volumes exist for your site.	Error
Right journal not found for replication group: {replicationGroupId} on site pair: {sitePairId}. Please make sure that free journal volumes exist for your site.	Error
Remote UCP job name: '{jobName}' with id: {jobId} failed at site: {siteId}.	Warning
The requested primary site id {requestedPrimarySiteId} does not match the current primary site id {currentPrimarySiteId}.	Error
The display name '{displayName}' provided for the UCP instance: {ucpId} is already used by another registered UCP instance. This operation is not allowed.	Error
The service URL '{serviceUrl}' provided for the UCP instance: {ucpId} is already used by another registered UCP Instance. This operation is not allowed.	Error
The physical replication links from site: {sourceSiteId} to site: {targetSiteId} are in an error state. Verify that the physical replication links between the storage arrays at both sites are in a healthy state and try again.	Error
The replication link id: {pathId} on storage port: {portName} in path group: {pathGroupId} at site: {siteId} is in an error state. For optimal replication performance, verify that the physical replication links between the storage arrays at sites: {siteIds} are in a healthy state.	Warning
Replication group: {replicationGroupId} contains replicated volume pairs that are replicated in oposite directions. This is not supported. All replicated volume pairs in the same replication group must be replicated in the same direction.	Error
At least one of the test replicated volume pairs in the replication group: {replicationGroupId} at site: {siteId} from site pair: {sitePairId} is in a 'PAIR' state. Verify that all test replicated volume pairs in the replication group is in a 'SUSPEND' or 'SIMPLEX' state and try again.	Error
Unable to allocate journal volumes on site: {ucpInstanceId}. Reason: {message}	Error
Cannot find any pool with sufficient capacity for a volume of this size at site: {siteId}, MaxPercentUsedCapacity: {maxPercentUsedCapacity} VolumeSizeInByte: {volumeSizeInBytes}.	Error
Could not find any test volume pairs for for replicated volume pair id: {replicatedVolumePairId}.	Error
Cannot add new volumes to this replication group since the replication group's direction cannot be determined. Please pair and resync the replication group before adding new volumes to this group.	Error
The site pair cache is invalid. Refresh the cache and retry.	Error

Event	Severity
The volume: {volumeId} is currently a boot volume and cannot be replicated.	Error
The volume is attached to a source server {sourceServerId} . Mismatch in image type for the source server image:{sourceImageType} and target server image:{targetImageType}.	Error
The target cluster with clusterId:{clusterId} does not have any servers to attach the volume.	Error
The appliance cannot be onboarded in the current deployment state.	Error
The appliance with the UCP serial number:{ucpSerialNumber} could not be found.	Error
Failed to assign proposed new IP addresses to elements in the appliance. {errorMessage}	Error
Failed to generate: {numberIpAddressesRequired} number of IP addresses for subnet: {subnetMask} and starting IP address: {startingIpAddress}.	Error
Failed to load appliance settings and IDC configuration. {errorMessage}	Error
Insufficient number of IP addresses are available for subnet: {subnetMask} and starting IP address: {startingIpAddress}. The number of IP addresses required is: {numberIpAddressesRequired}, whereas the number of IP addresses available is: {numberIpAddressesAvailable}.	Error
The onboarding of the appliance has completed successfully.	Info
The onboarding of the appliance has started.	Info
Could not find HUS storage system with UCP Serial Number: '{ucpSerialNumber}', ID: {storageId}	Error
Could not find HUSVM storage system with UCP Serial Number: '{ucpSerialNumber}', ID: {storageId}	Error
Failed to update available config of syslog server. {errorMessage}	Error
The available configuration of syslog server has successfully completed.	Info
Starting to update the available configuration of syslog server.	Info
Could not find Blade {bladeID} for Chassis {chassisID} for appliance with serial number '{ucpSerialNumber}'	Error
Could not find Chassis {chassisID} for appliance with serial number '{ucpSerialNumber}'	Error
Could not find management server network {networkId} for management server {managementServerID} on UCP with serial number '{ucpSerialNumber}'	Error
Could not find management server {managementServerID} on UCP with serial number '{ucpSerialNumber}'	Error
Could not find Service VM Network {networkId} on UCP with serial number '{ucpSerialNumber}'	Error
Could not find Virtual Switch Port Group {vspgID} for management server {managementServerID} on UCP with serial number '{ucpSerialNumber}'	Error
The HUS Storage available configuration was successfully updated.	Info

Event	Severity
Started updating HUS Storage available configuration.	Info
Failed to update the HUS Storage available configuration. {errorMessage}	Error
The HUSVM Storage available configuration was successfully updated.	Info
Started updating HUSVM Storage available configuration.	Info
Failed to update the HUSVM Storage available configuration. {errorMessage}	Error
Could not find management virtual machine {virtualMachineId} on UCP with serial number '{ucpSerialNumber}'.	Error
Could not find running configuration for management virtual machine {virtualMachineId} on UCP with serial number '{ucpSerialNumber}'.	Error
Successfully updated the Active Directory configuration	Info
Starting to update the Active Directory configuration.	Info
An error occurred updating the Active Directory configuration: {error}	Error
The active directory at '{ipAddress}' does not have a listener on the SSL port. Verify this is expected before proceeding.	Warning
The following OU was not found in the active directory at {ipAddress}: {ou}	Error
The security group '{securityGroup}' in property '{propertyName}' does not exist.	Error
Failed to validate external active directory information.	Error
Completed validating external active directory settings.	Info
Started validating external active directory settings.	Info
The property '{accountProperty}' contains credentials that are either incorrect or not in the active directory. User Account: {userAccount}	Error
No domain controller with IP address '{ipAddress}' was found.	Error
The account '{userAccount}' does not have permission in the specified domain to add computers to the domain.	Error
No test volume pair were removed from replication group: {replicationGroupId}.	Info
All existing test volumes' pool type does not match selected pool type for desired test pool id {poolId}.	Error
Desired test volumes does not have all the same types.	Error
Volume pair id: {replicatedVolumePairId} for replication group id: {replicationGroupId} is attached to servers that are in different clusters.	Error
Volume pair id: {replicatedVolumePairId} for replication group id: {replicationGroupId} is either not in Pair status or missing a left or right volume.	Error
Volume pair id: {replicatedVolumePairId} for replication group id: {replicationGroupId} already contains a test volume and will not be able to add a new test volume to the volume pair.	Error

Event	Severity
The volume is attached to a source server of an image type that is not allowed for test volume creation (i.e. not ESXI).	Error
Failed to update blade running configuration. {errorMessage}	Error
Successfully updated blade running configuration.	Info
Started updating blade running configuration chassis: {chassisId} blade: {slotNumber}.	Info
An error occurred during active directory validation: {errorMessage}	Error
Could not access root directory entry from external active directory: {errorMessage}	Error
Cannot find any HTI pool with at site: {siteId}.	Error
Cannot find any HTI pool with sufficient capacity at site: {siteId}.	Error
Cannot update running configuration for specified blade. Specified BmcIpAddress: {bmcIpAddress} is not in the management network	Error
Waiting to communicate with chassis {chassisId} (position {chassisPosition}) after re-ip timed out.	Error
Completed updating chassis running config for chassis: {chassisId} (position {chassisPosition})	Info
Starting the re-ip of chassis: {chassisId} (position {chassisPosition}) to IP address: {ipAddress}, Default Gateway: {defaultGateway}, Subnet Mask: {subnetMask}	Info
Started updating chassis running config for chassis: {chassisId} (position {chassisPosition}) from IP address {currentIpAddress} to {newIpAddress}	Info
Failed to update chassis running config for chassis: {chassisId} (position {chassisPosition}). {errorMessage}	Error
Successfully completed updating the inventory.	Info
A failure occurred while updating the inventory: {message}	Error
Cannot update running configuration for specified blade. Specified blade is not installed.	Error
Updating the inventory	Info
Failed to update management server switch port group running configuration. {errorMessage}	Error
Successfully updated running configuration for management server switch port group {switchPortGroupId}.	Info
Started updating running configuration for management server switch port group {switchPortGroupId}.	Info
Cannot update running configuration for specified management server network. Specified IpAddress: {ipAddress} is not in the {networkType} network	Error
Appliance is not in ReipInProgress state. Cannot update management server network.	Error
Failed to update management server network running configuration. {errorMessage}	Error
Successfully updated running configuration for management server network {networkId}.	Info

Event	Severity
Started updating running configuration for management server network {networkId}.	Info
Appliance is not in ReipInProgress state. Cannot update management server switch port group.	Error
Failed to delete volume {volumeId} in volume pair {volumePairId} from replication group: {replicationGroupId}.	Error
Successfully deleted volume {volumeId} in volume pair {volumePairId} from replication group: {replicationGroupId}.	Info
Detach and delete of secondary/test volume from replication group: {replicationGroupId} has started.	Info
No secondary/test volumes to detach and delete from replication group: {replicationGroupId}.	Info
Failed to detach volume {volumeId} from server {serverId} in volume pair {volumePairId} from replication group: {replicationGroupId}.	Error
Successfully detached volume {volumeId} from servers in volume pair {volumePairId} from replication group: {replicationGroupId}.	Info
Cannot update running configuration for HUS 130 storage system. Controller 0 IpAddress: {ipAddress} is not in the management server network	Error
Appliance is not in ReipInProgress state. Cannot update HUS 130 storage settings.	Error
Failed to update HUS 130 storage running configuration. {errorMessage}	Error
Successfully updated running configuration for HUS 130 storage {storageSystemId}.	Info
Started updating running configuration for HUS 130 storage {storageSystemId}.	Info
Failed to update management server running configuration. {errorMessage}	Error
Successfully updated management server running configuration.	Info
Started updating management server with Id: {managementServerId} running configuration.	Info
Failed to update management server running configuration. Specified BmcIpAddress: {bmcIpAddress} is not in the management network.	Error
Appliance is not in ReipInProgress state. Cannot update management server BmcIpAddress.	Error
Cannot update running configuration for HUS 130 storage system. Appliance is using a different storage system	Error
Cannot update running configuration for HUS VM storage system. Appliance is using a different storage system	Error
Cannot update running configuration for HUS VM storage system. Specified IpAddress 1: {ipAddress} is not in the management server network	Error
Appliance is not in ReipInProgress state. Cannot update HUS VM storage settings.	Error
Failed to update HUS VM storage running configuration. {errorMessage}	Error

Event	Severity
Successfully updated running configuration for HUS VM storage {storageSystemId}.	Info
Started updating running configuration for HUS VM storage {storageSystemId}.	Info
Cannot update running configuration for HUS 130 storage system. Controller 1 IpAddress: {ipAddress} is not in the management server network	Error
Cannot update running configuration for HUS VM storage system. Specified IpAddress 2: {ipAddress} is not in the management server network	Error
Completed the re-ip of chassis\blade: {chassisId}\{bladeId} to IP address: {ipAddress}, Default Gateway: {defaultGateway}, Subnet Mask: {subnetMask}	Info
Starting the re-ip of chassis\blade: {chassisId}\{bladeId} to IP address: {ipAddress}, Default Gateway: {defaultGateway}, Subnet Mask: {subnetMask}	Info
Completed setting the power status of chassis\blade: {chassisId}\{bladeId} to {powerStatus}	Info
Starting to set the power status of chassis\blade: {chassisId}\{bladeId} to {powerStatus}	Info
Failed to update service VM: {networkId} running configuration. {errorMessage}	Error
Started updating service VM: {networkId} running configuration.	Info
Test volumes configuration mismatch between existing replication group and requested replicated volume pairs. Ensure the entire group's test volume configuration matches requested replicated volume pairs.	Error
Failed to delete HTI volume {volumeId} in volume pair {volumePairId} from replication group: {replicationGroupId}.	Error
Successfully deleted HTI volume {volumeId} in volume pair {volumePairId} from replication group: {replicationGroupId}.	Info
Starting the reconfiguration of management server switch port group {switchPortGroupId}.	Info
Completed the reconfiguration of management server switch port group {switchPortGroupId}.	Info
Started updating the reconfiguration of IPAddress for management server network {networkId}.	Info
Completed updating the reconfiguration of IPAddress {IPAddress} for management server network {networkId}.	Info
Detach and delete failed for volume {volumeId} in volume pair {volumePairId} from replication group: {replicationGroupId}.	Error
No test volume pair will be added to replication group: {replicationGroupId}.	Info
Unable to detach and delete the secondary volume in the volume pair {volumePairId}, since the pair are in simplex and both volumes are on same storage system {storageSystemId}.	Error

Event	Severity
Unable to find, detach and delete the secondary volume in volume pair {volumePairId} because left volume's storage system id {leftStorageSystemId} and right volume's storage system id {rightStorageSystemId} does not match with provided storage system id {storageSystemId}.	Error
Successfully forced storage system to resync for site {siteId} in site pair: {sitePairId}.	Info
Forced storage system to resync for site {siteId} in site pair: {sitePairId} failed.	Error
Started forced storage system to resync for site {siteId} in site pair: {sitePairId}.	Info
Started refresh inventory for site pair: {sitePairId}.	Info
The performance characteristics of the journal volumes available for this operation are inconsistent and outside of acceptable bounds. All journal volumes should have the disk throughput value in MBPerSec within +/- 10%. Maximum Throughput: {max}, Minimum Throughput: {min}. Contact your storage administrator to fix the issue and re-run the operation.	Error
Appliance is not in OnboardingCompleted or ReipInProgress state. Cannot update blade settings.	Error
Appliance is not in ReipInProgress state. Cannot update chassis settings.	Error
Appliance is not in ReipInProgress state. Cannot update service VM network settings.	Error
The TFTP configuration template file is invalid.	Error
Generating TFTP configuration file.	Info
Cannot deploy CentOS on blades until appliance re-ip is completed.	Error
An error occurred deploying CentOS on all blades: {errormessage}	Error
Completed deployment of CentOS on all blades	Info
Starting deployment of CentOS on all blades	Info
An error occurred starting the TFTP server: {errorMessage}	Error
Starting up the TFTP server	Info
An error occurred starting the FTP server: {errorMessage}	Error
TFTP Server has been stopped.	Info
Completed powering on blade {bladeId} in chassis {chassisId}.	Info
Powering on blade {bladeId} in chassis {chassisId} failed: {errorMessage}	Error
Started powering on blade {bladeId} in chassis {chassisId}.	Info
Chassis {chassisId} blade {bladeId} validation completed.	Info
Chassis {chassisId} blade {bladeId} validation failed: {errorMessage}	Error
Chassis {chassisId} blade {bladeId} validation started	Info
Cannot validate a blade until appliance re-ip is completed.	Error

Event	Severity
Cannot validate a chassis until appliance re-ip is completed.	Error
Cannot validate HUS storage until appliance re-ip is completed.	Error
Cannot validate HUS VM storage until appliance re-ip is completed.	Error
Cannot validate a management server until appliance re-ip is completed.	Error
Chassis {chassisId} validation completed	Info
Chassis {chassisId} validation failed: {errorMessage}	Error
Chassis {chassisId} validation started	Info
HUS storage {storageSystemId} validation completed	Info
HUS storage {storageSystemId} validation failed: {errorMessage}	Error
HUS storage {storageSystemId} validation started	Info
HUS VM storage {storageSystemId} validation completed	Info
HUS VM storage {storageSystemId} validation failed: {errorMessage}	Error
HUS VM storage {storageSystemId} validation started	Info
Management server {serverId} validation completed	Info
Management server {serverId} validation failed: {errorMessage}	Error
Management server {serverId} validation started	Info
Ping test to IP address {IpAddress} completed.	Info
Ping test to IP address {IpAddress} failed. Ping status: {status}	Error
Ping test to IP address {IpAddress} started.	Info
Network ethernet switch {switchId} validation completed.	Info
Network ethernet switch {switchId} validation failed: {errorMessage}	Error
Network ethernet switch {switchId} validation started.	Info
Cannot validate a network ethernet switch until appliance re-ip is completed.	Error
Could not find network ethernet switch {switchId} on UCP with serial number '{ucpSerialNumber}'.	Error
Completed powering off blade {bladeId} in chassis {chassisId}.	Info
Powering off blade {bladeId} in chassis {chassisId} failed: {errorMessage}	Error
Started powering off blade {bladeId} in chassis {chassisId}.	Info
Chassis {chassisId} blade {bladeId} has expected firmware version '{firmwareVersion}'	Info
Chassis {chassisId} blade {bladeId} firmware version was '{foundFirmware}'. Expected was '{expectedFirmware}'	Error
Cannot validate a management server network until appliance re-ip is completed.	Error

Event	Severity
Management server network {networkId} validation completed	Info
Management server network {networkId} validation failed: {errorMessage}	Error
Management server network {networkId} validation started	Info
Chassis {chassisId} has expected firmware version '{firmwareVersion}'	Info
Chassis {chassisId} firmware version was '{foundFirmware}'. Expected was '{expectedFirmware}'	Error
Appliance is not in ReipInProgress state. Cannot update converged switch settings.	Error
Could not find converged switch {switchId} for appliance with serial number '{ucpSerialNumber}'	Error
Failed to update converged switch: {switchId} running configuration. {errorMessage}	Error
Started updating converged switch: {switchId} running configuration.	Info
Generating converged switch: {switchId} configuration.	Info
Completed updating converged switch: {switchId} phase 1 configuration.	Info
Started updating converged switch: {switchId} phase 1 configuration. This will re-ip the switch.	Info
Network ethernet switch {switchId} has expected firmware version '{firmwareVersion}'	Info
Network ethernet switch {switchId} firmware version was '{foundFirmware}'. Expected was '{expectedFirmware}'	Error
HUS storage system {storageSystemId} controllers have the expected firmware version '{firmwareVersion}'	Info
HUS VM storage system {storageSystemId} has expected firmware version '{firmwareVersion}'	Info
HUS storage system {storageSystemId} controller {controllerNumber} firmware version was '{foundFirmware}'. Expected was '{expectedFirmware}'	Error
HUS VM storage system {storageSystemId} firmware version was '{foundFirmware}'. Expected was '{expectedFirmware}'	Error
HUS storage array port {portName} has the expected connection type of {connectionType}	Info
HUS storage array port {portName} has the expected security enabled status of {status}	Info
HUS VM storage array port {portName} has the expected connection type of {connectionType}	Info
HUS VM storage array port {portName} has the expected security enabled status of {status}	Info
HUS storage array port {portName} does not have the expected connection type of {connectionType}	Error

Event	Severity
The following HUS storage array ports do not have the expected connection type of {connectionType}: {portList}	Error
HUS storage array port {portName} does not have the expected security enabled status of {status}	Error
The following HUS storage array ports do not have the expected security enabled status of {status}: {portList}	Error
HUS VM storage array port {portName} does not have the expected connection type of {connectionType}	Error
The following HUS VM storage array ports do not have the expected connection type of {connectionType}: {portList}	Error
HUS VM storage array port {portName} does not have the expected security enabled status of {status}	Error
The following HUS VM storage array ports do not have the expected security enabled status of {status}: {portList}	Error
Validating HUS storage array port connection type configuration.	Info
Validating HUS storage array port security configuration.	Info
Validating HUS VM storage array port connection type configuration.	Info
Validating HUS VM storage array port security configuration.	Info
The following HUS storage system {storageSystemId} controllers did not have the expected firmware of '{expectedFirmware}': {controllerList}	Error
Completed blade configuration validation for chassis {chassisId}.	Info
Chassis {chassisId} had blades fail configuration validation. The following blades had properties that did not match blade 0: {bladeList}	Error
Starting blade configuration validation for chassis {chassisId}.	Info
Appliance is not in ReipCompleted state. Cannot configure converged settings on the switch.	Error
Committing the converged configuration on converged switch: {switchId}.	Info
Completed configuring FCOE settings on converged switch: {switchId}.	Info
Started configuring FCOE settings on converged switch: {switchId}.	Info
Completed configuring FC settings on converged switch: {switchId}.	Info
Started configuring FC settings on converged switch: {switchId}.	Info
Completed removing VLAN: {vlanId} on all ISL port channels on converged switch: {switchId}.	Info
Started removing VLAN: {vlanId} on all ISL port channels on converged switch: {switchId}.	Info
Completed updating converged switch: {switchId} phase 2 configuration.	Info

Event	Severity
Started updating converged switch: {switchId} phase 2 configuration. This will configure the converged settings.	Info
Cannot configure converged setting on converged switch: {switchId} as these are not yet available.	Error
Chassis {chassisId} blade {bladeId} configuration property 'CPU Model' did not match blade 0. Expected value: '{expectedValue}'. Actual value: '{actualValue}'	Error
Chassis {chassisId} blade {bladeId} configuration property 'CPU Physical Count' did not match blade 0. Expected value: '{expectedValue}'. Actual value: '{actualValue}'	Error
Chassis {chassisId} blade {bladeId} configuration property 'Memory' did not match blade 0. Expected value: '{expectedValue}'. Actual value: '{actualValue}'	Error
Chassis {chassisId} blade {bladeId} configuration property 'Number Of CPU Cores' did not match blade 0. Expected value: '{expectedValue}'. Actual value: '{actualValue}'	Error
The new blade BMC IP address: {newIpAddress} provided is not unique.	Error
The blade hypervisor IP address: {newIpAddress} provided is not unique.	Error
Cannot update running configuration for specified blade. Specified Hypervisor IP Address: {ipAddress} is not in the management network.	Error
Cannot update running configuration for specified chassis. The provided chassis SVP IP address: {newIpAddress} is not in the management network.	Error
Cannot update running configuration of the converged switch. The provided IP address: {newIpAddress} is not in the management network.	Error
Cannot update running configuration of the service VM. The provided IP address: {newIpAddress} is not in the management network.	Error
The new chassis SVP IP address: {newIpAddress} provided is not unique.	Error
The converged switch IP address:{newIpAddress} provided is not unique.	Error
The new HUS Controller 0 IP address: {newIpAddress} provided is not unique.	Error
The new HUS Controller 1 IP address: {newIpAddress} provided is not unique.	Error
The new HUS VM IP address 1: {newIpAddress} provided is not unique.	Error
The new HUS VM IP address 2: {newIpAddress} provided is not unique.	Error
The management server IP address: {newIpAddress} provided is not unique.	Error
The management server network IP address: {newIpAddress} provided is not unique.	Error
The service VM IP address: {newIpAddress} provided is not unique.	Error
Could not retrieve the hardware configuration for the following blades for chassis {chassisId}: {bladeList}	Error
The operation to retrieve the hardware configuration for chassis {chassisId} blade {bladeId} timed out.	Error

Event	Severity
Completed updating the reconfiguration of IPAddresses for the HUS storage array to controller0: {controller0IpAddress} controller1: {controller1IpAddress}.	Info
Started updating the reconfiguration of IPAddresses for the HUS storage array to controller0: {controller0IpAddress} controller1: {controller1IpAddress}.	Info
Management Virtual Machine {managementVmId} is not available for deployment.	Error
Management Server {serverId} has an invalid serial number: {serialNumber}	Error
Management Server {serverId} has a valid serial number: {serialNumber}	Info
Cannot update running configuration for specified virtual machine. The provided IP address: {newIpAddress} is not in the management network.	Error
Completed updating running config for virtual machine: {vmId} (role {vmRole})	Info
Started updating running config for virtual machine: {vmId} (role {vmRole})	Info
Failed to update running config for virtual machine: {vmId} (role {vmRole}). {errorMessage}	Error
The new virtual machine IP address: {newIpAddress} provided is not unique.	Error
Successfully updated converged switch: {switchId} running configuration.	Info
Successfully updated running configuration for service VM: {networkId}.	Info
Cannot update active directory configuration until validation is complete.	Error
Could not retrieve Net BIOS Domain Name for domain {domainName}.	Error
Could not retrieve Net BIOS Domain Name for domain {domainName}. {errorMessage}	Error
Failed to find exactly one HDP pool with the journal pool label.	Error
Unable to find newly created journal volume.	Error
Successfully Completed the re-ip of chassis: {chassisId} (position {chassisPosition}) to IP address: {ipAddress}, Default Gateway: {defaultGateway}, Subnet Mask: {subnetMask}	Info
Primary network ethernet switches cannot be reconfigured before secondary network ethernet switches.	

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-92UCP054-01