Hewlett Packard Enterprise Helion and Veritas Continuity Deployment Guide

1.0

May 2016

VERITAS™

Hewlett Packard Enterprise Helion and Veritas Continuity Deployment Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: 1.0

Document version: 1.0 Rev 0

Legal Notice

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Contents

Chapter 1 Overview of HPE Helion and Veritas Continuity deployment ... 8

About HPE Helion and Veritas Continuity ... 8
About HPE Helion and Veritas Continuity features and components ... 9
Resiliency domain ... 11
Resiliency Manager ... 11
Infrastructure Management Server (IMS) ... 12
Replication Gateways ... 12
Storage Proxy ... 13
Planning a resiliency domain for efficiency and fault tolerance ... 13
Deploying and configuring HPE Helion and Veritas Continuity virtual appliance components ... 13

Chapter 2 System requirements ... 15

Supported hypervisors for HPE Helion and Veritas Continuity virtual appliance ... 15
System resource requirements for HPE Helion and Veritas Continuity ... 16
Network and firewall requirements ... 17
Web browser requirements for HPE Helion and Veritas Continuity ... 21

Chapter 3 Deploying HPE Helion and Veritas Continuity ... 22

About deploying the HPE Helion and Veritas Continuity virtual appliance ... 22
HPE Helion and Veritas Continuity virtual appliance file names ... 23
Deploying the virtual appliance on-premises through Hyper-V Manager ... 23
Deploying the virtual appliance on-premises through VMware vSphere Client ... 24

Chapter 4 Configuring the settings on the virtual appliance 27

About configuring the HPE Helion and Veritas Continuity components 27
Prerequisites for configuring HPE Helion and Veritas Continuity components 28
Configuring an Infrastructure Management Server 28
Configuring a Replication Gateway 29
Configuring a Storage Proxy 30

Chapter 5 Adding the asset infrastructure to an Infrastructure Management Server (IMS) 33

About the asset infrastructure 33
Adding the asset infrastructure to an Infrastructure Management Server (IMS) 34
Managing host assets for an IMS 35
  About adding host assets to an IMS 36
  Prerequisites for adding hosts to an IMS 36
  Packages required on Linux hosts 37
  Additional prerequisites for protecting virtual machines 38
  Adding hosts to an IMS 39
  Installing the host package on a Windows host 40
  About using a CSV file for adding hosts to an IMS 41
  Refreshing host discovery information for an IMS 41
  Removing hosts from an IMS 42
  Uninstalling the host package from a Linux host 43
  Uninstalling the host package from a Windows host 44
Managing Hyper-V assets for an IMS 44
  About Microsoft Hyper-V virtualization discovery 44
  Prerequisites for Microsoft Hyper-V virtualization discovery by the IMS 45
Managing VMware virtualization servers for an IMS 46
  Prerequisites for adding VMware servers for discovery by the IMS 46
  About near real-time discovery of VMware events 47
  Setting up near real-time discovery of VMware events 49
  Configuring the VMware vCenter Server to generate SNMP traps 50
  Adding virtualization servers for VMware discovery by the IMS 51

Editing a VMware virtualization discovery configuration in the IMS ... 53
Removing a virtualization discovery configuration from the IMS ... 54
Refreshing a VMware virtualization discovery configuration ... 54
Refreshing an ESX Server discovery ... 54
Managing add-ons for the hosts ... 55
Installing add-ons on the hosts ... 55
Uninstalling add-ons from the hosts ... 57

Chapter 6 Managing users and global settings ... 59

Managing user authentication and permissions ... 59
About user authentication in the web console ... 60
About user permissions in the web console ... 61
Predefined personas ... 62
About limiting object scope for personas ... 65
Configuring authentication domains ... 66
Unconfiguring authentication domains ... 68
Configuring user groups and users ... 69
Assigning permissions to user groups and users ... 69
Adding custom personas ... 71
Predefined jobs that can be used for custom personas ... 72
Custom persona required for starting or stopping resiliency groups ... 74
Managing settings for alerts and notifications and general product settings ... 74
Adding, modifying, or deleting email settings ... 74
Adding, modifying, or deleting SNMP settings ... 76
Setting up rules for event notifications ... 76
Viewing events and logs in the console ... 77
Modifying purge settings for logs and SNMP traps ... 78
Enabling or disabling telemetry collection ... 79

Chapter 7 Using the Web console ... 80

Tour of the HPE Helion and Veritas Continuity web console screen ... 80
Menu bar options ... 81
Navigation pane options ... 82
Filtering and searching for objects in the web console ... 82
About the HPE Helion and Veritas Continuity Dashboard ... 83
Web console icons ... 85

Chapter 8 Updating HPE Helion and Veritas Continuity 87

About updating HPE Helion and Veritas Continuity 87
About applying updates to HPE Helion and Veritas Continuity 88
Prerequisites for a repository server 90
Setting up the repository server and downloading updates 90
Adding a repository server in HPE Helion and Veritas Continuity 92
Assigning a repository server in HPE Helion and Veritas Continuity 92
Applying updates to virtual appliances using the console 93
Applying updates to virtual appliance using CLISH menu 94
Refreshing the information about applicable updates 95
Removing an update from the repository server 95

Chapter 9 Uninstalling HPE Helion and Veritas Continuity 96

About uninstalling HPE Helion and Veritas Continuity 96

Chapter 10 Troubleshooting and maintenance 97

Accessing HPE Helion and Veritas Continuity log files 97
Troubleshooting replication 98
Components of HPE Helion and Veritas Continuity virtual appliances 98
Using Veritas Services and Operations Readiness Tools to find a Unique Message Identifier description and solution 99
Displaying risk information 100

Appendix A Using CLISH menu in HPE Helion and Veritas Continuity 101

About CLISH 101
Using CLISH 102

Glossary 110

Index 113

Chapter 1

Overview of HPE Helion and Veritas Continuity deployment

This chapter includes the following topics:

- About HPE Helion and Veritas Continuity
- About HPE Helion and Veritas Continuity features and components
- Planning a resiliency domain for efficiency and fault tolerance
- Deploying and configuring HPE Helion and Veritas Continuity virtual appliance components

About HPE Helion and Veritas Continuity

HPE Helion and Veritas Continuity offers a unified approach for visibility and control of IT service continuity for virtual machines and complex, multi-tier business services across a global landscape.

HPE Helion and Veritas Continuity has the following core capabilities:

Recovery

HP Helion and Veritas Continuity provides a disaster recovery (DR) solution in the cloud for on-premises data centers. HPE Helion and Veritas Continuity provides the management console that enables the DR configuration.

Once DR is enabled, HPE Helion and Veritas Continuity provides single-click DR operations between the on-premises data center and the cloud. These single-click operations include rehearsal, rehearsal cleanup, migrate, takeover, prepare for failback, and failback. The HP Helion and Veritas Continuity service provider performs the DR operations as requested.

Visibility

The console Dashboard provides visibility into the health of virtual machines and multi-tier business services.

Orchestration

HPE Helion and Veritas Continuity can assist in data center day-to-day workload automation activities. For instance, virtual machines or IT services can be started and stopped for maintenance.

About HPE Helion and Veritas Continuity features and components

The following is a brief introduction to HPE Helion and Veritas Continuity key components and features. Administrators responsible for deploying and configuring the product need to understand these in more detail.

resiliency domain

The logical scope of a HPE Helion and Veritas Continuity deployment.

It can extend across multiple data centers.

See “Resiliency domain” on page 11.

Resiliency Manager

The component that provides resiliency capabilities within a resiliency domain. It is composed of loosely coupled services, a distributed data repository, and a management console. The Resiliency Manager is deployed as a virtual appliance.

See “Resiliency Manager” on page 11.

Infrastructure Management Server (IMS)

The component that discovers, monitors, and manages the asset infrastructure within a data center. The IMS transmits information about the asset infrastructure to the Resiliency Manager. The IMS is deployed as a virtual appliance.

To achieve scale, multiple IMSs can be deployed in the on-premises data center. One IMS is deployed in the cloud.

See “Infrastructure Management Server (IMS)” on page 12.

Replication Gateway

The component that performs replication between the on-premises storage and the cloud storage. Replication Gateways are deployed as virtual appliances.

See “Replication Gateways” on page 12.

Storage Proxy

The component that enables HPE Helion and Veritas Continuity to connect the primary storage as iSCSI targets to the on-premises gateway during preparation for failback to the on-premises data center. The Storage Proxy is deployed as a virtual appliance.

See “Storage Proxy” on page 13.

data center

The resiliency domain contains two data centers, an on-premises data center and the recovery data center in the cloud. The cloud data center has a Resiliency Manager, one or more cloud Replication Gateways, and one IMS; the on-premises data center has one or more on-premises Replication Gateways, one or more Storage Proxies, and one or more IMSs

asset infrastructure

The data center assets that you add to HPE Helion and Veritas Continuity for discovery and monitoring by the IMS.

The asset infrastructure includes hosts and virtualization servers. Once the asset infrastructure is discovered by the IMS, the discovered virtual machines are listed in the console as assets to manage or protect.

resiliency group

The unit of management and control in HPE Helion and Veritas Continuity. You organize related assets into a resiliency group and manage and monitor them as a single entity.

Virtual Business Service (VBS)	A multi-tier business service where each VBS tier hosts one or more resiliency groups. A VBS lets you group multiple services as a single unit for visualization, automation, and controlled start and stop in the desired order. VBS uses the vertical grouping mechanism to group the multiple services.You can also migrate, takeover, prepare failback, and failback the entire VBS.

Resiliency domain

A resiliency domain is the management domain of a HPE Helion and Veritas Continuity deployment. It represents the scope of the deployment, which can spread across multiple data centers and can include multiple HPE Helion and Veritas Continuity components, along with the infrastructure that is being managed and protected. Within the resiliency domain, HPE Helion and Veritas Continuity can protect assets, for example, virtual machines, and orchestrate automation of workload tasks for the assets.

The resiliency domain is a logical object that you create from the web console after you deploy the Resiliency Manager.

The resiliency domain must contain at least two data centers, an on-premises data center and the recovery data center in the cloud. The cloud data center has a Resiliency Manager, one or more cloud gateways, and one IMS; the on-premises data center has one or more on-premises gateways, one or more storage proxies, and one or more IMSs.

See “Resiliency Manager” on page 11.

See “Infrastructure Management Server (IMS)” on page 12.

Resiliency Manager

The Resiliency Manager includes a set of loosely coupled services, a distributed data repository, and a management web console. The Resiliency Manager provides the services required for protecting assets, such as virtual machines, within a resiliency domain. It also provides workload automation services.

The Resiliency Manager is deployed in the cloud data center.

The Resiliency Manager discovers and manages information about data center assets from an Infrastructure Management Server (IMS), which is another required HPE Helion and Veritas Continuity component. The Resiliency Manager stores the asset information in its data repository and displays the information in its management console.

See “Resiliency domain” on page 11.

See “Infrastructure Management Server (IMS)” on page 12.

Infrastructure Management Server (IMS)

Each Resiliency Manager requires one or more Infrastructure Management Servers (IMSs). An IMS discovers and monitors assets within a data center. You use the web console to add the asset infrastructure to the IMS so that assets can be discovered and monitored.

The asset infrastructure can include objects such as hosts and virtualization servers.

The IMS sends information about the assets to the Resiliency Manager so that the Resiliency Manager can manage the assets. Management operations on assets (for example, starting or stopping virtual machines) that you initiate from the web console are carried out by the IMS.

You can also configure multiple Infrastructure Management Servers in the same data center. For example, to achieve scale, you can add a separate IMS for a separate business unit such as Human Resources or Finance. More than one IMS can be managed by the same Resiliency Manager.

See “Resiliency domain” on page 11.

See “Resiliency Manager” on page 11.

Replication Gateways

The gateway component of HPE Helion and Veritas Continuity is a staging server that aggregates and batches data from multiple virtual machines during replication. The gateway also performs data optimization like write cancellation. The on-premises gateway is always paired with a cloud gateway. The cloud gateway is a staging server that applies the data on the cloud storage.

Each Replication Gateway includes the following components:

- I/O receiver

  Receives the application I/Os that were tapped and sent by the application host in a continuous fashion.

- Transceiver

  Transfers and receives data over the WAN link periodically.

- Applier

  Applies the data to the storage after it is received on the cloud gateway.

- Scheduler

  Manages the jobs and policies in the gateway.

- Engine

Maintains the state of replication and also coordinates with all other components.

During the deployment of the gateway, the gateway is registered as an asset to the respective IMS (on-premises or cloud).

Storage Proxy

The Storage Proxy enables HPE Helion and Veritas Continuity to connect the primary storage as iSCSI targets to the on-premises gateway. The Storage Proxy must be on the same hypervisor technology as the protected virtual machines. The Storage Proxy should also share the same datastore as the protected virtual machines. During deployment of the Storage Proxy, the Storage Proxy is registered with the on-premises IMS. The Storage Proxy is only active during the prepare for failback operation.

Planning a resiliency domain for efficiency and fault tolerance

Before you deploy HPE Helion and Veritas Continuity, you should plan how to scale the deployment for efficiency and fault tolerance.

For a cloud data center, you deploy a Resiliency Manager and Infrastructure Management Server (IMS) on the same virtual appliance in the cloud. You can deploy one or more IMSs as separate virtual appliances in the on-premises data center. At least one replication gateway is deployed both on-premises and in the cloud.

The on-premises and cloud data centers do not require a one-on-one mapping of IMSs. For example, you can have two IMSs on-premises and one IMS in the cloud.

See “Resiliency domain” on page 11.

See “Resiliency Manager” on page 11.

See “Infrastructure Management Server (IMS)” on page 12.

See “Replication Gateways” on page 12.

See “Storage Proxy” on page 13.

Deploying and configuring HPE Helion and Veritas Continuity virtual appliance components

The following is an overview of HPE Helion and Veritas Continuity deployment infrastructure:

Figure 1-1 Overview of HPE Helion and Veritas Continuity deployment infrastructure

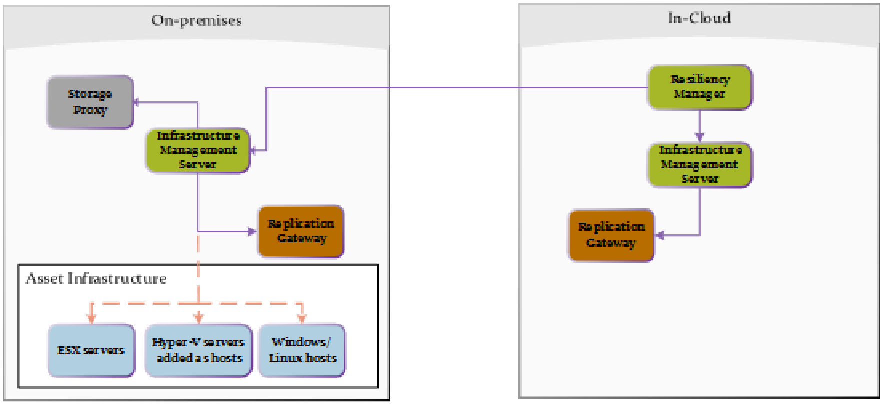


Table 1-1 describes the various steps involved in deploying and configuring HPE Helion and Veritas Continuity virtual appliance components:

Table 1-1 Deploying and configuring HPE Helion and Veritas Continuity virtual appliance components

Step	Action	Description
1	Deploy and configure IMS on-premises	See “Deploying the virtual appliance on-premises through Hyper-V Manager” on page 23. See “Deploying the virtual appliance on-premises through VMware vSphere Client” on page 24. See “Configuring an Infrastructure Management Server” on page 28.
2	Deploy and configure Replication Gateway on-premises	See “Deploying the virtual appliance on-premises through Hyper-V Manager” on page 23. See “Deploying the virtual appliance on-premises through VMware vSphere Client” on page 24. See “Configuring a Replication Gateway” on page 29.
3	Deploy and Configure Storage Proxy on-premises	See “Deploying the virtual appliance on-premises through Hyper-V Manager” on page 23. See “Deploying the virtual appliance on-premises through VMware vSphere Client” on page 24. See “Configuring a Storage Proxy” on page 30.

Chapter 2

System requirements

This chapter includes the following topics:

- Supported hypervisors for HPE Helion and Veritas Continuity virtual appliance
- System resource requirements for HPE Helion and Veritas Continuity
- Network and firewall requirements
- Web browser requirements for HPE Helion and Veritas Continuity

Supported hypervisors for HPE Helion and Veritas Continuity virtual appliance

This section lists the hypervisor versions that are supported for HPE Helion and Veritas Continuity virtual appliance.

Microsoft Hyper-V:

- Windows Server 2012 with Hyper-V
- Windows Server 2012 R2 with Hyper-V

VMware:

- ESX 5.1, 5.5, 6.0
- vCenter Server 5.1, 5.5, 6.0

Note: The lists of supported platforms for deployment of virtual appliance and for disaster recovery of virtual machines are different. For information on platform support for disaster recovery of virtual machines, see the *Veritas Resiliency Platform Hardware and Software Compatibility List*.

See “About deploying the HPE Helion and Veritas Continuity virtual appliance” on page 22.

System resource requirements for HPE Helion and Veritas Continuity

The amount of virtual CPUs, memory, and disk space that HPE Helion and Veritas Continuity requires are listed in this section.

The minimum configuration that is recommended for a virtual appliance for Resiliency Manager, Infrastructure Management Server (IMS), Gateway, and storage Proxy:

Table 2-1 Minimum configurations

Component	Minimum configuration
Resiliency Manager	Disk space 75 GB RAM 16 GB Virtual CPU 8
Infrastructure Management Server (IMS)	Disk space 75 GB RAM 16 GB Virtual CPU 8
Gateway	Disk space 40 GB RAM 16 GB Virtual CPU 8 Additional external disk of 100 GB Both the on-premises gateway and the cloud gateway must have external storage equivalent to 12GB for each virtual machine protected by the gateway pair.
Storage proxy	Disk space 40 GB RAM 16 GB Virtual CPU 8

If the virtual appliance does not meet the minimum configuration, you get a warning and you are required to confirm if you want to continue with the current configuration.

In addition to the above mentioned resources, you need a Linux server with a minimum of 50-GB disk space, to be configured as the repository server. Provisioning for the repository server is optional, it is required to install the HPE Helion and Veritas Continuity patches or updates in the future.

If you want to enable dynamic memory on Hyper-V, make sure that the following prerequisites are met:

- Startup memory and minimal memory should be equal to or greater than the amount of memory that the distribution vendor recommends.
- If you are using dynamic memory on a Windows Server 2012 operating system, specify Startup memory, Minimum memory, and Maximum memory parameters in multiples of 128 megabytes (MB). Failure to do so can lead to dynamic memory failures, and you may not see any memory increase in a guest operating system.

See “About deploying the HPE Helion and Veritas Continuity virtual appliance” on page 22.

Network and firewall requirements

The following are the network requirements for HPE Helion and Veritas Continuity:

- Before you use the hostname and the IP address in the **Network settings**, you need to register them with the DNS server.
- The hostname or the IP address which is used for product configuration, should not have multiple entries in the DNS server. For example, the IP address should not be associated with multiple hostnames, or the hostname should not be associated with multiple IP addresses.
- HPE Helion and Veritas Continuity supports only Internet protocol version (IPV) 4.
- If you plan to use the DHCP server, the DHCP server should be in the same subnet where you plan to deploy the product.
- If you want to assign multiple IP addresses to one network adapter on a host having Windows Server 2008 SP2 or Windows Vista SP2, you need to apply the following patch on the host. This patch lets you to add the skipassource flag in your network configuration.
  https://support.microsoft.com/en-us/kb/975808
  For Windows 2008 SP2 you need to apply one more patch to add the flag.
  https://support.microsoft.com/en-us/kb/2554859
  After applying the patch, the flag still does not show when you run the `netsh` command. You need to manually set the flag after performing any disaster recovery operations.

The following ports are used for HPE Helion and Veritas Continuity:

Table 2-2 Ports used for Resiliency Manager

Ports used	Purpose	For communication between	Direction	Protocol
443	Used for SSL communication	Resiliency Manager and web browser	Browser to Resiliency Manager	TCP
14176	Used for communication between the Resiliency Manager and Infrastructure Management Server (IMS)	Resiliency Manager and IMS	Bi-directional	TCP
7000	Used for database replication	Resiliency Manager and IMS	Bi-directional	TCP
7001	Used for database replication	Resiliency Manager and IMS	Bi-directional	TCP
389	Used for communication with LDAP/AD server	Resiliency Manager and LDAP/AD server	Bi-directional	TCP
636	Used for communication with LDAP/AD server	Resiliency Manager and LDAP/AD server	Bi-directional	TCP
3268	Used for communication with LDAP/AD server	Resiliency Manager and LDAP/AD server	Bi-directional	TCP
3269	Used for communication with LDAP/AD server	Resiliency Manager and LDAP/AD server	Bi-directional	TCP
22	Used for communication between remote host to the appliance CLISH access	Appliance and the hosts	Bi-directional	TCP
123	Used for NTP synchronization	Appliance and the NTP server	Bi-directional	TCP

Table 2-3 Ports used for on-premises IMS and in-cloud IMS

Ports used	Description	For communication between	Direction	Protocol
14176	Used for communication between the Resiliency Manager and Infrastructure Management Server (IMS)	Resiliency Manager and IMS	Bi-directional	TCP
5634	Used for IMS configuration	IMS and the hosts	Bi-directional	TCP
14161	Used for running the IMS console	Resiliency Manager and IMS	Resiliency Manager to IMS	TCP
22	Used for communication between remote host to the appliance CLISH access Used for remote deployment of the packages on remote UNIX host from IMS	IMS and the hosts	Bi-directional	TCP
135	Used for remote deployment on client computer (inbound)	Host and remote Windows hosts	Bi-directional	TCP
123	Used for NTP synchronization	Appliance and the NTP server	Bi-directional	TCP

Table 2-4 Ports used for on-premises Replication Gateway and in-cloud Replication Gateway

Ports used	Description	For communication between	Direction	Protocol
8088	Used for replication	On-premises virtual machine and Replication Gateway/Storage Proxy	Uni-directional	TCP

Table 2-4 Ports used for on-premises Replication Gateway and in-cloud Replication Gateway *(continued)*

Ports used	Description	For communication between	Direction	Protocol
5634	Used for communication with IMS	IMS and Replication Gateway/Storage Proxy	Bi-directional	TCP
8089	Used for replication	in-cloud component and on-premises component	Bi-directional	TCP
8080	Used for replication	in-cloud component and on-premises component	Bi-directional	TCP

Table 2-5 Ports used for Storage Proxy

Ports used	Description	For communication between	Direction	Protocol
5634	Used for communication with IMS	IMS and Replication Gateway/Storage Proxy	Bi-directional	TCP
8089	Used for replication	in-cloud component and on-premises component	Bi-directional	TCP
8080	Used for replication	in-cloud component and on-premises component	Bi-directional	TCP

Table 2-6 Ports used for virtual machines

Ports used	Description	For communication between	Direction	Protocol
22	Used for communication between remote host to the appliance CLISH access Used for remote deployment of the packages on remote UNIX host from IMS	IMS and the hosts	Bi-directional	TCP
5634	Used for communication with IMS	IMS and the hosts	Bi-directional	TCP
8088	Used for replication	On-premises virtual machine and Replication Gateway	Uni-directional	TCP

See “About deploying the HPE Helion and Veritas Continuity virtual appliance” on page 22.

Web browser requirements for HPE Helion and Veritas Continuity

The HPE Helion and Veritas Continuity web console is a graphical user interface that can be accessed through a standard web browser.

The web browsers that the HPE Helion and Veritas Continuity web console supports are:

- Internet Explorer versions 10, or later
- Firefox versions 33.*x*, or later
- Chrome versions 38.*x*, or later
- Safari versions 5.1, or later on Mac OS X

Your browser must be configured to accept cookies and enabled for JavaScript. If you use pop-up blockers, either disable them or configure them to accept cookies.

Chapter 3

Deploying HPE Helion and Veritas Continuity

This chapter includes the following topics:

- About deploying the HPE Helion and Veritas Continuity virtual appliance
- HPE Helion and Veritas Continuity virtual appliance file names
- Deploying the virtual appliance on-premises through Hyper-V Manager
- Deploying the virtual appliance on-premises through VMware vSphere Client

About deploying the HPE Helion and Veritas Continuity virtual appliance

HPE Helion and Veritas Continuity is installed as a virtual appliance. A virtual appliance is a virtual machine image consisting of a pre-configured operating system environment with a software application installed on it. This virtual machine image can be deployed on a hypervisor.

There are two virtual appliances available for HPE Helion and Veritas Continuity: one is used to deploy the Resiliency Manager and the Infrastructure Management Server (IMS) and the other is used to deploy the Replication Gateway and the Storage Proxy.

On-premises, you need to deploy the IMS, the Replication Gateway, and the Storage Proxy. You can deploy these components on-premises using any one of the following:

- Hyper-V Manager
- VMware vSphere Client

The service provider deploys the HPE Helion and Veritas Continuity components in the cloud.

Once the HPE Helion and Veritas Continuity virtual appliances are deployed, you are required to configure the HPE Helion and Veritas Continuity component through the product bootstrap.

See “Deploying the virtual appliance on-premises through Hyper-V Manager” on page 23.

See “Deploying the virtual appliance on-premises through VMware vSphere Client” on page 24.

HPE Helion and Veritas Continuity virtual appliance file names

To deployHPE Helion and Veritas Continuity, you need to download the following virtual appliances:

- To deploy HPE Helion and Veritas Continuity virtual appliance through Hyper-V, you need to download a .zip file. The .zip file contains the virtual hard disk (VHD) image file using which you can deploy the virtual appliance. The names of the .zip file for Hyper-V are as follows:
  - For Resiliency Manager and Infrastructure Management Server (IMS):
    `HPEHVC_RM_IMS_RaaS_Hyper-V_Virtual_Appliance_1.0.0.100_IE.zip`
  - For Replication Gateway and Storage Proxy:
    `HPEHVC_Gateway_SP_Hyper-V_Virtual_Appliance_1.0.0.100_IE.zip`
- To deploy HPE Helion and Veritas Continuity virtual appliance through VMware, you need to download an Open Virtualization Archive (OVA) file. The names of the OVA file for VMware are as follows:
  - For Resiliency Manager and Infrastructure Management Server (IMS):
    `HPEHVC_RM_IMS_RaaS_VMWare_Virtual_Appliance_1.0.0.100_IE.ova`
  - For Replication Gateway and Storage Proxy:
    `HPEHVC_Gateway_SP_VMWare_Virtual_Appliance_1.0.0.100_IE.ova`

Deploying the virtual appliance on-premises through Hyper-V Manager

You can deploy HPE Helion and Veritas Continuity virtual appliance through Hyper-V Manager using the Virtual Hard Disk (VHD) file that you have downloaded.

To deploy HPE Helion and Veritas Continuity through Hyper-V Manager

1. Download the Hyper-V supported VHD file for the HPE Helion and Veritas Continuity virtual appliance on a system where Hyper-V Manager is installed.
2. In the Hyper-V Manager console, right-click the Hyper-V server and select **New Virtual Machine**.
3. Provide a name for the virtual machine.
4. Select **Generation 1** while specifying generation.
5. Assign minimum 16 GB RAM.
6. Select a network adapter for the virtual machine.
7. Select the option **Attach a virtual hard disk later** while specifying option to connect virtual hard disk.
8. Review the virtual machine configuration details and click **Finish**.
9. Go to **Settings**, and increase the number of virtual processors as **8**.
10. Add the VHD file of the HPE Helion and Veritas Continuity virtual appliance as **IDE Controller 0**
11. Click **Apply**, and then click **OK**.
12. If you want to configure the role of Replication Gateway on this virtual appliance, go to the **Edit virtual machine settings** and attach an external disk of 100 GB. Note that the extra disk is initialized during the product bootstrap process and it may result in deletion of data that may already exist on the disk.
13. Right-click the name of the virtual machine and select **Start** to power on the virtual machine.

You can now configure the HPE Helion and Veritas Continuity component.

See “About configuring the HPE Helion and Veritas Continuity components” on page 27.

Deploying the virtual appliance on-premises through VMware vSphere Client

You can deploy HPE Helion and Veritas Continuity virtual appliance through VMware vSphere Desktop Client or VMware vSphere Web Client using the Open Virtualization Archive (OVA) file that you have downloaded.

To deploy HPE Helion and Veritas Continuity through VMware vSphere Desktop Client

1. In the VMware vSphere Desktop Client, click **File** and select **Deploy OVF Template**.
2. Select the source location of the HPE Helion and Veritas Continuity virtual appliance OVA file.
3. Specify a name for the virtual machine and location for the deployed template.
4. Select the host or cluster on which you want to deploy the template.
5. Select a destination where you want to store the virtual machine files.
6. Select the format in which you want to store the virtual disks.
7. If you have multiple networks configured, select the appropriate destination network.
8. Review the virtual machine configuration and click **Finish**.
9. If you want to configure the role of Replication Gateway on this virtual appliance, go to the **Edit virtual machine settings** and attach an external disk of minimum 50 GB.
10. Power on the virtual machine.

To deploy HPE Helion and Veritas Continuity through VMware vSphere Web Client

1. In the VMware vSphere Web Client, click **vCenter Servers** and select a vCenter Server. Click **Actions > Deploy OVF template**.
2. Select the source location of the HPE Helion and Veritas Continuity virtual appliance OVA file.
3. Specify a name and location for the deployed template.
4. Select a cluster, host, vApp, or resource pool in which to run the deployed template.
5. Select a location to store the files for the deployed template.
6. Configure the networks the deployed template should use.
7. Review the virtual machine configuration and click **Finish**.
8. If you want to configure the role of Replication Gateway on this virtual appliance, go to the **Edit virtual machine settings** and attach an external disk of minimum 100 GB. Note that the extra disk is initialized during the product bootstrap process and it may result in deletion of data that may already exist on the disk.
9. Power on the virtual machine.

You can now configure the HPE Helion and Veritas Continuity component.

See "About configuring the HPE Helion and Veritas Continuity components" on page 27.

Chapter 4

Configuring the settings on the virtual appliance

This chapter includes the following topics:

- About configuring the HPE Helion and Veritas Continuity components
- Prerequisites for configuring HPE Helion and Veritas Continuity components
- Configuring an Infrastructure Management Server
- Configuring a Replication Gateway
- Configuring a Storage Proxy

About configuring the HPE Helion and Veritas Continuity components

After the HPE Helion and Veritas Continuity virtual appliance deployment, the product requires you to configure the HPE Helion and Veritas Continuity components.

The following settings are configured for HPE Helion and Veritas Continuity components:

- **Network settings:** Settings such as hostname, IP address, subnet mask, default gateway, DNS server.
- **System settings:** Settings such as timezone and NTP server.
- **Product settings:**
  - Resiliency Manager or IMS: You can choose to configure the virtual appliance for the role of Resiliency Manager, or Infrastructure Management Server (IMS), or both (Resiliency Manager and IMS)

- Replication Gateway or a Storage Proxy: You can choose to configure the virtual appliance for the role of Replication Gateway or a Storage Proxy.

This configuration is done through the product bootstrap only for the first time. After the successful configuration, the product bootstrap is disabled. If you want to change these settings later, you need to use the CLISH menu for changing these settings.

Prerequisites for configuring HPE Helion and Veritas Continuity components

Before configuring the component through product bootstrap, make sure that following prerequisites are met:

- Make sure that you have disabled the dynamic or automatic MAC address change for your hypervisor. Follow the documentation of your hypervisor to set the MAC address manually or to disable the setting for automatic MAC address change.
- Make sure to attach an extra disk of 100 GB before configuring a Replication Gateway.

Configuring an Infrastructure Management Server

Once you have deployed and configured the Resiliency Manager, you need to deploy and configure the Infrastructure Management Server (IMS) in cloud and on-premises. If you have deployed and configured the Resiliency Manager along with the IMS on a single virtual appliance, then you only need to configure an IMS on-premises.

To configure an IMS

1. Log in to the virtual appliance console for the first time using the following credentials:

   - **Username:** admin
   - **Password:** P@ssw0rd

   After a successful login, you need to change the password of the Admin user. The new password that you enter should not be a dictionary word, and must be at least 6 characters long.

2. The product bootstrap is automatically invoked once you change the Admin password. The first step in the product bootstrap is to display the End User License Agreement (EULA). Accept the EULA to proceed with the configuration.

3. In the **Network Settings** section, do one of the following:

- To configure the IMS in cloud, see
- To configure the IMS on-premises, see

Once the network is configured successfully, press enter to go to the **System Settings**.

4. In the **System Settings** section, do the following:
   - Press Enter key to confirm the use of an NTP server for configuring the date and time.
   - You are required to select the timezone. Select the appropriate options to set your timezone and verify the displayed information.
   - Enter the FQDN or IP address of the NTP server.
5. In the **Product Settings** section, enter your choice for configuring the role of Infrastructure Management Server (IMS) on the virtual appliance.
6. After a successful product configuration, a message is displayed.
7. The product comes with the inbuilt SSL certificate. User can create/configure different SSL certificate and use it instead of default SSL:

   https://www.veritas.com/support/en_US/article.000100549

See “Deploying and configuring HPE Helion and Veritas Continuity virtual appliance components” on page 13.

Configuring a Replication Gateway

You need to deploy and configure a Replication Gateway in cloud as well as on-premises. Typically, a Replication Gateway should not be configured on the same virtualization server as the virtual machine to be protected.

To configure a Replication Gateway

1. Log in to the virtual appliance console for the first time using the following credentials:
   - **Username:** admin
   - **Password:** P@ssw0rd

   After a successful login, you need to change the password of the Admin user. The new password that you enter should not be a dictionary word, and must be at least 6 characters long.
2. The bootstrap process is automatically invoked once you change the Admin password. The first step in the bootstrap process is to display the End User License Agreement (EULA). Accept the EULA to proceed with the configuration.

3. In the **Network Settings** section, do one of the following:
   - To configure the IMS in cloud, see
   - To configure the IMS on-premises, see

   Once the network is configured successfully, press enter to go to the **System Settings**.
4. In the **System Settings** section, do the following:
   - Press Enter key to confirm the use of an NTP server for configuring the date and time.
   - You are required to select the timezone. Select the appropriate options to set your timezone and verify the displayed information.
   - Enter the FQDN or IP address of the NTP server.
5. In the **Product Settings** section, enter your choice for configuring the role of Replication Gateway on this virtual appliance.
6. You are prompted to attach an extra disk. If you have already attached the extra disk, press **Enter** key to confirm. Else, attach the extra disk and then confirm or select the extra disk to be used.
7. You are prompted to enter the hostname or IP address of the Infrastructure Management server (IMS) that you want to connect to this Replication Gateway. Enter the required information and the admin password for the IMS.
8. After a successful product configuration, a message is displayed and you are logged out of the virtual appliance console.

See “Deploying and configuring HPE Helion and Veritas Continuity virtual appliance components” on page 13.

Configuring a Storage Proxy

You need to configure a Storage Proxy on-premises in order to enable the failback operation. A Storage Proxy needs to be configured on the same virtualization server that hosts the virtual machines to be protected.

To configure a Storage Proxy

1. Log in to the virtual appliance console for the first time using the following credentials:
   - **Username:** admin
   - **Password:** P@ssw0rd

After a successful login, you need to change the password of the Admin user. The new password that you enter must not be a dictionary word, and must be at least six characters long.

2 The bootstrap process is automatically invoked once you change the Admin password. The first step in the bootstrap process is to display the End User License Agreement (EULA). Accept the EULA to proceed with the configuration.

3 In the **Network Settings** section, you need to enter your choice for the network type. Type **1** for static IP or **2** for static DHCP.

In case of static DHCP, you need to ensure that a Dynamic Host Configuration Protocol (DHCP) server is working in the subnet where the virtual appliance is deployed. In case of static IP, you need to respond to the following additional prompts:

- **Enter the fully qualified hostname:**
- **Enter the IP address:**
- **Enter the Subnet mask:**
- **Enter the Default Gateway:**
- **Enter the DNS server (space separated if more than one DNS, maximum 2 DNS entries):**

Once the network is configured successfully, press enter to go to the **System Settings**.

4 In the **System Settings** section, do the following:

- Press Enter key to confirm the use of an NTP server for configuring the date and time.
- You are required to select the timezone. Select the appropriate options to set your timezone and verify the displayed information.
- Enter the FQDN or IP address of the NTP server.

5 In the **Product Settings** section, enter your choice for configuring the role of Storage Proxy on this virtual appliance.

6 You are prompted to enter the hostname or IP address of the Infrastructure Management server (IMS) that you want to connect to this Storage Proxy. Enter the required information and the admin password for the IMS.

7 After a successful configuration of Storage Proxy, a message is displayed prompting you to enter your choice for shutting down the Storage Proxy as it is required only during failback. Enter **y** to turn off the Storage Proxy and **n** to keep the power on for Storage Proxy. You are then logged out of the virtual appliance console.

See “Deploying and configuring HPE Helion and Veritas Continuity virtual appliance components” on page 13.

Chapter 5

Adding the asset infrastructure to an Infrastructure Management Server (IMS)

This chapter includes the following topics:

- About the asset infrastructure
- Adding the asset infrastructure to an Infrastructure Management Server (IMS)
- Managing host assets for an IMS
- Managing Hyper-V assets for an IMS
- Managing VMware virtualization servers for an IMS
- Managing add-ons for the hosts

About the asset infrastructure

The data center assets that you add to the Infrastructure Management Server (IMS) for IMS discovery and monitoring are referred to as the asset infrastructure.

The asset infrastructure includes Windows or Linux virtual machines and virtualization servers. Both types of assets must be added to the on-premises IMS using the HPE Helion and Veritas Continuity web console.

- Add virtual machines as hosts.
- If using VMware vCenter servers, add them as virtualization servers.

- If using Hyper-V servers, add them as hosts.

See “Managing host assets for an IMS” on page 35.

See “Managing VMware virtualization servers for an IMS” on page 46.

See “Managing Hyper-V assets for an IMS” on page 44.

Once the asset infrastructure is discovered by the IMS, the discovered virtual machines are listed in the console as assets to manage or protect.

In addition, the following must also be added to the IMS:

- The virtualization server used to deploy the on-premises Replication Gateway must be added to the on-premises IMS.
- The cloud server must be added to the cloud IMS, either using the Getting Started wizard or later from the console.

See “Adding the asset infrastructure to an Infrastructure Management Server (IMS)” on page 34.

Adding the asset infrastructure to an Infrastructure Management Server (IMS)

After you add an Infrastructure Management Server (IMS) to the resiliency domain, you add the asset infrastructure to the IMS.

The asset infrastructure is added to the IMS as either hosts or virtualization servers:

See “About the asset infrastructure” on page 33.

To add the asset infrastructure to an IMS

1. Navigate

   ⚙ **Settings** (menu bar) > **Infrastructure**

   You can also access this page from the **Quick Actions** menu > **Manage Asset Infrastructure**.

2. Under the data center, locate the IMS and click **Manage Asset Infrastructure**.

   The **Settings** page for the IMS is displayed. You can add, edit, or remove assets.

   Tip: You must add Hyper-V servers as hosts rather than as virtualization servers.

   See “Managing host assets for an IMS” on page 35.

   See “Managing Hyper-V assets for an IMS” on page 44.

   See “Managing VMware virtualization servers for an IMS” on page 46.

Managing host assets for an IMS

The asset infrastructure that you must add to an Infrastructure Management Server (IMS) can include assets that you add as hosts. The following topics describe the types of assets you add as hosts, the prerequisites, and how to add and remove host assets.

See “About adding host assets to an IMS” on page 36.

See “Prerequisites for adding hosts to an IMS” on page 36.

See “Packages required on Linux hosts” on page 37.

See “Additional prerequisites for protecting virtual machines” on page 38.

See “Adding hosts to an IMS” on page 39.

See “About using a CSV file for adding hosts to an IMS” on page 41.

See “Removing hosts from an IMS ” on page 42.

See “Uninstalling the host package from a Linux host” on page 43.

See “Uninstalling the host package from a Windows host” on page 44.

See “Refreshing host discovery information for an IMS” on page 41.

About adding host assets to an IMS

You add several types of assets as hosts to an Infrastructure Management Server (IMS). All virtual machines that you want to manage and protect must be added to the IMS as hosts. In addition, if Hyper-V servers are used, they are added as hosts, rather than as virtualization servers.

Note: You must add a host to only one IMS.

When you add hosts to an IMS, the IMS installs the host package (VRTSsfmh) on the host. On Linux hosts, the VRTSsfmh package is installed in the /opt directory. On Windows hosts, the VRTSsfmh package is installed in the system drive.

The IMS also installs several add-on packages on the host for use by the IMS discovery:

- HPE Helion and Veritas Continuity Enablement add-on
- Applications Enablement add-on
- Replication add-on

Before you add hosts to the IMS, ensure that all prerequisites are met.

See “Prerequisites for adding hosts to an IMS” on page 36.

Prerequisites for adding hosts to an IMS

Before you add hosts to an Infrastructure Management Server (IMS), ensure that the following prerequisites are met. Prerequisites include general prerequisites for all hosts and additional prerequisites for Linux or Windows systems.

General prerequisites for adding host assets to an IMS:

- Ensure that the IMS can communicate with the host.
- Ensure that the time difference between the system clocks on the IMS and host is no more than 90 minutes. The managed hosts must report synchronized universal time clock time (UC/UTC).
- If a CSV file is used to add hosts, ensure that it uses the correct syntax.
  See “About using a CSV file for adding hosts to an IMS” on page 41.
- Ensure that you install on the virtual machines the software required for replication and disaster recovery.
  See “Additional prerequisites for protecting virtual machines” on page 38.

Additional prerequisites for Linux systems:

- In order to install the host package while adding the Linux host, ensure that the PasswordAuthentication field is set to **yes** in the `/etc/ssh/sshd_config file` on the host.
- Ensure that all required Linux packages are installed on the Linux host.
  See "Packages required on Linux hosts" on page 37.

Additional prerequisites for Windows systems:

- You must manually install the VRTSsfmh host package on one Windows host before you can add the Windows host to the IMS using the web console. You can then add any remaining Windows hosts from the same domain using the console, and the IMS installs the host package on the subsequent Windows hosts.
  See "Installing the host package on a Windows host" on page 40.
- If you install the host package using the web console, you should be a domain user having administrative privileges on the host. If you install the host package manually, then you need to be a local user having administrative privileges on the host.
- The Windows Management Instrumentation (WMI) service must be running.

More information is available about the add host operation.

See "About adding host assets to an IMS" on page 36.

Packages required on Linux hosts

Some packages are required on the Linux hosts as a prerequisite for discovery or operations.

Table 5-1 Packages required on Linux hosts

Package	RHEL6.6	RHEL7.0
NetworkManager	Required by the networking script. Install it from the same source from which the OS is installed	Installed by default.
net-tools	Not required	Required by VMware Tools for ifconfig command.
ntpupdate	Required to update the time in the cloud after a migrate/takeover.	Required to update the time in the cloud after a migrate/takeover.

Table 5-1 Packages required on Linux hosts *(continued)*

Package	RHEL6.6	RHEL7.0
VMware Tools	Required to perform operations on the virtual machines.	Required to perform operations on the virtual machines.
perl	Required to install the VMware Tools.	Required to install the VMware Tools.
openssh-clients	Required to add the Linux host to the Infrastructure Management Server (IMS)	Installed by default.
libstdc++	Installed by default.	Installed by default.
glibc	Installed by default.	Installed by default.
glibc-common	Installed by default.	Installed by default.

Additional prerequisites for protecting virtual machines

Before configuring disaster recovery protection for virtual machines, you should ensure that they meet the following configuration prerequisites. These are in addition to the prerequisites for adding virtual machines to the Infrastructure Management Server (IMS).

See "Prerequisites for adding hosts to an IMS" on page 36.

If you update the virtual machines configuration after adding them to the IMS, you may need to refresh them in the IMS for discovery. Therefore it is recommended to configure the following before adding the virtual machines as hosts to the IMS:

VMware environment	■ Enable the UUID for the virtual machines (disk.enableuuid=true). ■ Ensure that VMware Tools are installed on the virtual machines. See the VMware documentation for information about installing the VMware Tools. **Note:** VMware Tools must also be installed on the Storage Proxy.

Hyper-V environment	■ Ensure that Hyper-V integration services are installed on the virtual machines. See the Hyper-V documentation for information about installing Hyper-V integration services. ■ Ensure that the virtual machines are generation 1. Generation 2 virtual machines are not supported.

In addition, for Windows virtual machines to be protected, virtio drivers must be installed. Since the virtio drivers are bundled with the host package that is installed when you add the virtual machines to the IMS, you would typically do the installation after adding the Windows virtual machines to the IMS.

More information is available on installing virtio drivers on Windows virtual machines.

Adding hosts to an IMS

After adding an Infrastructure Management Server (IMS) to the resiliency domain, you can add host assets to the IMS.

To add hosts to an IMS

1. Prerequisites

   Ensure that you understand the use cases and prerequisites for adding hosts to an IMS.

   See "About adding host assets to an IMS" on page 36.

   See "Prerequisites for adding hosts to an IMS" on page 36.

2. Navigate

   ⚙ **Settings** (menu bar) > **Infrastructure**

   You can also access this page from the **Quick Actions** menu.

3. Under the data center, locate the IMS and click **Manage Asset Infrastructure**.

4. On the IMS **Settings** page, click **Host** to view information on already added hosts, then click **Add Hosts**.

   Or to go directly to the Add Hosts wizard, click **Add Hosts** in the **Settings** page menu bar.

5. In the wizard, select the installation option that corresponds to the platform of the hosts. The appropriate host package is automatically installed on the hosts by the IMS if you continue with the Add Host operation.

- If the host package is already present on the host that is being added, select **None**.
- If you select **Install managed host package on Linux/Unix**, the **Use root password** option is enabled. Select this option if you want to install the host package on a Linux/Unix host as a non-root user. Provide the non-root username, non-root password, and root password for the specified host. You can use this option if the Secure Shell (SSH) access is disabled for the root login on the host where you want to install the host package.
- Before you can add the first Windows host to the IMS, you must manually install the host package on the host. Then add the host using the **None** option in this wizard.
  See "Installing the host package on a Windows host" on page 40.
  After the first Windows host is added, to add more Windows hosts, run the wizard again and select **Install managed host package on Windows**. Then, for **Select Windows Managed Host**, select the host added previously. If there are multiple Windows hosts listed, you can select any one.

6. Choose from the following methods of adding a host:
   - Type the information on the table row. To add a blank table row, click **Add**.
   - Click **Clone** to clone the selected table row, and then edit the clone.
   - To import the information from a CSV file, click **Import**.
7. Verify that the host has been added successfully.
8. In the **Recent tasks** pane, verify that the **Install add-on** tasks for the **HPE Helion and Veritas Continuity Enablement** add-on, **HPE Helion and Veritas Continuity Applications Enablement** add-on, and **HPE Helion and Veritas Continuity Replication** add-on are successfully completed on the host.
9. For Windows hosts, reboot the hosts after successful installation.

If the add-ons are not successfully installed, then you need to manually install them on the host.

See "Installing add-ons on the hosts" on page 55.

See "Managing host assets for an IMS" on page 35.

Installing the host package on a Windows host

Before you can use the wizard in the web console to add Windows hosts to an Infrastructure Management Server, you must first manually install the `VRTSsfmh` host package on at least one Windows host.

Note: By default, the `VRTSsfmh` package is installed in the system drive. You cannot specify a different location to install the package.

To install the host package on a Windows host

1. Log on to the target host as a user with administrator privileges.
2. Make sure that the value for environment variable PATHEXT on the target host includes the extensions .exe, .bat, and .vbs.
3. Download the host installation files bundle, and unzip it.
4. From the directory to which you unzipped the installation files bundle, open an elevated command prompt and run `VRTSsfmh_7.0.0.107_Windows_arch_x64.msi`.
5. On the welcome screen of the Installation Wizard, click **Next**.
6. On the **Ready to Install the Program** screen, click **Install** to start the installation.
7. Click **Finish** to exit the Installation Wizard.

See “Managing host assets for an IMS” on page 35.

About using a CSV file for adding hosts to an IMS

When adding hosts to an Infrastructure Management Server (IMS), you have the option to import the information from a comma-separated (.csv) file. The CSV file must include the “.csv” extension. The following is an example of a CSV file:

```
Host,User,Password
host1.abc.com,username1,password1
host2.abc.com,username2,password2
```

The first line in the CSV file must appear as above. You replace the subsequent lines with your hosts, user names, and passwords.

See “Adding hosts to an IMS” on page 39.

Refreshing host discovery information for an IMS

You can submit a refresh request to update the information displayed for the hosts that have been added to the Infrastructure Management Server (IMS). Once the refresh operation is complete, the Assets page in the console is also updated.

To refresh a host discovery for the IMS

1. Navigate

   ⚙ **Settings** (menu bar) > **Infrastructure**

2. Under the data center, locate the IMS and click **Manage Asset Infrastructure**.
3. On the IMS **Settings** page, click **Host**.
4. Right-click the host (press CRTL to select multiple hosts) and select **Refresh**.
5. Click **OK**.

   The refresh operation is asynchronous. The wizard displays that the operation has triggered the refresh, but the discovery operation is in progress in the background. The Discovery State column shows a status of Refreshing. When it is complete, you can view the status change reflected in the Discovery State column.

See “Managing host assets for an IMS” on page 35.

Removing hosts from an IMS

You can remove one or more hosts that were added to an Infrastructure Management Server (IMS).

If the hosts contain assets that were added to a HPE Helion and Veritas Continuity resiliency group, after you remove the hosts, the assets are no longer shown as part of the resiliency group in the console. However, removing a resiliency group does not remove related hosts from the IMS. Removing hosts and removing resiliency groups are separate operations and can be performed in either sequence.

If Control Host add-on is installed on the host then you need to uninstall the add-on and then remove the host from the IMS.

For more information about resiliency groups, see the Solutions guides.

To remove hosts from an IMS

1 Prerequisites

Before removing a host, you need to uninstall all the add-ons that were installed on the host.

See "Uninstalling add-ons from the hosts" on page 57.

2 Navigate

⚙ **Settings** (menu bar) > **Infrastructure**

3 Under the data center, locate the IMS and click **Manage Asset Infrastructure**.

4 On the IMS **Settings** page, click **Host**.

5 Right-click the host and select **Remove**.

To remove more than one host, hold down **Ctrl** as you select hosts from the list.

6 Confirm that you want to remove the host.

Removing a host from the IMS does not uninstall the host package (VRTSsfmh) from the host. More information is available on uninstalling the host package.

See "Uninstalling the host package from a Linux host" on page 43.

See "Uninstalling the host package from a Windows host" on page 44.

See "Managing host assets for an IMS" on page 35.

Uninstalling the host package from a Linux host

You can use an operating system command to remove the VRTSsfmh package from a Linux host. Before you uninstall the host package, remove the host from the Infrastructure Management Server (IMS).

See "Removing hosts from an IMS " on page 42.

To uninstall the host package from a Linux host

1 Open an operating system console.

2 On the managed host where you plan to uninstall the host package, log on as root.

3 At the command prompt, enter the following command to uninstall the package:

```
rpm -e VRTSsfmh
```

Uninstalling the host package from a Windows host

You can use an operating system command to remove the VRTSsfmh package from a Windows host. Before you uninstall the host package, remove the host from the Infrastructure Management Server (IMS).

See “Removing hosts from an IMS ” on page 42.

To uninstall the host package from a Windows host

1. Log in to the target host as a user with administrator privileges.
2. Go to the Windows **Control Panel**, and click **Programs and Features**.
3. From the list of installed programs, select **Veritas InfoScale Operations Manager (Host Component)**.
4. Do one of the following:
   - Select **Uninstall** at the top of the list.
   - Right click and select **Uninstall**. Click **Yes** to confirm.

Managing Hyper-V assets for an IMS

You can add Hyper-V servers to an Infrastructure Management Server (IMS) for discovery of Hyper-V virtual machines. Hyper-V servers are added as hosts.

See “About Microsoft Hyper-V virtualization discovery” on page 44.

See “Prerequisites for Microsoft Hyper-V virtualization discovery by the IMS” on page 45.

See “Adding hosts to an IMS” on page 39.

See “Managing host assets for an IMS” on page 35.

About Microsoft Hyper-V virtualization discovery

Hyper-V is a hypervisor-based virtualization technology from Microsoft. The Infrastructure Management Server (IMS) can discover Hyper-V host and virtual machine-related information if the Hyper-V role is enabled on the host. The Hyper-V WMI API and Windows PowerShell commandlets are used for the discovery.

Hyper-V discovery can be grouped into the following categories:

- Virtual machine discovery: Discovery of the Hyper-V virtual machines and its correlation with the Hyper-V server.
  When you add the Hyper-V server to the IMS, IMS discovers all virtual machines including the virtual machines without the guest operating system installed.

- Exported storage discovery: Discovery of storage that is provisioned to the guests and its correlation with the virtual machine and Hyper-V server.

  IMS discovers the storage provisioned to the guests from the host's local storage, or storage area network (SAN). The Hyper-V guest, when added to the IMS domain, provides storage mapping discovery.

See "Managing Hyper-V assets for an IMS" on page 44.

Prerequisites for Microsoft Hyper-V virtualization discovery by the IMS

You can add Microsoft Hyper-V servers to an Infrastructure Management Server (IMS) for virtualization discovery.

Note: When adding Hyper-V servers to the IMS in the console, you choose the option to add hosts rather than to add virtualization servers.

For information on supported operating system versions for the Hyper-V Server, refer to the *Hardware and Software Compatibility List (HSCL)*.

Table 5-2 Requirements for Microsoft Hyper-V virtualization discovery

Type of discovery	Requirements
Virtual machine discovery	■ The `VRTSsfmh` package must be installed on the Hyper-V Server (parent partition). This is done automatically by the IMS when you add the Hyper-V server to the IMS as a host. ■ The Hyper-V role must be enabled. ■ The Windows Management Instrumentation (WMI) service must be running on the Hyper-V Server. There are additional prerequisites for adding hosts to an IMS. See "Prerequisites for adding hosts to an IMS" on page 36. In addition to the Hyper-V Server, the virtual machines to be protected must also be added as hosts.
Exported storage discovery	■ The Windows Management Instrumentation (WMI) service must be running on the guest.

See "Managing Hyper-V assets for an IMS" on page 44.

See "Managing host assets for an IMS" on page 35.

Managing VMware virtualization servers for an IMS

You can add VMware vCenter servers to an Infrastructure Management Server (IMS) for VMware discovery.

The VMware discovery provides the following the vCenter server information:

- Information on vCenter servers
- Information on the ESX servers managed by the vCenter servers
- Information on the virtual machines that are configured on the ESX servers

See "Prerequisites for adding VMware servers for discovery by the IMS" on page 46.

See "Adding virtualization servers for VMware discovery by the IMS" on page 51.

See "Editing a VMware virtualization discovery configuration in the IMS" on page 53.

See "Removing a virtualization discovery configuration from the IMS" on page 54.

See "Refreshing a VMware virtualization discovery configuration" on page 54.

See "Refreshing an ESX Server discovery" on page 54.

Prerequisites for adding VMware servers for discovery by the IMS

Ensure that the following requirements are met to add the VMware vCenter or ESX servers to the Infrastructure Management Server (IMS):

- Ensure that the IMS server can ping the vCenter servers or the ESX servers from which it can discover the information on VMware Infrastructure.

  Optionally, you can add a separate host to act as the Control Host for the vCenter Server.
- Ensure that you have configured near real-time discovery of VMware events.

  See "About near real-time discovery of VMware events" on page 47.

  See "Setting up near real-time discovery of VMware events" on page 49.

  See "Configuring the VMware vCenter Server to generate SNMP traps" on page 50.
- Ensure that the vCenter Server user account that is used to add the servers to IMS has the following privileges assigned:
  - System.Anonymous
  - System.View
  - System.Read
  - Datastore.FileManagement

- Datastore.Allocate space
- Datastore.Browse datastore
- Host.Configuration.Settings
- Host.Configuration.Network configuration
- Host.Local operations.Reconfigure virtual machine
- Virtual Machine.Configuration.Add new disk
- Virtual Machine.Configuration.Add existing disk
- Virtual Machine.Configuration.Add or remove device
- Virtual Machine.Configuration.Remove disk
- Virtual Machine.Configuration.Extend virtual disk
- Virtual Machine.Interaction.Power Off
- Virtual Machine.Interaction.Power On
- Virtual Machine.Inventory.Register

There are additional requirements for virtual machines if added to the IMS, depending on the use case.

See “Prerequisites for adding hosts to an IMS” on page 36.

About near real-time discovery of VMware events

The Infrastructure Management Server (IMS) uses VMware events to discover in near real-time a change in the state of a virtual machine (for example, virtual machine powered on) and changes occurring at the vCenter Server infrastructure level (for example, virtual machine created).

To set up the near real-time discovery of VMware events by the IMS, you must configure the vCenter Server to generate SNMP traps and send them to the IMS address. The recommended sequence is to do this before adding the vCenter Server to the IMS.

See “Setting up near real-time discovery of VMware events” on page 49.

The near real-time discovery of VMware infrastructure enables the partial discovery of ESX servers managed under a vCenter Server. This discovery is triggered by the event notification from the VMware vCenter Server to the IMS using SNMP traps. For example, if an SNMP trap is received for a virtual machine (VM1) hosted on ESX1, the IMS runs the discovery cycle only for ESX1. Other ESX servers under that vCenter Server are not re-discovered.

The IMS component of near real-time discovery is `xtrapd`. After you configure a vCenter Server to send the SNMP traps to the IMS, you add the vCenter Server to the IMS. The `xtrapd` daemon now detects the SNMP traps that are sent from the specified vCenter Server. The HPE Helion and Veritas Continuity database and console are updated with the latest state of the virtual machine or infrastructure changes.

Note: SNMP version 1 (SNMPv1) and version 2 (SNMPv2) are supported.

For details on supported events, see the following table.

Table 5-3 Supported events for near-real time discovery

Discovered state	Event as shown in VMware vCenter Server
Virtual machine powered on	VM powered on
Virtual machine powered off	VM powered off
Virtual machine Distributed Resource Scheduler (DRS) powered on	DRS VM powered on
Virtual machine suspended	VM suspended
Virtual machine created	VM created
Virtual machine migrated Hot migration: A powered-on virtual machine is migrated from one ESX server to another ESX server.	VM migrated
Virtual machine relocated from one ESX server to another Cold migration: A powered-off virtual machine is migrated from one ESX server to another ESX server.	VM relocating
Virtual machine renamed	VM renamed
Virtual machine migrated to another host by VMware DRS (Distributed Resource Scheduler)	DRS VM migrated

Setting up near real-time discovery of VMware events

To set up the near real-time discovery of VMware events, complete the following steps.

Table 5-4 Setting up near real-time (NRT) discovery of VMware events

Step	Action	Description
Using VMware vCenter Server console:		
Step 1	In the vCenter Server console, provide IMS details and configure the alarm for sending the SNMP traps.	Configure the IMS address as the SNMP trap receiver URL. Also configure the alarm to send the SNMP traps when the state of the virtual machine changes. See "Configuring the VMware vCenter Server to generate SNMP traps" on page 50.
Using the HPE Helion and Veritas Continuity console:		
Step 2	Add the vCenter Server to the IMS as a virtualization server.	See "Adding virtualization servers for VMware discovery by the IMS" on page 51. After you add the vCenter Server to the IMS, the `xtrapd` daemon on the IMS starts accepting SNMP traps from the specified vCenter Server. **Note:** If you have not configured the vCenter Server as in step 1 before adding it to the IMS, a warning message is displayed. It does not affect the vCenter Server discovery. However, near real-time discovery of VMware events is not functional. To enable the near real-time discovery subsequently, first configure the vCenter Server. Then refresh the vCenter Server configuration in the IMS using the HPE Helion and Veritas Continuity console. See "Refreshing a VMware virtualization discovery configuration" on page 54.

By default, near real-time discovery of VMware events is enabled. To disable it, you need to remove the IMS as the SNMP receiver in the vCenter Server and refresh the vCenter Server configuration in the IMS.

See "About near real-time discovery of VMware events" on page 47.

Configuring the VMware vCenter Server to generate SNMP traps

In the VMware vCenter Server console, provide the following information to configure the vCenter Server to generate SNMP traps and send them to the IMS:

- Configure the Infrastructure Management Server (IMS) as the SNMP trap receiver, as follows:
  Navigate to the SNMP configuration. Enable one of the SNMP receivers and enter the following details:

Field	Description
Receiver URL	Provide the host name of the IMS which will be connected to the vCenter Server. The vCenter Server sends the SNMP traps to this IMS. Also, configure port 162 as the SNMP port. Ensure that port 162 is not used by any other application in IMS.
Community String	Provide community string. SNMP versions v1 and v2 are supported.

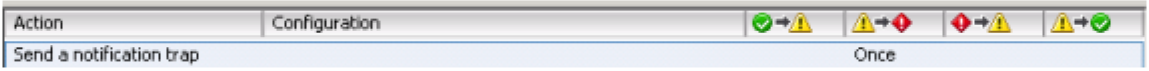
- Configure an alarm for generating SNMP traps when a virtual machine state changes or any virtual infrastructure-related change occurs.
  This step includes adding an alarm to monitor the changes related to virtual machine state and vCenter Server infrastructure, and then adding the appropriate action (for example, send a notification trap).
  - You can set the alarm at an individual virtual machine level, at the data center level, or at the entire VMware vCenter Server level. It is recommended to set it at the vCenter Server level.
  - For the alarm type details, make sure to specify the following
    - Set the alarm type to monitor virtual machines
    - Set the alarm to monitor for specific events occurring on this object, for example, VM powered on
    - Enable the alarm
  - Add the required triggers to monitor the states of the virtual machine. For example, VM created, VM migrated, VM powered on, VM powered off, VM suspended, DRS VM powered on (for clustered environment with DRS enabled) and so on. The values of the fields are as follows:

For the following value of an event...	Select the following status...
VM powered on	Unset
VM powered off	Unset
DRS VM powered on	Unset
VM suspended	Unset
VM created	Unset
VM migrated	Unset
VM relocating	Unset
VM renamed	Unset
DRS VM migrated	Unset

- Add the required triggers to monitor the states of the hosts. The values of the fields are as follows:

For the following value of an event...	Select the following status...
Host disconnected	Unset
Host connected	Unset

- Add a new action to send a notification trap. Specify to send the notification trap as in the following example:



Action	Configuration	✓→⚠	⚠→◆	◆→⚠	⚠→✓
Send a notification trap			Once		

See “About near real-time discovery of VMware events” on page 47.

See “Setting up near real-time discovery of VMware events” on page 49.

Adding virtualization servers for VMware discovery by the IMS

You can add VMware vCenter servers to an Infrastructure Management Server (IMS) for VMware discovery.

The VMware discovery provides the following information:

- Information on vCenter servers

- Information on the ESX servers that the vCenter Server manages

  When adding a vCenter Server, you have the option to automatically discover all ESX servers registered to the vCenter Server or manually specify names of selected ESX servers to discover.

- Information on the virtual machines that are configured on the ESX servers

Optionally, you can add a separate host to act as the Control Host for the vCenter Server, and then select that host while adding the virtualization server.

To add a virtualization server for VMware discovery by the IMS

1 Prerequisites:

See “Prerequisites for adding VMware servers for discovery by the IMS” on page 46.

2 Navigate

⚙ **Settings** (menu bar) > **Infrastructure**

You can also access this page from the **Quick Actions** menu.

3 Under the data center, locate the IMS and click **Manage Asset Infrastructure**.

4 On the IMS **Settings** page, click **Virtualization** to view information on existing virtualization servers, then click **Add Virtualization Server**.

Or to go directly to the Add Virtualization Server wizard, click **Add Virtualization Server** in the **Settings** page menu bar.

5 In the wizard, specify the information for the vCenter Server and click **Next**.

Tips:

- For Configuration Name, specify a name that will help you identify this configuration
- Specify the fully-qualified name of the vCenter Server that you want to discover along with its port number, separated by a colon. If the vCenter Web service is running on a default port, you do not need to specify the port number.
- When entering login credentials, an administrative vCenter Server user account is required.

6 Choose to automatically discover all ESX servers or manually specify names of ESX servers to discover. Click **Finish**.

7. In the **Result** panel, view the progress of the configuration. After the configuration is complete, click **OK**.
8. After you add a vCenter Server, to view all ESX servers that the vCenter Server manages, click **vCenter** under **Data Center**.

If any changes are made on the virtualization server after adding it to the IMS, you need to refresh the server discovery configuration.

See “Refreshing a VMware virtualization discovery configuration” on page 54.

Editing a VMware virtualization discovery configuration in the IMS

You can edit a virtualization discovery configuration in the Infrastructure Management Server (IMS) to modify the following information:

- Name of the configuration.
- Credentials to log on to the vCenter.
  When entering the username, you must enter in the format username@domainname, not domainname\username.

To edit a virtualization discovery configuration in the IMS

1. Navigate

   ⚙ **Settings** (menu bar) > **Infrastructure**

2. Under the data center, locate the IMS and click **Manage Asset Infrastructure**.
3. On the IMS **Settings** page, click **Virtualization**.
4. In the **Virtualization Configurations** details list, right-click the configuration that you want to edit.
5. In the **Edit Configuration** wizard panel, modify the required information, click **Next**.
6. In the **Edit Configuration** wizard panel, edit the method for virtualization discovery of the servers, click **Finish**.
7. In the **Result** panel, view the progress of the configuration, click **OK**.

See “Managing VMware virtualization servers for an IMS” on page 46.

Removing a virtualization discovery configuration from the IMS

To remove a virtualization discovery configuration from the IMS

1 Navigate

⚙ **Settings** (menu bar) > **Infrastructure**

2 Under the data center, locate the IMS and click **Manage Asset Infrastructure**.

3 On the IMS **Settings** page, click **Virtualization**.

4 Right-click the virtualization server and select **Remove Configuration**.

5 In the **Remove Virtualization Configuration** wizard panel, click **Remove**.

6 In the **Result** panel, click **OK**.

See “Managing VMware virtualization servers for an IMS” on page 46.

Refreshing a VMware virtualization discovery configuration

You can submit a refresh request to update the information displayed on the table of virtualization servers that have been added to the Infrastructure Management Server (IMS).

To refresh a virtualization discovery configuration

1 Navigate

⚙ **Settings** (menu bar) > **Infrastructure**

2 Under the data center, locate the IMS and click **Manage Asset Infrastructure**.

3 On the IMS **Settings** page, click **Virtualization**.

4 Right-click the virtualization configuration and select **Refresh Configuration**.

5 In the **Refresh Virtualization Configuration** wizard panel, click **Refresh**.

6 In the **Result** panel, click **OK**.

See “Managing VMware virtualization servers for an IMS” on page 46.

Refreshing an ESX Server discovery

You can refresh the Infrastructure Management Server (IMS) discovery of one or more ESX servers that are configured under a selected VMware vCenter Server.

To refresh the discovery of an ESX server

1 Navigate

⚙ **Settings** (menu bar) > **Infrastructure**

2 Under the data center, locate the IMS and click **Manage Asset Infrastructure**.

3 On the IMS **Settings** page, click **Virtualization**.

4 Under the **Virtualization Configurations** tab, you can view the details of virtualization configuration. For example, the name of the virtualization server (vCenter Server) used in the configuration, its type, and other parameters. Select the desired virtualization configuration.

5 The **Configured Virtualization Servers** tab lists the ESX servers managed under the vCenter Server that is part of the selected virtualization configuration.

6 Right-click the required ESX server and click **Refresh.** Press Ctrl or Shift for the selection of multiple ESX servers.

7 In the **Refresh Virtualization Server** wizard panel, click **Refresh**.

8 In the **Result** panel, click **OK**.

See “Managing VMware virtualization servers for an IMS” on page 46.

Managing add-ons for the hosts

Infrastructure Management Server (IMS) installs a host package and the following add-ons when you add hosts to the IMS.

- Enablement add-on
- Applications Enablement add-on
- Replication add-on

In some cases you may need to install add-ons manually. In addition, before removing the host package from hosts, you must uninstall the add-ons.

See “Installing add-ons on the hosts” on page 55.

See “Uninstalling add-ons from the hosts” on page 57.

Installing add-ons on the hosts

You can install the add-ons on the hosts that are added to the Infrastructure Management Server (IMS).

To install add-ons on the hosts

1 Navigate

⚙ **Settings** (menu bar) > **Infrastructure**

(Or, click **Quick Actions** (menu bar) > **Add Assets**)

2 Under the data center, locate the IMS and click **Manage Assets**.

3 On the IMS **Settings** page, click **Deployment**.

4 Expand **Add-ons** to select the add-on that you want to install.

5 In the **Add-ons** tab, right-click the add-on, and select **Install**.

6 In the **Install - Selects hosts** wizard panel, select the hosts, and click **Finish**.

See "Install - Select hosts panel options for add-ons" on page 56.

7 In the **Result** panel, click **Close**

8 Those add-ons which require web server restart, click **Restart Web server**.

Install - Select hosts panel options for add-ons

Use this wizard panel to select the hosts on which you want to install the add-on.

You can do one of the following:

- Select the hosts explicitly and install the add-on on the selected hosts.
- Select the platform.

If you select a specific platform, the add-on is installed on all the hosts using that platform. Also the add-on is installed on all the new hosts that are added to the IMS in the future.

For example, if you select Windows, the add-on is installed on all the hosts that use Windows platform. Also when a new Windows host is added to the IMS, the add-on is installed on the host.

Table 5-5 Select hosts panel options

Field	Description
Hosts	Select to view the list of all the hosts where the add-on is not installed. Select **Show all applicable hosts (Overwrites existing installation)** to list all the hosts on which you can install the add-on. It includes: ■ Hosts on which the add-on is not installed currently. ■ Hosts on which the add-on is installed currently. In this case, the existing add-on installation is overwritten.
Platform	Select to install the add-on on all the hosts using the specific platform. This option is useful for installing the add-on whenever a new host using the specific platform is added to the IMS. Select **Force install (Overwrites existing installation)** to overwrite existing add-on installation on the hosts.

See “Installing add-ons on the hosts” on page 55.

Uninstalling add-ons from the hosts

You need to manually uninstall all the add-ons before you uninstall the host packages from the Infrastructure Management Server (IMS).

Select **Ignore checks (if any) before uninstalling** if you want to remove all the configurations of the add-on. For example, if vCenter is discovered using Control Host add-on, then when you uninstall the add-on, the vCenter configuration is also removed.

To uninstall add-ons from the hosts

1. Navigate

   ⚙ **Settings** (menu bar) > **Infrastructure**

   (Or, click **Quick Actions** (menu bar) > **Add Assets**)

2. Under the data center, locate the IMS and click **Manage Assets**.
3. On the IMS **Settings** page, click **Deployment**.
4. Expand **Add-ons** to select the add-on that you want to uninstall.
5. In the **Add-ons** tab, right-click the add-on, and select **Uninstall**.
6. In the **Uninstall** panel, confirm the action of uninstalling the add-on from all the hosts. Select **Ignore checks (if any) before uninstalling** to ignore the checks before uninstalling.
7. Click Yes to uninstall the add-on from all the hosts.

You need to the reboot the host after you have uninstalled the Replication add-on to remove the redundant data related to replication that may appear.

Managing users and global settings

This chapter includes the following topics:

- Managing user authentication and permissions
- Managing settings for alerts and notifications and general product settings

Managing user authentication and permissions

HPE Helion and Veritas Continuity provides a console for viewing information and performing operations. Managing user authentication and permissions for the console involves the following tasks.

Table 6-1 Process for setting up user authentication and permissions

Task	Details
Configure authentication domains	You can add multiple authentication domains. See "About user authentication in the web console" on page 60. See "Configuring authentication domains " on page 66. See "Unconfiguring authentication domains" on page 68.
Configure user groups and users	Once you configure an authentication domain, you can configure user groups or users for HPE Helion and Veritas Continuity from that authentication domain. See "Configuring user groups and users" on page 69.

Table 6-1 Process for setting up user authentication and permissions *(continued)*

Task	Details
Assign permissions to groups and users	When you configure user groups or users for HPE Helion and Veritas Continuity, they are by default assigned the Guest persona, which gives permission to view information in the web console. Permission to perform operations in the console requires assigning additional personas. For some personas, you can also limit the scope of the operation to selected objects, for example, resiliency groups. See "About user permissions in the web console" on page 61. See "Predefined personas" on page 62. See "About limiting object scope for personas" on page 65. See "Assigning permissions to user groups and users" on page 69. You can also create custom personas. See "Adding custom personas" on page 71. See "Predefined jobs that can be used for custom personas" on page 72. See "Custom persona required for starting or stopping resiliency groups" on page 74.

About user authentication in the web console

By default, the Admin user of the HPE Helion and Veritas Continuity virtual appliance can log in to the web console with access to all views and operations.

The Admin user can configure authentication domains from external identity providers such as Active Directory (AD) and LDAP.

Once an authentication domain is configured, the Admin user can configure user groups and users for HPE Helion and Veritas Continuity from that domain. These users can log in to the console with their domain login credentials.

All users and groups that are configured for HPE Helion and Veritas Continuity have permission by default to view everything in the web console but not to perform any operations. Permissions for operations must be assigned separately by assigning the appropriate personas to users and groups.

Note: You need to define the user policies such as Account lockout policy in LDAP.

See “Managing user authentication and permissions” on page 59.

About user permissions in the web console

HPE Helion and Veritas Continuity uses the concepts of personas, job, and objects to define permissions for users in the web console.

Persona

A role that has access to a predefined set of jobs (operations).

The product comes with a set of predefined personas.

See “Predefined personas” on page 62.

You can also add custom personas.

See “Adding custom personas” on page 71.

See “Predefined jobs that can be used for custom personas” on page 72.

All users and groups that are added to HPE Helion and Veritas Continuity have the Guest persona by default. The Guest persona allows users to view everything in the web console but not to perform any operations.

Job

A type of task (operation) that a user can perform.

Examples:

Manage resiliency groups

Manage assets

Perform disaster recovery of resiliency groups

Object types and scope

Each job can be performed on certain types of HPE Helion and Veritas Continuity objects. Types of objects include data centers, resiliency groups, and virtual business services.

See “About HPE Helion and Veritas Continuity features and components” on page 9.

When you assign a persona to a user or group, you define the scope of some jobs by selecting from available objects. For some jobs, the scope is the resiliency domain, which would be the entire scope of the product deployment.

If you want a user to have permissions that are different from the user group to which they belong, you must add the user individually to HPE Helion and Veritas

Continuity. Permissions assigned at the individual user level override the permissions that the user has as a user group member.

If a user tries to perform an operation for which they do not have authorization, a message is displayed to notify them of the fact; in addition an entry for "authorization check failed" is available in the audit logs.

See “Managing user authentication and permissions” on page 59.

Predefined personas

The following table lists the predefined personas for HPE Helion and Veritas Continuity and their associated jobs and objects. You can assign one or more of these personas to a user or user group to define permissions. Some jobs let you limit the scope by specifying the assets (resiliency groups) on which permissions are assigned.

You can also create custom versions of these personas, except for the Guest and Super admin persona.

Table 6-2 Predefined personas and jobs

Persona	Description and scope	Jobs
Super admin	Can perform all operations on all objects in resiliency domain.	All jobs All objects in resiliency domain
Resiliency Platform admin	Manage Resiliency Managers and Infrastructure Management Servers (IMSs) and data centers. Manage assets for the IMS. Manage user security settings and other product settings. Manage product updates. Scope: Resiliency domain.	Manage assets Manage user security settings Manage product settings Manage product updates Manage server deployments

Table 6-2 Predefined personas and jobs *(continued)*

Persona	Description and scope	Jobs
Resiliency Platform Deployment admin	Manage Resiliency Managers and Infrastructure Management Servers (IMSs). Can add an IMS to an existing data center but not add a new data center to the Resiliency Manager. Manage product updates. Scope: Resiliency domain.	Manage product updates Manage server deployments
Data Center admin	Manage IMS assets and manage disaster recovery settings. Scope: Specified data center.	Manage assets Manage disaster recovery settings
Resiliency Domain admin	Create, update, and delete resiliency groups, virtual business services (VBSs), and resiliency plans and templates. Manage and perform disaster recovery on all resiliency groups and VBSs. Scope: Resiliency domain.	Manage resiliency groups Manage virtual business services (VBSs) Manage resiliency plan templates Manage resiliency plans Manage disaster recovery of resiliency groups Perform disaster recovery of resiliency groups Manage disaster recovery settings

Table 6-2 Predefined personas and jobs *(continued)*

Persona	Description and scope	Jobs
Resiliency Group admin	Update and delete specified resiliency groups. Manage and perform disaster recovery of resiliency groups Perform disaster recovery operations on VBSs as long as the VBS contains only the specified resiliency groups. Scope: Specified resiliency groups.	Manage resiliency groups Manage disaster recovery of resiliency groups Perform disaster recovery of resiliency groups **Note:** There is no separate job to perform disaster recovery of VBSs. If the VBS contains only the specified resiliency groups, DR operations can be performed on it. See "About limiting object scope for personas" on page 65.
Resiliency Group operator	Perform disaster recovery on specified resiliency groups. Perform disaster recovery operations on VBSs as long as the VBS contains only the specified resiliency groups. Scope: Specified resiliency groups.	Perform disaster recovery of resiliency groups **Note:** There is no separate job to perform disaster recovery of VBSs. If the VBS contains only the specified resiliency groups, DR operations can be performed on it. See "About limiting object scope for personas" on page 65.
VBS admin	Create, update, and delete all virtual business services (VBSs). Scope: Resiliency domain.	Manage virtual business services (VBSs) **Note:** This persona does not include permission to perform DR operations on VBSs.

Table 6-2 Predefined personas and jobs *(continued)*

Persona	Description and scope	Jobs
Guest	View all information in console. Assigned by default when user or group is configured for HPE Helion and Veritas Continuity.	No operations, only view permission

See "Managing user authentication and permissions" on page 59.

About limiting object scope for personas

For some personas, HPE Helion and Veritas Continuity lets you select a subset of objects such as resiliency groups to limit the scope of operations.

See "Predefined personas" on page 62.

For example, you can assign one user the permission to perform operations on resiliency group RG1 and assign another user the permission to perform operations on RG2.

When planning persona assignments in which you select objects to limit the scope, take the following into account:

- Before you can select the objects such as resiliency groups to limit the scope of operations for a persona, the objects must first be created in HPE Helion and Veritas Continuity.
- You need to plan for future maintenance on such limited scope personas. If more objects of that type are added later, you may need to edit existing personas for users or user groups in order to add permissions for the new objects.
- Keep in mind that operations on virtual business services (VBSs) that include multiple resiliency groups will fail unless the user performing the operation has permission for operations on all the resiliency groups in the VBS.
  The same limitation applies for workflow or resiliency plan operations that include multiple resiliency groups.
  For example: a VBS is composed of RG1 and RG2. The operator has permission to perform operations on RG1 but not RG2. If they try to perform operations on the VBS, the operation will fail.

Configuring authentication domains

By default, the Admin user on the HPE Helion and Veritas Continuity virtual appliance can log in to the HPE Helion and Veritas Continuity web console with access to all views and operations. The Admin user can configure authentication domains for HPE Helion and Veritas Continuity from external identity providers so that other users can be authenticated for access to the console.

To configure authentication domains

1. Prerequisites

   The fully qualified domain name (FQDN) or IP address and credentials for the LDAP/AD server

2. Navigate

   ⚙ **Settings** (menu bar)

   Under **Product Settings**, click **User Management > Domains**

   Note: You can also configure an authentication domain from the Getting Started wizard after setting up the Resiliency Manager and resiliency domain.

   ---

3. Click **Configure Domain**.

   Note: To edit an existing authentication domain, right-click it and select the appropriate option.

4. Enter the information in the **Provide Inputs** panel and click **Next**.

   See “Options for Configure Domain” on page 67.

5. Verify the organization unit name in **Search Base** and enter a friendly name for the authentication domain. Click **Submit**.

   Note: The **Search Base** field contains the name of the organization unit to which you belong. If you want to add or remove users from other organization units, then you need to delete the organization unit name.

   ---

6. Verify that the new domain is listed under **Domains**.

   You can now configure user groups and users from that domain and assign permissions.

See “Managing user authentication and permissions” on page 59.

Options for Configure Domain

Table 6-3 Options for Configure Domain

Option	Description
Server Name (Mandatory)	Enter the fully-qualified host name or IP address of the LDAP server. If a secure session is configured with the LDAP server using SSL certificates, you must enter the fully-qualified host name that matches with the fully-qualified host name in the LDAP server certificate.
Port (Mandatory)	Displays the number of the port on which the LDAP server is configured to run. By default, this field displays the port number as 389. You can edit this port number, if required.
This server requires me to log on.	Select this check box if the anonymous operations are disabled on the LDAP server and a bind user ID is required to proceed with configuring the LDAP-based authentication
Bind User Name/DN	Enter the complete Distinguished Name (DN) of the user that is used to bind to the LDAP server. If the LDAP server being used is Active Directory (AD), you can provide the DN in the following formats: username@domainname.com or domainname\username For example, you can provide the DN as Administrator@enterprise.domainname.com ENTERPRISE\Administrator For RFC 2307 compliant LDAP servers, specify complete bind DN. For example, cn=Manager,dc=vss,dc=Veritas,dc=com The LDAP or the AD administrator can provide you the bind user name that you can use.
Password	Enter the password that is assigned to the bind user name that you use.
Use Secure Sockets Layer	Select this check box to use the Secure Sockets Layer (SSL) certificates to establish a secure channel between the authentication broker and the LDAP server.
Certificate location	Browse to the location of the trusted root CA certificate of the vendor that issued the LDAP server certificate.
Query Information:	

Table 6-3 Options for Configure Domain *(continued)*

Option	Description
User (Mandatory)	Enter the user name based on which the system detects the LDAP server-related settings. Ensure that the user name does not contain any special characters. The system determines the search base based on the user name that you specify in this field.
Group	Enter the name of the user group based on which the system detects the LDAP server-related settings. Ensure that the group name does not contain any special characters. The system determines the search base based on the group name along with the user name that you have specified.

See “Configuring authentication domains ” on page 66.

Unconfiguring authentication domains

If an authentication domain is no longer applicable for a data center you can unconfigure it (remove it from HPE Helion and Veritas Continuity).

Warning: Any users or user groups that you added from that domain are also removed from HPE Helion and Veritas Continuity when you unconfigure an authentication domain.

To unconfigure an authentication domain

1 Navigate

⚙ **Settings** (menu bar)

Under **Product Settings**, click **User Management > Domains**

2 Right-click the domain and select **Unconfigure**.

3 Verify that the domain is removed under **Domains**.

See “Managing user authentication and permissions” on page 59.

Configuring user groups and users

After you configure an authentication domain for HPE Helion and Veritas Continuity, you can configure user groups and users for HPE Helion and Veritas Continuity from that domain.

If you want to assign permissions to a user that are different from the user group as a whole, you must configure the user separately from the group.

To configure user groups and users

1 Prerequisites

The names of the user groups or users that you want to configure, as configured in the authentication domain.

2 Navigate

⚙ **Settings** (menu bar)

Under **Product Settings**, click **User Management > Users & Groups**

Note: To edit or remove an existing user or group, right-click the name in the list and select the appropriate option.

3 Click **Configure User or Group**.

4 Select the authentication domain.

5 Type the name of the user group or user. Click **Verify** so that the wizard can verify the name in the domain.

6 Click **Submit** and verify that the group or user is listed under **Users & Groups**.

All groups and users that are added have the default persona of Guest. You can add other permissions.

See “Assigning permissions to user groups and users” on page 69.

See “Managing user authentication and permissions” on page 59.

Assigning permissions to user groups and users

In HPE Helion and Veritas Continuity, permissions use the concept of personas and jobs. When you first add user groups and users to HPE Helion and Veritas Continuity, they are assigned the Guest persona, which allows views but no operations. You can assign other permissions. For each persona, there is a set of jobs (operations) and for some jobs, you select objects.

See “About user permissions in the web console” on page 61.

To assign permissions to user groups and users

1 Prerequisites

The users and groups must be added to HPE Helion and Veritas Continuity before you can assign personas.

See “Configuring user groups and users” on page 69.'

2 Navigate

⚙ **Settings** (menu bar)

Under **Product Settings**, click **User Management > Users & Groups**

3 Double-click the user group or user.

4 Click **Assign Persona**.

5 In the **Assign Persona** page, you can assign one persona at a time. Complete the following steps:

- Select a persona that you want to assign to that user group or user.
- Verify that you want to assign the jobs that are listed for that persona.
- Under **Objects**, view the available objects on which jobs can be performed. To assign permission to selected objects, drag them from the left grid to the left grid. If there are multiple object types, they are listed on separate tabs. Click any remaining tab and select the objects.
- Click **Submit**.

6 Verify that the correct persona name and associated objects are listed on the user details page.

To edit permissions or unassign personas

1 Navigate

⚙ **Settings** (menu bar)

Under **Product Settings**, click **User Management > Users & Groups**

2 Double-click the user or group.

3 On the details page for the user or group, right-click the persona that you want to unassign or edit, and select the appropriate option.

See “Managing user authentication and permissions” on page 59.

Adding custom personas

HPE Helion and Veritas Continuity provides a set of predefined personas with access to predefined jobs.

You can add custom personas by selecting from the predefined jobs.

For example, the predefined persona Resiliency Platform Admin includes the jobs for managing assets, managing security settings, and managing product settings. You could create an "Asset Manager" persona that includes only the managing assets job.

You cannot customize the Super admin persona, which has access to all jobs and all objects in the resiliency domain. You also cannot customize the Guest persona, which can view all information in the console.

To add custom personas

1. Navigate

   ⚙ **Settings** (menu bar)

   Under **Product Settings**, click **User Management > Persona & Jobs** > **Add Persona**

2. In the **Add Persona** page, complete the following steps and submit:

   - Assign a name and description to the custom persona.
   - Select one or more jobs that you want to assign to the persona. The jobs are shown in categories depending on whether the scope is the entire resiliency domain or whether the scope can be customized to specific data centers or assets. Select the job from the appropriate category.
     For example, if you want to assign a permission related to managing any resiliency group in the resiliency domain, select **Manage Resiliency Group** under the category of **For entire Resiliency Domain**. But if you want to limit permissions to specific resiliency groups, select **Manage Resiliency Group** under the category **For specific resiliency groups**.
     See “Predefined jobs that can be used for custom personas” on page 72.

3. Verify that the correct persona name and associated jobs are listed.

   You can now assign this persona to users or user groups.

See “Managing user authentication and permissions” on page 59.

Predefined jobs that can be used for custom personas

The following table lists the predefined jobs that you can use to create custom personas for HPE Helion and Veritas Continuity. The jobs are categorized as to whether they provide permissions for the entire resiliency domain or can be customized to specific data centers or assets.

Table 6-4 Jobs for custom personas

Job	Description	Scope
View all information	View all information in console.	Resiliency domain
Manage assets	Add assets to the IMS, remove assets that were added previously.	Resiliency domain or specific data centers
Manage user security settings	Manage authentication domains, users and user groups, personas.	Resiliency domain
Manage product settings	Manage general product settings such as alerts and notifications.	Resiliency domain
Manage server deployments	Edit Resiliency Manager information. Manage IMSs, including add, remove, edit, reconnect operations.	Resiliency domain
Manage product updates	Perform the operations available from the Product Updates page of the console.	Resiliency domain
Manage resiliency groups	Create, update, and delete resiliency groups.	Resiliency domain or specific resiliency groups
Start/stop resiliency groups	Start/stop resiliency groups.	Resiliency domain or specific resiliency groups
Manage virtual business services (VBSs)	Create, update, and delete virtual business services (VBSs).	Resiliency domain or specific VBSs

Table 6-4 Jobs for custom personas *(continued)*

Job	Description	Scope
Manage resiliency plans	Create, update, and delete resiliency plans. **Note:** The permission to execute a resiliency plan depends on a cumulative check on permissions for individual resiliency groups and VBSs in the plan. See "About limiting object scope for personas" on page 65.	Resiliency domain
Manage resiliency plan templates	Create, update, and delete resiliency plan templates.	Resiliency domain
Execute custom script	Execute custom scripts as part of resiliency plans.	Resiliency domain or specific data centers
Manage disaster recovery of resiliency groups	Configure resiliency groups for disaster recovery (DR).	Resiliency domain or specific resiliency groups
Perform disaster recovery of resiliency groups	Perform DR operations: migrate, takeover, rehearsal **Note:** There is no separate job to perform disaster recovery of VBSs. If the assigned scope of this job includes all the resiliency groups in a VBS, DR operations can be performed on that VBS. See "About limiting object scope for personas" on page 65.	Resiliency domain or specific resiliency groups
Manage disaster recovery (DR) network settings	Configure disaster recovery network settings, for example, mapping network settings for disaster recovery. Also includes gateway pairing.	Resiliency domain or specific data centers

Table 6-4 Jobs for custom personas *(continued)*

Job	Description	Scope
Manage evacuation plans	Generate or regenerate evacuation plans. Perform evacuation, rehearse evacuation or cleanup evacuation rehearsal operations.	Data center

See “Predefined personas” on page 62.

See “Adding custom personas” on page 71.

Custom persona required for starting or stopping resiliency groups

The predefined "start/stop resiliency group" job is not included in any predefined personas except for the Super admin persona, which has access to all jobs.

If you want to give users or user groups permission to start or stop resiliency groups from the console, you can create a custom persona that includes this job.

See “Adding custom personas” on page 71.

See “Predefined jobs that can be used for custom personas” on page 72.

Managing settings for alerts and notifications and general product settings

See the following topics for information on configuring email and SNMP settings for notifications and reports, setting up rules for event notifications, and configuring purge settings for logs and traps, and some general product settings.

See “Adding, modifying, or deleting email settings” on page 74.

See “Adding, modifying, or deleting SNMP settings” on page 76.

See “Setting up rules for event notifications” on page 76.

See “Modifying purge settings for logs and SNMP traps” on page 78.

See “Enabling or disabling telemetry collection ” on page 79.

Adding, modifying, or deleting email settings

You can configure email settings to be used for different features, such as sending reports or receiving automatic email notifications of events. HPE Helion and Veritas

Continuity manages email notifications via Resiliency Managers. When Resiliency Managers are located in different geographical locations, the required email settings are likely different for each location. In that case, you add a separate email configuration for each location. You can send a test email to verify the settings. You can also modify or delete existing email configurations.

To add, modify, or delete email settings

1 Navigate

⚙ **Settings** (menu bar)

Under **Product Settings**, select **Alerts & Notifications** > **Email**

To add a new email configuration, select **Add Email Configuration**.

To modify or delete an existing one, right-click it and select **Modify** or **Delete.**

2 To add or modify an email configuration, go through the wizard pages and specify the options.

In **Server Information**, specify the following:

Name	Assign a unique name for the email configuration.
Email Server	Valid formats include: Fully Qualified Domain Name (FQDN), IP address, or, if the network handles DNS resolution for host names, a shortened host name. Examples: Host123, Host123.example.com, xxx.yyy.zzz.aaa.
SMTP Port	Enter the SMTP mail server port number. The default is 25.
From Email Address	Enter the email address to be shown as the sender of all the emails that are sent.
Friendly Email Name	Optionally, enter a name to be shown for the From address.

3 In **Security**, if you want to implement secure SMTP, select the checkbox and enter the user name and password.

4 In **Select Resiliency Managers**, select a Resiliency Manager in the data center location where these email settings apply.

5 In **Test Email Settings**, enter a valid email address, and enter a subject and message for the test email. Click **Send Test Email** to test your settings.

6 Review the information in the summary and submit

See “Managing settings for alerts and notifications and general product settings” on page 74.

Adding, modifying, or deleting SNMP settings

When an event takes place, you can configure SNMP traps to be sent. You can configure the SNMP settings in the web console.

To add, modify, or delete SNMP settings

1 Navigate

⚙ **Settings** (menu bar)

Under **Product Settings**, select **Alerts & Notifications** > **SNMP**

To add a new SNMP configuration, select **Add SNMP Configuration**.

To modify or delete an existing one, right-click it and select **Modify** or **Delete.**

2 To add or modify SNMP settings, specify the following:

Name	Assign a friendly name.
SNMP Server	Enter the IP Address or name of the host where the SNMP trap console is located. Example: Host123.example.com
SNMP Port	Enter the SNMP port number. The default port for the trap is 162.

See “Managing settings for alerts and notifications and general product settings” on page 74.

Setting up rules for event notifications

Logs of the type information, warning, or error generate an event. You can view HPE Helion and Veritas Continuity event logs in the web console and set up rules for receiving notifications of events. You can also modify or delete existing rules.

To set up rules for event notifications

1. Prerequisite

   Configure the email server for sending notifications. Optionally you can also configure SNMP.

   See “Adding, modifying, or deleting email settings” on page 74.

   See “Adding, modifying, or deleting SNMP settings” on page 76.

2. Navigate

   ⚙ **Settings** (menu bar)

   Under **Product Settings**, select **Alerts & Notifications**

   To add a new rule: Click the **Definition** tab > **New Rule**.

   To modify or delete an existing rule: Click the **Rules** tab, right-click the rule, and select **Modify** or **Delete.**

3. In **Configure Rule**, enter or modify the following:

Name	Enter a unique name for this rule.
Send emails to	Enter one or more email addresses separated by a comma
Send SNMP traps to	Optional
Select Events	Select one or more events that you want to be notified about

4. Click **Submit**.

   The rule is listed on the **Rules** tab.

Viewing events and logs in the console

HPE Helion and Veritas Continuity maintains the following types of logs that can be viewed in the web console:

System logs: System logs are typically the result of a user performing an operation in the console.

Audit logs: Audit logs are primarily used for security audits. They leave a chronological trail of activities performed on the system. They identify user, activity, affected objects, etc. They help track the individuals responsible for activities and detect security violations.

Event and notification logs: Event and notification logs are not necessarily related to user activity; they can include information such as a server going down. Events can be public or private. Rules can be configured to notify users by email of selected public events. Private events are typically unrelated to user-initiated operations. Private events are displayed in the console for troubleshooting but are not available to include in rules for notification.

See “Setting up rules for event notifications” on page 76.

By default, logs and SNMP traps are retained for 2 years. This retention period can be modified in the product settings in the console.

See “Modifying purge settings for logs and SNMP traps” on page 78.

To view events and logs

1 Navigate

   More Views (menu bar) > **Logs**

   You can also view new notifications from the **Notifications** icon.

2 To view logs by type (System, Audit, or Notification) select the appropriate tab. You can filter by the product service and by severity (information, warning, or errors) or type (public, private), depending on the tab.

Modifying purge settings for logs and SNMP traps

By default, logs and SNMP traps are retained for two years. You can modify this purge setting.

To modify the purge setting for logs and SNMP traps

1 Navigate

   Settings (menu bar)

   Under **General Settings**, click **General**

2 Under **Logs**, enter the new value for the purge settings, in months.

3 Click **Save**.

See “Managing settings for alerts and notifications and general product settings” on page 74.

Enabling or disabling telemetry collection

HPE Helion and Veritas Continuity can collect usage information via telemetry for the purpose of future product enhancements. You can enable or disable the collection.

The types of telemetry information collected include configuration information, mainly inventory counts, and license information.

For example, information can include the number of configured authentication domains, resiliency plans and templates, virtual business services, virtual machines by platform and virtualization technology, virtualization servers by type, gateways and gateway pairs, storage proxies, cloud virtual machines provisioned, cloud credentials, number of data centers, and number and size of cinder volumes.

You can view a file showing the collected information.

Telemetry collection requires that the Resiliency Manager have internet connectivity.

To enable or disable telemetry collection

1 Navigate

⚙ **Settings** (menu bar)

Under **General Settings**, click **General**

2 Under **Telemetry**, select the setting to turn it on or off. To download a file showing the information that is collected, click **Show what is collected**.

Chapter 7

Using the Web console

This chapter includes the following topics:

- Tour of the HPE Helion and Veritas Continuity web console screen
- Filtering and searching for objects in the web console
- About the HPE Helion and Veritas Continuity Dashboard
- Web console icons

Tour of the HPE Helion and Veritas Continuity web console screen

Table 7-1 Overview of the web console screen areas

Screen areas	Description
Menu bar	Menu options for reports, resiliency plans, views, settings, notifications, inbox, and online help. See “Menu bar options” on page 81.
Navigation pane	Icons to open pages for configuring and implementing start/stop and disaster recovery operations. See “Navigation pane options” on page 82.
Dashboard	The console home page - clicking the Home icon in the navigation pane returns to the Dashboard. View an overview of assets in the resiliency domain and their current status. Drill down for details. See “About the HPE Helion and Veritas Continuity Dashboard” on page 83.

Menu bar options

The menu bar is located at the top of the console window.

Table 7-2 Menu bar options for the HPE Helion and Veritas Continuity web console

Options	Description
Quick Actions ▾	Open drop-down selection of shortcuts to common tasks.
Reports	Schedule and run reports. View reports showing data center and asset status.
Resiliency Plans	Create and run custom resiliency plans for starting, stopping, and migrating resiliency groups. See the Solutions guide for details on resiliency plans.
⊞	More views View activities, risks, and logs.
⚙	Settings Open Settings page for configuring and maintaining product infrastructure and other settings.
🔔	Notifications Display most recent notifications. Requires alerts and notifications to be enabled using Settings page. See "Viewing events and logs in the console" on page 77. See "Managing settings for alerts and notifications and general product settings" on page 74.
✉	Inbox View actions to be completed.
?	Help Open Help window where you can search all help or filter by category.

Table 7-2 Menu bar options for the HPE Helion and Veritas Continuity web console *(continued)*

Options	Description
👤	Log out of console. Shows Resiliency Manager, resiliency domain, and data center.

Navigation pane options

The navigation pane is located on the left side of the console window.

Note: Click the arrow on the top of the navigation pane to expand or contract the pane and view labels for icons.

Table 7-3 Left navigation pane options for the HPE Helion and Veritas Continuity web console

Options	Description
🏠	Returns to Home page Dashboard
🗔	Opens Assets page for configuring and viewing resiliency groups and performing start/stop operations or disaster recovery
🗐	Opens configuration page for disaster recovery settings

Filtering and searching for objects in the web console

On pages that list multiple objects, for example, virtual machines listed on the Assets page, the web console lets you select object types as a filter or search by first letters of a name. To see the full list again, clear the filter or search field.

You can also double-click to drill down to a more detailed view. For example, you can drill down from a row of a table that lists virtual machines, or from a Dashboard graphic showing information on virtual machine status.

About the HPE Helion and Veritas Continuity Dashboard

The HPE Helion and Veritas Continuity Dashboard gives you an overview of your resiliency domain. Use the Dashboard to answer questions such as the following:

- Which of my data centers have HPE Helion and Veritas Continuity managed assets?
- What is the mix of my assets by type and platform?
- Which assets are configured for disaster recovery?

The Dashboard has the following areas:

Global View

A world map that identifies the data centers that contain HPE Helion and Veritas Continuity managed assets.

A cloud icon indicates that the data center is in a cloud.

Mouse over an icon for basic HPE Helion and Veritas Continuity platform configuration and asset configuration information for that data center. Click **More** for detailed information and recent activity.

Resiliency Groups and **Virtual Business Services** summaries

The upper right section of the dashboard displays total number of resiliency groups and virtual business services in the resiliency domain, as well as those at risk and normal.

Click a square in either the **Resiliency Groups** or **Virtual Business Services** summary to display a tab of detailed information.

Virtual Machine Distribution

Identifies which virtual machines are on-premises and which are the cloud. When you create a resiliency group from virtual machines, the on-premises number increases. When you migrate the resiliency group, the number of cloud virtual machines increases.

Virtual Machines and Applications by Recovery Readiness

Displays the percentage of virtual machines and applications that are managed (configured for disaster recovery) and unmanaged (not configured for disaster recovery).

Use the drop-down list to filter your results.

Recovery Time (Top 5 Resiliency Groups)

Ranks the resiliency groups according to the time it takes the disaster recovery data center to take over.

Click on a resiliency group to display its details page.

Recovery Point (Top 5 Resiliency Groups)

Ranks resiliency groups according to their recovery point objective (RPO).

DR Activity Summary (For last 2 months)

Displays the statistics on recent disaster recovery activity, including the following:

- The number of takeovers and migrations run, how many were successful, and how many failed.
- The number of rehearsals run, how many were successful, and how many failed.
- The number of failbacks run, how many were successful, and how many failed.

Click on any of the squares to display the **Activities** screen and more detailed information.

VBS DR Activity Summary (For last 2 months)

Displays the statistics on recent disaster recovery activity for VBSs, including the following:

- The number of takeovers and migrations run, how many were successful, and how many failed.
- The number of rehearsals run, how many were successful, and how many failed.
- The number of failbacks run, how many were successful, and how many failed.

You can use the Assets icon in the navigation pane to display more detailed information on resiliency groups.

Web console icons

The following is a summary of icons that appear on the HPE Helion and Veritas Continuity web console.

Table 7-4 Web console icons

Icon	Description	Location
⊞	More views Menu options for Activities, Logs, Risks	Menu bar
⚙	Settings Opens Settings page	Menu bar
🔔	Notifications Displays notifications Requires alerts and notifications to be enabled using Settings page	Menu bar
✉	Inbox View actions to be completed.	Menu bar
?	Help Opens Help window where you can search all help or filter by category	Menu bar
👤	Log out of console Shows user login and information about Resiliency Manager, resiliency domain, and data center	Menu bar
⌂	Home Returns to the Home page Dashboard	Navigation pane
🗔	Assets Opens the Assets page for configuring and viewing resiliency groups and performing start/stop operations or disaster recovery	Navigation pane
🖥	DR Capability Opens configuration page for disaster recovery settings	Navigation pane

Table 7-4 Web console icons *(continued)*

Icon	Description	Location
⋮	Vertical ellipsis Displays list of actions for selected object	To the right of a selected object in a list

Chapter 8

Updating HPE Helion and Veritas Continuity

This chapter includes the following topics:

- About updating HPE Helion and Veritas Continuity
- About applying updates to HPE Helion and Veritas Continuity
- Prerequisites for a repository server
- Setting up the repository server and downloading updates
- Adding a repository server in HPE Helion and Veritas Continuity
- Assigning a repository server in HPE Helion and Veritas Continuity
- Applying updates to virtual appliances using the console
- Applying updates to virtual appliance using CLISH menu
- Refreshing the information about applicable updates
- Removing an update from the repository server

About updating HPE Helion and Veritas Continuity

This chapter covers common aspects of updating a HPE Helion and Veritas Continuity deployment.

The topics in this chapter cover the process of applying updates (patches and maintenance release) to the virtual appliance, add-ons, and host packages.

About applying updates to HPE Helion and Veritas Continuity

Updates to HPE Helion and Veritas Continuity provide significant benefits, such as improved functionality, performance, security, and reliability.

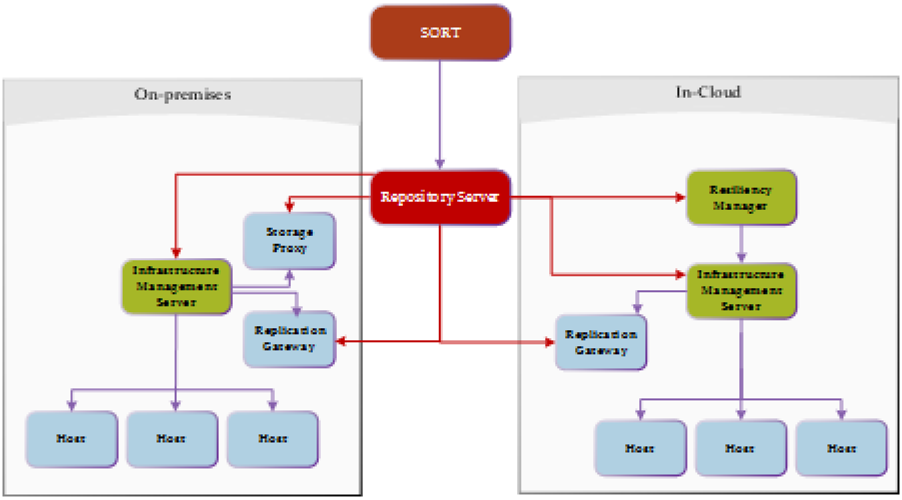
In HPE Helion and Veritas Continuity, you can apply updates to the following:

- HPE Helion and Veritas Continuity virtual appliance
- HPE Helion and Veritas Continuity add-ons
- Host packages on the assets that are added to the Infrastructure Management Server (IMS) as a host

For applying updates to HPE Helion and Veritas Continuity, you need to set up a repository server and download the updates to the repository server. Then, you assign the repository server to the HPE Helion and Veritas Continuity virtual appliance, where you want to apply the update. You can apply the updates using the web console or using the CLISH menu. It is recommended to take a snapshot of the appliance before applying the updates.

Note: After applying the update to a virtual appliance, if you add a virtual machine on which the host package is installed manually, to the IMS, then you need to explicitly apply the update (Hotfix) to that virtual machine.

The following figure shows how a repository server is used to apply the updates to HPE Helion and Veritas Continuity:



Note: While applying updates, ensure that the virtual appliance remains powered on. Restarting the appliance during the process of applying updates may adversely affect the functionality. In case the appliance gets restarted, you need to reassign the repository to the appliance.

The following is an overview of the process of applying updates in HPE Helion and Veritas Continuity:

Table 8-1 Applying updates to HPE Helion and Veritas Continuity

Step	Task	Description
1	Make sure that the prerequisites for the repository server are met.	See "Prerequisites for a repository server" on page 90.
2	Set up a repository server and download the updates from SORT	See "Setting up the repository server and downloading updates" on page 90.
3	Add the repository server to HPE Helion and Veritas Continuity. There can be multiple repository servers added to HPE Helion and Veritas Continuity at a time.	See "Adding a repository server in HPE Helion and Veritas Continuity" on page 92.
4	Assign a repository server to the virtual appliance where you want to apply the update. A single repository server can be assigned to multiple virtual appliances but one virtual appliance can be assigned only one repository server at a time.	See "Assigning a repository server in HPE Helion and Veritas Continuity" on page 92.
5	For a major upgrade: ■ Apply updates using CLISH menu For a minor upgrade: ■ Apply updates using web console or using CLISH menu	See "Applying updates to virtual appliances using the console" on page 93. See "Applying updates to virtual appliance using CLISH menu" on page 94.
6	Refresh the information about applicable updates	See "Refreshing the information about applicable updates" on page 95.
7	Remove an update from the repository server	See "Removing an update from the repository server" on page 95.

Prerequisites for a repository server

To set up a repository server, make sure that the following prerequisites are met:

- Repository server should be RHEL server version 6.5 with minimum yum version 3.2.29. Base server installation is recommended for the repository server.
- Perl and Python should be installed on the server. Perl modules `JSON.pm` and `Config::Simple.pm` need to be installed on the Linux server.
- Web server (HTTP/HTTPS) should be configured on the server. Two-way SSL configuration is recommended for HTTPS.
  Default ports are 80 for HTTP and 443 for HTTPS.
- Repository server should have minimum 50 GB disk space available for repository data.
- Repository server should have connectivity with SORT as well as with the virtual appliances.

See “About applying updates to HPE Helion and Veritas Continuity” on page 88.

Setting up the repository server and downloading updates

You need to set up a repository server in your environment, download the updates from SORT, and make them available on your repository server.

You have following three options to set up a repository and download the updates from SORT:

- Download a specified update or download all the updates released after a specified date.
- Download a specified update on your local system and then update the repository system with the downloaded updates. You can use this option if your repository server does not have SORT connectivity. To use this option, you need to download `master.xml` file from SORT.
- Download the metadata of the applicable updates to your repository server. Once you add the repository server using the Resiliency Manager console, you can view the list of applicable updates in the Resiliency Manager console. You can then decide which update you want to download.

Note: In case you plan to update the repository server with the updates or metadata that you have saved on you local system, you need to always use the latest `master.xml` file, irrespective of which update you plan to use.

To set up a repository server and download the updates

1. Create a repository path under root directory of the web server.

   ```
   mkdir path_to_repository
   ```

2. Download the `setup_conf_repo.pl` file from SORT.

3. Do one of the following:

   - To download the updates and update the repository server with those updates, do one of the following:

     - To download a particular update to the repository server, and update the repository:

       ```
       ./setup_conf_repo.pl --download-updates --repo-location
       path_to_repository --product-version base_version --product
       product_abbreviation --release-name release_name
       ```

     - To download multiple updates that are released after a particular date or after a particular update version, and update the repository:

       ```
       ./setup_conf_repo.pl --download-updates --repo-location
       path_to_repository product-version base_version --product
       product_abbreviation --start-date yyyy-mm-dd
       ```

   - To update the repository server with the updates that you have saved on your local system:

     ```
     ./setup_conf_repo.pl --add-local-updates --repo-location
     path_to_repository --update-location path_to_tar
     --metadata-location path_to_master.xml
     ```

   - To download the metadata of the applicable updates to your repository server:

     ```
     ./setup_conf_repo.pl --refresh-metadata --repo-location
     path_to_repository --product-version base_version --product
     product_abbreviation
     ```

   - To update the repository server with the metadata file `master.xml` that you have saved on your local system:

     ```
     ./setup_conf_repo.pl --refresh-metadata --repo-location
     path_to_repository --metadata-location path_to_master.xml
     ```

See “About applying updates to HPE Helion and Veritas Continuity” on page 88.

Adding a repository server in HPE Helion and Veritas Continuity

After configuring a repository server, you need to add the repository server in HPE Helion and Veritas Continuity.

To add a repository server in HPE Helion and Veritas Continuity

1. Navigate

   ⚙ **Settings** (menu bar) > **Updates** > **Repository Servers**

2. Click **Add**.
3. In the **Add Repository** Wizard panel, do the following:
   - Select the protocol for adding the repository server.
   - Enter the fully qualified hostname (FQDN) or IP address of the server that you want to configure as the repository server.
   - If you want to modify the default port, enter the port number.
   - Enter the repository path that is created under root directory of web server.
   - Click **Submit**.

See “About applying updates to HPE Helion and Veritas Continuity” on page 88.

Assigning a repository server in HPE Helion and Veritas Continuity

You need to assign a repository server to every virtual appliance where you want to apply the updates. You can store all the available updates on this server and apply it on the virtual appliance whenever required.

Note: Before assigning a repository server to a virtual appliance, make sure that the path where repository server is configured has read permissions.

To assign a repository server to a virtual appliance

1 Navigate

⚙ **Settings** (menu bar) > **Updates**

2 Select the server names (virtual appliances) to which you want to assign a repository server.

3 Click **Assign Repository**. Select the repository server that you want to assign to the virtual appliances.

Click **Submit**.

See “About applying updates to HPE Helion and Veritas Continuity” on page 88.

Applying updates to virtual appliances using the console

You can apply updates to the virtual appliances using the console.

Replication gateway updates must be applied on the cloud replication gateway first and then on the on-premises gateway.

To apply updates to the virtual appliances using the console

1 Prerequisites:

Ensure that following services are running on the Resiliency Manager:

- User Interface service
- Database service
- Messaging service
- Core service
- Task service
- Event service

2 Navigate

⚙ **Settings** (menu bar) > **Updates**

3 Select the server name or virtual appliance on which you want to apply the update.

4 Select the update that you want to apply from **New Updates**.

5 Click **Upgrade**.

6 Verify the details of the update and click **Submit**.

Note: If the process of applying updates on the appliance takes more than 30 minutes, the session times out and you need to confirm if you want to continue the session and refresh the page. The progress of the task of applying updates can be tracked from **Recent Activities**.

See "About applying updates to HPE Helion and Veritas Continuity" on page 88.

Applying updates to virtual appliance using CLISH menu

You can use the CLISH menu to perform the upgrade related tasks in HPE Helion and Veritas Continuity.

Replication gateway updates must be applied on the cloud replication gateway first and then on the on-premises gateway.

You need to log into the virtual appliance as admin and go to the updates sub-menu. Following is a list of commands that you can run to perform the operations that are related to the updates:

- To configure the repository:

  ```
  config-repository FQDN_or_IP_of_the _repository_server protocol
  port_number Repository _path_on_repository_server
  ```

  If you enter HTTPS as protocol, you are required to copy the content from the SSL certificate, paste it on prompt, and press enter key.

- To view the current configuration of the repository:

  ```
  show-repo
  ```

- To view the current version of the appliance or the version of the update installed on the appliance:

  ```
  list-updates
  ```

- To show the readme file for the specified update:

  ```
  show-readme version_of_the_update
  ```

- To apply the specified update:

  ```
  apply-update version_of_the_update
  ```

- To remove the current repository configuration:

```
   remove_repo
```

See “Using CLISH” on page 102. for a complete list of options available with `Updates` command.

See “About applying updates to HPE Helion and Veritas Continuity” on page 88.

Refreshing the information about applicable updates

After applying updates, you may want to refresh the information about the applicable updates on each of the virtual appliances or servers. If you apply the updates using CLISH, you need to refresh the information to reflect the current status of the updates in the Resiliency Manager web console.

To refresh the information about applicable updates

1 Navigate

⚙ **Settings** (menu bar) > **Updates** > **Available Updates**

2 Click **Refresh**.

See “About applying updates to HPE Helion and Veritas Continuity” on page 88.

Removing an update from the repository server

You can remove a particular update from the repository server.

To remove an update from the repository server

1 Go to the `ITRP/RM` directory on the repository server. This directory is created under the repository path that you had provided while setting up the repository.

2 Run the following commands:

- To remove the directory created for a particular update:

  ```
  rm -rf patch_version_dir
  ```

- To clear the older data, and then refresh and build the repository with the existing patches in the `RM` directory:

  ```
  createrepo --update RM
  ```

Chapter 9

Uninstalling HPE Helion and Veritas Continuity

This chapter includes the following topics:

- About uninstalling HPE Helion and Veritas Continuity

About uninstalling HPE Helion and Veritas Continuity

In the current version, there is no provision for uninstalling HPE Helion and Veritas Continuity. If you do not want to use the HPE Helion and Veritas Continuity product any longer, you can remove the HPE Helion and Veritas Continuity virtual appliance node using the appropriate hypervisor manager in your environment.

If you want to decommision a HPE Helion and Veritas Continuity virtual appliance node while continuing to use the product on other nodes in the resiliency domain, you should first use the web console to remove the node from the Resiliency Manager database. For example, you can remove a Resiliency Manager node from the domain if another Resiliency Manager node is active.

Chapter 10

Troubleshooting and maintenance

This chapter includes the following topics:

- Accessing HPE Helion and Veritas Continuity log files
- Troubleshooting replication
- Components of HPE Helion and Veritas Continuity virtual appliances
- Using Veritas Services and Operations Readiness Tools to find a Unique Message Identifier description and solution
- Displaying risk information

Accessing HPE Helion and Veritas Continuity log files

You can use `logs-gather` option available with `support` command of CLISH menu to access the HPE Helion and Veritas Continuity log files.

To access HPE Helion and Veritas Continuity log files

1. Log in to the HPE Helion and Veritas Continuity virtual appliance console as an admin user.
2. Go to the **support** under **main menu**.

3 Run the logs-gather command with any of the log collection options that are available.

See "Using CLISH" on page 102.

The command collects the logs according to the option that you use with the command.

4 Once the logs are collected, a URL for downloading the log zip file is provided to you. You can enter the URL in a browser on any host connected to the virtual appliance. Log in as an admin user and download the zip file.

Troubleshooting replication

In addition to the logging information that is provided on the web console, additional log information may be required to troubleshoot certain issues. For debugging purposes, refer to the following log files locations.

The Replication Gateway services write logs to the following location:

```
/var/opt/VRTSitrpgw/log
```

The Storage Proxy writes logs to the following location:

```
/var/opt/VRTSitrpsp/log
```

Components of HPE Helion and Veritas Continuity virtual appliances

Following components are deployed while deploying the HPE Helion and Veritas Continuity virtual appliance:

Table 10-1

Components	Description
Operating System	Hardened CentOS 6.7 Minimal operating system. The operating system is hardened or customized to contain only those packages that are required to run the application.
HPE Helion and Veritas Continuity	HPE Helion and Veritas Continuity provides core and standard services framework for the solution.
Resiliency Manager	Serves as the management console for HPE Helion and Veritas Continuity. It also includes the database and the HPE Helion and Veritas Continuity services.

Table 10-1 *(continued)*

Components	Description
Infrastructure Management Server (IMS)	Serves as the infrastructure manager or asset manager for HPE Helion and Veritas Continuity.
Replication Gateway	Used for replication between on-premises components and cloud components.
Storage Proxy	Used for replication from cloud components to on-premises components.
Command Line Interface Shell (CLISH)	Command Line Interface Shell (CLISH) is used to provide the user a limited menu-based access to the operating system and the application.

See “About deploying the HPE Helion and Veritas Continuity virtual appliance” on page 22.

Using Veritas Services and Operations Readiness Tools to find a Unique Message Identifier description and solution

You can use Veritas Services and Operations Readiness Tools (SORT) to find a Unique Message Identifier (UMI) description and solution.

To find a Unique Message Identifier description and solution

1 Point your Web browser to the following URL:

   http://sort.veritas.com

2 In the search field on the top right of any SORT page, enter the UMI code, and then click the search icon.

3 On the **Search Result** page, in the **Error codes** pane, click the link to your message code. If you have a large number of search results, use the check boxes at the top of the page to display only error codes to find your code more easily.

   The **Error Code details** page for the UMI code displays, which provides the description and any possible solutions.

4 If the information on the page does not provide an adequate solution to your issue, you can click one of the links on the page to do one of the following things:

- Comment on the UMI or its solution.
- Request a solution.
- Add a solution of your own.

Displaying risk information

HPE Helion and Veritas Continuity identifies and flags several risks that may occur during data center operations. Some of these risks are transient. They are temporary and resolve themselves without your intervention. Other risks require intervention and troubleshooting to resolve.

You can display risks in the following ways:

Table 10-2 Ways to display risks

To display ...	Do the following:
A complete list of risks across the resiliency domain	**1** On the menu bar, select ⊞ **More Views** > **Risks** **2** On the **Risk** page, double-click a risk in the table to display detailed information.
Risks that are associated with a specific resiliency group or virtual business service	**1** On the navigation pane, select 🗔 (Assets) and the tab for either **Resiliency Groups** or **Virtual Business Services**. **2** On the tab, double-click a resiliency group or virtual business service to display detailed information. **3** On the details page, note any risks that are listed in the **At Risk** area, and double-click the risk for details.

In addition to the above mentioned views, the **More views** > **Logs** > **All** view and the **More views** > **Logs** > **Notification** view also includes the notification about the risks in your environment. You can double-click any row to view the detailed description of the error and suggested resolution for the error.

Using CLISH menu in HPE Helion and Veritas Continuity

This appendix includes the following topics:

- About CLISH
- Using CLISH

About CLISH

Once the HPE Helion and Veritas Continuity virtual appliance is deployed and configured, you are given limited, menu-based access to the operating system and the product. You need to use Command Line Interface Shell (CLISH) menu to manage the configuration-related changes to the product.

You can use CLISH menu to do the following:

- Manage the HPE Helion and Veritas Continuity appliance
- Monitor the HPE Helion and Veritas Continuity appliance activities
- Change some of the network configurations
- Change the system settings
- Access the HPE Helion and Veritas Continuity logs
- Manage HPE Helion and Veritas Continuity updates and patches

See “Using CLISH” on page 102.

Using CLISH

After the product configuration, when you log in to the HPE Helion and Veritas Continuity appliance, you get the main menu of CLISH. This menu is the starting point, from which you can configure, manage, monitor, and support your application using the command line.

You can reconfigure or modify some of the appliance settings that are configured through the product bootstrap. Following are the settings that you can reconfigure using CLISH:

- **Network settings:** You can reconfigure the subnet mask, default gateway, DNS server, and search domains using the CLISH menu.
  You cannot reconfigure the hostname that you had configured through the bootstrap process. In case of static DHCP, you cannot change the network settings using the CLISH menu. You cannot change the network settings for any component that is configured in the cloud environment.
- **System settings:** You can reset the timezone and NTP server using CLISH menu. Changing the system settings can affect the product functionality if incorrect values are set.

You can also perform logical volume management (LVM) operations such as adding a disk or removing a disk using the CLISH menu.

You can press the **tab** or **space** key to display the menu options. Press **?** key to display detailed help.

Table A-1 Options available in the **main** menu

Menu option	Description
back	Return to the previous menu
exit	Log out from the current CLI session
help	Display an overview of the CLI syntax
manage	Manage appliance Table A-2
monitor	Monitor appliance activities Table A-5
network	Network configuration Table A-6

Table A-1 Options available in the **main** menu *(continued)*

Menu option	Description
settings	Appliance settings Table A-12
support	Access logs Table A-16
updates	Manage updates and patches Table A-18

Table A-2 Options available with **manage** command

Menu option	Description
back	Return to the previous menu
configure	Configure HPE Helion and Veritas Continuity component or show the configured component Table A-3
exit	Log out from the current CLI session
help	Display an overview of the CLI syntax
services	Manage the appliance services ■ If the appliance has been configured as a Resiliency Manager or IMS, use **rm** or **ims** as first parameter and options available in the services menu as second parameter. Table A-4 ■ If the appliance has been configured as a Replication Gateway or Storage Proxy, use the options available in the services menu as first parameter.

Table A-3 Options available with **configure** command

Menu option	Description
ims	Configure Infrastructure Management Server
rm	Configure Resiliency Manager
show	Show the configured component

Table A-4 Options available with **services** command

Menu option	Description
show	Show HPE Helion and Veritas Continuity services
restart	Restart HPE Helion and Veritas Continuity services Two options available are: `restart` *`all`* where, *all* means all the services. `restart` *`service name`* where, *service name* is the name of a particular service. You can provide multiple service names (comma separated).
start	Start HPE Helion and Veritas Continuity services Two options available are: `start` *`all`* where, *all* means all the services. `start` *`service name`* where, *service name* is the name of a particular service. You can provide multiple service names (comma separated).
status	Check the status of HPE Helion and Veritas Continuity services Two options available are: `status` *`all`* where, *all* means all the services. `status` *`service name`* where, *service name* is the name of a particular service. You can provide multiple service names (comma separated).
stop	Stop HPE Helion and Veritas Continuity services Two options available are: `stop` *`all`* where, *all* means all the services. `stop` *`service name`* where, *service name* is the name of a particular service. You can provide multiple service names (comma separated).

Table A-5 Options available with **monitor** command

Menu option	Description
back	Return to the previous menu
exit	Log out from the current CLI session
FSusage	Display filesystem usage

Table A-5 Options available with **monitor** command *(continued)*

Menu option	Description
help	Display an overview of the CLI syntax
top	Display the top process information
uptime	Display the uptime statistics for the appliance
who	Display who is currently logged into the appliance

Table A-6 Options available with **network** command

Menu option	Description
back	Return to the previous menu
dns	Show or change the DNS Table A-7
exit	Log out from the current CLI session
gateway	Show or change the Gateway Table A-8
help	Display an overview of the CLI syntax
hostname	Show the hostname
ip	Show or change the IP address Table A-9
netmask	Show or change the netmask Table A-10
search-domain	Show or change the domain Table A-11

Table A-7 Options available with **dns** command

Menu option	Description
set	Configure Domain Name Server
show	Show the current Domain Name Server

Table A-8 Options available with **gateway** command

Menu option	Description
set	Configure Gateway
show	Show the current Gateway

Table A-9 Options available with **ip** command

Menu option	Description
set	Configure the IP address
show	Show the current IP address

Table A-10 Options available with **netmask** command

Menu option	Description
set	Configure the netmask
show	Show the current netmask

Table A-11 Options available with **search-domain** command

Menu option	Description
add	Add search-domain
remove	Remove the search domain name
show	Show the search domain settings

Table A-12 Options available with **settings** command

Menu option	Description
back	Return to the previous menu
change-password	Change the admin user password for the appliance
date	Display the current date and time for the appliance Table A-13
exit	Log out from the current CLI session
help	Display an overview of the CLI syntax

Table A-12 Options available with **settings** command *(continued)*

Menu option	Description
lvm	Perform operations related to logical volume manager on the appliance See Table A-14 on page 107.
ntp	Perform operations related to NTP server
poweroff	Shut down the appliance
reboot	Restart the appliance
timezone	Show or change the timezone for the appliance See Table A-15 on page 107.

Table A-13 Options available with **date** command

Menu option	Description
show	Show the time and date

Table A-14 Options available with **lvm** command

Menu option	Description
add-disk	Add disk to the data volume. You need to attach a disk before adding it.
list-free-disk	List the free disks
initialize-free-disk	Initialize the newly attached free disk
list-used-disk	List the disks used by the data volume
remove-disk	Remove disk from the data volume. Make sure that you have an extra disk to migrate the data before removing a disk.

Note: In case you initialize the newely-added disk during add-disk or remove-disk operation, the existing data on the new disk is deleted.

Table A-15 Options available with **timezone** command

Menu option	Description
set	Set the timezone for the appliance
show	Show the current timezone for the appliance

Table A-16 Options available with **support** command

Menu option	Description
back	Return to the previous menu
exit	Log out from the current CLI session
help	Display an overview of the CLI syntax
loggather	■ If the appliance has been configured as a Resiliency Manager or an IMS, then various options will be available for collecting the Resiliency Manager and IMS logs. Table A-17 ■ If the appliance has been configured as a Replication Gateway or a Storage Proxy, then `loggather` command will collect the logs of the Replication gateway or the Storage Proxy.
shell	Open the bash shell prompt for support user

Table A-17 Options available with **loggather** command

Menu option	Description
basic	Gather logs of Resiliency Manager and IMS without database
full	Gather logs of Resiliency Manager and IMS with database
fullims	Gather logs of IMS with database
fullrm	Gather logs of Resiliency Manager with database
ims	Gather logs of IMS
rm	Gather logs of Resiliency Manager

Table A-18 Options available with **updates** command

Menu option	Description
apply-update	Apply the specified update
back	Return to the previous menu
config-repository	Configure the repository Table A-19
exit	Log out from the current CLI session
help	Display an overview of the CLI syntax

Table A-18 Options available with **updates** command *(continued)*

Menu option	Description
list-updates	List the applicable updates
remove-repository	Remove current repository configuration
show-readme	Show readme for the specified update
show-repository	Show current repository configuration
show-version	Show appliance version

Table A-19 Options available with **config-repository** command

Menu option	Description
hostname	hostname of the repository server
protocol	Protocol on which the repository server is configured
port	Port on which the repository server is configured
RepoPath	Path on which the repository server is configured

See “About CLISH” on page 101.

See “Accessing HPE Helion and Veritas Continuity log files” on page 97.

Glossary

activity

A task or an operation performed on a resiliency group.

add-on

An additional software package that can be installed on hosts by the Infrastructure Management Server (IMS) for specialized uses.

asset infrastructure

The data center assets that can be added to the Infrastructure Management Server (IMS) for IMS discovery and monitoring. For example, virtual machines or virtualization servers.

assets

In HPE Helion and Veritas Continuity, the virtual machines that have been discovered by the Infrastructure Management Server (IMS) and that can be grouped into resiliency groups.

CLISH

Command Line Interface SHell. Provides the command line menu on the virtual appliance for use after the initial bootstrap configuration.

data center

A location that contains asset infrastructure to be managed by HPE Helion and Veritas Continuity.

For the disaster recovery use case, the resiliency domain contains at least two data centers, an on-premises data center and the recovery data center in the cloud. The cloud data center has a Resiliency Manager, one or more cloud gateways, and one or more IMSs; the on-premises data center has one or more on-premises gateways, one or more storage proxies, and one or more IMSs

failback

A planned activity after a failover operation, which involves graceful shutdown of virtual machines at the recovery data center and starting them at the production data center.

Before the failback operation is performed, the data at the recovery data center must be replicated back to the production data center.

host

Physical servers, virtual machines, or Hyper-V servers that are added to the Infrastructure Management Server (IMS) as hosts.

Adding the assets as hosts installs the host package that is used by the IMS for discovery and monitoring.

Infrastructure Management Server (IMS)

The HPE Helion and Veritas Continuity component that discovers, monitors, and manages the asset infrastructure within a data center. The IMS transmits information about the asset infrastructure to the Resiliency Manager.

migrate A planned activity involving graceful shutdown of virtual machines at the production data center and starting them at the recovery data center. In this process, replication ensures that consistent virtual machine data is made available at the recovery data center.

persona A user role that has access to a predefined set of jobs (operations). Used to assign permissions to users and groups for HPE Helion and Veritas Continuity web console operations.

product role The function configured for a HPE Helion and Veritas Continuity virtual appliance.

For example, a virtual appliance can be configured as a Resiliency Manager, Infrastructure Management Server (IMS) or both.

production data center The data center that is normally used for business. See also recovery data center.

recovery data center The data center that is used if a disaster scenario occurs. See also production data center.

rehearsal A zero-downtime test that mimics the configuration, application data, storage, and the failover behavior of the resiliency group.

Rehearsal verifies the ability of the resiliency group to fail over to the recovery data center during a disaster.

Replication Gateway The HPE Helion and Veritas Continuity component that performs replication between the on-premises storage and the cloud storage.

resiliency domain The logical scope of a HPE Helion and Veritas Continuity deployment. It can extend across multiple data centers.

resiliency group The unit of management and control in HPE Helion and Veritas Continuity. Related assets are organized into a resiliency group and managed and monitored as a single entity.

Resiliency Manager The HPE Helion and Veritas Continuity component that provides resiliency capabilities within a resiliency domain. It is composed of loosely coupled services, a distributed data repository, and a management console.

resiliency plan A collection of tasks or operations, along with the relevant assets, which are performed in a predefined sequence.

resiliency plan template A template defining the execution sequence of a collection of tasks or operations.

Storage Proxy The HPE Helion and Veritas Continuity component that enables HPE Helion and Veritas Continuity to connect the primary storage as iSCSI targets to the on-premises gateway during preparation for failback to the on-premises data center.

takeover An activity initiated by a user when the production data center is down due to a disaster and the virtual machines need to be restored at the recovery data center to provide business continuity.

tier

Within a virtual business service (VBS), resiliency groups are arranged as tiers. Tiers represent the logical dependencies between the resiliency groups and determine the relative order in which the resiliency groups start and stop.

virtual appliance

An appliance that includes the operating system environment and the software application which are deployed together as a virtual machine.

The HPE Helion and Veritas Continuity virtual appliance is deployed as a virtual machine and then configured with basic settings and a role (for example, Resiliency Manager).

virtual business service (VBS)

A multi-tier IT service where each VBS tier hosts one or more resiliency groups. A VBS groups multiple services as a single unit for visualization, automation, and controlled start and stop in the desired order. You can also migrate/takeover the entire VBS.

web console

The web-based management console on the Resiliency Manager that is used to configure the settings for the resiliency domain and perform operations.

Index

A

alert settings
- email 74
- SNMP 76

asset infrastructure
- about adding assets as hosts 36
- adding hosts 39
- adding to IMS 34
- adding VMware virtualization servers 51
- CSV file for adding hosts 41
- editing VMware virtualization servers in IMS 53
- Linux packages required 37
- prerequisites for hosts 36
- prerequisites for Hyper-V virtualization discovery 45
- prerequisites for VMware discovery 46
- refreshing ESX Servers in IMS 54
- refreshing hosts 41
- refreshing VMware virtualization servers 54
- removing hosts 42
- removing VMware virtualization servers 54
- Windows host installation 40

authentication domains
- configuring 66
- unconfiguring 68

C

Configure DR
- prerequisites 38

configuring
- IMS 28
- ReplicationGateway 29
- Storage Proxy 30
- virtual appliances 27

CSV file for adding hosts to IMS 41

D

dashboard 83

deploying
- Hyper-V Manager 23

deploying *(continued)*
- VA 22
- VMware vSphere Client 24

E

email settings 74

events 77

F

firewall 17

H

hosts
- adding to IMS 39
- installing host package on Windows host 40
- refreshing in IMS 41
- removing in IMS 42

HPE Helion and Veritas Continuity
- features and components 9

Hyper-V servers
- discovery in IMS 44
- prerequisites for IMS discovery 45

I

icons 85

Infrastructure Management Server
- about adding assets as hosts 36
- adding asset infrastructure 34
- adding hosts 39
- adding VMware virtualization servers 51
- CSV file for adding hosts 41
- editing VMware virtualization servers in IMS 53
- Linux packages required for discovery 37
- overview 12
- prerequisites for adding hosts 36
- prerequisites for adding VMware vCenter servers 46
- prerequisites for Hyper-V virtualization discovery 45
- refreshing ESX Servers 54

Infrastructure Management Server *(continued)*
- refreshing hosts 41
- refreshing VMware virtualization servers 54
- removing hosts 42
- removing VMware virtualization servers 54
- Windows host installation 40

IPV 17

J

jobs for custom personas 72

L

logs
- purge settings 78
- viewing in console 77

M

menu bar 81

N

notification settings
- email 74
- rules 76
- SNMP 76

P

permissions 59
- assigning to users 69
- overview 61

personas
- custom 71–72
- limiting object scope for operations 65
- predefined 62

ports 17

purge settings for logs and SNMP traps 78

R

resiliency domain
- overview 11

Resiliency Manager
- overview 11

risk information
- view 100

rules for event notifications 76

S

SNMP
- configuring settings 76
- purge settings for traps 78

supported hypervisors 15

system requirements 16

T

telemetry collection 79

U

Update
- refresh 95
- remove 95
- virtual appliance 93

update
- about 87–88

Updating
- virtual appliance 94

upgrade
- adding repository server 92
- assigning repository server 92
- downloading updates 90
- prerequisites of repository server 90
- setting up repository server 90

user authentication 59–60

user permissions
- overview 61

users
- assigning permissions 69
- configuring 69

V

virtual appliance
- components 98
- filenames 23

virtual appliances
- configuring 27

VMware virtualization server
- adding to IMS 51
- configuring the VMware vCenter Server to generate SNMP traps 50
- editing configuration in IMS 53
- near real-time update in IMS 47
- refreshing configuration in IMS 54
- refreshing ESX Servers in IMS 54
- removing configuration in IMS 54
- requirements for IMS discovery 46

VMware virtualization server *(continued)*
setting up near real-time update of virtual machine states 49

W

web browser requirements 21