

Hewlett Packard Enterprise Helion and Veritas Continuity 2.0 Deployment Guide

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: 2.0

Document version: 2.0 Rev 1

Legal Notice

Copyright © 2017 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, Veritas InfoScale, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third party software for which Veritas is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the third party legal notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

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.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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 | 12 |
| | Infrastructure Management Server (IMS) | 12 |
| | Resiliency Platform 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 | 14 |
| Chapter 2 | System requirements | 16 |
| | Supported hypervisors for deploying HPE Helion and Veritas Continuity virtual appliance | 16 |
| | System resource requirements for HPE Helion and Veritas Continuity | 16 |
| | Network and firewall requirements | 18 |
| | Web browser requirements for HPE Helion and Veritas Continuity | 22 |
| Chapter 3 | Deploying HPE Helion and Veritas Continuity | 24 |
| | About deploying the HPE Helion and Veritas Continuity virtual appliance | 24 |
| | HPE Helion and Veritas Continuity virtual appliance file names | 25 |
| | Deploying the virtual appliance on-premises through Hyper-V Manager | 25 |
| | Deploying the virtual appliance on-premises through VMware vSphere Client | 26 |

| | | |
|------------------|---|-----------|
| Chapter 4 | Configuring the settings on the virtual appliance | 29 |
| | | 29 |
| | About configuring the HPE Helion and Veritas Continuity components | 29 |
| | | 29 |
| | Prerequisites for configuring HPE Helion and Veritas Continuity components | 30 |
| | | 30 |
| Chapter 5 | Adding the asset infrastructure to an Infrastructure Management Server (IMS) | 31 |
| | About the asset infrastructure | 31 |
| | Adding the asset infrastructure | 32 |
| | Managing host assets | 33 |
| | About adding host assets | 33 |
| | Prerequisites for adding hosts | 34 |
| | Packages required on Linux hosts | 35 |
| | Additional prerequisites for protecting virtual machines | 36 |
| | Adding a Windows Install host | 36 |
| | Installing the host package on a Windows host | 37 |
| | Refreshing host discovery information | 38 |
| | Removing hosts | 38 |
| | Uninstalling the host package from a Linux host | 39 |
| | Uninstalling the host package from a Windows host | 40 |
| | Managing Hyper-V assets | 40 |
| | About Microsoft Hyper-V virtualization discovery | 40 |
| | Prerequisites for Microsoft Hyper-V virtualization discovery | 41 |
| | Adding Hyper-V virtualization servers | 42 |
| | Removing Hyper-V virtualization servers | 42 |
| | Refreshing Hyper-V virtualization servers | 43 |
| | Managing VMware virtualization servers | 43 |
| | Prerequisites for adding VMware virtualization servers | 44 |
| | Adding VMware virtualization servers | 45 |
| | Editing a VMware virtualization discovery configuration | 47 |
| | Removing a VMware vCenter Server discovery configuration | 48 |
| | | 48 |
| | Refreshing VMware vCenter Server discovery information | 49 |
| | Viewing the details of a VMware virtualization discovery configuration | 50 |
| | | 50 |
| Chapter 6 | Managing users and global settings | 51 |
| | Managing user authentication and permissions | 51 |
| | About user authentication in the web console | 52 |

| | |
|--|----|
| About user permissions in the web console | 53 |
| Predefined personas | 54 |
| About limiting object scope for personas | 59 |
| Configuring authentication domains | 60 |
| Unconfiguring authentication domains | 62 |
| Configuring user groups and users | 63 |
| Assigning permissions to user groups and users | 64 |
| Adding custom personas | 65 |
| Predefined jobs that can be used for custom personas | 66 |
| Custom persona required for starting or stopping resiliency groups | 69 |
| Configuring Windows global user | 70 |
| Managing settings for alerts and notifications and miscellaneous product settings | 70 |
| Adding, modifying, or deleting email settings | 71 |
| Adding, modifying, or deleting SNMP settings | 73 |
| Setting up rules for event notifications | 73 |
| Viewing events and logs in the console | 74 |
| Modifying the purge setting for logs and SNMP traps | 75 |
| Modifying the purge setting for reports | 76 |
| Modifying the purge setting for activities | 76 |
| Enabling or disabling telemetry collection | 76 |

Chapter 7 Using the Web console 78

| | |
|---|----|
| Tour of the HPE Helion and Veritas Continuity web console screen | 78 |
| Menu bar options | 79 |
| Navigation pane options | 80 |
| Filtering and searching for objects in the web console | 81 |
| About the HPE Helion and Veritas Continuity Dashboard | 81 |
| Web console icons | 82 |

Chapter 8 Updating HPE Helion and Veritas Continuity 84

| | |
|---|----|
| About updating HPE Helion and Veritas Continuity | 84 |
| About applying updates to HPE Helion and Veritas Continuity | 85 |
| Prerequisites for a repository server | 87 |
| Setting up the repository server | 88 |
| Adding a repository server in HPE Helion and Veritas Continuity | 89 |
| Assigning a repository server in HPE Helion and Veritas Continuity | 90 |
| Applying updates to virtual appliances using the console | 90 |
| Applying updates to virtual appliance using klish menu | 91 |

| | | |
|-----------------------|---|------------|
| | Applying updates to the hosts | 93 |
| | Refreshing the information about applicable updates | 93 |
| | Removing an update from the repository server | 93 |
| Chapter 9 | Uninstalling HPE Helion and Veritas Continuity | 95 |
| | About uninstalling HPE Helion and Veritas Continuity | 95 |
| Chapter 10 | Troubleshooting and maintenance | 96 |
| | Accessing HPE Helion and Veritas Continuity log files | 96 |
| | Troubleshooting replication | 97 |
| | Components of HPE Helion and Veritas Continuity virtual appliances | 99 |
| | Using Veritas Services and Operations Readiness Tools to find a Unique Message Identifier description and solution | 100 |
| | Displaying risk information | 100 |
| Appendix A | Using CLISH menu in HPE Helion and Veritas Continuity | 102 |
| | About klish | 102 |
| | Using klish | 103 |
| Glossary | | 113 |
| Index | | 116 |

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 is a managed service based on a scalable platform to build recovery solutions across data centers specific to your business needs. The solution offers a unified approach for visibility and control of IT service continuity for physical machines, virtual machines, and complex multi-tier business services across a global landscape.

HPE Helion and Veritas Continuity has the following core capabilities:

Effective Recovery with strong ROI

HPE Helion and Veritas Continuity enables the service provider (HPE) to manage disaster recovery operations such as recovery, and rehearsal of your assets from an on-premises datacenter to HPE continuity centers (based on HPE Helion OpenStack®).

The solution is backed with a proprietary replication technology optimized for cloud ecosystems. The replication enables effective movement of data from your on-premises datacenter to the HP continuity centers.

Visibility into continuity readiness

The console dashboard provides visibility into the health of your protected assets such as physical machines, virtual machines, and multi-tier business services. HPE Helion and Veritas Continuity enables workload automation of your assets to perform DR readiness and recovery operations ensuring simplified continuity.

See [“About HPE Helion and Veritas Continuity features and components”](#) on page 9.

About HPE Helion and Veritas Continuity features and components

The following is a brief introduction to HPE Helion and Veritas Continuity key components and their relationships. 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 12.

| | |
|--|---|
| Infrastructure Management Server (IMS) | <p>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.</p> <p>To achieve scale, multiple IMSs can be deployed in the production data center. One IMS is deployed in the cloud.</p> <p>See “Infrastructure Management Server (IMS)” on page 12.</p> |
| Replication Gateway | <p>The component that transfers data tapped by IO tap module from one data center to another. Replication Gateways are deployed as virtual appliances.</p> <p>See “Resiliency Platform Replication Gateways” on page 12.</p> |
| Storage Proxy | <p>The component that enables HPE Helion and Veritas Continuity to connect the primary storage as iSCSI targets to the production gateway during the Resync operation. The Storage Proxy is deployed as a virtual appliance.</p> <p>See “Storage Proxy” on page 13.</p> |
| data center | <p>The resiliency domain contains two data centers, a production data center and a recovery data center in the cloud. The cloud data center has a Resiliency Manager, one or more cloud Replication Gateways, and one IMS; the production data center has one or more on-premises Replication Gateways, one or more Storage Proxies, and one or more IMSs.</p> |
| asset infrastructure | <p>The data center assets that you add to HPE Helion and Veritas Continuity for discovery and monitoring by the IMS.</p> <p>The asset infrastructure includes hosts and virtualization servers. Once the asset infrastructure is discovered by the IMS, the discovered physical and virtual machines are listed in the console as assets to manage or protect.</p> |
| resiliency group | <p>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.</p> |

| | |
|--------------------------------|---|
| service objective | <p>A template to define the type of operations and technologies that are supported for a group of assets. You apply a service objective to each resiliency group.</p> <p>A template which identifies the characteristics of a service. These could be availability related characteristics such as local redundancy, and number of nodes in a cluster or DR characteristics such as remote recovery, Recovery Point Objective (RPO) SLAs, rehearsal support etc. Service objective is applied when a group of assets are being added to a resiliency group.</p> <p>HPE Helion and Veritas Continuity monitors the resiliency groups based on the service objective definition and raises the risks as applicable.</p> |
| Virtual Business Service (VBS) | <p>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, and resync the entire VBS.</p> |

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 12.

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 HPE Helion and Veritas Continuity so that assets can be discovered and monitored by an IMS.

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 12.

Resiliency Platform Replication Gateways

The Replication 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.

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 have access to the data stores of 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 12.

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

See “Resiliency Platform 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

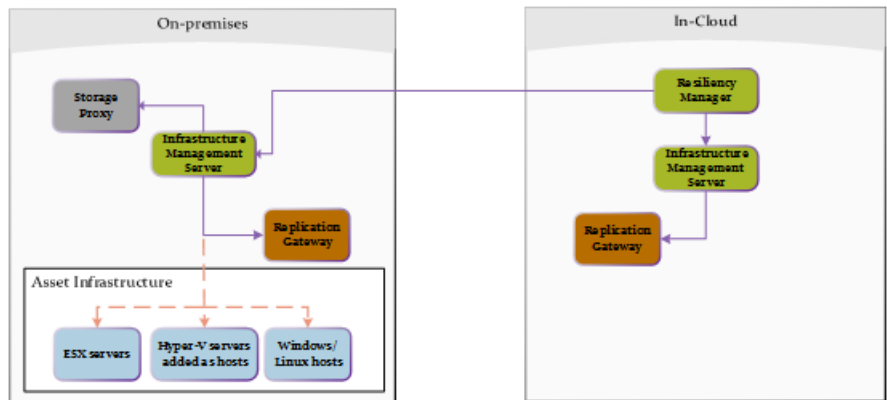


Table 1-1 describes the various steps involved in deploying and configuring HPE Helion and Veritas Continuity virtual appliance components:

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 25. See “Deploying the virtual appliance on-premises through VMware vSphere Client” on page 26. |

Table 1-1 Deploying and configuring HPE Helion and Veritas Continuity virtual appliance components (*continued*)

| Step | Action | Description |
|------|--|--|
| 2 | Deploy and configure Replication Gateway on-premises | See “Deploying the virtual appliance on-premises through Hyper-V Manager” on page 25. See “Deploying the virtual appliance on-premises through VMware vSphere Client” on page 26. |
| 3 | Deploy and Configure Storage Proxy on-premises | See “Deploying the virtual appliance on-premises through Hyper-V Manager” on page 25. See “Deploying the virtual appliance on-premises through VMware vSphere Client” on page 26. |

System requirements

This chapter includes the following topics:

- [Supported hypervisors for deploying 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 deploying HPE Helion and Veritas Continuity virtual appliance

For the list of supported platforms for deployment of virtual appliances, see the *Hewlett Packard Enterprise Helion and Veritas Continuity Hardware and Software Compatibility List*.

See [“About deploying the HPE Helion and Veritas Continuity virtual appliance”](#) on page 24.

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, storage Proxy, and YUM repository server:

Table 2-1 Minimum configurations

| Component | Minimum configuration |
|--|--|
| Resiliency Manager | Disk space 60 GB RAM 32 GB Virtual CPU 8 |
| Infrastructure Management Server (IMS) | Disk space 60 GB RAM 16 GB Virtual CPU 8 |
| Gateway | Disk space 40 GB RAM 16 GB Virtual CPU 8 Additional external disk of 100 GB |
| Storage proxy | Disk space 40 GB RAM 16 GB Virtual CPU 8 |
| YUM repository server | Disk space 60 GB RAM 4 GB Virtual CPU 2 |

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

If you plan not to use the YUM virtual appliance, you need an 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.

See [“Setting up the repository server”](#) on page 88.

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. Even if you are using dynamic memory, the above mentioned minimum configuration should be met.

See “[About deploying the HPE Helion and Veritas Continuity virtual appliance](#)” on page 24.

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.
- The hostname that you use for a virtual appliance must not start with a digit and must not contain the underscore (_) character.
- 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 |
| 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 klish 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 klish 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 |
|------------|----------------------|---|-----------------|----------|
| 33056 | 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 |

Table 2-5 Ports used for target Gateway in resync operation

| Ports used | Description | For communication between | Direction | Protocol |
|------------|---------------|---|-----------------|----------|
| 67 | BOOTP server | Target Gateway enabled with DHCP role and physical host | Uni-directional | UDP |
| 68 | BOOTP client | Target Gateway enabled with DHCP role and physical host | Uni-directional | UDP |
| 69 | TFTP protocol | Target Gateway enabled with PXE role and physical host | Uni-directional | TCP/UDP |

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 klish access Used for remote deployment of the packages on remote UNIX host from IMS | IMS and the hosts | Bi-directional | TCP |

Table 2-6 Ports used for virtual machines (*continued*)

| Ports used | Description | For communication between | Direction | Protocol |
|------------|---------------------------------|---|-----------------|----------|
| 5634 | Used for communication with IMS | IMS and the hosts | Bi-directional | TCP |
| 33056 | Used for replication | On-premises virtual machine and Replication Gateway | Uni-directional | TCP |

Table 2-7 Ports used for physical machines

| Ports used | Description | For communication between | Direction | Protocol |
|------------|--|--|-----------------|----------|
| 443 | Used for SSL communication | Recovery site Gateway and Physical Host in resync operation. | Uni-directional | TCP |
| 3260 | Used by <code>tgtd</code> daemon for communication between gateway and Storage Proxy | Recovery site Gateway and Storage Proxy in resync operation. | Uni-directional | TCP |

See [“About deploying the HPE Helion and Veritas Continuity virtual appliance”](#) on page 24.

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

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.

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 deployed 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 25.

See [“Deploying the virtual appliance on-premises through VMware vSphere Client”](#) on page 26.

HPE Helion and Veritas Continuity virtual appliance file names

To deploy HPE 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_2.0.1.0_IE.zip`
 - For Replication Gateway and Storage Proxy:
`HPEHVC_Gateway_SP_Hyper-V_Virtual_Appliance_2.0.1.0_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_2.0.1.0_IE.ova`
 - For Replication Gateway and Storage Proxy:
`HPEHVC_Gateway_SP_VMWare_Virtual_Appliance_2.0.1.0_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 this virtual appliance as a Replication Gateway, 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 If you want to use DHCP as your network, enter the MAC address of the appliance in the DHCP server. For information on obtaining the MAC address of the appliance, see the documentation of Hyper-V Manager.
- 14 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 29.

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 this virtual appliance as Replication Gateway, go to the **Edit virtual machine settings** and attach an external disk of minimum 100 GB.
- 10 If you want to use DHCP as your network, enter the MAC address of the appliance in the DHCP server. For information on obtaining the MAC address of the appliance, see the documentation of VMware vSphere client.
- 11 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 this virtual appliance as Replication Gateway, 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** If you want to use DHCP as your network, enter the MAC address of the appliance in the DHCP server. For information on obtaining the MAC address of the appliance, see the documentation of VMware vSphere client.
- 10** 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 29.

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](#)

About configuring the HPE Helion and Veritas Continuity components

After the HPE Helion and Veritas Continuity virtual appliance deployment, you are expected to configure the HPE Helion and Veritas Continuity component that you have deployed, through the bootstrap process. Resiliency Manager is the first component to be configured in HPE Helion and Veritas Continuity.

It is recommended that you configure the Resiliency Manager and Infrastructure Management Server (IMS) together on a single virtual appliance in cloud and then configure one IMS on-premises. If you plan not to configure the Resiliency Manager and Infrastructure Management Server (IMS) together on a single virtual appliance, then you have to configure one Resiliency Manager and one IMS in cloud and another IMS on-premises. You also need to configure one Replication Gateway on cloud and another on-premises and one Storage Proxy on-premises. The steps for configuring all these components are similar except the product settings, where you need to select the component that you want to configure on that particular virtual appliance.

The bootstrap process is automatically invoked when you log in to the virtual appliance console for the first time using the admin user login. The following settings are configured as part of this process to set up the component:

- **Host Network settings:** Settings such as hostname, IP address, subnet mask, default gateway, and DNS server.
- **Appliance settings:** Settings such as 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.

Note: Before using the hostname and the IP address in the **Host Network settings**, you need to register them with the DNS server. The hostname and the IP address that you use for product configuration, cannot be changed later.

This configuration is done through the bootstrap process only for the first time. After the successful configuration, the bootstrap process is disabled. The subsequent admin user logins to the virtual appliance will automatically start with Command Line Interface SHell (klish) menu. If you want to change these settings later, you can use klish 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 the 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.
- To use DHCP network, you need to reserve an IP address for the appliance in the DHCP server along with the corresponding MAC address.
- Before you use the hostname and the IP address in the Network settings, make sure that the reverse lookup for that IP works.
- In case of a Replication Gateway, make sure to attach an extra disk of at least 100 GB before configuring the Gateway.

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

This chapter includes the following topics:

- [About the asset infrastructure](#)
- [Adding the asset infrastructure](#)
- [Managing host assets](#)
- [Managing Hyper-V assets](#)
- [Managing VMware virtualization servers](#)

About the asset infrastructure

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

The asset infrastructure includes Windows or Linux virtual machines, virtualization servers and physical machines. All 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 virtualization servers.

See [“Managing host assets”](#) on page 33.

See [“Managing VMware virtualization servers”](#) on page 43.

See [“Managing Hyper-V assets ”](#) on page 40.

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”](#) on page 32.

Adding the asset infrastructure

Before you can monitor and manage data center assets from the console, you must add the asset infrastructure to HPE Helion and Veritas Continuity. The Infrastructure Management Server (IMS) then discovers the asset information for monitoring and operations in the console.

The asset infrastructure is added as hosts or virtualization servers.

To add the asset infrastructure

- 1 Navigate



Settings (menu bar) > **Infrastructure** > **Details View**

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

- 2 Expand the data center and locate the technology category for the asset.

See [“Managing host assets”](#) on page 33.

See [“Managing Hyper-V assets ”](#) on page 40.

See [“Managing VMware virtualization servers”](#) on page 43.

Managing host assets

The asset infrastructure that you must add to HPE Helion and Veritas Continuity for discovery and monitoring by 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”](#) on page 33.

See [“Prerequisites for adding hosts ”](#) on page 34.

See [“Packages required on Linux hosts”](#) on page 35.

See [“Additional prerequisites for protecting virtual machines”](#) on page 36.

See [“Removing hosts ”](#) on page 38.

See [“Refreshing host discovery information”](#) on page 38.

See [“Uninstalling the host package from a Linux host”](#) on page 39.

See [“Uninstalling the host package from a Windows host”](#) on page 40.

See [“Refreshing host discovery information”](#) on page 38.

About adding host assets

You add several types of assets as hosts to an Infrastructure Management Server (IMS). All assets that you want to manage and protect must be added to the IMS.

Note: You must add a host for discovery only once.

When you add hosts to HPE Helion and Veritas Continuity, 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, ensure that all prerequisites are met.

Note: When you add a Linux virtual machine, the device paths are replaced by the file system UUID in `/etc/fstab`. When a Linux virtual machine is booted in the cloud after the migrate, takeover, or rehearse operation, the device path of the disks change. For example if on the production data center the path of the disk is `/dev/sdb`, then on the cloud it may change to `/dev/vdb`. This change disrupts the boot process. To fix this, UUID is enabled in `/etc/fstab`.

See [“Prerequisites for adding hosts”](#) on page 34.

Prerequisites for adding hosts

Before you add hosts to HPE Helion and Veritas Continuity for discovery and monitoring by 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:

- 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.
- 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 36.

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 35.

Additional prerequisites for Windows systems:

- You must have at least one Windows Install host already added to the IMS, where you want to add the Windows host. If you do not have any Windows Install host associated with the IMS, you first need to add a Windows Install host, and then you can add any number of Windows hosts using the Windows Install host.
See [“Installing the host package on a Windows host”](#) on page 37.

- 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”](#) on page 33.

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. |
| 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”](#) on page 34.

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 a Windows Install host

Before you add a Windows host to any Infrastructure Management Server (IMS) for applications discovery or as a discovery host, you need to have at least one Windows Install host associated with that IMS. This Windows Install host acts as a control host that enables the process of adding a Windows host to the IMS.

To add a Windows Install host

1 Prerequisites

Ensure that the managed host package (VRTSsfmh) is installed on the host.
 See [“Installing the host package on a Windows host”](#) on page 37.

2 Navigate



Settings (menu bar) > **Infrastructure** > **Details View**

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

3 Under the data center, locate the IMS, and do the following:



Select the vertical ellipsis for the IMS > **Manage Windows Install Hosts**.

4 Under **Enter Host Details**, enter the host name, username, and password for the host to be added, and click **Submit**.

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_7.0.0.0_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”](#) on page 33.

Refreshing host discovery information

You can submit a refresh request to update the information displayed for the hosts that have been added to HPE Helion and Veritas Continuity. Once the refresh operation is complete, the Assets page in the console is also updated.

To refresh a host discovery

- 1 Navigate



Settings (menu bar) > **Infrastructure** > **Details View**

- 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 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”](#) on page 33.

Removing hosts

You can remove one or more hosts that were added to HPE Helion and Veritas Continuity for discovery and monitoring by 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.

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

When you perform the remove host operation on any host, it first uninstalls all the add-ons that were installed on that host, and then removes the host from the IMS. The host is not removed in case the uninstallation of any of the add-ons fails. If the same host is being used in any other context in add-ons such as discovery host, the add-ons that are required for that particular context are not removed from the host. If a host is used in multiple contexts, then it is removed only from the context from where you perform the remove host operation.

To remove hosts

1 Navigate



Settings (menu bar) > **Infrastructure** > **Details View**

- 2 Go to the section from where you want to remove the host. For example, the **Managed Host** section or the **Storage** section.
- 3 On the host listing page, right-click the host and select **Remove**.
- 4 Confirm that you want to remove the host.
- 5 You can check the details of the remove host workflow in the **Recent Activities** pane.

Removing a host 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 39.

See [“Uninstalling the host package from a Windows host”](#) on page 40.

See [“Managing host assets”](#) on page 33.

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”](#) on page 38.

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”](#) on page 38.

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

You can add Hyper-V servers to HPE Helion and Veritas Continuity for discovery of Hyper-V virtual machines by an Infrastructure Management Server (IMS). Hyper-V servers are added as virtualization servers.

See [“About Microsoft Hyper-V virtualization discovery”](#) on page 40.

See [“Prerequisites for Microsoft Hyper-V virtualization discovery”](#) on page 41.

See [“Adding Hyper-V virtualization servers”](#) on page 42.

See [“Removing Hyper-V virtualization servers”](#) on page 42.

See [“Refreshing Hyper-V virtualization servers”](#) on page 43.

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”](#) on page 40.

Prerequisites for Microsoft Hyper-V virtualization discovery

You can add Microsoft Hyper-V servers to HPE Helion and Veritas Continuity for virtualization discovery by an Infrastructure Management Server (IMS).

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 | <ul style="list-style-type: none"> ■ If there is no Control host associated with the IMS, then you need to install the VRTSsfmh package on the Hyper-V Server (parent partition). The VRTSsfmh package is installed automatically by the IMS when you add the Hyper-V server to HPE Helion and Veritas Continuity. ■ The Hyper-V role must be enabled. ■ The Windows Management Instrumentation (WMI) service must be running on the Hyper-V Server. <p>In addition to the Hyper-V Server, the virtual machines to be protected must also be added as hosts.</p> <p>There are additional prerequisites for adding hosts.</p> <p>See “Prerequisites for adding hosts” on page 34.</p> |
| Exported storage discovery | <ul style="list-style-type: none"> ■ The Windows Management Instrumentation (WMI) service must be running on the guest. |

See [“Managing Hyper-V assets”](#) on page 40.

See [“Managing host assets”](#) on page 33.

Adding Hyper-V virtualization servers

You can add Microsoft Hyper-V servers to HPE Helion and Veritas Continuity for virtualization discovery by an Infrastructure Management Server (IMS).

To add Hyper-V virtualization servers

1 Prerequisites:

See [“Prerequisites for Microsoft Hyper-V virtualization discovery”](#) on page 41.

2 Navigate



Settings (menu bar) > **Infrastructure** > **Details View**

Expand the data center > **Virtualization** > **Hyper-V** tab

Launch the **+ Hyper-V Server** wizard

Tip: You can also access **Manage Asset Infrastructure** from the **Quick Actions** menu.

3 In the wizard, specify the required information about the Hyper-V server, and click **Submit**.

4 The Hyper-V server that has been added is listed on the **Hyper-V** tab. Discovery of the Hyper-V virtual machines occurs in the background. You can view the progress on the **Activities** page.

If changes are made after the IMS discovery is complete, you need to refresh the discovery of the Hyper-V server.

See [“Managing Hyper-V assets”](#) on page 40.

Removing Hyper-V virtualization servers

You can remove a Hyper-V virtualization server that has been added to HPE Helion and Veritas Continuity.

To remove a Hyper-V virtualization server

1 Navigate



Settings (menu bar) > **Infrastructure** > **Details View**

Expand the data center > **Virtualization** > **Hyper-V** tab

Tip: You can also access **Manage Asset Infrastructure** from the **Quick Actions** menu.

2



On the row for the Hyper-V server that you want to remove, select the vertical ellipsis > **Remove**.

Refreshing Hyper-V virtualization servers

You can refresh the IMS discovery for a Hyper-V virtualization server that has been added to HPE Helion and Veritas Continuity.

To refresh Hyper-V virtualization servers

1 Navigate



Settings (menu bar) > **Infrastructure** > **Details View**

Expand the data center > **Virtualization** > **Hyper-V** tab

Tip: You can also access **Manage Asset Infrastructure** from the **Quick Actions** menu.

2



On the row for the Hyper-V server that you want to refresh, select the vertical ellipsis > **Refresh**.

See [“Managing Hyper-V assets ”](#) on page 40.

Managing VMware virtualization servers

You can add VMware vCenter servers to HPE Helion and Veritas Continuity for discovery by an Infrastructure Management Server (IMS).

The VMware discovery provides the following 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 virtualization servers”](#) on page 44.
- See [“Adding VMware virtualization servers ”](#) on page 45.
- See [“Editing a VMware virtualization discovery configuration”](#) on page 47.
- See [“Viewing the details of a VMware virtualization discovery configuration”](#) on page 50.
- See [“Removing a VMware vCenter Server discovery configuration ”](#) on page 48.
- See [“Refreshing VMware vCenter Server discovery information”](#) on page 49.

Prerequisites for adding VMware virtualization servers

Ensure that the following requirements are met to add the VMware vCenter or ESX servers to HPE Helion and Veritas Continuity for discovery by an Infrastructure Management Server (IMS):

- Ensure that the IMS 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 discovery host for the vCenter Server.
- Ensure that you have configured near real-time discovery of VMware events.
- 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”](#) on page 34.

Adding VMware virtualization servers

You can add VMware vCenter servers to HPE Helion and Veritas Continuity for discovery by an Infrastructure Management Server (IMS). The VMware discovery provides the following information:

- Information on the vCenter Server
- 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 select which of the available ESX servers to discover.
- Information on the virtual machines that are configured on the ESX servers

Note: If there is more than one IMS in a data center, you can add the same vCenter Server to more than one IMS. For example, you may want to split up the ESX server discovery between multiple IMSs. To accomplish this, you first add the vCenter Server to one IMS for one set of ESX servers. Then once discovery is complete, you use the Edit option on the existing vCenter Server to add it to another IMS and select a different set of ESX servers.

To add VMware virtualization servers

1 Prerequisites:

See [“Prerequisites for adding VMware virtualization servers”](#) on page 44.

Optionally, you can add a separate host to act as the discovery host for the vCenter Server and select it while adding the VMware server.

2 Navigate



Settings (menu bar) > **Infrastructure** > **Details View**

Expand the data center > **Virtualization** > **VMware** tab

Launch the + **vCenter** wizard

Tip: You can also access **Manage Asset Infrastructure** from the **Quick Actions** menu.

- 3 In the wizard, specify the following information and click **Next**.
 - Specify the fully-qualified name of the vCenter Server that you want to discover along with its port number. The default port is 443.
 - When entering login credentials, an administrative vCenter Server user account is required.
 - If the data center has more than one IMS, a list of IMS names is shown. Select the IMS that you want to use to discover and monitor the vCenter Server and ESX servers.
 - If you have added a separate discovery host, select it.
- 4 Choose to automatically discover all ESX servers or select ESX servers to discover. If multiple clusters are available, you can use **Group By** to sort the list of ESX servers by cluster. Click **Next**. It is recommended to select all ESX servers within a cluster.
- 5 Review the configured vCenter Server, ESX servers, and IMS on the verification screen and submit the configuration.

If you choose the auto discover option, all currently available ESX servers are discovered. In addition, ESX servers later added to the vCenter Server will be automatically discovered.

The wizard notifies you of any issues.

The vCenter Server that has been added is listed on the **VMware** tab. Discovery of the ESX servers occurs in the background. You can view the progress on the **Activities** page.

If changes are made on the virtualization servers after the IMS discovery is complete, you need to refresh the discovery of the vCenter Server.

See [“Refreshing VMware vCenter Server discovery information”](#) on page 49.

See [“Editing a VMware virtualization discovery configuration”](#) on page 47.

Editing a VMware virtualization discovery configuration

You can edit a vCenter Server discovery configuration that was added to HPE Helion and Veritas Continuity to modify the information for an existing IMS or to add the vCenter Server to another IMS (if there is more than one in the data center). For example, you may choose to split ESX discovery between multiple IMSs.

For an existing IMS previously selected for the vCenter Server, you can modify:

- The credentials to log on to the vCenter Server
When entering login credentials, an administrative vCenter Server user account is required.
- The ESX server discovery
You can add or remove selected ESX servers or change between individual server discovery and auto discovery.

Note: You can only use autodiscovery if the vCenter Server is configured with only one IMS. If an existing IMS is autodiscovering the ESX servers, you are not able to add another IMS for that vCenter Server without first editing the configuration for the existing IMS to change from auto discovery.

To edit a virtualization discovery configuration

1 Navigate



Settings (menu bar) > **Infrastructure** > **Details View**

Expand the data center > **Virtualization** > **VMware** tab

2



On the row for the vCenter server, select the vertical ellipsis > **Edit**.

3 In the **Edit vCenter** wizard:

- To edit the vCenter configuration for the current IMS:
If more than one IMS is listed, select the IMS that currently discovers the vCenter Server.
Optionally, edit the credentials to log on to the vCenter.
On the next screen, you can add or remove selected ESX servers or change between individual server discovery and auto discovery.
- To add the vCenter to a new IMS for discovery (only available if first IMS is not configured for autodiscovery):

Select the new IMS and enter the vCenter Server logon credentials.

On the next screen, any ESX servers not yet selected for the existing IMS are listed. Select those you want the new IMS to discover.

To see the ESX servers already added to the first IMS, select **Show ESX in other IMS**. These are not available for selection. To return to the list of available servers, uncheck the box.

- 4 Review the configured vCenter Server, ESX servers, and IMS on the verification screen and proceed with the configuration.

The wizard notifies you of any issues. Discovery of the modifications occurs in the background. You can view the progress on the **Activities** page.

On the VMware tab, if you have added an IMS, both the existing and new IMS are listed on the row for the vCenter Server.

See [“Managing VMware virtualization servers”](#) on page 43.

Removing a VMware vCenter Server discovery configuration

You can remove a VMware vCenter Server from HPE Helion and Veritas Continuity. If the vCenter Server has been configured for discovery by more than one Infrastructure Management Server (IMS), you can choose whether to select the IMS to remove it from or remove it from all the IMSs.

To remove a VMware virtualization discovery configuration

1 Prerequisites

Ensure that you consider how removing the virtualization discovery may affect resiliency groups. If you remove a vCenter Server (or associated ESX servers) from discovery by an IMS, any virtual machines from those ESX servers are no longer discovered and monitored by the IMS. Therefore, if any of those virtual machines are currently in a resiliency group, they will be automatically removed from the resiliency group.

Reviewer question: Per demo feedback discussion, the decision was that if the ESX servers affected contain VMs that are part of RGs, a risk will be raised for the affected RGs - will need more info on this. Also need more info on implications for a resiliency group configured for DR -in particular. Do you need to perform any update DR operation on an affected resiliency group after removing ESX servers with VMs in the RG?

2 Navigate



Settings (menu bar) > **Infrastructure** > **Details View**

Expand the data center > **Virtualization** > **VMware** tab

3



On the row for the vCenter server, select the vertical ellipsis > **Remove**.

4

If more than one IMS is configured for discovery of the vCenter Server, the wizard prompts you to choose whether to remove the vCenter configuration from all IMSs or from selected IMSs. When you choose **from selected Infrastructure Management Servers**, the list of IMSs is displayed for you to make your selection.

5

Confirm that you want to remove the vCenter Server configuration from one or more IMSs. Discovery occurs in the background. You can view the progress on the **Activities** page.

See [“Managing VMware virtualization servers”](#) on page 43.

Refreshing VMware vCenter Server discovery information

You can refresh the information displayed for VMware virtualization servers that have been added to HPE Helion and Veritas Continuity.

To refresh a virtualization discovery

1 Navigate



Settings (menu bar) > **Infrastructure** > **Details View**

Expand the data center > **Virtualization** > **VMware** tab

2



On the row for the vCenter Server that you want to refresh, select the vertical ellipsis > **Refresh**.

If more than one IMS is configured for discovery of the ESX servers managed by this vCenter Server, the refresh operation applies to all of the IMSs. Discovery occurs in the background. You can view the progress on the **Activities** page.

See [“Managing VMware virtualization servers”](#) on page 43.

Viewing the details of a VMware virtualization discovery configuration

You can view details for a vCenter Server that has been added to HPE Helion and Veritas Continuity. Details include whether autodiscovery is enabled, the ESX servers that are discovered, and the number of virtual machines for each ESX server.

To view the details of a virtualization discovery configuration

1 Navigate



Settings (menu bar) > **Infrastructure** > **Details View**

Expand the data center > **Virtualization** > **VMware** tab

2



On the row for the vCenter Server, select the vertical ellipsis > **Details**.

On the Details page, if more than one IMS is configured to discover the vCenter Server, the ESX servers are grouped under the IMS that is configured to discover them.

See [“Managing VMware virtualization servers”](#) on page 43.

Managing users and global settings

This chapter includes the following topics:

- [Managing user authentication and permissions](#)
- [Managing settings for alerts and notifications and miscellaneous 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 52. See “Configuring authentication domains” on page 60. See “Unconfiguring authentication domains” on page 62. |
| 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 63. |

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

| Task | Details |
|--|---|
| Assign permissions to groups and users | <p>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.</p> <p>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.</p> <p>See “About user permissions in the web console” on page 53.</p> <p>See “Predefined personas” on page 54.</p> <p>See “About limiting object scope for personas” on page 59.</p> <p>See “Assigning permissions to user groups and users” on page 64.</p> <p>You can also create custom personas.</p> <p>See “Adding custom personas” on page 65.</p> <p>See “Predefined jobs that can be used for custom personas” on page 66.</p> <p>See “Custom persona required for starting or stopping resiliency groups” on page 69.</p> |
| Configure Windows global user | <p>To customize the static IP of Windows guest virtual machines in the VMware environment, you need to provide the administrator user name and password to log on to the Windows virtual machines.</p> <p>See “Configuring Windows global user” on page 70.</p> |

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.

It is recommended not to remove the default Resiliency Platform users or reduce the permissions of the default Resiliency Platform users.

If you change the password of a user who was configured to logon to the domain, you need to edit the configured domain and enter the new password for the user.

See [“Managing user authentication and permissions”](#) on page 51.

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 | <p>A role that has access to a predefined set of jobs (operations).</p> <p>The product comes with a set of predefined personas.</p> <p>See “Predefined personas” on page 54.</p> <p>You can also add custom personas.</p> <p>See “Adding custom personas” on page 65.</p> <p>See “Predefined jobs that can be used for custom personas” on page 66.</p> <p>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.</p> |
| Job | <p>A type of task (operation) that a user can perform.</p> <p>Examples:</p> <ul style="list-style-type: none"> 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 51.

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 |

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

| Persona | Description and scope | Jobs |
|--------------------------------------|--|--|
| Resiliency Platform admin | <p>Manage Resiliency Managers and Infrastructure Management Servers (IMs) and data centers.</p> <p>Manage assets.</p> <p>Manage user security settings and other product settings.</p> <p>Manage product updates.</p> <p>Scope: Resiliency domain.</p> | <p>Manage assets (jobs separated by type):</p> <ul style="list-style-type: none"> ■ Manage host assets ■ Manage virtualization assets ■ Manage data mover assets ■ Manage application cluster assets ■ Manage cloud assets ■ Manage copy manager assets ■ Manage enclosure assets ■ Manage access profiles <p>Manage user security settings</p> <p>Manage product settings</p> <p>Manage product updates</p> <p>Manage server deployments</p> |
| Resiliency Platform Deployment admin | <p>Manage Resiliency Managers and Infrastructure Management Servers (IMs).</p> <p>Can add an IMS to an existing data center.</p> <p>Manage product updates.</p> <p>Scope: Resiliency domain.</p> | <p>Manage product updates</p> <p>Manage server deployments</p> |

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

| Persona | Description and scope | Jobs |
|-------------------------|--|---|
| Data Center admin | <p>Manage disaster recovery settings and manage assets of specified types.</p> <p>Scope: Specified data center.</p> | <p>Manage DR settings</p> <p>Manage assets (jobs separated by type):</p> <ul style="list-style-type: none"> ■ Manage host assets ■ Manage virtualization assets ■ Manage data mover assets ■ Manage application cluster assets ■ Manage cloud assets ■ Manage copy manager assets ■ Manage enclosure assets ■ Manage access profiles |
| Resiliency Domain admin | <p>Create, update, and delete resiliency groups, virtual business services (VBSs), and resiliency plans and templates.</p> <p>Start/stop all resiliency groups and VBSs.</p> <p>Scope: Resiliency domain.</p> | <p>Manage resiliency groups</p> <p>Start/stop resiliency groups</p> <p>Manage virtual business services</p> <p>Manage resiliency plan templates</p> <p>Manage resiliency plans</p> <p>Execute custom scripts</p> |
| Resiliency Group admin | <p>Update and delete specified resiliency groups.</p> <p>Start/stop specified resiliency groups.</p> <p>Start/stop VBSs as long as the VBS contains only the specified resiliency groups.</p> <p>Scope: Specified resiliency groups.</p> | <p>Manage resiliency groups</p> <p>Start/stop resiliency groups</p> |

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

| Persona | Description and scope | Jobs |
|----------------------------------|--|---|
| Resiliency Group operator | <p>Start/stop specified resiliency groups.</p> <p>Start/stop VBSs as long as the VBS contains only the specified resiliency groups.</p> <p>Scope: Specified resiliency groups.</p> | Start/stop resiliency groups |
| VBS admin | <p>Create, update, and delete all virtual business services (VBSs).</p> <p>Start/stop all resiliency groups and VBSs.</p> <p>Scope: Resiliency domain.</p> | <p>Manage virtual business services</p> <p>Start/stop resiliency groups</p> |
| Resiliency Domain Recovery admin | <p>Configure all resiliency groups for disaster recovery (DR). ??</p> <p>Perform rehearsal and DR operations: migrate, takeover.</p> <p>Create, update, and delete resiliency plans and templates.</p> <p>Manage disaster recovery network settings.</p> <p>Start/stop all resiliency groups.</p> <p>Scope: Resiliency domain.</p> | <p>Manage resiliency groups</p> <p>Rehearse resiliency groups</p> <p>Recover resiliency groups</p> <p>Manage resiliency plans</p> <p>Manage resiliency plan templates</p> <p>Manage DR settings</p> <p>Start/stop resiliency groups</p> |

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

| Persona | Description and scope | Jobs |
|------------------------------------|---|--|
| Resiliency Group Recovery admin | <p>Manage and perform disaster recovery of resiliency groups</p> <p>Start/stop specified resiliency groups.</p> <p>Start/stop or perform DR operations on VBSs as long as the VBS contains only the specified resiliency groups.</p> <p>Scope: Specified resiliency groups.</p> | <p>Manage resiliency groups</p> <p>Start/stop resiliency groups</p> <p>Rehearse resiliency groups</p> <p>Recover resiliency groups</p> |
| Resiliency Group Recovery operator | <p>Start/stop specified resiliency groups.</p> <p>Perform disaster recovery on specified resiliency groups.</p> <p>Start/stop or perform DR operations on VBSs as long as the VBS contains only the specified resiliency groups.</p> <p>Scope: Specified resiliency groups.</p> | <p>Start/stop resiliency groups</p> <p>Perform disaster recovery of resiliency groups</p> <p>Rehearse resiliency groups</p> |
| Guest | <p>View all information in console.</p> <p>Assigned by default when user or group is configured for HPE Helion and Veritas Continuity.</p> | <p>No operations, only view permission</p> |

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

| Persona | Description and scope | Jobs |
|----------------------------------|--|---|
| Resiliency Platform Assets admin | Manage all assets such as enclosure, application, application cluster assets, virtualization, data mover, and cloud. | Manage assets (jobs separated by type): <ul style="list-style-type: none"> ■ Manage enclosure assets ■ Manage application assets ■ Manage virtualization assets ■ Manage access profiles ■ Manage cloud assets ■ Manage application cluster assets ■ Manage data mover assets |

See [“Managing user authentication and permissions”](#) on page 51.

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 54.

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 61.

- 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 51.

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. |
| Connect using SSL/TLS | 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 | Browse to the location of the trusted root CA certificate of the vendor that issued the LDAP server certificate. |
| The authentication servers require 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 |

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

| Option | Description |
|--------------------|--|
| Bind User Name/DN | <p>Enter the complete Distinguished Name (DN) of the user that is used to bind to the LDAP server.</p> <p>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</p> <p>For example, you can provide the DN as Administrator@enterprise.domainname.com ENTERPRISE\Administrator</p> <p>For RFC 2307 compliant LDAP servers, specify complete bind DN.</p> <p>For example, cn=Manager,dc=vss,dc=Veritas,dc=com</p> <p>The LDAP or the AD administrator can provide you the bind user name that you can use.</p> |
| Password | <p>Enter the password that is assigned to the bind user name that you use.</p> |
| Query Information: | |
| User (Mandatory) | <p>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.</p> <p>The system determines the search base based on the user name that you specify in this field.</p> |
| Group | <p>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.</p> <p>The system determines the search base based on the group name along with the user name that you have specified.</p> |

See [“Configuring authentication domains”](#) on page 60.

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 51.

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 64.
 See [“Managing user authentication and permissions”](#) on page 51.

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 53.

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 63.'

- 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 51.

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 > New Persona**

2 In the **New 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 66.

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 51.

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

| Jobs | Description | Scope |
|-------------------------------|---|-------------------|
| View all information | View all information in console. | Resiliency domain |
| Manage user security settings | Manage authentication domains, users and user groups, personas. | Resiliency domain |

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

| Jobs | Description | Scope |
|--|---|---|
| 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 service objectives | Activate service objectives from templates; manage activated service objectives. | Resiliency domain |
| Manage assets, by type: <ul style="list-style-type: none"> ■ Manage host assets ■ Manage virtualization assets ■ Manage data mover assets ■ Manage application cluster assets ■ Manage cloud assets ■ Manage copy manager assets ■ Manage enclosure assets ■ Manage access profiles | Add, edit, or remove specific types of asset infrastructure | Resiliency domain or specific data centers |
| Manage resiliency groups | Create, update, and delete resiliency groups. | Resiliency domain or specific resiliency groups |
| Start/stop resiliency groups | Start and stop resiliency groups. | Resiliency domain or specific resiliency groups |
| Manage virtual business services | Create, update, and delete virtual business services (VBSs). | Resiliency domain or specific VBSs |

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

| Jobs | Description | Scope |
|----------------------------------|--|---|
| Manage resiliency plans | <p>Create, update, and delete resiliency plans.</p> <p>Note: The permission to execute a resiliency plan depends on a cumulative check on permissions for individual resiliency groups and VBSs in the plan.</p> <p>See “About limiting object scope for personas” on page 59.</p> | Resiliency domain |
| Manage resiliency plan templates | <p>Create, update, and delete resiliency plan templates.</p> | Resiliency domain |
| Execute custom scripts | <p>Execute custom scripts as part of resiliency plans.</p> | Resiliency domain or specific data centers |
| Rehearse resiliency groups | <p>Perform rehearsal and rehearsal cleanup.</p> <p>Note: There is no separate job to perform rehearsal of VBSs. If the assigned scope of this job includes all the resiliency groups in a VBS, Rehearsal operations can be performed on that VBS.</p> <p>See “About limiting object scope for personas” on page 59.</p> | Resiliency domain or specific resiliency groups |

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

| Jobs | Description | Scope |
|---------------------------|--|---|
| Recover resiliency groups | Perform Recovery operations such as migrate, takeover, resync. 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 59. | Resiliency domain or specific resiliency groups |
| Manage DR settings | Configure disaster recovery network settings, for example, mapping network settings for disaster recovery or replication gateway pairing. | Resiliency domain or specific data centers |
| Manage evacuation plans | Generate or regenerate evacuation plans. Perform evacuation, rehearse evacuation or cleanup evacuation rehearsal operations. | Data center |

See [“Predefined personas”](#) on page 54.

See [“Adding custom personas”](#) on page 65.

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 65.

See [“Predefined jobs that can be used for custom personas”](#) on page 66.

Configuring Windows global user

To customize the static IP of Windows guest virtual machines in the VMware environment, HPE Helion and Veritas Continuity requires the administrator user name and password to log on to the Windows virtual machines. The user credentials can be Windows Active Directory user or Workgroup user.

For Windows Active Directory user, the Active Directory should be common for both, the primary and the recovery data center.

If a Windows virtual machine is part of a Windows Active Directory, ensure that you log on to the virtual machine at-least once using the Active Directory credentials.

For more information on customizing network, refer to the *Solutions Guide*.

To configure Windows global user

- 1 Navigate



Settings (menu bar)

Under **Product Settings**, click **User Management > Windows Global User**

- 2 Click **+ Configure User** to configure the user.
- 3 Select between Active Directory and Workgroup.
- 4 Enter the administrator user name and password. Click **Verify**.
For Workgroup user, enter user name as workgroupname\username. If the workgroup name is not customized then you can enter only the user name.
- 5 On successful verification, click **Next** and then **Finish** to submit the information.

Managing settings for alerts and notifications and miscellaneous product settings

See the following topics for information on configuring email and SNMP settings for notifications and reports, setting up rules for event notifications, configuring purge intervals, and changing telemetry settings.

See [“Adding, modifying, or deleting email settings”](#) on page 71.

See [“Adding, modifying, or deleting SNMP settings”](#) on page 73.

See [“Setting up rules for event notifications”](#) on page 73.

See [“Modifying the purge setting for logs and SNMP traps”](#) on page 75.

See [“Modifying the purge setting for reports”](#) on page 76.

See [“Modifying the purge setting for activities”](#) on page 76.

See [“Enabling or disabling telemetry collection ”](#) on page 76.

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.

Managing settings for alerts and notifications and miscellaneous product settings**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. |
| Send To | Enter the email address to which you want to send the email. |

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. Select **Send Test Email** to test your settings.**6** Review the information in the summary and submit

See [“Managing settings for alerts and notifications and miscellaneous product settings”](#) on page 70.

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 miscellaneous product settings”](#) on page 70.

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 71.

See [“Adding, modifying, or deleting SNMP settings”](#) on page 73.

2 Navigate



Settings (menu bar)

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

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

To modify or delete an existing rule: Select 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 Notifications | Select one or more events that you want to be notified about |

4 Select **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 73.

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 the purge setting for logs and SNMP traps”](#) on page 75.

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 the purge setting 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 **Product Settings**, click **Miscellaneous**

- 2 Under **Log Settings**, enter the new value for the purge setting, in months, and save the setting.

See [“Managing settings for alerts and notifications and miscellaneous product settings”](#) on page 70.

Modifying the purge setting for reports

By default, reports are saved for 7 days. You can modify this purge interval.

To modify the purge setting for reports

- 1 Navigate



Settings (menu bar)

Under **Product Settings**, click **Miscellaneous**

- 2 Under **Reports Retention Policy Settings**, enter the new value for the purge setting and save the setting.

See [“Managing settings for alerts and notifications and miscellaneous product settings”](#) on page 70.

Modifying the purge setting for activities

By default, the information on tasks performed in activities is saved for 6 months. You can modify this purge setting.

To modify the purge setting for activities

- 1 Navigate



Settings (menu bar)

Under **Product Settings**, click **Miscellaneous**

- 2 Under **Activities Settings**, enter the new value for the purge setting and save the setting.

See [“Managing settings for alerts and notifications and miscellaneous product settings”](#) on page 70.

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.

Managing settings for alerts and notifications and miscellaneous product settings

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 **Product Settings**, select **Miscellaneous**

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

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. Links to quick actions and user management are also present in the menu bar. See "Menu bar options" on page 79. |
| Navigation pane | Icons to open pages for configuring and implementing start/stop and disaster recovery operations. See "Navigation pane options" on page 80. |

Table 7-1 Overview of the web console screen areas (*continued*)

| Screen areas | Description |
|--------------|--|
| Dashboard | <p>The console home page - clicking the Home icon in the navigation pane returns to the Dashboard.</p> <p>View an overview of assets in the resiliency domain and their current status. Drill down for details.</p> <p>See “About the HPE Helion and Veritas Continuity Dashboard” on page 81.</p> |

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

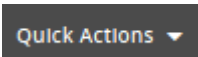

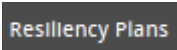






| Options | Description |
|---|--|
|  | Open drop-down selection of shortcuts to common tasks. |
|  | Schedule and run reports. View reports showing data center and asset status. |
|  | <p>Create and run custom resiliency plans for starting, stopping, and migrating resiliency groups.</p> <p>See the Solutions guide for details on resiliency plans.</p> |
|  | <p>More views</p> <p>View activities, risks, and logs.</p> <p>See “Viewing events and logs in the console” on page 74.</p> |
|  | <p>Settings</p> <p>Open Settings page for configuring and maintaining product infrastructure and other settings.</p> |

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




| Options | Description |
|---|---|
|  | <p>Notifications</p> <p>Display most recent notifications.</p> <p>Requires alerts and notifications to be enabled using Settings page.</p> <p>See "Managing settings for alerts and notifications and miscellaneous product settings" on page 70.</p> |
|  | <p>Inbox</p> <p>View actions to be completed.</p> |
|  | <p>Help</p> <p>Open Help window where you can search all help or filter by category.</p> |
|  | <p>Log out of console.</p> <p>Shows Resiliency Manager, resiliency domain, and data center.</p> |

Navigation pane options

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

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 the Assets page for configuring resiliency groups, viewing details of assets, and performing start and stop or disaster recovery operations |
|  | Opens page for configuring disaster recovery settings such as network mapping and replication gateway pairs |

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.

A point icon indicates that the data center is on premises.











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

| | |
|--|---|
| Resiliency Groups and Virtual Business Services summaries | <p>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.</p> <p>Click a square in either the Resiliency Groups or Virtual Business Services summary to display a tab of detailed information.</p> |
| DR Activity Summary | <p>Displays the statistics on recent disaster recovery activities, including the following:</p> <ul style="list-style-type: none">■ 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. <p>Click on any of the squares to display the Activities screen and more detailed information.</p> |
| Virtual Machines by Platform and OS | <p>Displays a summary of virtual machines in all data centers or information on a single data center. Use the drop-down list to filter your results. The summary lists the virtual machine types by percentage and the platform types by number.</p> |
| Top Resiliency Groups by Replication Lag | <p>Ranks the resiliency groups according to how long it takes the recovery data center to be in sync with the active data center.</p> |
| By Service Objective | <p>Displays the percentage of virtual machines that are configured for disaster recovery and unmanaged (not configured for disaster recovery).</p> <p>Use the drop-down list to filter your results.</p> |

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 resiliency groups, viewing details of assets, and performing start and stop or disaster recovery operations | Navigation pane |
|  | Disaster Recovery Settings Opens page for configuring disaster recovery settings such as network mapping and replication gateway pairs | Navigation pane |
|  | Vertical ellipsis Displays list of actions for selected object | To the right of a selected object in a list |

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](#)
- [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 klish menu](#)
- [Applying updates to the hosts](#)
- [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.

Note: Upgrade from HPE Helion and Veritas Continuity 2.0 to HPE Helion and Veritas Continuity 2.1 using the Resiliency Manager console is not supported. This upgrade can be done only through klish menu.

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:

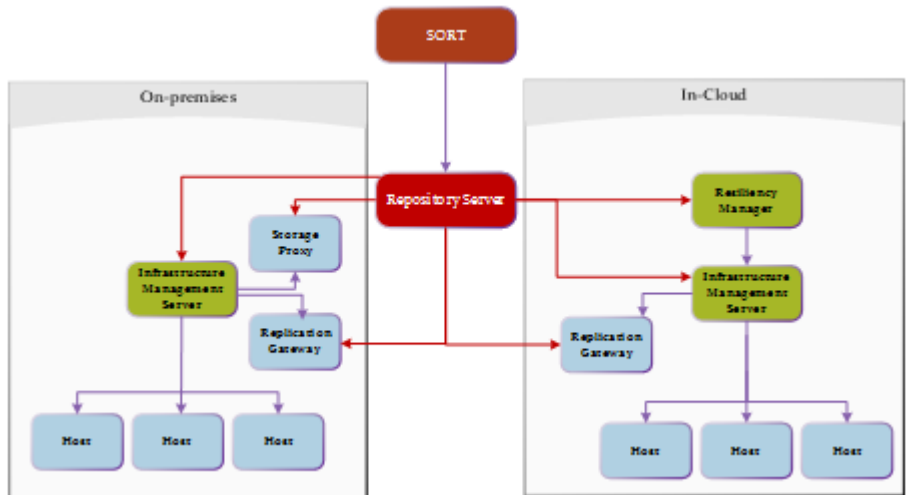
- HPE Helion and Veritas Continuity virtual appliance
- HPE Helion and Veritas Continuity add-ons
- Host packages on the assets that are added to the Infrastructure Management Server (IMS) as a host

Note: It is recommended to apply the update to all the HPE Helion and Veritas Continuity components to take the complete advantage of the changes available in the updates.

you can apply the update either across all the appliances in your environment through Resiliency Manager console, or through individual appliance's klish menu. Refer to the readme file shipped with the update to check if the update should be applied using the console or using klish menu.

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.

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 and the virtual appliance may go into an irrecoverable condition.

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 87. |
| 2 | Set up a repository server | See “Setting up the repository server ” on page 88. |

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

| Step | Task | Description |
|------|---|---|
| 3 | Apply update to the virtual appliances and hosts in the given sequence: Resiliency Manager IMS at recovery data center IMS at production data center Replication Gateway at recovery data center. After applying the update on the Replication Gateway, the add-ons also need to be updated. Replication Gateway at production data center. After applying the update on the Replication Gateway, the add-ons also need to be updated. | Refer to the readme file shipped with the update to check if the update should be applied using the console or using klish menu See “Applying updates to virtual appliance using klish menu” on page 91. See “Applying updates to virtual appliances using the console” on page 90. For updating the add-ons on Replication Gateway See “Applying updates to the hosts” on page 93. |
| 4 | Apply update on the host packages | See “Applying updates to the hosts” on page 93. |
| 5 | Remove an update from the repository server | See “Removing an update from the repository server” on page 93. |

You also have an option of applying a private hotfix, if veritas support provides you one.

Note: All the updates should be downloaded and stored in a common location.

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.
- 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.
- `createrepo` should be installed on the server.
- Perl and Python should be installed on the server. The following modules need to be installed:
 - `Archive::Extract`
 - `Archive::Tar`
 - `Config::Simple`
 - `Cwd`
 - `File::Basename`
 - `File::Copy`
 - `File::Fetch`
 - `File::Path`
 - `Getopt::Long`
 - `JSON`
 - `LWP::Simple`
 - `Time::Local`
 - `XML::Twig`

See “[About applying updates to HPE Helion and Veritas Continuity](#)” on page 85.

Setting up the repository server

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

To set up a repository server

- 1 Go to the following location and select the product and version:
<https://sort.veritas.com/patch>
- 2 You can see a list of all the applicable updates for a particular version. Select the required version and click the required update. On the next page, download the file by clicking the **Setup Repository Bundle Download** link.
- 3 Copy the file that you have downloaded to a temporary location and extract this tar file.

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

```
mkdir path_to_repository
```

- 5 The `setup_conf_repo.pl` file is one of the files that are extracted from the update that is downloaded from SORT. This file is used to configure the repository.
- 6 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
```

See [“About applying updates to HPE Helion and Veritas Continuity”](#) on page 85.

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. There can be multiple repository servers added to HPE Helion and Veritas Continuity at a time.

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 85.

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.

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.

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 85.

Applying updates to virtual appliances using the console

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

Before applying the update using the console, you need to first add a repository server to HPE Helion and Veritas Continuity and then assign a repository server to the virtual appliance.

See [“Adding a repository server in HPE Helion and Veritas Continuity”](#) on page 89.

See [“Assigning a repository server in HPE Helion and Veritas Continuity”](#) on page 90.

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 85.

Applying updates to virtual appliance using klish menu

You can use the klish 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.

To apply updates to virtual appliance using klish menu

- 1 It is recommended to power off the appliance and take a snapshot of the appliance before applying the updates.
- 2 You need to log into the virtual appliance as admin and go to the updates sub-menu.
- 3 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-repository
```
 - 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_repository
```
- 4 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 klish, you need to refresh the information to reflect the current status of the updates in the Resiliency Manager web console.
- 5 Navigate



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

Click **Refresh**.

See [“Using klish”](#) on page 103. for a complete list of options available with `Updates` command.

See [“About applying updates to HPE Helion and Veritas Continuity”](#) on page 85.

Applying updates to the hosts

Updates for the add-ons and for the host packages installed on the assets that are added as a host, becomes available under the **Managed Hosts** section in the Resiliency Platform console. These components can be upgraded from the console.

To apply updates to the hosts

- 1 Navigate



Settings (menu bar) > Updates

- 2 Under **Available updates**, go to **Managed Hosts** section. Select the hosts on which you want to apply the update, and click **Upgrade**.

In the list of hosts, some of the hosts may be listed for both the production as well as recovery data centers. You need to apply the update only on a host which is listed under production data center.

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 klish, 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 85.

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
```

See [“About applying updates to HPE Helion and Veritas Continuity”](#) on page 85.

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 decommission 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.

If you want to remove an Infrastructure Management Server (IMS), you first need to remove the association of the IMS with the resiliency Manager before removing the virtual appliance node:

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 klish 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 or SSH session 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 klish” on page 103.

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. You will be prompted to enter the admin user credentials and download the zip file.

Troubleshooting replication

Log information

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
```

Replication states and actions required

The following table lists the cases when replication is in paused or stopped state, the reason and action required to fix it.

Table 10-1 Replication state and required action

| State | Common behaviour in Linux and Windows | Windows specific behaviour | Linux specific behaviour | Admin action |
|---------------|---|--|---|---|
| Paused state | Network disconnect Memory cap hit Flow control received from gateway | | | No action is required in these cases. Replication resumes automatically once the reason that caused it to go in pause state is fixed. |
| | If the resume replication task fails due to network reconnect or flow control, then replication goes to CLI paused state | | | You need to verify the cause of the CLI pause state and then resume replication operation. |
| | | If disk is removed then an event is generated and the Veritas Replication Set goes into a CLI pause state. | | You need to verify the cause of the CLI pause state and then resume replication operation using the commands mentioned after the table. |
| Stopped state | At configuration (includes reboot), if there is a mismatch between the provided and available disk-ids (including DRL disk) Failure to read or write to DRL disk Write failure on any configured disk If there is a write beyond configured disk size Failure to allocate memory for IO Context structure | | If heart beating (polls every 5 minutes) detects that a configured disk is unavailable due to disk failure or removal | User intervention is required in all these cases to start replication. You need to validate the reason of failure that led replication to a stopped state and accordingly take corrective action. |

Commands to resume replication:

- **Linux:** `/opt/VRTSitrptap/bin/vxtapaction resume -cg CG_ID`
- **Windows:** `"C:\Program Files\Veritas\VRTSitrptap\cli\vxtapaction" resume -cg CG_ID`

Components of HPE Helion and Veritas Continuity virtual appliances

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

Table 10-2

| 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. |
| 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 (klish) | Command Line Interface Shell (klish) 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 24.

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 10-3 Ways to display risks

| To display ... | Do the following: |
|--|--|
| A complete list of risks across the resiliency domain | <ol style="list-style-type: none"> <li data-bbox="794 319 1220 442"> 1 On the menu bar, select  More Views > Risks <li data-bbox="794 447 1220 517"> 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 | <ol style="list-style-type: none"> <li data-bbox="794 522 1220 703"> 1 On the navigation pane, select  (Assets) and the tab for either Resiliency Groups or Virtual Business Services. <li data-bbox="794 708 1220 807"> 2 On the tab, double-click a resiliency group or virtual business service to display detailed information. <li data-bbox="794 812 1220 904"> 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 klish](#)
- [Using klish](#)

About klish

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 (klish) menu to manage the configuration-related changes to the product.

You can use klish 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 klish”](#) on page 103.

Using klish

After the product configuration, whenever you log in to the HPE Helion and Veritas Continuity appliance, you get the main menu of klish. 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 klish:

- **Network settings:** You can reconfigure the subnet mask, default gateway, DNS server, and search domains using the klish 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 klish 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 klish 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 klish 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-7 |
| network | Network configuration Table A-9 |

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

| Menu option | Description |
|-------------|--|
| settings | Appliance settings Table A-15 |
| support | Access logs Table A-19 |
| updates | Manage updates and patches Table A-21 |

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 |
| datamover | Manage Resiliency Platform Data Mover activities and objects This option is available only on a Replication Gateway or Storage Proxy appliance Table A-4 |
| exit | Log out from the current CLI session |
| help | Display an overview of the CLI syntax |
| infra-appliance | List Replication gateway or Storage Proxy appliances or remove the Replication gateway appliance Table A-5 |
| services | Manage the appliance services <ul style="list-style-type: none"> ■ 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-6 ■ 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_register | Register the IMS using the registration URL obtained after initiating the Add IMS operation |
| ims | Configure Infrastructure Management Server |
| rm | Configure Resiliency Manager |
| show | Show the configured component |

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

| Menu option | Description |
|------------------|---|
| start | Start a Veritas Replication Set |
| abort | Stop a Veritas Replication Set |
| delete | Delete a Veritas Replication Set |
| clear-admin-wait | Clear the admin Wait status for the Veritas Replication Set |

Table A-5 Options available with **infra-appliance** command

| Menu option | Description |
|-------------|--|
| list | List the Storage Proxy or Replication gateway appliance. |
| remove | Remove the Replication Gateway or Storage Proxy appliance. You need to remove the Gateway pair before you remove the Gateway. |

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

| Menu option | Description |
|-------------|---|
| show | Show HPE Helion and Veritas Continuity services. the short service names displayed here are used while exercising other options with services command such as restart, start, status. |

Table A-6 Options available with **services** command (*continued*)

| Menu option | Description |
|-------------|---|
| restart | Restart HPE Helion and Veritas Continuity services Two options available are: <code>restart all</code> where, <i>all</i> means all the services. <code>restart service name</code> where, <i>service name</i> 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: <code>start all</code> where, <i>all</i> means all the services. <code>start service name</code> where, <i>service name</i> 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: <code>status all</code> where, <i>all</i> means all the services. <code>status service name</code> where, <i>service name</i> 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: <code>stop all</code> where, <i>all</i> means all the services. <code>stop service name</code> where, <i>service name</i> is the name of a particular service. You can provide multiple service names (comma separated). |

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

| Menu option | Description |
|-------------|--------------------------------------|
| back | Return to the previous menu |
| exit | Log out from the current CLI session |

Table A-7 Options available with **monitor** command (*continued*)

| Menu option | Description |
|-------------|--|
| datamover | Display VRP Datamover activities and objects This option is available only on a Replication Gateway or Storage Proxy appliance Table A-8 |
| FSusage | Display filesystem usage |
| 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-8 Options available with **datamover** command

| Menu option | Description |
|--------------|---|
| repl-sets | Display the details about Veritas Replication Sets including RPO, connection state, replication state |
| update-sets | Display the list of current update sets which are in transit |
| ingress-data | Display the IO statistics for the data transfer from protected virtual or physical machine to Gateway (IOReceiver statistics) |
| network-data | Display the network related statistics for data transfer between production site Gateway and recovery site Gateway (Transceiver statistics) |
| disk-data | Display the IO statistics for the data write on recovery site disks (Applier statistics) |

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

| Menu option | Description |
|-------------|--|
| back | Return to the previous menu |
| dns | Show or change the DNS Table A-10 |
| exit | Log out from the current CLI session |

Table A-9 Options available with **network** command (*continued*)

| Menu option | Description |
|---------------|---|
| gateway | Show or change the Gateway Table A-11 |
| help | Display an overview of the CLI syntax |
| hostname | Show the hostname |
| ip | Show or change the IP address Table A-12 |
| netmask | Show or change the netmask Table A-13 |
| search-domain | Show or change the domain Table A-14 |

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

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

Table A-11 Options available with **gateway** command

| Menu option | Description |
|-------------|--------------------------|
| set | Configure Gateway |
| show | Show the current Gateway |

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

| Menu option | Description |
|-------------|---|
| set | Configure the IP address for additional NIC |
| show | Show the current IP address |

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

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

Table A-14 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-15 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-16 |
| exit | Log out from the current CLI session |
| help | Display an overview of the CLI syntax |
| lvm | Perform operations related to logical volume manager on the appliance Table A-17 |
| 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 Table A-18 |

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

| Menu option | Description |
|-------------|------------------------|
| show | Show the time and date |

Table A-17 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 newly-added disk during add-disk or remove-disk operation, the existing data on the new disk is deleted.

Table A-18 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-19 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 |

Table A-19 Options available with **support** command (*continued*)

| Menu option | Description |
|-------------|---|
| loggather | <ul style="list-style-type: none"> 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-20 If the appliance has been configured as a Replication Gateway or a Storage Proxy, then <code>loggather</code> command will collect the logs of the Replication gateway or the Storage Proxy. |
| shell | Open the bash shell prompt for support user |

Table A-20 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-21 Options available with **updates** command

| Menu option | Description |
|-----------------------------|---|
| config-local-iso-repository | Configure the repository from locally mounted ISO image on CD-ROM |
| apply-update | Apply the specified update |
| back | Return to the previous menu |
| config-repository | Configure the repository Table A-22 |
| exit | Log out from the current CLI session |
| help | Display an overview of the CLI syntax |
| list-updates | List the applicable updates |

Table A-21 Options available with **updates** command (*continued*)

| Menu option | Description |
|-------------------|---|
| 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-22 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 klish”](#) on page 102.

See [“Accessing HPE Helion and Veritas Continuity log files”](#) on page 96.

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, physical machines, virtual machines, or virtualization servers. |
| assets | In HPE Helion and Veritas Continuity, the physical and the virtual machines that have been discovered by the Infrastructure Management Server (IMS) and that can be grouped into resiliency groups. |
| klsh | Command Line Interface SHell. Provides the command line menu on the virtual appliance for use after the initial bootstrap configuration. |
| data center | <p>A location that contains asset infrastructure to be managed by HPE Helion and Veritas Continuity.</p> <p>For the disaster recovery use case, the resiliency domain contains at least two data centers, the production data center and the recovery data center in the cloud. The cloud data center has a Resiliency Manager, one or more replication gateways, and one or more IMSs; the production data center has one or more replication gateways, one or more storage proxies, and one or more IMSs</p> |
| host | <p>Physical servers, virtual machines, or Hyper-V servers that are added to the Infrastructure Management Server (IMS) as hosts.</p> <p>Adding the assets as hosts installs the host package that is used by the IMS for discovery and monitoring.</p> |
| 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 | Migration refers to a planned activity involving graceful shutdown of physical and virtual machines at the production data center and starting them at the recovery cloud data center or vice versa. In this process, replication ensures that consistent data of the assets is made available at the target data center which could be the production data center or the cloud. |

| | |
|---------------------------------|---|
| 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 storage on the production data center and the Cloud. |
| 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 replication gateway on the production data center during the Resync operation. |
| take over | An activity initiated by a user when the production data center is down due to a disaster and the assets 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 | <p>An appliance that includes the operating system environment and the software application which are deployed together as a virtual machine.</p> <p>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).</p> |
| virtual business service (VBS) | <p>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.</p> |
| web console | <p>The web-based management console on the Resiliency Manager that is used to configure the settings for the resiliency domain and perform operations.</p> |

Index

A

- activities
 - purge interval 76
- alert settings
 - email 71
 - SNMP 73
- asset infrastructure
 - about adding assets as hosts 33
 - adding 32
 - adding Hyper-V virtualization servers 42
 - adding VMware virtualization servers 45
 - editing VMware virtualization servers 47
 - Linux packages required for discovery of hosts 35
 - prerequisites for hosts 34
 - prerequisites for Hyper-V virtualization discovery 41
 - prerequisites for VMware discovery 44
 - refreshing hosts 38
 - refreshing VMware virtualization servers 49
 - removing hosts 38
 - removing VMware virtualization servers 48
 - viewing VMware virtualization server details 50
 - Windows host installation 37
- authentication domains
 - configuring 60
 - unconfiguring 62

C

- Configure DR
 - prerequisites 36

D

- dashboard 81
- deploying
 - Hyper-V Manager 25
 - virtual appliance 24
 - VMware vSphere Client 26

E

- email settings 71

- events 74

F

- firewall 18

G

- global user
 - configuring 70

H

- host
 - Windows install 36
- hosts
 - installing host package on Windows host 37
 - prerequisites for adding 34
 - refreshing IMS discovery 38
 - removing 38
 - uninstalling host package from a Linux host 39
 - uninstalling host package from a Windows host 40
- HPE Helion and Veritas Continuity
 - about 8
 - features and components 9
- Hyper-V servers
 - adding 42
 - discovery in IMS 40
 - prerequisites 41
 - refreshing 43
 - removing 42

I

- icons 82
- Infrastructure Management Server
 - overview 12
- IPV 18

J

- jobs for custom personas 66

K

- klish
 - about 102
 - using 103

L

- Linux packages required for discovery of hosts 35
- logs
 - purge settings 75
 - viewing in console 74

M

- menu bar 79

N

- notification settings
 - email 71
 - rules 73
 - SNMP 73

P

- permissions 51
 - assigning to users 64
 - overview 53
- personas
 - custom 65–66
 - limiting object scope for operations 59
 - predefined 54
- ports 18
- purge setting
 - activities 76
 - logs and SNMP traps 75
 - reports 76

R

- reports
 - purge settings 76
- resiliency domain
 - overview 11
- Resiliency Manager
 - overview 12
- risks
 - view information 100
- rules for event notifications 73

S

- SNMP
 - configuring settings 73
 - purge settings for traps 75
- supported hypervisors
 - virtual appliance 16
- system requirements 16

T

- telemetry collection 76

U

- Uninstalling
 - about 95
- updates
 - about 84–85
 - add-ons 93
 - hosts 93
 - refreshing 93
 - removing 93
 - through console 90
 - through klish 91
- upgrade
 - adding repository server 89
 - assigning repository server 90
 - downloading updates 88
 - prerequisites of repository server 87
 - setting up repository server 88
- user authentication 51–52
- user permissions
 - overview 53
- users
 - assigning permissions 64
 - configuring 63

V

- virtual appliance
 - components 99
 - deploying 24
 - filenames 25
- virtual appliances
 - about 29
- VMware virtualization server
 - adding 45
 - editing configuration 47
 - refreshing configuration 49
 - removing configuration 48
 - requirements for IMS discovery 44

VMware virtualization server *(continued)*
viewing details 50

W

web browser requirements 22