

# Hewlett Packard Enterprise Helion and Veritas Continuity 2.0 User's Guide

# Hewlett Packard Enterprise Helion and Veritas Continuity User's 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

|                  |  |           |
|------------------|--|-----------|
| <b>Chapter 1</b> | <b>Overview of HPE Helion and Veritas Continuity</b>                                 | <b>6</b>  |
|                  | .....  | 6         |
|                  | About HPE Helion and Veritas Continuity .....  | 6         |
|                  | About HPE Helion and Veritas Continuity features and components .....                | 7         |
|                  | HPE Helion and Veritas Continuity capabilities .....                                 | 9         |
|                  | About HPE Helion and Veritas Continuity user permissions .....                       | 9         |
| <b>Chapter 2</b> | <b>Understanding replication</b>   | <b>10</b> |
|                  | About HPE Helion and Veritas Continuity replication .....                            | 10        |
|                  | About HPE Helion and Veritas Continuity replication architecture .....               | 11        |
|                  | About full synchronization .....   | 13        |
|                  | How HPE Helion and Veritas Continuity handles application writes .....               | 14        |
|                  | How HPE Helion and Veritas Continuity handles disk multipathing .....                | 15        |
|                  | How HPE Helion and Veritas Continuity supports encryption for data replication ..... | 16        |
| <b>Chapter 3</b> | <b>Understanding disaster recovery</b>   | <b>17</b> |
|                  | About disaster recovery using HPE Helion and Veritas Continuity .....                | 17        |
|                  | How HPE Helion and Veritas Continuity handles take over .....                        | 18        |
|                  | How HPE Helion and Veritas Continuity handles migrate .....                          | 18        |
|                  | How HPE Helion and Veritas Continuity handles rehearsal .....                        | 19        |
| <b>Chapter 4</b> | <b>Organizing assets into resiliency groups</b>                                      | <b>20</b> |
|                  | About resiliency groups .....  | 20        |
|                  | Guidelines for organizing resiliency groups .....                                    | 21        |
|                  | Displaying resiliency group information and status .....                             | 21        |
|                  | Viewing resiliency group details .....   | 24        |

|                       |   |    |
|-----------------------|---|----|
| <b>Chapter 5</b>      | <b>Managing Virtual Business Services using HPE Helion and Veritas Continuity</b> ..... | 27 |
|                       | About virtual business services .....   | 27 |
|                       | Understanding virtual business service tiers .....                                      | 27 |
|                       | Displaying virtual business service details .....                                       | 28 |
| <b>Chapter 6</b>      | <b>Monitoring operations and tasks</b> .....  | 29 |
|                       | Viewing activities .....  | 29 |
| <b>Chapter 7</b>      | <b>Monitoring and reporting on assets status</b> .....                                  | 31 |
|                       | About the HPE Helion and Veritas Continuity Dashboard .....                             | 31 |
|                       | Understanding asset types .....   | 33 |
|                       | Displaying an overview of your assets .....   | 33 |
|                       | About reports .....   | 34 |
|                       | Managing report preferences .....   | 35 |
|                       | Scheduling a report .....   | 37 |
|                       | Running a report .....  | 39 |
|                       | Viewing and managing report schedules .....   | 40 |
|                       | Viewing reports .....   | 41 |
| <b>Chapter 8</b>      | <b>Monitoring risks</b> .....   | 43 |
|                       | About risk insight .....  | 43 |
|                       | Displaying risk information .....   | 44 |
|                       | Predefined risks in HPE Helion and Veritas Continuity .....                             | 45 |
|                       | Viewing the current risk report .....   | 51 |
|                       | Viewing the historical risk report .....  | 52 |
| <b>Appendix A</b>     | <b>Replication prerequisites for protected virtual machines</b> .....                   | 53 |
|                       | Additional prerequisites for protecting virtual machines .....                          | 53 |
|                       | Installing virtio drivers on the on-premises Windows virtual machines .....             | 54 |
|                       | Enabling disk UUID on virtual machines .....  | 57 |
| <b>Glossary</b> ..... |   | 58 |
| <b>Index</b> .....    |   | 61 |

# Overview of HPE Helion and Veritas Continuity

This chapter includes the following topics:

- [About HPE Helion and Veritas Continuity](#)
- [About HPE Helion and Veritas Continuity features and components](#)
- [HPE Helion and Veritas Continuity capabilities](#)
- [About HPE Helion and Veritas Continuity user permissions](#)

## 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 7.

## 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.

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.

Infrastructure Management Server (IMS)

The component that discovers, monitors, and manages the asset infrastructure within a data center. The IMS transmits information about the asset infrastructure to the Resiliency Manager. The IMS is deployed as a virtual appliance.  
To achieve scale, multiple IMSs can be deployed in the production data center. One IMS is deployed in the cloud.

Replication Gateway

The component that transfers data tapped by IO tap module from one data center to another. Replication Gateways are deployed as virtual appliances.

Storage Proxy

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.

|                                |   |
|--------------------------------|---|
| 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>  |

For more information on the above components, refer to the Deployment Guide.



## HPE Helion and Veritas Continuity capabilities

HPE Helion and Veritas Continuity helps you monitor and manage recovery across multiple data centers. It provides the following capabilities:

- Protecting and managing virtual machines as a single entity.
- Displaying an overview of your resiliency domain including the number and health of your resiliency groups.
- Starting and stopping resiliency groups for maintenance.
- Configuring disaster recovery for a resiliency group
- Rehearsing disaster recovery
- Migrating a resiliency group
- Taking over resiliency groups
- Viewing reports
- Managing activities and resiliency plans

## About HPE Helion and Veritas Continuity user permissions

Users that are configured for HPE Helion and Veritas Continuity have permission by default to view the web console but not to perform any operations. Permissions for operations must be assigned separately by a HPE Helion and Veritas Continuity administrator, who assigns the appropriate personas to users or groups. A persona is a role with access to a set of operations. The administrator can further limit the scope of some operations by selecting the objects, such as resiliency groups, to which the user has access.

For example, an administrator can assign one user the permission to perform operations on resiliency group RG1 and assign another user the permission to perform operations on RG2. If more resiliency groups are added later, the administrator needs to update permissions to assign access to the new resiliency groups.

Some objects, such as resiliency plans or virtual business services, can include multiple resiliency groups. To perform an operation on such an object, a user must have access to all its resiliency groups. Otherwise, the operation fails.

For more information on setting up user access to operations, refer to the *Deployment Guide*.

# Understanding replication

This chapter includes the following topics:

- [About HPE Helion and Veritas Continuity replication](#)
- [About HPE Helion and Veritas Continuity replication architecture](#)
- [About full synchronization](#)
- [How HPE Helion and Veritas Continuity handles application writes](#)
- [How HPE Helion and Veritas Continuity handles disk multipathing](#)
- [How HPE Helion and Veritas Continuity supports encryption for data replication](#)

## About HPE Helion and Veritas Continuity replication

HPE Helion and Veritas Continuity provides data replication between the production data center and the cloud data center. The software-based replication contributes to an effective disaster recovery solution.

HPE Helion and Veritas Continuity replicates the physical and virtual machine writes at the source location to the cloud, which provides a consistent copy of the data. If a disaster occurs at the source location, HPE Helion and Veritas Continuity uses the copy of the data on the cloud to start the virtual machine. During normal operations, the direction of replication is from the source data center to the target data center on the cloud. The source data center on which the physical or the virtual machine is running is known as the production data center. The data center at the target cloud location is known as the recovery data center.

To set up replication, group the assets (physical and virtual machines) into resiliency groups and configure for disaster recovery. The resiliency group is the unit of recovery, so group the assets that need to be recovered together into the same

resiliency group. When you configure a resiliency group for disaster recovery, HPE Helion and Veritas Continuity puts the assets into Veritas Replication Sets and associated replication units. Each Veritas Replication Set comprises all of the disks for a single physical or virtual machine, which usually includes a boot disk and multiple data disks. Each disk is a replication unit.

See “[About resiliency groups](#)” on page 20.

When an application or virtual machine runs, several processes perform writes to disks, in a specific order. For example, a database posts any database change to the log before writing to the table space. The term write-order fidelity means that the write order is maintained at all times, including when recovering from a disk failure.

HPE Helion and Veritas Continuity maintains write-order fidelity for a Veritas Replication Set when the replication is in the Active state. Write-order fidelity ensures that the data in the cloud recovery data center is consistent. While the data at the recovery data center can be behind in time, it must be a consistent image of the production data center at a point of time in the past.

The HPE Helion and Veritas Continuity replication tracks writes for the assets on the production data center in the order in which they are received. The HPE Helion and Veritas Continuity replication then applies the writes on the recovery data center in the same order. The recovery data center in the cloud is available to take over if required.

Features of HPE Helion and Veritas Continuity replication include the following:

- Replicates the data of the assets in a resiliency group to the cloud over any IP network in a LAN or WAN environment.  
You can choose to apply an encryption scheme to data replication.
- Enables you to easily recover your physical and virtual machines in the cloud.
- Ensures the data consistency at the physical and virtual machine level.

## About HPE Helion and Veritas Continuity replication architecture

The deployment includes at least two virtual appliances that are known as Replication Gateways. One Replication Gateway is deployed on the production data center and one Replication Gateway is deployed in the cloud. The administrator installs and configures the Replication Gateway services.

For details about deploying HPE Helion and Veritas Continuity, see *HPE Helion and Veritas Continuity Deployment Guide*.

The production Replication Gateway and the cloud Replication Gateway are linked together into a Replication Gateway pair, which establishes the replication channel between the source and the target. A Replication Gateway pair is a one-to-one mapping of production Replication Gateway to the cloud Replication Gateway. Communication between the Replication Gateways occurs through the WAN - usually a dedicated VPN link. You can choose to apply an encryption scheme to data replication. The Replication Gateway need not be on the same virtualization server as the protected physical or virtual machines.

The on-premises assets have a kernel module installed that is used to intercept and replicate the I/O's on the server. This module is called the `vxtap`.

Each Replication Gateway includes four daemons that run when replication is active: replication engine, I/O receiver, transceiver, and applier. The replication engine includes a scheduler, which manages the jobs and policies in the Replication Gateway. Each Replication Gateway has a configuration database that tracks the paired Replication Gateways, the Veritas Replication Sets, and the corresponding replication units with their sizes.

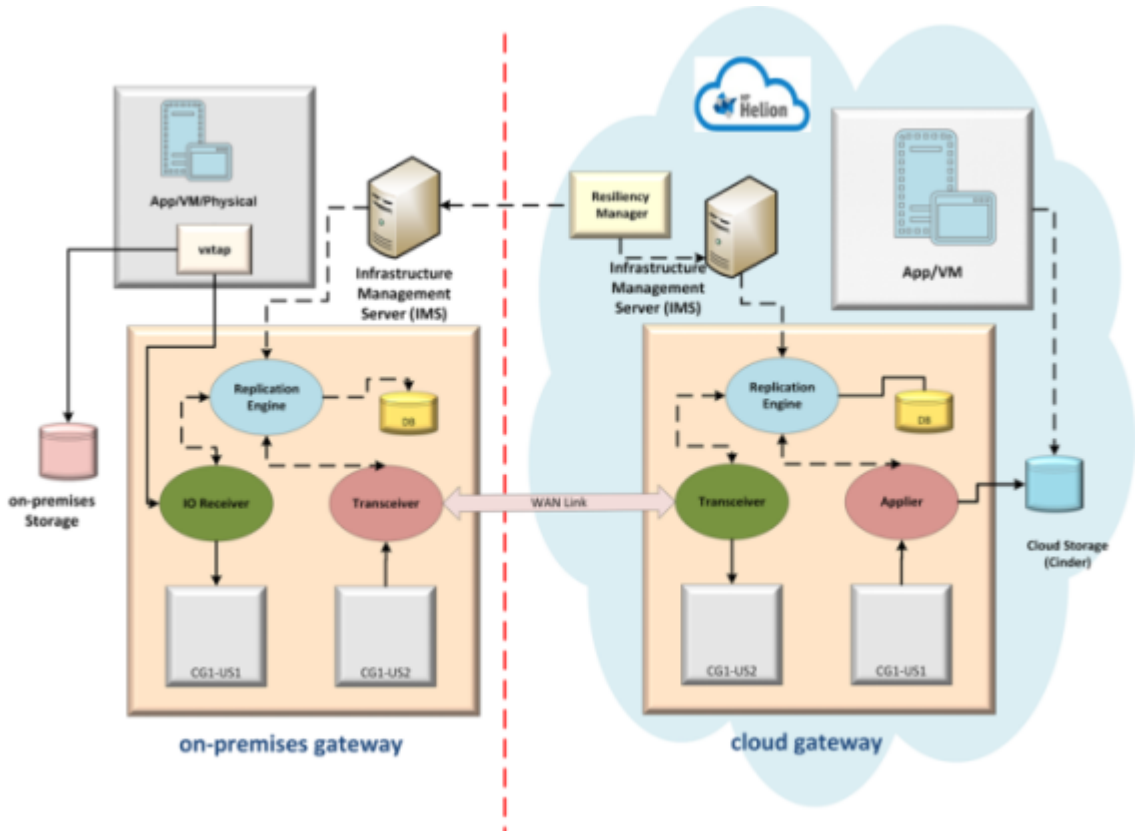
During the asynchronous replication, HPE Helion and Veritas Continuity processes an incoming write by performing the following steps in the order listed:

- The application issues a write to the storage on the production data center.
- The I/O tap module (`vxtap`) records the location of the I/O on the Replication Block Tracking (RBT) disk.
- The `vxtap` kernel module sends the I/O to the production storage.
- If the I/O is successful, then `vxtap` sends the I/O data over the network to the I/O receiver in the production Replication Gateway.
- The I/O receiver aggregates the I/Os.
- Periodically, the aggregated I/Os are sent to the transceiver.
- The transceiver sends the I/Os across the network to the transceiver on the cloud Replication Gateway.
- The transceiver on the cloud Replication Gateway sends it to the applier.
- The applier writes the I/O to the cloud storage.

The Storage Proxy is another virtual appliance that is deployed and configured on the assets at the production data center. The Storage Proxy is deployed on the same virtualization server as the protected virtual machines. The Storage Proxy is used so that the production Replication Gateway can be managed independently of the protected physical or virtual machines. The Storage Proxy is used during the Resync operation and while migrating from the Cloud data center to the production data center, to synchronize the data on the production data center with that on the

recovery data center. The Storage Proxy exports the physical and virtual machine storage to the on-premises Replication Gateway as iSCSI disks. The Replication Gateway can then replicate the recovery cloud data to that storage. You can provision multiple Storage Proxies from different virtualization servers that export virtual machine storage to the same Replication Gateway.

**Figure 2-1** Replication architecture



## About full synchronization

When replication is started, the cloud storage must be synchronized with the data from the production data center. This process of synchronizing the entire set of data from the production to cloud data center is known as full synchronization. The amount of time that is required for full synchronization depends on several factors. These factors include the size of the replication disks, the network speed of the LAN and the WAN network, resiliency, and the amount of I/O occurring during the

synchronization. After the full synchronization is completed, the replication moves into an active state. In the active state, the replication solution maintains write-order fidelity.

A full synchronization is also required before you migrate from the cloud to the production data center. When you perform the migrate operation, the application runs in the cloud data center. Before you migrate from the cloud data center back to the production data center, you need to run the Resync operation. The Resync operation synchronizes the data on the production data center with the data in the cloud storage.

When the synchronization completes, the production data center is up-to-date. You can then proceed with the DR operations.

## How HPE Helion and Veritas Continuity handles application writes

HPE Helion and Veritas Continuity replication uses the vxtap kernel module to intercept and process application writes on the protected asset (physical or virtual machines). When HPE Helion and Veritas Continuity replication is configured, the vxtap kernel module resides between the application on the protected physical or virtual machine and the underlying data storage. The vxtap kernel module intercepts the writes to the storage, while reads are directly processed from the on-premises storage.

The vxtap kernel module uses a disk called the Replication Block Tracking (RBT) disk to persistently record the location of the write I/Os. The RBT disk is an on-premises disk that should not be used by any other application, physical machine, or virtual machine. Each Veritas Replication Set (which represents a physical or virtual machine being protected) has its own RBT disk. The RBT disk is not replicated.

If the protected asset is a virtual machine, then HPE Helion and Veritas Continuity creates the required RBT disks.

If the protected asset is a physical machine, then that physical machine must have a RAW disk that can be used as the DRL disk. This DRL disk should be selected when you configure resiliency groups for disaster recovery.

The vxtap kernel module records the location of the write I/O, and sequences the writes, and accumulates them on the Replication Gateway on the production data center. The writes are then applied to the storage. The writes accumulated on the production Replication Gateway are periodically sent to the cloud Replication Gateway. The cloud Replication Gateway applies the writes to the cloud storage.

The replication includes any changes to the boot disks of the physical and virtual machines as well as the writes from the applications on the assets. The replication results in bootable copies of the virtual machines on the cloud. The virtual machines in the cloud are created and used only if a disaster occurs on the production data center. If the production data center fails, the assets that were running on the production data center can be brought up on the recovery data center.

## How HPE Helion and Veritas Continuity handles disk multipathing

HPE Helion and Veritas Continuity can handle disk multipathing for physical machines when Device Mapper for Linux hosts and MPIO feature for Windows hosts are enabled.

On a Linux machine, if the multipathing software detects multipathed disks, then for each disk that is multipathed the software creates a new disk device. This device is referred to as a 'metanode'. The metanode abstracts all paths to the disk. Any I/O operation that is performed using the metanode is reflected on the disk. For example, the file systems are mounted using the metanode device, and not any of the disk path devices. Hence if disks are multipathed, then the software must be enabled for I/O tap module (vxtap) to work.

On Windows, the operating system detects the multipathed disks and presents a single disk object which can be used for all I/Os.

While migrating from Cloud data center to physical machines on the production data center, HPE Helion and Veritas Continuity detects and groups all the multipathed disks found in the device tree. One path for every disk is selected and is used for exporting that disk as an iSCSI target. Remaining paths are ignored. If a disk is unreachable from its selected path, then the migrate operation fails.

Ensure that you have enable Device Mapper on Linux hosts and MPIO feature on Windows hosts before you create resiliency groups using your assets.

If you disable multipathing after configuring the resiliency group for remote recover, then you need to perform full synchronization of data. Use the following commands to synchronize the data.

Stop the consistency group using following command:

```
/opt/VRTSitrptap/bin/vxtapaction stop -cg <cgid>
```

Start full synchronization of the data using the following command:

```
/opt/VRTSitrptap/bin/vxtapaction start -cg <cgid>
```

Where <cgid> is the ID of the consistency group.

## How HPE Helion and Veritas Continuity supports encryption for data replication

The Replication Gateway supports encryption using OpenSSL for data transfer. When creating or modifying a Replication Gateway pair, you can choose whether to apply an encryption scheme to the data replication. Applying an encryption scheme results in increased CPU usage and reduced data transfer throughput. Encryption schemes available are AES128-GCM-SHA256 and AES256-GCM-SHA384. The default scheme is AES256-GCM-SHA384.

If you modify the gateway pair to enable or disable encryption, the transceiver on the Replication Gateways is restarted. When the transceiver restarts, it resumes sending or receiving update sets from where it left off. Full synchronization is not required.



# Understanding disaster recovery

This chapter includes the following topics:

- [About disaster recovery using HPE Helion and Veritas Continuity](#)
- [How HPE Helion and Veritas Continuity handles take over](#)
- [How HPE Helion and Veritas Continuity handles migrate](#)
- [How HPE Helion and Veritas Continuity handles rehearsal](#)

## About disaster recovery using HPE Helion and Veritas Continuity

A comprehensive disaster recovery strategy ensures that your mission-critical IT functions can continue during and after a disaster and any unforeseen risk can be mitigated to the extent possible.

HPE Helion and Veritas Continuity lets you perform disaster recovery operations on your critical IT services. This section introduces you to the key features of HPE Helion and Veritas Continuity:

- Monitoring of data center assets
- Ability to group your physical and virtual machines in resiliency groups based on your production environment and business needs.
- Making business services more resilient by providing the ability to perform disaster recovery operations on physical and virtual machines. For example, migrate and take over.

- Ability to replicate data from production data centers to recovery data centers using Resiliency Platform Data Mover.
- Resiliency plan (a sequential execution of predefined steps) to automate site-level recovery operations on your IT infrastructure in the event of downtime.
- Auto-discovery and real-time tracking for recovery objectives.
- Ability to perform non-disruptive testing (rehearsal) on your assets to ensure that your infrastructure is adequately prepared for protection in the event of disaster.
- Reporting capabilities providing details about resiliency health of your assets.

## How HPE Helion and Veritas Continuity handles take over

Take over is an activity initiated by a user when the production data center is down due to a disaster, and the assets in your data center need to be restored at the recovery data center to provide business continuity.

In the event of disaster, you can use the Takeover operation to provision and start the physical and the virtual machines at the recovery data center with the available data. Since it is an unplanned event, the data available at the recovery data center may not be up-to-date. You need to evaluate the tolerable limit of data loss. If the available data is within the acceptable limits, perform the Takeover operation to move the on-premises workloads to the cloud. The Takeover operation brings up the assets at the recovery data center using the latest data on the cloud storage.

In HPE Helion and Veritas Continuity, you first group the assets into a resiliency group and configure disaster recovery for the resiliency group. Select a resiliency group to perform the take over. The take over activity operates on an entire resiliency group, even if the disaster affects only certain hosts in the resiliency group.

After a take over, the virtual machine in the cloud runs the application and writes to the storage in the cloud.

## How HPE Helion and Veritas Continuity handles migrate

Migration refers to a planned activity involving graceful shutdown of the physical and the virtual machines at the production data center and starting them at the recovery cloud data center and 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.

When you migrate a resiliency group, the replication should be active and in a consistent state. When you initiate a Migrate operation, HPE Helion and Veritas Continuity checks whether the physical machines, virtual machines, and on-premises gateways are up.

The Migrate operation is similar to the Takeover operation, except that the Migrate operation is used when the physical and the virtual machines on the production data center can be gracefully shut down. The Takeover operation is used in case of disaster, when the physical and the virtual machines on the production data center are not reachable.

## How HPE Helion and Veritas Continuity handles rehearsal

A disaster recovery rehearsal is an operation to verify the ability of your configured resiliency group to fail over on to the recovery data center during disaster. A rehearsal is a zero-downtime test that mimics the configuration, the application data, the storage, and the failover behavior of your resiliency group.

Before you can perform a rehearse operation, you must configure a network in the cloud that is isolated from the recovery cloud network. The configuration maps the cloud network that is used for the recovery data center to the cloud network to use for the rehearsal. The rehearsal network simulates the production network environment so that the tests of the application and the workload on the rehearsal network represent a realistic scenario.

When you perform the disaster recovery rehearsal, HPE Helion and Veritas Continuity creates a snapshot of the physical and virtual machines data in the cloud. HPE Helion and Veritas Continuity then provisions the virtual machines in the rehearsal cloud network. The virtual machines in the cloud are populated with the data from the snapshot. You can bring up the virtual machines in the cloud, to test that the failover or migration works as expected. When you are satisfied with the testing of the simulated failover or migration to the recovery data center, use the rehearsal cleanup operation to clean up the rehearsal virtual machines in the resiliency group. The cleanup operation deletes all of the temporary objects that were created during the rehearsal.

# Organizing assets into resiliency groups

This chapter includes the following topics:

- [About resiliency groups](#)
- [Displaying resiliency group information and status](#)
- [Viewing resiliency group details](#)

## About resiliency groups

Resiliency groups are the unit of management and control in HPE Helion and Veritas Continuity. After assets are added to HPE Helion and Veritas Continuity, you organize related assets into a resiliency group that you can protect and manage as a single entity.

For example, you can organize several physical or virtual machines into a resiliency group, and name it `Asset_Group`. Note that a resiliency group can have only physical machines or only virtual machines, a mix of physical and virtual machines is not supported. When you perform an action on `Asset_Group` from the HPE Helion and Veritas Continuity console, all the assets in the group are included. For example, if you start `Asset_Group`, all the assets in the group start, similarly when you stop `Asset_Group` all assets stop.

The operations available for a resiliency group depend on how it is configured. During the configuration of a resiliency group, you apply a service objective that identifies the objective or intent for that group of assets. If you apply a service objective that supports remote recovery, the resiliency group supports operations like migrate and take over.

You can optionally use a service objective that only monitors the assets and provides only basic operation capabilities like start and stop operations and no remote recovery operations.

## Guidelines for organizing resiliency groups

Resiliency groups are most useful when the assets in the group share common characteristics.


While creating a resiliency group follow these guidelines for selecting the assets:

- If the assets are virtual machines, ensure that all the virtual machines that are to be grouped in a single resiliency group are from a single hypervisor or virtualization server (if not clustered) or a single cluster.
- A resiliency group can have only physical machines or only virtual machines, a mix of physical and virtual machines is not supported.

## Displaying resiliency group information and status

You can display resiliency group information and status in the following ways:

**Table 4-1**      Displaying resiliency group information and status

| Location   | Level of detail   | Useful for  |
|--|---|---|
| HPE Helion and Veritas Continuity Dashboard  | Lowest. Displays the number of resiliency groups under HPE Helion and Veritas Continuity control and the total number of groups in error, at risk, and healthy. | Getting a quick overview of the resiliency group population and health throughout HPE Helion and Veritas Continuity.<br><br>See " <a href="#">About the HPE Helion and Veritas Continuity Dashboard</a> " on page 31. |
|  <b>Assets &gt; Resiliency Groups</b> tab | Medium. Lists all your resiliency groups in one place.  | Seeing what is in each of your data centers, the state of the groups, and so on.  |

**Table 4-1** Displaying resiliency group information and status (*continued*)

| Location                         | Level of detail   | Useful for  |
|----------------------------------|---|---|
| Resiliency group-specific screen | Highest. Lists each asset in the resiliency group, their type, and state. | Getting detailed information on a resiliency group and its underlying assets, including disaster recovery status. This screen lists available operations for the group.<br><br>See <a href="#">“Viewing resiliency group details”</a> on page 24. |

This section discusses the second method of displaying resiliency group information and status: using the **Assets** page. The **Assets** page gives you a quick overview of all your resiliency groups.

## To display resiliency group information and status

### 1 Navigate



**Assets** (navigation pane) > **Resiliency Groups** tab

### 2 Review information and status

For a quick health check of your resiliency groups, review the colored boxes above the table. Select a box to show only the resiliency groups in that category; for example, select the green square to display only the resiliency groups that are healthy.

|        |  |
|--------|--|
| Blue   | The total number of resiliency groups            |
| Yellow | The number of resiliency groups at risk          |
| Green  | The number of resiliency groups that are healthy |

By default, the table lists all resiliency groups. Use the drop-list and search field to filter your results, and select a table heading to sort the groups.

In the table, the key fields are **State**, **Service Objective**, and **Data Availability**. Possible states are:

|                   |  |
|-------------------|--|
| Status            | <p><b>Normal</b> - the assets within the resiliency group are normal.</p> <p><b>At Risk</b> - the assets within the resiliency group are at risk.</p>  |
| State             | <p><b>Online</b> - The assets within the resiliency group are running.</p> <p><b>Partial</b> - One or more of the assets in the resiliency group are offline.</p> <p><b>Offline</b> - The assets in the resiliency group are powered off or not running.</p> |
| Active DC         | Name of the active data center.  |
| Type              | <p>Virtual Machine Group: The resiliency group comprises of virtual machines.</p> <p>Physical Machine Group: The resiliency group comprises of physical machines.</p>  |
| Service Objective | Service objective selected for the resiliency group.   |
| Data Availability | The replication technology.  |

# Viewing resiliency group details

Using the HPE Helion and Veritas Continuity console, you can view detailed information on each of your resiliency groups. The overall health of the resiliency group, its underlying assets and their current state is displayed.

Resiliency group for which disaster recovery (DR) operation is configured successfully, you can view information which includes the state of the replication for the resiliency group (for example, consistent, active), associated alerts, the details about the assets in the resiliency group, replication lag, recovery time, and so on. Note that the recovery time is available only after the rehearse operation is complete.

Note that for virtual machines, the recovery time is available only after the rehearse operation is complete.

## Replication state

This is a combination of replication state and . The tables describes the function of each state.

Some possible states:

- Consistent | Active (Connected, Consistent)
- Consistent | Inactive (Connected, Inconsistent)
- Inconsistent | Not Syncing | Inactive (Disconnected, Inconsistent)
- Inconsistent | Syncing | Inactive (Connected, Consistent)
- Consistent | Stopped (Connected, Consistent)

**Table 4-2** State of the replication add-on

| Replication add-on state                 | Description   |
|--|---|
| <b>Consistent</b> or <b>Inconsistent</b> | Data state on the target data center.   |
| <b>Syncing</b> or <b>Not Syncing</b>     | The <b>Syncing</b> state represents that data is in <b>inconsistent</b> state and data transfer is in full synchronization mode.  |
| <b>Active</b> or <b>Inactive</b>         | Replication state on the target data center.<br>Other possible replication states are: <b>Stopped</b> , <b>Stopped on Target Forcefully</b> , <b>Aborted</b> , or <b>Frozen</b> . |



**Table 4-3** HPE Helion and Veritas Continuity replication states

| HPE Helion and Veritas Continuity replication state   | Description   |
|---|---|
| <b>Connected</b> or <b>Disconnected</b>   | Replication state of HPE Helion and Veritas Continuity on the target data center. |
| <b>Consistent</b> , <b>Inconsistent good</b> , or <b>Inconsistent</b><br><br>Note that <b>Inconsistent good</b> state is not applicable to Veritas HPE Helion and Veritas Continuity Data Mover | Data state on the target data center.   |

Based on the HPE Helion and Veritas Continuity replication states, note that some disaster recovery operations are restricted:

- Migrate operation: Is allowed when replication state is **Connected** and data state is **Consistent** or **Inconsistent Good**.
- Takeover operation: Is allowed when replication state is any and data state is **Consistent**.
- Rehearsal operation: Is allowed when replication state is **Connected** and data state is **Consistent**.
- Resync and Rehearsal Cleanup operations: Is allowed with all states.

### To view details of a resiliency group

#### 1 Navigate



**Assets** (navigation pane) > **Resiliency Groups** tab

#### 2 Locate your resiliency group. Use filters and search as needed.

#### 3



On the row for the resiliency group, select the vertical ellipsis > **Details**.

You can also double-click the row to view details.

The details page includes the following:

- Menu options for operations that you can perform on the resiliency group.
- Details of how the resiliency group is configured.
- Status information.
- A list of the resiliency group assets and their state.

See [“Displaying resiliency group information and status”](#) on page 21.

# Managing Virtual Business Services using HPE Helion and Veritas Continuity

This chapter includes the following topics:

- [About virtual business services](#)
- [Displaying virtual business service details](#)

## About virtual business services

For a business service to work properly, it is important that all of its tiers and components are up and working together. From a business continuity point of view, it is important to not just ensure that individual tiers are up and running but also the entire business service.

A virtual business service (VBS) is a logical collection of resiliency groups that function together to perform a particular business service. A VBS enables easy management of multi-tier business services. For example, you can group a web server resiliency group, a database resiliency group, and a payroll business logic resiliency group into a VBS called `payroll`. You can start, stop, monitor, manage, or recover that VBS as a single entity.

An Asymmetric VBS is a combination of resiliency groups having Recovery service objective and resiliency groups having Monitor service objective.

## Understanding virtual business service tiers

Within a VBS, resiliency groups are arranged in tiers. Tiers represent the logical dependencies between the resiliency groups and determine the relative order in

which the resiliency groups start and stop. For example, the database resiliency group must start before the application server resiliency group and the web server resiliency group, so the database resiliency group must go in the lowest tier. The application server resiliency group must start after the database resiliency group, so it goes in the next tier. The web server resiliency group must start last, so it goes into the top tier. Later, if you add a resiliency group to the VBS, you can manage it as part of the IT service by placing it in the appropriate tier.

## Displaying virtual business service details

The details screen shows the virtual business services (VBS) configuration and state information of the VBS.

The top left section lists the **Active Data Centers** and the VBS state. You can also view the current activity, last successful activity, and last unsuccessful activity below the active data center.

The top right section lists the **Risks** that are associated with the VBS. You can see the category wise distribution of risks and also view the details of these risks.

In the lower section, the VBS configuration is displayed. This section has the following tabs:

- |                  |  |
|------------------|--|
| <b>List</b>      | The <b>List</b> tab lists the resiliency groups that are part of the VBS. Each row shows information about the type, active data centers, and states for the resiliency group. Depending on where the resiliency groups are located, you can click the links above the table to display all the resiliency groups or only the resiliency groups in a particular data center. |
| <b>Tier View</b> | The <b>Tier View</b> tab lets you visualize how the resiliency groups are arranged into logical tiers.   |
| <b>Plan View</b> | The <b>Plan View</b> tab shows the relative start and stop ordering of the resiliency groups within the VBS.   |

This screen is read only.

On the rightmost side of the screen, you can see the menu options for operations that you can perform on the VBS.

# Monitoring operations and tasks

This chapter includes the following topics:

- [Viewing activities](#)

## Viewing activities

Using the HPE Helion and Veritas Continuity console, you can view the sub task information for a task or an operation that is performed on the console. You can view the details on the **Activities** page. Details such as the status of the operation (in-progress, finished, or failed), start and end time, and the objects on which the operation was performed are displayed. You can view these details for a currently running task and for the completed tasks. On the **Current** page you can abort a running task.

Click on a currently running task, to view the details in a graphical representation. The steps that are completed are shown in green color along with the success icon. The ongoing steps are in blue color with the loader image, and the future steps are in gray. Expand **Execution Details** to view all the sub-tasks that comprise the task.

### To view activities

- 1 Navigate



**Activities** (menu bar).

- 2 Choose either of the following:
  - Select **Current** to view the currently running tasks.
  - Select **Completed** to view the historical tasks.

To view recent activities, click **Recent Activities** on the bottom pane.

# Monitoring and reporting on assets status

This chapter includes the following topics:

- [About the HPE Helion and Veritas Continuity Dashboard](#)
- [Understanding asset types](#)
- [Displaying an overview of your assets](#)
- [About reports](#)
- [Managing report preferences](#)
- [Scheduling a report](#)
- [Running a report](#)
- [Viewing and managing report schedules](#)
- [Viewing reports](#)

## 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

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

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

**DR Activity Summary**

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

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

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

**Virtual Machines by Platform and OS**

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.

**Top Resiliency Groups by Replication Lag**

Ranks the resiliency groups according to how long it takes the recovery data center to be in sync with the active data center.



**By Service Objective**

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

Use the drop-down list to filter your results.

See [“Displaying resiliency group information and status”](#) on page 21.

## Understanding asset types

On the HPE Helion and Veritas Continuity console Assets page, assets are classified as follows.

| <b>Asset</b>             | <b>Description</b>   |
|--------------------------|--|
| Resiliency Group         | <p>A group of virtual machines under HPE Helion and Veritas Continuity control. You can use HPE Helion and Veritas Continuity to start and stop the resiliency group, as well as protect and manage it.</p> <p>The Overview tab identifies whether or not resiliency groups are protected. An unprotected resiliency group is one that is configured to support monitoring and start and stop operations only. A protected resiliency group supports data recovery operations as well.</p> |
| Virtual Business Service | <p>A collection of resiliency groups logically grouped for a specific business purpose.</p>  |
| Unmanaged                | <p>A virtual machine that HPE Helion and Veritas Continuity discovers in your environment, but that is not under HPE Helion and Veritas Continuity management. You cannot use any HPE Helion and Veritas Continuity features with this asset. After you add the virtual machine to a resiliency group, it comes under HPE Helion and Veritas Continuity control.</p>   |

## Displaying an overview of your assets

The **Assets** page gives you an overview of all your resiliency groups and virtual business services (VBSs). You can also click links on the page to create resiliency groups and VBSs.

To access the **Assets** page, go to the navigation pane on the left side of the screen, and click:



The **Assets** page is organized into the following categories:

- Unprotected resiliency groups, are groups under HPE Helion and Veritas Continuity control, but that do not have disaster recovery configured.

For unprotected and protected resiliency groups, the screen also displays the following:

- The number of resiliency groups that are based on virtual machines and the number that are based on applications
- The number of unmanaged virtual machines or applications; that is, the assets that HPE Helion and Veritas Continuity is aware of but that are not managed or protected in resiliency groups.

For VBSs, the screen displays the following:

- The number of VBSs that are created from virtual machines and the number that are created from physical assets.
- The number of resiliency groups within the VBSs that are protected and the number that are only managed (not protected).

## About reports

Using the HPE Helion and Veritas Continuity console, you can generate a variety of reports. The following are the broad categories under which the reports are grouped:

- **Inventory:** Reports in this category provide information about the data centers and applications, and the virtual machines that are deployed in the data centers.
- **Recovery Assessment:** This category lists the reports that are related to the disaster recovery operations such as the migrate and take over report, and the rehearsal report.
- **Risk:** This category has two reports; Current Risk and Risk History. These reports show the summary and details of all the current and historical risks that occurred in the environment.

Reports can be scoped on the data center or global. You can subscribe for a report on a daily, weekly, monthly, quarterly, or yearly basis, or on predefined days of the week, or run on demand. Reports are available in the HTML and PDF format, or as a comma-separated file (CSV) file.

You can send a report to multiple recipients by entering the email addresses separated by a comma (,) or a semicolon (;).

See “[Managing report preferences](#)” on page 35.

See “[Scheduling a report](#)” on page 37.

See “[Running a report](#)” on page 39.

## Managing report preferences

Using the HPE Helion and Veritas Continuity console, you can create, update, and view your preferences for generating and receiving reports.

### To create report preferences

#### 1 Navigate

**Reports** (menu bar) > **Settings**.

#### 2 In the **Report preferences** wizard panel, specify the following information and click **Save**.

|          |  |
|----------|--|
| Scope    | Select the scope of the report such as Global or specific data center.   |
| Duration | Select the duration for which you want to receive the report.  |
| Format   | Select the delivery format as HTML or CSV.   |
| Email    | Enter an email address at which you want to send the report.<br><br>You can enter multiple email addresses that are separated by a comma (,) or a semicolon (;). |

## Frequency

Select the start and the end date and the time at which you want to generate and receive the report.

Select **Daily** to generate the report on a daily basis.

Select **Weekly** to avail the following options:

- Select **Every Weekday** to receive the report on all week days.
- Select **Recur every week on** and select one or more week days on which you want to receive the report.

Select **Monthly** to avail the following options:

- Set the monthly recurrence. For example every one month, or every 3 months.
- Select the day of the month on which you want to receive the report.
- Or select every weekday of the month on which you want to receive the report. For example every first Monday of the month or every fourth Saturday of the month.

Select **Yearly** to avail the following options:

- Set the yearly recurrence. For example every one year, or every 3 years.
- Select the day of the month on which you want to receive the report.
- Or select every weekday of a month on which you want to receive the report. For example every first Monday of January or every fourth Saturday of April.

Select **Once** to generate the report only one time.

See [“Scheduling a report”](#) on page 37.

See [“Running a report”](#) on page 39.

# Scheduling a report

Using the HPE Helion and Veritas Continuity console, you can update the report generation schedule for a selected report. The schedule that is defined in the template is then overwritten. You can also enable or disable the report schedule.

## To schedule a report

- 1 Navigate **Reports** (menu bar).
- 2 In the report row, click on **Schedule**.
- 3 In the **Schedule Report** wizard panel, specify the following information and click **Schedule**.

|             |  |
|-------------|--|
| 4 Name      | Enter a name for the report schedule. Only special character under score (_) is allowed. |
| Description | Enter a description for the report schedule.   |

## Frequency

Select the start and the end date and the time at which you want to generate and receive the report.

Select **Daily** to generate the report on a daily basis.

Select **Weekly** to avail the following options:

- Select **Every Weekday** to receive the report on all week days.
- Select **Recur every week on** and select one or more week days on which you want to receive the report.

Select **Monthly** to avail the following options:

- Set the monthly recurrence. For example every one month, or every 3 months.
- Select the day of the month on which you want to receive the report.
- Or select every weekday of the month on which you want to receive the report. For example every first Monday of the month or every fourth Saturday of the month.

Select **Yearly** to avail the following options:

- Set the yearly recurrence. For example every one year, or every 3 years.
- Select the day of the month on which you want to receive the report.
- Or select every weekday of a month on which you want to receive the report. For example every first Monday of January or every fourth Saturday of April.

Select **Once** to generate the report only one time.

## Scope

Select the scope of the report such as Global or specific data center.

## From and To

Select the duration for which you want to generate the report.

|        |  |
|--------|--|
| Format | Select the delivery format as HTML or CSV.   |
| Email  | Enter an email address at which you want to send the report.<br><br>You can enter multiple email addresses that are separated by a comma (,) or semicolon (;). |

See [“Managing report preferences”](#) on page 35.

See [“Running a report”](#) on page 39.

## Running a report

On the HPE Helion and Veritas Continuity console, you can run a report on demand. The report is generated and sent to the specified email address. To view the generated report in the browser, do one of the following:

- Click on the report notification.
- Click **Saved** to expand the table, and then double-click on the saved report row.
- Click **Saved** to expand the table, click on the **Action** menu, and then click **View**.

### To run a report

- 1 Navigate **Reports** (menu bar).
- 2 Click **Run** on the desired report, specify the following information in the wizard panel, and click **Run**.

|             |  |
|-------------|--|
| Scope       | Select the scope of the report such as Global or specific data center.   |
| From and To | Select the duration for which you want to generate the report.   |
| Format      | Select the delivery format as HTML or CSV.   |
| Email       | Enter an email address at which you want to send the report.<br><br>You can enter multiple email addresses that are separated by a comma (,) or semicolon (;). |

See [“Scheduling a report”](#) on page 37.

## Viewing and managing report schedules

You can use the HPE Helion and Veritas Continuity console to view the details of all the reports and manage the report schedules. You can view a brief description about the report along with the following information:

- Number of times the report is saved.
- Number of times the report is scheduled to run.
- Number of currently running instances of the report.

When a currently running instance of a report is complete, the number of saved report count increases by one and the number of currently running instances count decreases by one.

In each report row you can do the following:

### Saved

Click to view additional details such as the generation time, format, status, scope, and user information of all the saved instances of the report.

Double-click on a saved report row to view the report.

Click on the vertical ellipses to view or remove the report.

Saved reports are purged depending on the number of days defined in the **Reports Retention Policy Settings**.

### Schedules

Click to view the report generation schedules such as the format, recipient email address, recurrence, and whether the report is enabled or disabled.

Click on the **Actions** column to enable, disable, update, or delete the report schedule.

### Running

Click to view the format, scope, and user information.

You can abort the generation process.

### Run

Click to run the report on demand.



|                 |  |
|-----------------|--|
| <b>Schedule</b> | Click to update the report generation schedule.    |
| <b>Last Run</b> | Displays the last run date and time of the report. |

### To view reports

- ◆ Navigate

**Reports** (menu bar)

See [“Managing report preferences”](#) on page 35.

See [“Scheduling a report”](#) on page 37.

See [“Running a report”](#) on page 39.

## Viewing reports

HPE Helion and Veritas Continuity provides a console for viewing the following reports:

|                                   |   |
|-----------------------------------|---|
| Resiliency Groups and VBS Summary | Provides details about the resiliency groups and VBSs in the data centers across all sites.   |
| VM Inventory                      | Provides the platform distribution and the OS distribution details of the virtual machines that are deployed in the data centers in the form of a pie chart.<br><br>The <b>Details</b> table provides additional information for each virtual machine.  |
| Virtual Infrastructure Inventory  | Provides information about the virtual infrastructure inventory across data centers. A pie chart shows the platform and virtualization technology distribution of the virtual servers across all data centers.<br><br>The <b>Details</b> table provides additional information for each virtual server. |
| Activity Distribution History     | Provides information about tasks, such as migrate, takeover, rehearse, start, and stop, performed for a specified duration.   |

|                                  |  |
|----------------------------------|--|
| Recovery Activity History by RG  | Provides historical information about recovery tasks, such as migrate, takeover, rehearse, for each resiliency group.  |
| Recovery Activity History by VBS | Provides historical information about recovery tasks, such as migrate, takeover, rehearse, for each VBS.   |
| Metering                         | <p>Provides details of the virtualization servers that are protected for disaster recovery.</p> <p>You can view the total number of servers that are protected for disaster recovery. For these servers you can view the total memory, processor cores, and the total storage.</p>                                     |
| VBS RPO                          | <p>Provides Recovery Point Objective (RPO) details for all the virtual business services (VBS) in the resiliency domain.</p> <p>The bar chart provides information on the top VBS with maximum RPO lag.</p> <p>You can view the lag in the last replication and the replication date for all the VBS in the table.</p> |

### To view a report

#### 1 Navigation

Click **Reports** (menu bar).

#### 2 Do one of the following:

- Click **Run** to receive the report on the specified email address in HTML or PDF format, or as a comma separated (.CSV) file. You can also view the saved report on the console.
- Click **Schedule** to create a report generation schedule.

# Monitoring risks

This chapter includes the following topics:

- [About risk insight](#)
- [Displaying risk information](#)
- [Predefined risks in HPE Helion and Veritas Continuity](#)
- [Viewing the current risk report](#)
- [Viewing the historical risk report](#)

## About risk insight

The objective of the Risk Insight feature is to notify you about the vulnerabilities that might impact the recoverability or continuity of your protected assets.

Risk Insight detects the changes to the state and configuration of your protected assets. It identifies if there is a risk to the recoverability or continuity of your protected assets.

HPE Helion and Veritas Continuity also enables you to set up the replication lag threshold or service level threshold. Risk insight alerts you when the replication lags beyond the threshold that you specified.

Risk insight generates two types of reports:

- **Current risk reports:** Provides the summary and detail information about all the current risks in your data center.
- **Historical risk reports:** Provides a summary and a detailed analysis of information about the risks in your environment during the specified period.

These reports help you take actions to prevent such risks. The historical risk data is purged after a period of two years.

The risks covered by risk insight can be classified into three main categories:

**Table 8-1**

| Risk Type      | Description  |
|----------------|--|
| Recoverability | Risks that may impact the ability to recover and run the application on the recovery site.   |
| Continuity     | Risks that may impact the ability to run your applications without disruption either on your production site or on your recovery site. |
| SLA            | Risks that may impact the ability to fulfill the service level agreements (SLA) for your applications.                                 |

On the basis of criticality, the risks can be classified into two types:

**Table 8-2**

| Risk type | Description  |
|-----------|--|
| Error     | A risk that disrupts any stated goals of the product. An error must be fixed to make the product work as expected.           |
| Warning   | A risk that jeopardizes any stated goals of the product. A warning alerts you about a potential problem in your environment. |

See [“Displaying risk information”](#) on page 44.

See [“Predefined risks in HPE Helion and Veritas Continuity”](#) on page 45.

See [“Viewing the current risk report”](#) on page 51.



See [“Viewing the historical risk report”](#) on page 52.

## 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 8-3** 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>1 On the menu bar, select  <b>More Views &gt; Risks</b></li> <li>2 On the <b>Risk</b> page, double-click a risk in the table to display detailed information.</li> </ol>   |
| Risks that are associated with a specific resiliency group or virtual business service | <ol style="list-style-type: none"> <li>1 On the navigation pane, select  (Assets) and the tab for either <b>Resiliency Groups</b> or <b>Virtual Business Services</b>.</li> <li>2 On the tab, double-click a resiliency group or virtual business service to display detailed information.</li> <li>3 On the details page, note any risks that are listed in the <b>At Risk</b> area, and double-click the risk for details.</li> </ol> |

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.

## Predefined risks in HPE Helion and Veritas Continuity

[Table 8-4](#) lists the predefined risks available in HPE Helion and Veritas Continuity. These risks are reflected in the current risk report and the historical risk report.

**Table 8-4** Predefined risks

| Risks                                 | Description   | Risk detection time                         | Risk type | Affected operation   | Fix if violated  |
|---------------------------------------|---|---|-----------|--|--|
| vCenter Password Incorrect            | Checks if vCenter password is incorrect   | 5 minutes                                   | Error     | <ul style="list-style-type: none"> <li>■ On primary site: start or stop operations</li> <li>■ On secondary site: migrate or takeover operations</li> </ul> | In case of a password change, resolve the password issue and refresh the vCenter configuration   |
| VM tools not installed                | Checks if VM Tools are not Installed. It may affect IP Customization and VM Shutdown. | Real time, when resiliency group is created | Error     | <ul style="list-style-type: none"> <li>■ Migrate</li> <li>■ Stop</li> </ul>  | <ul style="list-style-type: none"> <li>■ In case of VMWare, install VMWare Tools</li> <li>■ In case of Hyper-V, install Hyper-V Integration Tools</li> </ul>   |
| Snapshot removed from Virtual Machine | Checks if snapshot has been removed from virtual machine.                             | 5 minutes                                   | Error     | Resiliency Platform Data Mover replication   | Edit the resiliency group to refresh configuration   |
| Snapshot reverted on Virtual Machine  | Checks if snapshot has been reverted on virtual machine.                              | 5 minutes                                   | Error     | Resiliency Platform Data Mover replication   | Remove and re-add the virtual machine to the Resiliency group by editing Resiliency group  |
| Data Mover Daemon Crash               | Checks if VM Data Mover filter is not able to connect to its counterpart in ESX.      | 5 minutes                                   | Error     | Resiliency Platform Data Mover replication   | In order to continue the replication, you can move (VMotion) the VM to a different ESX node in the cluster and either troubleshoot the issue with this ESX node or raise a support case with Veritas |
| Snapshot created on Virtual Machine   | Checks if a snapshot has been created on Virtual machine.                             | 5 minutes                                   | Error     | Resiliency Platform Data Mover replication   | Edit the resiliency group to refresh configuration   |

**Table 8-4**      Predefined risks (*continued*)

| Risks   | Description  | Risk detection time | Risk type | Affected operation  | Fix if violated  |
|---|--|---------------------|-----------|---|--|
| DataMover virtual machine in noop mode        | Checks if VM Data Mover filter is not able to connect to its counterpart in ESX.   | 5 minutes           | Error     | Resiliency Platform Data Mover replication                                      | In order to continue the replication, you can move (VMotion) the VM to a different ESX node in the cluster and either troubleshoot the issue with this ESX node or raise a support case with Veritas |
| Resiliency group configuration drift          | Checks if disk configuration of any of the assets in the resiliency group has changed.   | 30 minutes          | Error     | <ul style="list-style-type: none"> <li>■ Migrate</li> <li>■ Resync</li> </ul>   | Perform the edit resiliency group  |
| Global user deleted                           | Checks if there are no global users. In this case, the user will not be able to customize the IP for Windows machines in VMware environment. | Real time           | Warning   | <ul style="list-style-type: none"> <li>■ Migrate</li> <li>■ Takeover</li> </ul> | Edit the resiliency group or add a Global user   |
| Missing heartbeat from Resiliency Manager     | Checks for heartbeat failure from a Resiliency Manager.  | 5 minutes           | Error     | All   | Fix the Resiliency Manager connectivity issue  |
| Infrastructure Management Server disconnected | Check for Infrastructure Management Server(IMS) to Resiliency Manager(RM) connection state.  | 1 minute            | Error     | All   | Check IMS reachability<br>Try to reconnect IMS   |
| Storage Discovery Host down                   | Checks if the discovery daemon is down on the storage discovery host   | 15 minutes          | Error     | Migrate   | Resolve the discovery daemon issue   |
| DNS removed                                   | Checks if DNS is removed from the resiliency group where DNS customization is enabled  | real time           | Warning   | <ul style="list-style-type: none"> <li>■ Migrate</li> <li>■ Takeover</li> </ul> | Edit the Resiliency Group and disable DNS customization  |

**Table 8-4** Predefined risks (*continued*)

| Risks                               | Description   | Risk detection time | Risk type | Affected operation   | Fix if violated  |
|-------------------------------------|---|---------------------|-----------|--|--|
| IOTap driver not configured         | Checks if the IOTap driver is not configured  | 2 hours             | Error     | None   | Configure the IOTap driver<br><br>This risk is removed when the workload is configured for disaster recovery |
| VMware Discovery Host Down          | Checks if the discovery daemon is down on the VMware Discovery Host   | 15 minutes          | Error     | Migrate  | Resolve the discovery daemon issue   |
| VM restart is pending               | Checks if the VM has not been restarted after add host operation  | 2 hours             | Error     | Configure DR   | Restart the VM after add host operation  |
| New VM added to replication storage | Checks if a virtual machine that is added to a Veritas Replication Set on a primary site, is not a part of the resiliency group.  | 5 minutes           | Error     | <ul style="list-style-type: none"> <li>■ Migrate</li> <li>■ Takeover</li> <li>■ Rehearsal</li> </ul> | Add the virtual machine to the resiliency group.   |
| Replication lag exceeding RPO       | Checks if the replication lag exceeds the thresholds defined for the resiliency group. This risk affects the SLA for the services running on your production data center. | 5 minutes           | Warning   | <ul style="list-style-type: none"> <li>■ Migrate</li> <li>■ Takeover</li> </ul>                      | Check if the replication lag exceeds the RPO that is defined in the Service Objective                        |
| Replication state broken/critical   | Checks if the replication is not working or is in a critical condition for each resiliency group.   | 5 minutes           | Error     | <ul style="list-style-type: none"> <li>■ Migrate</li> <li>■ Takeover</li> </ul>                      | Contact the enclosure vendor.  |



**Table 8-4** Predefined risks (*continued*)

| Risks                              | Description  | Risk detection time   | Risk type | Affected operation   | Fix if violated  |
|------------------------------------|--|---|-----------|--|--|
| Remote mount point already mounted | Checks if the mount point is not available for mounting on target site for any of the following reasons: <ul style="list-style-type: none"> <li>Mount point is already mounted.</li> <li>Mount point is being used by other assets.</li> </ul> | <ul style="list-style-type: none"> <li>Native (ext3, ext4,NTFS): 30 minutes</li> <li>Virtualization (VMFS, NFS): 6 hours</li> </ul> | Warning   | <ul style="list-style-type: none"> <li>Migrate</li> <li>Takeover</li> </ul>  | Unmount the mount point that is already mounted or is being used by other assets.                                    |
| Disk utilization critical          | Checks if at least 80% of the disk capacity is being utilized. The risk is generated for all the resiliency groups associated with that particular file system.  | <ul style="list-style-type: none"> <li>Native (ext3, ext4,NTFS): 30 minutes</li> <li>Virtualization (VMFS, NFS): 6 hours</li> </ul> | Warning   | <ul style="list-style-type: none"> <li>Migrate</li> <li>Takeover</li> <li>Rehearsal</li> </ul>   | Delete or move some files or uninstall some non-critical applications to free up some disk space.                    |
| ESX not reachable                  | Checks if the ESX server is in a disconnected state.   | 5 minutes   | Error     | <ul style="list-style-type: none"> <li>On primary site: start or stop operations</li> <li>On secondary site: migrate or takeover operations</li> </ul> | Resolve the ESX server connection issue.   |
| vCenter Server not reachable       | Checks if the virtualization server is unreachable or if the password for the virtualization server has changed.   | 5 minutes   | Error     | <ul style="list-style-type: none"> <li>On primary site: start or stop operations</li> <li>On secondary site: migrate or takeover operations</li> </ul> | Resolve the virtualization server connection issue.<br><br>In case of a password change, resolve the password issue. |

**Table 8-4** Predefined risks (*continued*)

| Risks   | Description   | Risk detection time | Risk type | Affected operation  | Fix if violated  |
|---|---|---------------------|-----------|---|--|
| Insufficient compute resources on failover target | Checks if there are insufficient CPU resources on failover target in a virtual environment. | 6 hours             | Warning   | <ul style="list-style-type: none"> <li>■ Migrate</li> <li>■ Takeover</li> </ul> | Reduce the number of CPUs assigned to the virtual machines on the primary site to match the available CPU resources on failover target.  |
| Host not added on recovery data center            | Checks if the host is not added to the IMS on the recovery data center.                     | 30 minutes          | Error     | Migrate   | Check the following and fix: <ul style="list-style-type: none"> <li>■ Host is up on recovery data center.</li> <li>■ Host is accessible from recovery datacenter IMS.</li> <li>■ Time is synchronized between host and recovery datacenter IMS.</li> </ul> |
| NetBackup Notification channel disconnected       | Checks for NetBackup Notification channel connection state                                  | 5 minutes           | Error     | Restore   | Check if the NetBackup Notification channel is added to the NetBackup master server.   |
| Backup image violates the defined RPO             | Checks if the backup image violates the defined RPO   | 30 minutes          | Warning   | No operation  | <ul style="list-style-type: none"> <li>■ Check the connection state of NetBackup Notification channel</li> <li>■ Check for issues due to which backup images are not available</li> </ul>  |
| NetBackup master server disconnected              | Checks if NetBackup master server is disconnected or not reachable                          | 5 minutes           | Error     | Restore   | Check if IMS is added as an additional server to the NetBackup master server   |

Table 8-4 Predefined risks (continued)

| Risks                                       | Description   | Risk detection time | Risk type | Affected operation | Fix if violated  |
|---|---|---------------------|-----------|--------------------|--|
| Assets do not have copy policy              | Checks if the assets do not have a copy policy                          | 3 hours             | Warning   | No operation       | Set up copy policy and then refresh the NetBackup master server                      |
| Target replication is not configured        | Checks if the target replication is not configured                      | 3 hours             | Warning   | No operation       | Configure target replication and then refresh the NetBackup master server            |
| Replication gateway appliance not reachable | The replication gateway appliance is down or not reachable from the IMS | 15 minutes          | Error     | Migrate            | Make sure the replication gateway appliance is running and is reachable from the IMS |

## Viewing the current risk report

This report provides the summary and detail information about all the current risks in your data center. The high-level summary shows the total number of risks and its distribution by severity.

The **Distribution by type** chart displays the severity-wise distribution for recoverability, continuity, and service level agreement (SLA).

The **Unresolved risks** chart shows the risks that are unresolved for more than one month, for last one month, and for last one week. The **Recent Risks** chart shows the recent risks that are generated in the last 24 hours.

The **Current risks details by type** table provides detailed information such as the name of the resiliency group which is at risk, the name of the risk, its description, object at which the risk is generated, severity, and date and time on which the risk was generated.

### To view the current risk report

- 1 Navigation:  
Click **Reports** (menu bar).
- 2 In the **Risk > Current Risk Report** section, click **Run** or **Schedule** to receive the report on the specified email address.

# Viewing the historical risk report

This report provides a summary and a detailed analysis of information about the risks in your environment during the specified period.

The high-level summary shows the total number of risks and its distribution by the time the risks have been open. The information is categorized under various headings such as **Carried forward**, **New**, **Closed**, and **Still open**.

Within these categories, you can see severity wise distribution (high or low) and category wise distribution (recoverability, continuity, and service level agreement) of the risks.

The detailed analysis is displayed in the form of various charts:

- The various charts under **Risk by Category** display the open risks and new risks in the recoverability, continuity, and SLA categories at specific points of time within the duration specified by you.
- The **Resolving time chart** shows the average time to resolve the risk within the recoverability, continuity, and SLA categories.
- The **5 risks that took the longest time to resolve** chart shows the top 5 risks that took the longest time to be resolved, within the recoverability, continuity, and SLA categories. This information is displayed per resiliency group or per Virtual Business Service (VBS).

## To view the historical risk report

- 1 Navigation:  
Click **Reports** (menu bar).
- 2 In the **Risk > Risk History Report** section, click **Run** or **Schedule** to receive the report on the specified email address.

# Replication prerequisites for protected virtual machines

This appendix includes the following topics:

- [Additional prerequisites for protecting virtual machines](#)
- [Installing virtio drivers on the on-premises Windows virtual machines](#)
- [Enabling disk UUID on virtual machines](#)

## 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).

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  | <ul style="list-style-type: none"> <li>■ Enable the UUID for the virtual machines (disk.enableuuid=true).<br/>See <a href="#">“Enabling disk UUID on virtual machines”</a> on page 57.</li> <li>■ Ensure that VMware Tools are installed on the virtual machines.<br/>See the VMware documentation for information about installing the VMware Tools.<br/><b>Note:</b> VMware Tools must also be installed on the Storage Proxy.</li> </ul> |
| Hyper-V environment | <ul style="list-style-type: none"> <li>■ Ensure that Hyper-V integration services are installed on the virtual machines.<br/>See the Hyper-V documentation for information about installing Hyper-V integration services.</li> <li>■ Ensure that the virtual machines are generation 1. Generation 2 virtual machines are not supported.</li> </ul>   |

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.

See [“Installing virtio drivers on the on-premises Windows virtual machines”](#) on page 54.

## Installing virtio drivers on the on-premises Windows virtual machines

In KVM hypervisor, it is required to install virtio drivers for storage and networking purposes. If the Openstack deployment is KVM based, any virtual machine that needs to run in the cloud should have the virtio drivers installed.

For Windows virtual machines to boot in the cloud, you need to manually install virtio drivers on the virtual machines. In Linux, the drivers are bundled along with the Linux kernel packages, so you do not have to install virtio drivers for Linux based systems.

When you add virtual machines as hosts to the Infrastructure Management Server (IMS), the Veritas Resiliency Platform Replication add-on is installed on the host. The virtio storage and network drivers are packaged within this add-on. You can install the virtio drivers that are packaged in the add-on. Optionally you can download drivers for installation.

For more information on downloading the virtio drivers, source code of the drivers, and license information refer to the following Technote:

[https://www.veritas.com/support/en\\_US/article.TECH231650](https://www.veritas.com/support/en_US/article.TECH231650)

Refer to the following table for information on the driver files and their location on the Windows host on which the add-on is installed.

**Table A-1** Virtio driver file locations

| Operating system | Virtio driver directory for storage   | Virtio driver directory for network  |
|------------------|---|--|
| Windows 2008 x64 | C:\ProgramData\Symantec<br>\VRTSsfmh\spool\addons\store<br>\VRTSitrptap-2.0.1.0\virtio-win-0.1.118\viostor\2k8    | C:\ProgramData\Symantec<br>\VRTSsfmh\spool\addons\store<br>\VRTSitrptap-2.0.1.0\virtio-win-0.1.118\NetKVM\2k8    |
| Windows 2008 R2  | C:\ProgramData\Symantec<br>\VRTSsfmh\spool\addons\store<br>\VRTSitrptap-2.0.1.0\virtio-win-0.1.118\viostor\2k8R2  | C:\ProgramData\Symantec<br>\VRTSsfmh\spool\addons\store<br>\VRTSitrptap-2.0.1.0\virtio-win-0.1.118\NetKVM\2k8R2  |
| Windows 2012     | C:\ProgramData\Symantec<br>\VRTSsfmh\spool\addons\store<br>\VRTSitrptap-2.0.1.0\virtio-win-0.1.118\viostor\2k12   | C:\ProgramData\Symantec<br>\VRTSsfmh\spool\addons\store<br>\VRTSitrptap-2.0.1.0\virtio-win-0.1.118\NetKVM\2k12   |
| Windows 2012 R2  | C:\ProgramData\Symantec<br>\VRTSsfmh\spool\addons\store<br>\VRTSitrptap-2.0.1.0\virtio-win-0.1.118\viostor\2k12R2 | C:\ProgramData\Symantec<br>\VRTSsfmh\spool\addons\store<br>\VRTSitrptap-2.0.1.0\virtio-win-0.1.118\NetKVM\2k12R2 |

Above path is assuming that the host package (VRTSsfmh) is installed on 'C:\' drive. Refer to the appropriate host installation path in case you have installed it on any other drive.

## To install virtio storage and network drivers

### 1 Prerequisites

You need the DevCon utility to install the virtio drivers. The `devcon.exe` is shipped along with the solution and is available at “C:\Program Files\Veritas\VRTSsfmh\util\devcon.exe”.

### 2 For installing storage driver, enter the following command,

```
devcon.exe install viostor.inf <device ID>
```

The *Device ID* can be derived from the `viostor.inf` file. For example,

```
%RHELScsi.DeviceDesc% =  
rhelscsi_inst, PCI\VEN_1AF4&DEV_1001&SUBSYS_00021AF4&REV_00
```

Sample command,

```
devcon.exe install viostor.inf  
"PCI\VEN_1AF4&DEV_1001&SUBSYS_00021AF4&REV_00"
```

### 3 For installing network driver, enter the following command,

```
devcon.exe install netkvm.inf <device ID>
```

The *device ID* can be derived from the `netkvm.inf` file. For example,

```
[RedHat.NTamd64]  
%kvmnet6.DeviceDesc% =  
kvmnet6.ndi, PCI\VEN_1AF4&DEV_1000&SUBSYS_00011AF4&REV_00
```

Sample command,

```
devcon.exe install netkvm.inf  
"PCI\VEN_1AF4&DEV_1000&SUBSYS_00011AF4&REV_00"
```

### 4 You can verify the virtio driver installation using the following command,

```
devcon.exe dp_enum
```

The following third-party driver packages are installed on this computer:

```
oem1.inf  
    Provider: Red Hat, Inc.  
    Class: Storage controllers  
oem2.inf  
    Provider: Red Hat, Inc.  
    Class: Network adapters
```



# Enabling disk UUID on virtual machines

You must set the **disk.EnableUUID** parameter for each VM to "TRUE". This step is necessary so that the VMDK always presents a consistent UUID to the VM, thus allowing the disk to be mounted properly. For each of the virtual machine nodes (VMs), follow the steps below from the vSphere client:

## To enable disk UUID on a virtual machine

- 1 Power off the guest.
- 2 Select the guest and select **Edit Settings**.
- 3 Select the **Options** tab on top.
- 4 Select **General** under the **Advanced** section.
- 5 Select the **Configuration Parameters...** on right hand side.
- 6 Check to see if the parameter **disk.EnableUUID** is set, if it is there then make sure it is set to **TRUE**.

If the parameter is not there, select **Add Row** and add it.

- 7 Power on the guest.

# Glossary

|   |  |
|---|--|
| <b>activity</b>                               | A task or an operation performed on a resiliency group.  |
| <b>add-on</b>                                 | An additional software package that can be installed on hosts by the Infrastructure Management Server (IMS) for specialized uses.  |
| <b>asset infrastructure</b>                   | 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.  |
| <b>assets</b>                                 | 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.  |
| <b>klish</b>                                  | Command Line Interface SHell. Provides the command line menu on the virtual appliance for use after the initial bootstrap configuration.   |
| <b>data center</b>                            | <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> |
| <b>host</b>                                   | <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>   |
| <b>Infrastructure Management Server (IMS)</b> | 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.   |
| <b>migrate</b>                                | 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.   |

|                                 |  |
|---------------------------------|--|
| <b>persona</b>                  | 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.   |
| <b>product role</b>             | 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.   |
| <b>production data center</b>   | The data center that is normally used for business. See also recovery data center.   |
| <b>recovery data center</b>     | The data center that is used if a disaster scenario occurs. See also production data center.   |
| <b>rehearsal</b>                | <p>A zero-downtime test that mimics the configuration, application data, storage, and the failover behavior of the resiliency group.</p> <p>Rehearsal verifies the ability of the resiliency group to fail over to the recovery data center during a disaster.</p> |
| <b>Replication Gateway</b>      | The HPE Helion and Veritas Continuity component that performs replication between the storage on the production data center and the Cloud.   |
| <b>resiliency domain</b>        | The logical scope of a HPE Helion and Veritas Continuity deployment. It can extend across multiple data centers.   |
| <b>resiliency group</b>         | 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.  |
| <b>Resiliency Manager</b>       | 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.   |
| <b>resiliency plan</b>          | A collection of tasks or operations, along with the relevant assets, which are performed in a predefined sequence.   |
| <b>resiliency plan template</b> | A template defining the execution sequence of a collection of tasks or operations.   |
| <b>Storage Proxy</b>            | 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.                               |
| <b>take over</b>                | 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.   |
| <b>tier</b>                     | 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.                           |

|                                       |   |
|---------------------------------------|---|
| <b>virtual appliance</b>              | <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> |
| <b>virtual business service (VBS)</b> | <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>  |
| <b>web console</b>                    | <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
  - view 29
- asset types
  - about 33
- assets
  - display overview 33

## C

- cloud replication
  - about 10
  - handling application writes 14
  - handling migration 18
  - handling rehearsal 19
  - handling take over 18
  - solution architecture 11
  - synchronizing data 13
- components 11
- Configure DR
  - prerequisites 53

## D

- dashboard 31
- data replication
  - handling application writes 14
  - handling migration 18
  - handling rehearsal 19
  - handling take over 18
  - solution architecture 11
  - synchronizing data 13
  - to cloud data center 10
- Device Mapper 15
- disaster recovery
  - using Resiliency Platform 17
- disk multipathing
  - about 15
- disk UUID
  - enabling 57

## F

- full synchronization
  - about 13

## H

- HPE Helion and Veritas Continuity
  - about 6
  - capabilities 9
  - features and components 7

## M

- migration
  - about 18
- MPIO feature
  - Windows 15

## P

- permissions
  - about 9

## R

- RBT disk
  - see Replication Block Tracking disk 14
- rehearsal
  - about 19
- Replication Block Tracking disk
  - about 14
- replication lag 24
- replication status 24
- reports
  - about 34
  - current risk 51
  - historical risk 52
  - inventory 34
  - managing preferences 35
  - managing schedule 40
  - risk assessment 34
  - running 39
  - scheduling 37
  - viewing 40–41

- resiliency groups
  - about 20
  - displaying information and status 21
  - guidelines for organizing 21
  - viewing detailed information 24
- risk insight
  - about 43
- risks
  - current risk report 51
  - description 45
  - historical risk report 52
  - view information 44

## **S**

- synchronizing data
  - about 13

## **T**

- take over
  - about 18

## **V**

- virtual business services
  - about 27
  - displaying details 28
  - understanding tiers 27
- vxtap
  - about 14