Hewlett Packard Enterprise Helion and Veritas Continuity 2.0 Release Notes

February 2017

VERITAS™

Hewlett Packard Enterprise Helion and Veritas Continuity Release Notes

Product version: 2.0

Document version: 2.0 Rev 2

Legal Notice

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

http://www.veritas.com

Contents

Chapter 1

Overview

This chapter includes the following topics:

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 8.

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	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.
asset infrastructure	The data center assets that you add to HPE Helion and Veritas Continuity for discovery and monitoring by the IMS. The asset infrastructure includes hosts and virtualization servers. Once the asset infrastructure is discovered by the IMS, the discovered physical and virtual machines are listed in the console as assets to manage or protect.
resiliency group	The unit of management and control in HPE Helion and Veritas Continuity. You organize related assets into a resiliency group and manage and monitor them as a single entity.
service objective	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. 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. HPE Helion and Veritas Continuity monitors the resiliency groups based on the service objective definition and raises the risks as applicable.
Virtual Business Service (VBS)	A multi-tier business service where each VBS tier hosts one or more resiliency groups. A VBS lets you group multiple services as a single unit for visualization, automation, and controlled start and stop in the desired order. VBS uses the vertical grouping mechanism to group the multiple services. You can also migrate, takeover, and resync the entire VBS.

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

New features and changes in HPE Helion and Veritas Continuity

This release of HPE Helion and Veritas Continuity includes the following new features, changes, and enhancements.

Introduction of service objectives

HPE Helion and Veritas Continuity introduces the concept of service objective. A service objective defines the type of protection to be applied on a group of data center assets. When you create a resiliency group of assets in Veritas Resiliency Platform, you select a service objective to apply to that group of assets.

Service objectives are provided as templates that must be activated before use. A set of pre-activated service objectives with default settings is provided.

There are two types of pre-activated service objectives:

- Monitor - provides only monitoring, start, and stop operations
- Recovery - provides recovery operations as well as the start and stop operations

Support for disaster recovery of physical machines

HPE Helion and Veritas Continuity 2.0 lets you perform disaster recovery operations on physical machines.

Introducing encryption for data replication

The Replication Gateway now supports encryption using OpenSSL for data transfer. You can choose to apply an encryption scheme to the data replication while creating or modifying a Replication Gateway pair. Supported encryption schemes are AES128-GCM-SHA256 and AES256-GCM-SHA384.

Change in functionality of some operations

The functionality of the following operations has changed since the last release.

- Updating the DR configuration: This functionality is merged with Editing a resiliency group operation.
- Unconfiguring disaster recovery for a resiliency group: This functionality is merged with Deleting a resiliency group operation.
- Prepare for Failback operation: This is now renamed as Resync. There is no change in the workflow or the functionality.

- Failback operation: Instead of using the Failback operation to migrate the data from the Cloud data center to the on-premises data center, you now need to use the Migrate operation.

Change in terminology

Consistency groups are now called as Veritas Replication Sets.

Update 3 handles the change of MAC address of NIC

In case of NIC teaming, the MAC address of the network interface card may change after reboot, which changes the OS-UUID of the physical host. This is fixed in the `VRTSsfmh` package, which is part of Update 3.

Using the product documentation

Product documentation includes a full set of documents for the HP Helion and Veritas Continuity service provider and a set of less detailed documents for HP Helion and Veritas Continuity customers.

In addition, help content is hosted on the web and is available from the HPE Helion and Veritas Continuity console.

Table 1-1 Service provider guides

Title	Description
Software Compatibility List	The list of compatible software.
HPE Helion and Veritas Continuity Getting Started Guide	An overview of processes of deployment, configuration, and disaster recovery in the product.
HPE Helion and Veritas Continuity Release Notes	The release information such as main features, known issues, and limitations.
HPE Helion and Veritas Continuity Deployment Guide	Information about deploying the product virtual appliances, configuring the product components, and configuring product settings. Also includes information about updating and uninstalling the product.
HPE Helion and Veritas Continuity Solutions Guide	Information about configuring and using the disaster recovery solution, including configuring resiliency groups, configuring disaster recovery, performing disaster recovery operations, and monitoring status.

Table 1-1 Service provider guides *(continued)*

Title	Description
HPE Helion and Veritas Continuity Third-Party Software License Agreements	Information about the third-party software that is used in the product.

Table 1-2 Customer guides

Title	Description
HPE Helion and Veritas Continuity Release Notes	The release information such as main features, known issues, and limitations.
HPE Helion and Veritas Continuity Deployment Guide	Information about deploying the product virtual appliances, applying updates, uninstalling, and using the console.
HPE Helion and Veritas Continuity User's Guide	Basic concepts and information about using the console to monitor status.

Chapter 2

Fixed issues

This chapter includes the following topics:

Fixed issues

This chapter lists the issues that have been fixed in the HPE Helion and Veritas Continuity .

Table 2-1

Incident number	Abstract
3765450	Hosts having Replication add-on should have /boot mounted on its own partition
3695785	Internal host names are displayed on certain screens
3775091	Resiliency group state is shown as PARTIAL although all assets are online
3865460	IP of the on-premises virtual machine is not configured on the cloud virtual machine for Windows after performing Migrate or Takeover operation
3839708	Network may not come up on cloud after performing the Migrate or Takeover operation
NA	The vxtap kernel module is not supported on a RHEL host if the initramfs name follows the ‘module’ keyword in the grub configuration file
3864965	RHEL virtual machine on cloud having multiple NICs does not attach to the cloud IMS after Migrate or Takeover operation

Table 2-1 *(continued)*

Incident number	Abstract
NA	Disaster recovery configuration fails in case of same cloud network for multiple NICs of cloud virtual machine
NA	Network does not start automatically on the cloud when multiple NICs are configured

Chapter 3

Known issues

This chapter includes the following topics:

- Network does not come up after performing Migrate or Takeover operation on Windows virtual machine (3865462)
- Status of physical machines is online on production and cloud recovery data center after Takeover operation (1462)
- State of the consistency group is sometimes incorrectly displayed on the Replication Gateway (3866243)
- Network details page is empty during the protect resiliency groups for remote recovery operation (1253)
- Sometimes data centers and assets names are not displayed in Recent Activities
- Configuring for remote recovery operation may fail if IP address of a virtual machine is updated (1436)
- IPv6 settings are not preserved after migration (1538)
- Vxtap kernel module is unable to connect to IO Receiver (1141)
- When disks are deleted from protected assets, and if the asset is rebooted before resolving the drift then replication configuration is deleted (1454)
- Configure for remote recovery operation fails if host device paths have changed and the host discovery is not complete
- Some operations fail if disk paths of VMware virtual machines change after configuring for remote recovery
- Edit resiliency group operation fails with an error
- Resync may fail in case of physical machines with GPT disks that are not iSCSI supported (1698)
- Unable to add Windows host to IMS after migrating to the production data center (1765)

Modifying the default GRUB entries may cause the vxtap module to be installed in the wrong initramfs image (3792354)

When you install the Replication Add-on to a Linux system, the `vxtap` module is installed in the default `initramfs` image, with the name `initramfs-`*`kernel_version`*`.img`.

By default, the GRUB entries for an RHEL installation use the `initramfs-kernel_version.img`. However, if you modify the default GRUB entry to refer to a different `initramfs`, then the `vxtap` module is not loaded at boot time.

Workaround:

None. The `vxtap` module cannot parse the GRUB configuration and determine which `initramfs` image needs to be modified.

Make sure that the GRUB entries refer to the `initramfs-kernel_version.img`.

NRT discovery not performed for Hyper-V guest services (3774516)

Near real-time (NRT) discovery is not performed for Hyper-V guest services. Due to this reason, create resiliency wizard displays a warning that the guest services are not installed, even after you enable the guest services.

Workaround:

Refresh the host after enabling the guest services.

Unable to access a virtual machine using a floating IP that is attached to a private IP (3783556)

After performing the Migrate or Takeover operation, if you associate the floating IP of the virtual machine to a private IP address that is not the default route, then the virtual machine cannot be accessed using the floating IP.

Workaround:

You need to associate the floating IP to the interface that is marked for default route.

To identify the interface that is marked for the default route inside the virtual machine run the following command:

```
#netstat -ar
```

Restart host only after the first discovery cycle is complete (3815519)

Restart a host only after the first discovery cycle by the Infrastructure Manager Server (IMS) is complete. If you restart the host before the discovery cycle is complete, you need to re-add the host to the IMS.

Sometimes incorrect disk size may be displayed after you attach a new disk (3759137)

If you remove a disk and then attach a new disk of different size to the appliance, the new disk size may be shown incorrectly as the size of the previous disk.

Even if the disk size is displayed incorrectly, it does not affect any operation and the operation uses the correct size of the disk.

Replication state does not change when Replication add-on is removed (3803650)

Replication state of a resiliency group reflects the replication states from the source and the target gateway. It does not consider the replication state from the host on which the add-on is installed.

Adding Ephemeral CA certificate to access HP Helion cloud (3748624)

You need to manually import the Ephemeral CA certificate to access the HP Helion cloud. Steps to manually add the certificate are as follows:

Manually adding the certificate

1. Log on to Infrastructure Management Server (IMS).
2. Go to the directory: mkdir /usr/local/share/ca-certificates
3. Copy the **ephemeralca-cacert.crt** certificate from HP Helion cloud controller node to the above directory.
4. Import the certificate using following command:

   ```
   /opt/VRTSsfmcs/webgui/jre/bin/keytool -import -alias ca -file
   ephemeralca-cacert.crt -keystore
   /opt/VRTSsfmcs/webgui/jre/lib/security/cacerts -storepass changeit
   ```

5. Restart the web service on the IMS, using the following commands:

   ```
   /opt/VRTSsfmcs/bin/vomsc --stop web
   ```

   ```
   /opt/VRTSsfmcs/bin/vomsc --start web
   ```

Rehearse Cleanup operation does not delete cloud instances that are in ERROR state (3795935)

During the Rehearse operation, if any cloud instances are in ERROR state, then during the Rehearse Cleanup operation, these instances and their volumes are not deleted.

Workaround:

Manually delete the instances on cloud.

Manually adding virtual machines to the cloud IMS after migration is not supported (3816251)

After the Migrate operation is complete, the cloud virtual machine should automatically get added to the cloud IMS on booting. If the cloud virtual machine is not added to the cloud IMS, it means that one of the pre-requisites for add host operation is not met.

Workaround:

Check the `dr_sites.logs` file to identify which of the pre-requisites for add host operation is not met and fix the issue.

Log file location is:

- Linux: /var/opt/VRTSsfmh/logs/dr_sites.log
- Windows: C:\ProgramData\Symantec\VRTSsfmh\logs\dr_sites.log

OpenStack cloud configuration name should be different from the OpenStack server name (3840196)

While adding the cloud server, ensure that the OpenStack cloud configuration name is not the same as OpenStack server name.

Inability to move the cursor from second line to first while entering bootstrap options

While entering the bootstrap options, if your cursor is on the second line, you cannot move it back or use Backspace to delete the entries.

Workaround:

Use CTRL C to either move the cursor back or to use Backspace for deleting the entries.

Errors may occur when host having vxtap kernel module is migrated to another Hyper-V server (3848426)

In the failover cluster environment of Hyper-V servers, a host having vxtap kernel module can migrate to another Hyper-V server. The registration information of the host to the new Hyper-V server is available in the Resiliency Manager's database only after refreshing the Hyper-V server discovery by the Infrastructure Management Server (IMS).

The Hyper-V server discovery interval is 120 minutes, hence the association of the host with the new Hyper-V server is displayed only after the next discovery cycle is complete.

If the Migrate operation is performed on the host before the refresh of Hyper-V servers happens, you may see errors.

This issue does not occur for VMware servers if the IMS is configured to receive SNMP traps from the vCenter. If a virtual machine is migrated across the ESX server, IMS receives the trap for virtual machines migration. IMS then executes the discovery for ESX servers and maps the virtual machines to the new ESX server.

Network does not come up after performing Migrate or Takeover operation on Windows virtual machine (3865462)

After performing the Migrate or Takeover operation on a Windows virtual machine, the network adapter details are not displayed when you run the ipconfig command. This issue occurs if the driver for the network adaptor is not detected.

Workaround:

Do the following to update the driver for the network adapter device.

1. Open **Device Manager**.
2. Go to **Other Device** and locate the network adaptor in the list.
3. Right click the adapter and select **Update driver software**.

   This detects the Red Hat VirtIO driver for the network adaptor.

After updating the driver, attach the virtual machine to cloud Infrastructure Management Server (IMS) using the following commands:

```
C:\program Files\Verias\VRTSsfmh\bin\perl.exe C:\program
Files\Verias\VRTSsfmh\adm\local_ims_attach.pl
```

Status of physical machines is online on production and cloud recovery data center after Takeover operation (1462)

After successful completion of the Takeover operation, the status of physical machines is shown online on both the production and the cloud recovery data center. The status is refreshed after the next discovery cycle is complete. You can manually refresh the hosts on the production data center to show the correct status.

State of the consistency group is sometimes incorrectly displayed on the Replication Gateway (3866243)

When the consistency group on a Windows hosts having the vxtap kernel module is in PAUSED state, the state of the consistency group on the Replication Gateway is displayed as ACTIVE.

Network details page is empty during the protect resiliency groups for remote recovery operation (1253)

For physical machines, during the protect resiliency groups for remote recovery operation, the network details page does not show any records, although network mapping is already configured.

Sometimes data centers and assets names are not displayed in Recent Activities

For some operations the names of the data centers or the assets are not displayed in the details view of **Recent Activities** panel.

Configuring for remote recovery operation may fail if IP address of a virtual machine is updated (1436)

If the IP address of a virtual machine is updated after adding the vCenter to the Resiliency platform, the new IP address may not be considered while configuring the asset for remote recovery.

Workaround

To fix this, you need to remove the vCenter and add it again.

IPv6 settings are not preserved after migration (1538)

IPv6 settings on the virtual machines are not preserved after migration from production data center to Cloud and vice versa.

Vxtap kernel module is unable to connect to IO Receiver (1141)

If Symantec Endpoint protection is enabled, then the vxtap kernel module is unable to connect to IOR. You need to create an exception to handle IO Receiver requests.

When disks are deleted from protected assets, and if the asset is rebooted before resolving the drift then replication configuration is deleted (1454)

If one or more disks are deleted from an asset (physical or virtual machine) that is configured for remote recover, then a risk is raised on the resiliency group.

To fix the risk, you need to run the Edit resiliency group operation. Before performing the Edit resiliency group operation if you reboot the asset, then the replication configuration is deleted.

Workaround

To fix the replication configuration, you need to delete the resiliency group and re-configure it for remote recovery.

Configure for remote recovery operation fails if host device paths have changed and the host discovery is not complete

When disks are added or deleted and the host is rebooted, the device paths of the hosts may change. If you perform the configure for remote recovery operation before the next discovery cycle is complete then the operation fails.

Workaround

You can wait for the next host discovery cycle to complete or you can manually refresh the host and then perform the configure for remote recovery operation.

Some operations fail if disk paths of VMware virtual machines change after configuring for remote recovery

After you configure a resiliency group, consisting of VMware virtual machines, for remote recovery, the disk paths of the virtual machines change. VMware Storage vMotion changes the disk paths. Due to this change, the resync and delete resiliency group operations fail.

During the resync operation, the data at the cloud data center is replicated back to the production data center. Since the paths to the disks have changed, the resync operation fails.

Similarly during the delete resiliency group operation, the replication block tracking disk (RBT) is detached and deleted from the protected virtual machine. Since the paths to the disks have changed, the delete operation fails.

Edit resiliency group operation fails with an error

Scenario 1 (1684)

When you delete a disk from a protected virtual machine, a risk is raised, and you need to run the edit resiliency group operation. In this case sometimes the edit operation fails with the error: "Replication state of the VRS is not active". The replication state on the resiliency group details page is INACTIVE and the vxtap kernel module stops intercepting and replicating the I/O's.

Workaround

To fix this, you need to start the replication by executing the following command, and then relaunch the edit resiliency group operation.

```
vxtapaction start -cg <cgid>
```

Where cgid is the Veritas Replication Set ID.

While launching the edit resiliency group operation, you may see the "Replication is not in active state" warning. Ignore the warning and continue.

Scenario 2 (1688)

Edit resiliency group operation fails at 'Attach disk' task with the error: "Invalid technology workflow. Technology workflow is not specified."

This happens if there are multiple disks of the same size on the cloud virtual machine. While configuring the resiliency group for remote recovery, the operation fails after creating a disk on the virtual machine on the cloud data center.

Workaround

To fix this remove all the disks from the virtual machine on the cloud data center. Refresh the cloud server and then run the configure for remote recovery operation.

Resync may fail in case of physical machines with GPT disks that are not iSCSI supported (1698)

The resync operation may fail if the physical machines have GUID partition table (GPT)disks that are not iSCSI supported.

Workaround:

Perform the following steps in the given sequence:

- Identify RUID for GPT disks by running the following command on IOTap host:
  `C:\Program Files\Veritas\VRTSitrptap\cli>vxtapinfo.exe config`
- Check the existing DiskID by running the following command on the on-premises Gateway:
  `srdb=# select * from ReplicationUnit;`
- update the "DiskId" column in the "ReplicationUnit" table with following command:
  `srdb=# update "ReplicationUnit" set "DiskID"='your_DiskID' where "RUID"='your_RUID';`
  Where, your_DiskID and your_RUID are the DISKID and RUID that you had obtained after using the above commands.
- Verify the DiskID is updated as expected by again running following command:
  `srdb=# select * from "ReplicationUnit";`

Unable to add Windows host to IMS after migrating to the production data center (1765)

Sometimes after migrating from Cloud to the production data center, the Windows host fails to attach to the local Infrastructure Management Server (IMS). This happens because the `xprtld` service fails to restart after migration.

Workaround:

Manually restart the `VRTSsfmh` service using the CLISH menu.

Chapter 4

Limitations

This chapter includes the following topics:

Adding the same asset to cloud IMS and on-premises IMS

If you add an asset such as a virtualization server or virtual machine to the cloud Infrastructure Management Server (IMS) in error, you should ensure that it is fully removed from the cloud IMS before adding it to the on-premises IMS. Otherwise, the discovery cannot complete on the on-premises IMS.

Ensure that the asset is completely removed from both IMSs. Then add it back to the correct IMS.

Viewing the virtual machine boot status on Cloud after performing the Migrate and Takeover operation

Currently on the HPE Helion and Veritas Continuity console, you cannot view whether the operating system of the virtual machine has booted on the Cloud after performing the Migrate and Takeover operations.

You need to check the status of the operating system of the virtual machine on the Helion OpenStack console.

Limitations for on-premises Windows hosts

Following limitations are applicable only for on-premises hosts on Windows platform:

- To perform the Initialize Disk operation, consistency group must be in PAUSED or STOPPED state.
- If system recovery is done manually, then you need to first stop the replication and then start the replication using the CLI.
  - "C:\Program Files\Veritas\VRTSitrptap\cli\vxtapaction.exe" stop –cg <*CGID*>
  - "C:\Program Files\Veritas\VRTSitrptap\cli\vxtapaction.exe" start –cg <*CGID*> where *CGID* is the consistency group ID.

Consistency group goes in PAUSED state if disk is detached during SYNC state

If a disk is detached during SYNC state, then consistency group goes in PAUSED state. After attaching the disk manually resume SYNC operation using the following CLI.

Windows:

```
C:\Program Files\Veritas\VRTSitrptap\cli\ vxtapaction resume -cg CGID
```

Linux:

```
/opt/VRTSitrptap/cli/ vxtapaction resume -cg CGID
```

Where CGID is the Consistency Group ID.

The vxtap kernel module disables certain operations on Windows hosts

The vxtap kernel module disables the Automatic Recovery operation and the Windows Hibernate option on the on-premises Windows hosts only.

Adding the skipassource flag is not supported for Windows Server 2008 R2

Adding the skipassource flag in network configuration, to manage IP addresses being registered in DNS, on a host having Windows Server 2008 R2 is not supported.

Chapter 5

What is not supported?

This chapter includes the following topics:

What is not supported?

HPE Helion and Veritas Continuity 2.0 does not support the following features:

- Removing disks from a configured HPE Helion and Veritas Continuity appliance and attaching the same disk to another HPE Helion and Veritas Continuity appliance for the purpose of increasing the File System size is not supported. The logical volume management (LVM) configurations are same across the appliance node and this movement of disks from one appliance to another appliance may result in failure of LVM operations.
- EFI (Extensible Firmware Interface) enabled Hyper-V Generation 2 virtual machines are not supported.
- Mapping of one V-Switch with multiple cloud networks is not supported.
- Third-party disk filter driver is not supported with vxtap kernel module on the on-premises Windows hosts.
- BitLocker Drive Encryption Software is not supported with vxtap kernel module on the on-premises Windows hosts.
- A Windows physical host with Hyper-V enabled on it cannot be protected in physical-to-virtual mode.
- Addition of host and vServer on different IMS is not supported.
- Upgrade from version 1.0 to version 2.0 is not supported.
- KVM enabled physical machines are not supported.
- Networking using vSphere Distributed Switches is not supported.

- For physical machines, removable devices are not ignored during configuration for remote recovery, and hence the operation fails.
- For physical machines, when you migrate from the Cloud data center to the production data center, you must migrate to the same physical machine. Migrating to another physical machine is not supported.
- External PXE server is not supported.
- Adding the skipassource flag in network configuration is not supported for hosts having Windows Server 2008.

Appendix A

Virtual appliance security features

This appendix includes the following topics:

Operating system security

HPE Helion and Veritas Continuity appliance operating system is hardened against potential security exploitation by removing the operating system packages that are not used by the HPE Helion and Veritas Continuity. All the default yum repository files that are shipped with the operating system are removed.

The Control + Alt + Delete key combination has been disabled to avoid any accidental reboot of the virtual appliance. Exec-shied is enabled to protect the virtual appliance from stack, heap, and integer overflows.

Management Security

Only admin login is available for the appliance. The password policy of admin login is modified to prompt the user to change the password on the first login.

If the admin user password is lost, you need to contact Veritas support for resetting the admin user password.

Support and root user accesses are limited to Veritas Corporation only.

On successful completion of the Resiliency Platform bootstrap, admin user can only access a limited menu of commands through klish. Besides admin user, support user is also supported in the appliance but remote login of support user is disabled. To access the support user, one needs to login as an admin and go through **klish**. An option `support > shell` is provided in the **klish** menu to switch the user to support and access the bash shell of support. This option is available to the user only after password verification and the password is available with Veritas Corporation. After password verification, the support user is given the superuser privileges.

The following table summarizes the password policy and access for various users in HPE Helion and Veritas Continuity:

Table A-1 User passwords to access the appliance

Users	Default password	Password expiry	Login prompt	Remote login	Access
Grub	Not-known-to-user	None	Shell	N/A (only console)	Single user mode
Root	Not-known-to-user	None	Shell	Disable	Full access
Support	Not-known-to-user	On first login	Shell	Disable	Full access
Admin	password	On first login	klish	Enable	klish menu

Timeout of the bash shells of all users is set to 900 seconds.

Network security

The TCP timestamp responses are disabled in HPE Helion and Veritas Continuity virtual appliance. Another network security feature of the appliance is that during the product bootstrap process, only those ports that are used by the product for communication and data transfer, are opened through the firewall and all the other communications are blocked.

Uncommon network protocols such as DCCP, SCTP, RDC, TIPC have been disabled so that any process cannot load them dynamically.

Access control security

HPE Helion and Veritas Continuity virtual appliance implements certain access control measures. The umask is set to 0700 across the appliance. The access

permissions of some of the files such as home folder of root, the log directory etc. is restricted. All the security and the authorization messages are logged into the appliance.

Physical security

In the HPE Helion and Veritas Continuity virtual appliance, the USB storage access is disabled.