Hewlett Packard Enterprise Helion and Veritas Continuity Release Notes

1.0

May 2016

VERITAS™

Hewlett Packard Enterprise Helion and Veritas Continuity Release Notes

Product version: 1.0

Document version: 1.0 Rev 0

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

HPE Helion and Veritas Continuity has the following core capabilities:

Recovery	HP Helion and Veritas Continuity provides a disaster recovery (DR) solution in the cloud for on-premises data centers. HPE Helion and Veritas Continuity provides the management console that enables the DR configuration. Once DR is enabled, HPE Helion and Veritas Continuity provides single-click DR operations between the on-premises data center and the cloud. These single-click operations include rehearsal, rehearsal cleanup, migrate, takeover, prepare for failback, and failback. The HP Helion and Veritas Continuity service provider performs the DR operations as requested.
Visibility	The console Dashboard provides visibility into the health of virtual machines and multi-tier business services.

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

About HPE Helion and Veritas Continuity features and components

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

resiliency domain	The logical scope of a HPE Helion and Veritas Continuity deployment. It can extend across multiple data centers.
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 on-premises data center. One IMS is deployed in the cloud.
Replication Gateway	The component that performs replication between the on-premises storage and the cloud storage. 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 on-premises gateway during preparation for failback to the on-premises data center. The Storage Proxy is deployed as a virtual appliance.

data center	The resiliency domain contains two data centers, an on-premises data center and the recovery data center in the cloud. The cloud data center has a Resiliency Manager, one or more cloud Replication Gateways, and one IMS; the on-premises data center has one or more on-premises Replication Gateways, one or more Storage Proxies, and one or more IMSs
asset infrastructure	The data center assets that you add to HPE Helion and Veritas Continuity for discovery and monitoring by the IMS. The asset infrastructure includes hosts and virtualization servers. Once the asset infrastructure is discovered by the IMS, the discovered virtual machines are listed in the console as assets to manage or protect.
resiliency group	The unit of management and control in HPE Helion and Veritas Continuity. You organize related assets into a resiliency group and manage and monitor them as a single entity.
Virtual Business Service (VBS)	A multi-tier business service where each VBS tier hosts one or more resiliency groups. A VBS lets you group multiple services as a single unit for visualization, automation, and controlled start and stop in the desired order. VBS uses the vertical grouping mechanism to group the multiple services.You can also migrate, takeover, prepare failback, and failback the entire VBS.

Using the product documentation

Product documentation includes a set of guides in PDF format 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 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.

Table 1-1 Customer guides *(continued)*

Title	Description
HPE Helion and Veritas Continuity User's Guide	Basic concepts and information about using the console to monitor status.

Chapter 2

Known issues

This chapter includes the following topics:

- Errors may occur when host having vxtap kernel module is migrated to another Hyper-V server (3848426)
- RHEL virtual machine on cloud having multiple NICs does not attach to the cloud IMS after Migrate or Takeover operation (3864965)
- IP of the on-premises virtual machine is not configured on the cloud virtual machine for Windows after performing Migrate or Takeover operation (3865460)
- Network does not come up after performing Migrate or Takeover operation on Windows virtual machine (3865462)
- State of the consistency group is sometimes incorrectly displayed on the Replication Gateway (3866243)
- Prepare for failback workflow is stuck at the Stop Replication on Host step (3868388)

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`.

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
   ```

Hosts having Replication add-on should have /boot mounted on its own partition (3765450)

If /boot is a directory on a root file system and not a mount point on a separate partition, then the voltap driver fails to load during the disaster recovery configuration.

Workaround:

Voltap driver requires root and boot to be independent file systems and partitions. Create a separate partition for /boot.

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.

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.

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.

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.

Internal host names are displayed on certain screens (3695785)

Internal host names are displayed on the following screens:

- **Applicable Hosts** tab on the **Deployment** page.
- **Add Virtualization Server** panel while adding the virtualization server.
- Host details page

Network may not come up on cloud after performing the Migrate or Takeover operation (3839708)

If you maintain a backup of network configuration files such as `ifcfg-eth0.org` for RHEL6 and `ifscf-ens192.bkp` for RHEL7 in the directory `/etc/systemconfig/network-scripts/`, then the network may not come up on the cloud after performing the Migrate or Takeover operation.

Workaround:

Move the backup files from `/etc/systemconfig/network-scripts/` directory to another location.

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.

Resiliency group state is shown as PARTIAL although all assets are online (3775091)

The state of a resiliency group is shown as PARTIAL even if all the assets within the resiliency group are online on one of the sites.

Workaround:

You can ignore the state, and instead review the individual asset state. To do this, go to the **Resiliency Groups** details page and check the state of each asset within the resiliency group.

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.

RHEL virtual machine on cloud having multiple NICs does not attach to the cloud IMS after Migrate or Takeover operation (3864965)

After performing the Migrate or Takeover operation, the RHEL virtual machine on cloud, having multiple NICs, does not attach to the cloud Infrastructure Management Server (IMS). This issue may occur because the DNS in the cloud virtual machine is unable to resolve to the IMS host name.

Workaround:

Fix the DNS issue to resolve the IMS host name, and then use the following command to attach the cloud virtual machine to the cloud IMS.

```
/opt/VRTSsfmh/bin/perl /opt/VRTSsfmh/adm/local_ims_attach.pl
```

IP of the on-premises virtual machine is not configured on the cloud virtual machine for Windows after performing Migrate or Takeover operation (3865460)

After performing the Migrate or Takeover operation, the IP of the on-premises virtual machine is not configured on the cloud virtual machine for Windows. The `netsh` command fails with the `object already exists` error.

Workaround:

Run the following command to configure the IP:

For primary IP:

```
netsh interface ip add address <NIC_NAME> static "IPADDRESS" "NETMASK"
"GATEWAY"
```

For secondary IP:

```
netsh interface ip add address <NIC_NAME> static "IPADDRESS" "NETMASK"
```

Run the following commands to attach the virtual machine to the cloud Infrastructure Management Server (IMS):

```
C:\Program Files\Veritas\VRTSsfmh\bin\perl.exe C:\program
files\Veritas\VRTSsfmh\adm\local_ims_attach.pl
```

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
```

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.

Prepare for failback workflow is stuck at the Stop Replication on Host step (3868388)

If the Prepare for failback workflow is stuck at the Stop Replication on Host step, then do not rerun the workflow. Manually start the replication for the failed resiliency group in the following sequence:

- On the on-premises replication gateway
- On the cloud replication gateway

- On the cloud host

Initiate failback operation when the replication state of the resiliency group is active.

Chapter 3

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:

- Do not enable "Automatic Install Updates" on the on-premises hosts.
- 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.
- To perform the initialize disk operation on a Windows hosts having the vxtap kernel module, the consistency group must be in PAUSED or STOPPED state. Use the following CLI to pause the consistency groups:

  ```
  C:\Program Files\Veritas\VRTSitrptap\cli\vxtapaction pause -cg
  <CGID>
  ```

  Proceed with the disk initialize operation using the Windows operating system commands, and then use then use the following CLI to resume the consistency group.

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

  where <CGID> is the ID of the consistency group.

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.

NIC teaming within guest virtual machines is not supported for DR operation

Using a bridge network adapter during the Migrate operation is not supported for RHEL and Windows virtual machines.

Network does not start automatically on the cloud when multiple NICs are configured

If multiple NICs are configured and you do not specify MAC address in each interface configuration file, then after performing the Migrate and Takeover operation, the network does not start automatically on the cloud for virtual machines on RHEL 6 and RHEL 7.

Workaround:

Specify the MAC address in key HWADDR in the network interface configuration file.

The vxtap kernel module is not supported on a RHEL host if the initramfs name follows the 'module' keyword in the grub configuration file

The vxtap kernel module is not supported on a RHEL host if the initramfs name follows the module keyword in the grub configuration file. For example, `module initramfs-image` is not supported.

Chapter 4

What is not supported?

This chapter includes the following topics:

What is not supported?

HPE Helion and Veritas Continuity 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.
- NIC teaming is not supported for guest VMware virtual machines.
- 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.

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. The new password must not be a Dictionary word and must be at least six characters long.

If the admin user password is lost, Veritas may access the root using the grub access, and reset 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 CLISH. 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 **CLISH**. An option `support > shell` is provided in the **CLISH** 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	CLISH	Enable	CLISH 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.