Veritas InfoScale™ Availability Agents

4Q 2023

VERITAS™

Last updated: 2024-01-12

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054
http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:
https://www.veritas.com/support

You can manage your Veritas account information at the following URL:
https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:
https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:
infoscaledocs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:
http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:
https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Release notes for Cluster Server Agent Pack

This document includes the following topics:

Introduction

This document provides important information about the Cluster Server Agent Pack release. Review this entire document before installing and configuring the agents.

For more information about Cluster Server Agent Pack, refer to the Getting Started Guide, which is available on the Veritas Services and Operations Readiness Tools (SORT) site: https://sort.veritas.com/agents.

Note: This document does not contain information about the Cluster Server agents for Microsoft applications on Windows. For information about these agents, see the *Cluster Server Agent Pack Readme*. The Readme is available on the VCS Agent Details page on SORT and also in the agent zip file.

Changes introduced in this release

This section lists the new features and enhancements in this Agent Pack release.

Application agents

The following table displays a list of the changes that are made to the VCS application agents in this agent pack release:

Table 1-1 Application agents

Agent	New feature or enhancement
SAPNW	Added support for SAP S4HANA 2022.
SAPHDB	■ Added support to stop the DevQA DB instances before PROD DB performs the takeover action. ■ Added support for SAP HANA 2.0 SP07. ■ Added support for SAP HANA HA/DR hook as an optional option.
IBM WebSphereMQ	■ Added support for WebSphere MQ 9.3 on RHEL 9.0. ■ Added support for IBM WebSphere MQ Replicated Data Queue Manager (RDQM) HA/DR using WebSphereMQ agent, Veritas cluster file system, and Veritas Volume Replication (VVR).
SAP agent - SAPHDB, SAPNW, SAPLiveCache	Renamed package `VRTSsapnw` to `VRTSsap` on Linux to avoid confusion.

Replication agents

The following table lists the changes that are made to the VCS replication agents in this agent pack release:

Table 1-2 Replication agents

Agent	New feature or enhancement
Pure Storage ActiveDR	Added support for Pure Storage ActiveDR agent for InfoScale 8.0.2 on Windows 2019.

Table 1-2 Replication agents *(continued)*

Agent	New feature or enhancement
EMC SRDF, EMC SRDF Storage Group, Hitachi TrueCopy, Hitachi Universal Replicator, IBM MetroMirror, IBM Global Mirror, EMC Clariion MirrorView, Pure Storage, Pure Storage Synchronous Replication, IBM SVCCopyServices , Dell EMC Unity, IBM XIV Mirror	Added support to automatically detect installation and upgrades of the agent on Linux. Removed manual passing of arguments to the `addAgentType.sh` script to distinguish install and upgrade scenarios.
EMC SRDF	Added support for Solutions Enabler version 10.0.1.0.
Pure Storage, Pure Storage Synchronous Replication	Added support for Purity for FlashArray (Purity//FA) version 6.3.3.
EMC Unity	Added support for Dell Unity Operating Environment (OE) version 5.3.

Fixed issues

This section describes the incidents that are fixed in this Agent Pack release.

Application agents

The following table lists the issues that are fixed in the VCS application agents.

Table 1-3 VCS application agents fixed issues

Incident	Description
4145798	Symptom: The WebSphere MQ resource fails to go online when "amqzmuf0" process is already running. Description: During online operation, the agent does not stop all the WebSphere MQ related process including “amqzmuf0” as part of clean-up activity. This results in failure of online operation of WebSphere MQ resource. Resolution: The WebSphere MQ agent is updated to perform the clean-up activity correctly during online operation.

Table 1-3 VCS application agents fixed issues *(continued)*

Incident	Description

4124681	Symptom: Few agents display Notice messages during the agent upgrade process.
	
	Description: Agents attempt to delete directories, `/opt/VRTSagents/ha/bin/<AgentDir>` and `etc/VRTSagents/ha/conf/<AgentDir>` during the upgrade of the agents.
	
	As a result, the following two notice messages are displayed:
	
	`Notice: Directory [/opt/VRTSagents/ha/bin/<agentdir>] is not empty and will not be removed.`
	
	`Notice: Directory [/etc/VRTSagents/ha/conf/<agentdir>] is not empty and will not be removed.`
	
	The following agents are affected:
	
	AgentBuilder, MySQL, OracleApps, OracleAppsCM, SAPNW, SAPHDB, SAPLiveCache, SAPHotStandby, WebLogic, WebSphere, TibcoEMS, WebSphereMQ, WebSphereMQFTE, DockerContainer, and DockerDaemon.
	
	Resolution: The code changes have been made in the postinstall scripts of the affected agents to avoid the attempt of removal of the agent directories during the agent upgrade process.

Replication agents

The following table lists the issues that are fixed for the VCS replication agents.

Table 1-4 VCS replication agents fixed issues

Incident	Description
4145614	Symptom: The SRDF agent marks the SRDF resource as UNKNOWN, when the remote SYMAPI server is configured and LogStateChange value is set to 1. Description: When the value of LogStateChange attribute is set to 1 and a remote SYMAPI server is configured using the Symapi Servers attribute, the agent marks the SRDF resource state as UNKNOWN. In this process, it fails to set the environment for the configured remote SYMAPI server, which causes to fail the SRDF commands for fetching the device group state during monitor, offline, and open operations. Resolution: The code changes are done in the SRDF agent to set the environment for the configured remote SYMAPI server.

Table 1-4 VCS replication agents fixed issues *(continued)*

Incident	Description
4143187	Symptom: The Sigma utility of EMC SRDF agent fails to run. Description: The Sigma utility of EMC SRDF agent fails due to missing module and displays the following error message: `SRDFAgent Undefined subroutine &SRDFAgent::remove_space called at /opt/VRTSvcs/bin/SRDF/sigma line 75.` Resolution: The code changes are done to add the missing module.

4142576	Symptom: The generate_token utility displays a false message about a failure of updating the value of RestToken attribute of a PURESync resource.
	
	Description: The utility updates the RestToken attribute correctly but fails with following message:
	
	`# ./generate_token`
	`Enter PURESync resource name: PUREres1`
	`Enter Pure Storage array "dspure11.sample.host.veritas.com" username: replication`
	`Enter replication's password for Pure Storage array:`
	`Generating token, please wait...`
	`Failed to update token value.`
	`Failed to configure RestToken for resource "PUREres1"`
	
	Resolution: The code changes are done in the generate_token utility to fix the issue.

4123543	Symptom: The Oracle GoldenGate resource fails to come online when multiple Oracle instances are configured in case of GCO. Description: The agent fails to bring the Oracle GoldenGate resource online when multiple Oracle instances are configured on the same node. The GoldenGate manager process remains in a stopped state. The issue is specific to a GCO configuration. Resolution: The code changes are done to detect the manager processes when multiple Oracle instances are configured on the same node.

4123109	Symptom: Agent type NetAppSnapMirrorSnap does not exist.
	
	Description: On installation of the NetAppSnapMirrorSnap agent, the agent fails to import the agent type and the type definition is not available in the agent configuration file at `/etc/VRTSvcs/conf/config/NetAppSnapMirrorTypes.cf`.
	
	The following warning message appears:
	
	`hatype -display NetAppSnapMirrorSnap | grep -i source`
	`VCS WARNING V-16-1-10409 Type does not exist: NetAppSnapMirrorSnap`
	
	Resolution: Code changes are done in the agent's configuration file to fix the issue.

Table 1-4 VCS replication agents fixed issues *(continued)*

Incident	Description
4071130	Symptom: Installation and upgrade of replication agents fails on RHEL 8.x and later due to a dependency on Perl. Description: Installation and upgrades of the IBM MetroMirror, EMC Clariion MirrorView, Oracle DataGuard, and IBM SVCCopyServices agents fails on RHEL 8.x and later due to an unresolved dependency on Perl. The following error message appears: `error:Failed dependencies: perl >= 0:5.000 is needed by <PackageName>.rpm` Resolution: The agent-specific Perl module file is updated to fix the issue.

Known issues

This section lists the known issues that are applicable in this agent pack release.

VCS application agents

The following known issues exist with the application agents.

Cisco UCS

This section describes the known issues in the Cluster Server agent for Cisco UCS.

The UCSHA starts monitoring even after being stopped (3628291)

Symptom: The command "`ucsha -stop`" fails to stop the UCSHA from monitoring the associated service profiles.

Workaround: When the "`ucsha -stop`" command fails to stop monitoring the health of the service profiles, execute the following commands to stop UCSHA:

1. Probe the CiscoUCS resources after the `ucsha -stop` command fails using the following command:

   ```
   # hares -probe <resource_name> -sys <system_name>
   ```

2. Check the state of the CiscoUCS resource using the following command:

   ```
   # hares -state <resource_name>
   ```

3 If the resource still reports ONLINE, offline the resource.

```
# hares -offline <resource_name> -sys <system_name>
```

4 Check the state of the CiscoUCS resource.

```
# hares -state <resource_name>
```

The state of the resource must be reported as OFFLINE.

IBM WebSphere MQ

This section describes the known issues in the Cluster Server agent for IBM WebSphere MQ.

Discovery of WebsphereMQ fails, if there are special characters in the WebSphereMQ installation path (3847969)

Symptom: The WebSphereMQ agent is not discovered when the installation path contains special characters, such as **)** and **(**.

Workaround: Configure resources manually. For more information on how to configure WebSphereMQ resource, refer to the *Cluster Server Agent for WebSphere MQ Installation and Configuration Guide*.

Queue Managers with the same resource dependencies cannot be configured using different runs of the Symantec High Availability Configuration wizard (3678377)

Symptom: When you configure queue managers having the same resource dependencies such as, shared mount points and IP addresses, using multiple runs of the wizard, the queue managers are configured separately and not merged with the existing configuration. This issue occurs on the Windows and Linux operating systems.

Workaround: Configure multiple queue managers that have the same resource dependencies in a single run of the Symantec High Availability Configuration wizard.

Listener for Queue Manager may not be configured if you do not select the Monitor Listener for the Queue Manager check box (3678386)

Symptom: On the **Queue Manager** selection panel, if you click **Next** without selecting the **Monitor Listener for the Queue Manager** check box, you might not be able to return to that panel to configure monitoring for a queue manager listener. This issue occurs on the Windows operating system.

Workaround: To configure monitoring for a queue manager listener, ensure that you select the **Monitor Listener for the Queue Manager** check box on the**Queue Manager** selection panel before you click **Next**.

Support for only one listener associated with each queue manager (3678391)

Symptom: The Symantec High Availability Configuration wizard supports only one listener associated with each queue manager.

Workaround: Manually add the listener resource in the Queue Manager service group using the ha commands.

Oracle e-Business Components

This section describes the known issues in the Cluster Server agent for Oracle e-Business Components.

The NodeManager component is not yet supported by the OracleApps agent (3923578)

Symptom: In an EBS 12.2 service group, the AdminServer component is the parent of the Mount resource. AdminServer starts the NodeManager component when the service group is brought online, but does not stop it when the service group is taken offline. Therefore, the Mount resource kills the NodeManager component.

Workaround: There is no workaround for this issue yet.

SAP HANA

This section describes the known issues in the Cluster Server agent for SAP HANA.

When the ClusterFailOverPolicy attribute is set as Auto, the preonline trigger may cause the system to behave unexpectedly resulting in execution of the -sr_takeover command on the system several times (3864243)

Symptom: If the ClusterFailOverPolicy attribute is set as Auto, the PreOnline trigger can run multiple times on the same system resulting in the execution of the -sr_takeover command on the system several times. This may result in an unexpected behavior.

Workaround: There is no workaround for this issue.

The agent does not take the OnlineTimeout value into account when overriding the value at the resource level (3864341)

Symptom: The SAP HANA agent does not take the OnlineTimeout value into account when overriding the value at the resource level and performing the takeover action. The following error message is displayed:

```
Replication Takeover is not successful.
```

Workaround: Change the value at the type level.

```
# hatype -modify SAPHDB OnlineTimeout 900
```

The SAP HANA agent fails to register with new primary automatically when GCO (2 + 1) is configured (4148759)

Symptom: In case, GCO (2 + 1) is configured, the SAP HANA agent fails to register secondary with new primary automatically. The following message is displayed in the agent's logs:

```
Could not determine the host name on which the previous primary was
running. Offline service group [SAPHDB_SG] manually.
```

Workaround: The user must manually register the old primary as secondary.

SAP agents

This section describes the known issues that are applicable to Cluster Server agents for SAP.

Directory removal failed error/warning appears for SAP agents while upgrading from older versions to version 8.0.2 and later (4122876)

Symptom: This issue is applicable to the SAP NetWeaver, SAP liveCache, and the SAP HANA agents. While upgrading the agents from older versions to version 8.0.2 and later, you may see the following directory removal failed error/warning messages:

```
/bin/rmdir: failed to remove '/opt/VRTSagents/ha/bin/SAPHDB/actions':
Directory not empty
Warning: Problems removing directory [/opt/VRTSagents/ha/bin/SAPHDB/
actions]
```

Note: This issue does not occur in case of upgrades directly from version 8.0.2 to a later version.

Workaround: No workaround required. The error does not affect the upgrade process. Ignore the error and continue with the agent upgrade.

VCS application configuration wizard

This section describes the known issues in the VCS application configuration wizard.

The VCS application configuration wizard fails while adding a new system to the existing configured application (3666881)

Symptom: When the user adds another system from another ESX as a failover system to the existing configured application, the VCS application configuration wizard fails while adding the ESX details. This issue occurs on the Linux operating system.

Workaround: Unconfigure the application monitoring from the existing node and reconfigure the application monitoring with all the required nodes.

The custom application configuration fails when the force stop option is not selected (3688195)

Symptom: For 4Q2014 Agentpack for applicationha 6.1, the custom application configuration fails when the force stop option is not selected.

Description: While configuring custom application using wizard, if you do not select the force stop option, the configuration fails displaying the "Value tag for CleanProgram tag is not provided" error. The configuration expects the value for the CleanProgram attribute for the custom application to be provided. If the value is not provided, the configuration fails.

Workaround: Configure the custom application with the selected force stop option. Value for the force stop option should be provided.

VCS replication agents

The following known issues exist with the replication agents.

Multiple replication agents

This section describes the known issues in multiple replication agents.

A fire drill service group fails to come online on a slave node (4033975)

Symptom: A fire drill service group does not come online on a slave node when you try to bring it online on both the cluster nodes simultaneously or on the slave node first.

Description: This issue occurs because the replication agent resource in a fire drill service group faults. The following error is logged:

```
Could not get list of diskgroups: vxdg list failed; exiting
```

Workaround: You can use one of the following methods to work around this issue.

Note: When you follow these instructions, use the resource names that correspond to your replication environment.

To bring the service group online sequentially

- Bring the fire drill service group online on the master node first and then on the slave node.

  ```
  # hagrp -online fireDrillServiceGroup -sys masterNodeSystemName
  ```

  Replace *fireDrillServiceGroup* and *masterNodeSystemName* with the appropriate values.

To use the OnlineRetryLimit attribute value

1. Set the OnlineRetryLimit attribute to 1 or greater for the fire drill service group.
2. Bring the group online on both the nodes.

   ```
   # hagrp -online fireDrillServiceGroup -any -localclus
   ```

   Replace *FIREDRILLSERVICEGROUP* with the appropriate value.
3. Verify that the group is online on both the nodes.

   In this case, the replication agent resource faults on the first attempt but succeeds on the second attempt, and the service group does not fault.

Import operation for firedrill diskgroup fails on Solaris x86 (3905747)

Symptom: The diskgroup resource in a firedrill service group faults, because the DiskGroup agent fails to import the firedrill disks. Therefore, the firedrill service group fails to come online.

Workaround: Perform the following steps to work around this issue.

Note: These steps use SRDF as an example. In other replication environments, use the appropriate resource names for that environment.

1. Bring the SRDFSnap resource online using the command:

   ```
   hares -online SRDFSnapResource -sys system
   ```

   where, *SRDFSnapResource* is the name of the SRDFSnap resource in the fire drill service group, and *system* is the system on which the fire drill service group must be brought online.
2. Import the diskgroup using the command:

   ```
   vxdg -tfC -o useclonedev=on import diskgroup
   ```

   where, *diskgroup* is a fire drill disk group name.

3. Bring the rest of the fire drill service group online using the command:

   ```
   hagrp -online FiredrillSG -sys system
   ```

   where, *FiredrillSG* is the name of the fire drill service group, and *system* is the system on which the fire drill service group must be brought online.

User's attempt to add a disk to a VxVM disk group may fail (3683553)

Symptom: The user's attempt to add a disk to a VxVM disk group, after the replication roles have changed from Secondary to Primary, might fail.

This issue occurs because of a stale VxVM cache and a VxVM rule that does not permit a user to add a primary disk to a disk group that contains secondary disks.

Note: This issue is applicable for VCS versions prior to VCS 6.2.

Workaround: To resolve this issue, use the Veritas preonline trigger; contact Veritas Technical Support to obtain the Veritas preonline trigger.

Fire drill fails with the error message on the Windows operating system with SFW HA (3123099)

Symptom: On the Windows operating system with SFW HA versions 6.0 or 6.0.1, fire drill might fail with the following error message:

```
ERROR: Disk group: No Disk found with matching tag SIRemote-*
```

Workaround: Follow the instructions given in the TechNote: http://www.veritas.com/docs/000017930 .

File conflict error message displayed while installing the replication agent package in an SFCFS environment (2392131)

Symptom: The replication agents currently ship action entry points on the CVMVolDg resource, which is part of the VRTScavf package. This package is part of the SFCFS package set. The VRTScavf package also ships the same action entry points. As a result, while installing the replication agent package in an SFCFS environment, the installer might display file conflict error messages. This problem occurs on the AIX, HP-UX, Linux, and Solaris operating systems.

Workaround: Veritas recommends installing the replication agent package with the appropriate force option so as to overwrite the conflicting files installed by the VRTScavf package.

Agents might not compute RPO correctly (3681513)

Symptom: Agents might not compute the RPO correctly, if snapshot devices are attached to the replication luns at the DR site and are mapped to the same DR site

hosts. When you invoke the `GetCurrentRPO` action, the agent might display an error message or report an incorrect RPO.

Workaround: Unmap the snapshot devices that are attached to the replication luns from the DR site hosts and then enable RPO computation on the resource.

The HTC and SRDF Replication Agent installation may fail (3875317)

Symptom: The HTC and SRDF replication agents installation may fail on RHEL 7 due to "import" and "deport" files already owned by some other packages.

Workaround: Use the **--replacefiles** option during the installation.

Dell EMC MirrorView

This section describes the known issues in Cluster Server agent for EMC MirrorView.

The MirrorviewSnap resource might fail to come online (2325877)

Symptom: The MirrorviewSnap resource might fail to come online. VxVM does not assign the "_1" suffix to the MirrorView snapshot LUN. As a result, the LUN is not identified as a snapshot LUN and the VCS MirrorViewSnap agent cannot proceed to tag this Snapshot LUN and import the diskgroup.

Workaround: Run the following command:

```
vxconfigd -kr reset
```

If the disk access records are not refreshed on running this command, contact Veritas Technical Support.

Dell EMC SRDF

This section describes the known issues in the Cluster Server agent for EMC SRDF.

SRDF resource goes into a faulted state if ConfValidate is set to 1 (4120957)

Symptom: The SRDF resource goes into a faulted state when the agent attribute `ConfValidate` is set to 1. This issue is applicable on Windows platform.

The `validate_config` action entry point requires that the user SYSTEM@NT AUTHORITY has Group Operator privilege on the remote cluster to be run successfully. Adding the user SYSTEM@NT AUTHORITY does not work correctly due to which it is not possible to give Group Operator privileges to that user account.

Workaround: Set the `ConfValidate` attribute value to 0 to disable the configuration validation.

Silver fire drill configuration may fail with SFHA 6.1 and SFCFS HA 6.1 (3337677)

Symptom: Silver fire drill configuration may fail with SFHA 6.1 and SFCFS HA 6.1.

The Diskgroup agent resource in the fire drill service group may not be able to import the fire drill diskgroup. This is due to a change in the VxVM semantics for importing a clone DiskGroup. The import command may fail with the error:

```
VxVM vxdg ERROR V-5-1-16514 Disk group mera_dg_fd: import failed:
DG import duplicate clone detected.
Please refer to system log for details.
```

Workaround: Perform the following steps for the fire drill to succeed:

- Bring the SRDFSnap resource(s) online.

  `/opt/VRTSvcs/bin/hares -online <SRDFSnapResource> -sys <system>`

  where, *SRDFSnapResource* is the name of the SRDFSnap resource in the fire drill service group, and *system* is the system on which the fire drill service group must be brought online.

- Run the following script to clear the clone_disk flag on the fire drill devices:

  ```
  /usr/sbin/vxdisk listtag |grep <DeviceGroup> |while read x y;
  do echo disk: [$x]; vxdisk set $x clone=off; done
  ```

  where, *DeviceGroup* is the name of the Symmetrix device group.

- Bring the rest of the fire drill service group online.

  `hagrp -online <FiredrilSG> -sys <system>`

  where *FiredrillSG* is the name of the fire drill service group, and *system* is the system on which the fire drill service group must be brought online.

The SRDFSnap resource might not come online (3686816)

Symptom: The SRDFSnap resource might not come online if the host is rebooted while the fire drill luns are in sync with their corresponding source luns.

This issue occurs on the AIX operating system.

Workaround: Bring the devices back to their normal (online) state.

To bring the devices back to their normal (online) state:

1. Find the disks that correspond to the fire drill luns, and run the `vxdisk path` command to find the corresponding VxVM disks.
2. Run the command `vxdisk rm disk1 disk2 ...` to delete the vmdisks corresponding to the fire drill luns.

3 Run the appropriate SYMCLI command to split the devices from their sources and to make the fire drill luns read-write enabled.

4 Use the `vxdisk scandisks` command to rescan the VxVM disks.

5 Run the appropriate SYMCLI `establish` command to resynchronize the fire drill luns with their corresponding sources.

Some of the resources might not come online when a service group has multiple SRDFSnap resources (3231314)

Symptom: When a service group has multiple SRDFSnap resources, some of the resources might not come online.

The `symcfg discover` command locks the Symmetrix configuration database, causing this command to fail for other agents.

Workaround: Run the following command to set the NumThreads attribute of the SRDFSnap agent to 1:

```
$hatype -modify SRDFSnap NumThreads 1
```

The DiskGroup resource may not come online on an AIX LPAR with SYMAPI servers configured (3683665)

Symptom: The DiskGroup resource may not come online on an AIX LPAR with SYMAPI servers configured.

If the host on which the SRDF agent is running is an AIX LPAR, then SymapiServer is required for managing the replication since the Gatekeeper devices cannot be mapped to the LPARs. If the LPAR is rebooted while the underlying SRDF devices are in R2 (secondary) mode, and the VCS service group is subsequently switched to go online on the same LPAR, the DiskGroup resource may not go online. This problem occurs only on the AIX operating system.

Workaround

To work around this issue

1 After the reboot, log on to the AIX LPAR.

2 Find the disks that correspond to the SRDF R2 luns, and run the `vxdisk path` command to find the corresponding VxVM disks.

3 Run the `vxdisk rm` *`disk1 disk2`* command to delete the selected vmdisks.

4 Use the `vxdisk scandisks` command to rescan VxVM disks.

IBM Global Mirror

This section describes the known issue in the Cluster Server agent for IBM Global Mirror.

VxVM disk group might not get imported after failover to DR site in some conditions (3235270)

Symptom: VxVM disk groups might not get imported after a failover to the DR site in the following conditions:

- If VxVM disk groups are configured using IBM GlobalMirror volumes.
- If FlashCopy and Global Copy volumes are attached to the same host.

Workaround: Use the Veritas preonline trigger; contact Veritas Technical Support to obtain the Veritas preonline trigger.

IBM SVCCopyServices

This section describes the known issues in the Cluster Server agent for IBM SVCCopyServices.

The `recreatevg` command fails to create a volume group on the IBM FlashCopy target disks in some cases (3686811)

Symptom: In some cases, the `recreatevg` command fails to create a volume group on the IBM FlashCopy target disks. As a result, the SVCCopyServicesSnap resource fails to come online.

Workaround: Contact Veritas Technical Support.

The application service group fails to come online at the DR site after running the Silver fire drill (3686814)

Symptom: After you run the Silver fire drill, the application service group fails to come online at the disaster recovery site.

Workaround: After running the Silver fire drill for SVCCopyServices at the disaster recovery site, the replication target is resynchronized from the primary when the fire drill service group is taken offline. If a disaster happens before the resynchronization is complete, restore the replication target from the snapshot. After the resynchronization from the primary or restore from the snapshot is complete, you must discard the snapshot to bring the application service group online at the disaster recovery site.

IBM XIV Mirror

This section describes the known issues in the Cluster Server agent for IBM XIV Mirror.

The XCLI script fails to run (3686815)

Symptom: When you use the Cluster Server agent for IBM XIV Mirror with IBM XCLI version 3.1.1, the XCLI script fails to run. This issue is observed on the AIX and Solaris operating systems.

This error is a result of a known issue in the IBM XIV XCLI.

Workaround: For more details about the issue and the resolution, see the release notes for IBM XIV Storage System Management Tools version 3.1.1.

NetApp SnapMirror

This section describes the known issue in the Cluster Server agent for NetAppSnapMirror.

Installation and upgrade of NetApp SnapMirror agent fails on RHEL 8.x and later due to a dependency on Perl (4123104)

Symptom: The installation and upgrade of the NetApp SnapMirror agent fails on RHEL 8.x and later systems.

An error such as the following occurs:

For installation:

```
# rpm -ihv VRTSvcsna-AgentVersion-Linux_GENERIC.noarch.rpm
error: Failed dependencies:
perl(LWP::UserAgent) is needed by
VRTSvcsna-AgentVersion-Linux_GENERIC.noarch
perl(XML::Parser) is needed by
VRTSvcsna-AgentVersion-Linux_GENERIC.noarch
```

For upgrade:

```
# rpm -Uvh VRTSvcsna-AgentVersion-Linux_GENERIC.noarch.rpm
error: Failed dependencies:
perl(LWP::UserAgent) is needed by
VRTSvcsna-AgentVersion-Linux_GENERIC.noarch
perl(XML::Parser) is needed by
VRTSvcsna-AgentVersion-Linux_GENERIC.noarch
```

Description: This issue occurs due to an unresolved dependency on Perl modules.

Workaround: Use the **--nodeps** option to work around this issue and complete the agent RPM installation and upgrade.

For installation:

```
# rpm -ivh VRTSvcsna-AgentVersion-Linux_GENERIC.noarch.rpm --nodeps
```

For upgrade:

```
# rpm -Uvh VRTSvcsna-AgentVersion-Linux_GENERIC.noarch.rpm --nodeps
```

Remote failover of NetApp resource fails (3513500)

Symptom: If the schedule for QSM or VSM is not present in the `\etc\snapmirror.conf` file at the destination filer, then the remote failover of NetApp resource fails.

Workaround: Manually add schedule entry to the `\etc\snapmirror.conf` file of the destination filer and then perform remote failover operation.

Oracle DataGuard

This section describes the known issue in the Cluster Server agent for Oracle Data Guard.

The Oracle Data Guard Broker resource comes online on the first RAC node, but might fail to come online on the remaining RAC nodes (3612692)

Symptom: In an Oracle RAC configuration, the Oracle Data Guard Broker resource comes online on the first RAC node, but might fail to come online on the remaining RAC nodes. This issue occurs when the DGMGRL status on the primary database is ERROR.

Workaround: Run the `show configuration` DGMGRL command and resolve the error. You can then bring the resource online.

Oracle GoldenGate

This section describes the known issues in the Cluster Server agent for Oracle GoldenGate.

The GetCurrentRPO action function is likely to time out (3681336)

Symptom: The GetCurrentRPO action function is likely to time out when the application is writing continuously to the database.

Workaround: Increase the timeout value of the GetCurrentRPO action function for the GoldenGate type.

The data written to the database might not be replicated (3681338)

Symptom: When a system on which the GoldenGate resource is online faults and fails over to another system in the same cluster, data that is written to the database after the fault occurs might not be replicated.

Workaround: When the GoldenGate resource comes online on another system in the same cluster, perform the following tasks:

- In the remote cluster, remove the lock on the trail file on the remote system. To do this, temporarily rename the file and then revert to the original file name.
- Restart the Replicat process in the remote cluster. To do this, run the StopReplicat action function and then run the StartReplicat action function.

Oracle GoldenGate resource fails to come online in case of GCO (4123543)

Symptoms: Oracle GoldenGate resource faults and fails to start the manager process if multiple Oracle instances are configured on the same node.

Description: The agent fails to bring the Oracle GoldenGate resource online when multiple Oracle instances are configured on the same node and the GoldenGate manager process is stopped. The issue is specific to GCO configuration.

Workaround: Start the manager process manually for all the instances by following these steps:

1. Navigate to Oracle GoldenGate home directory.
2. Login to ggsci.
3. Execute command `start mgr`.
4. To check the manager status, execute command `info all`.

Pure Storage replication agents

This section describes the known issues in the Cluster Server agents for Pure Storage replication.

Failed to probe a Pure Storage resource on an InfoScale 7.4.1 system (4033982)

Symptom: A service group that contains Pure Storage resources (PURE type) fails to come online.

Description: This issue occurs after the agent encounters the following error:

```
ImportError: No module named 'requests'
```

Workaround: Perform the following steps.

To use the OnlineRetryLimit attribute value

1. Install the `requests` module on the InfoScale 7.4.1 system by using the command:

   ```
   # /opt/VRTSpython/bin/pip install requests
   ```

2. Probe the PURE resource.

   ```
   # hares -probe resourceName -sys systemName
   ```

   Replace *resourceName* and *systemName* with the appropriate values.

3. Bring the resource online.

   ```
   # hares -online resourceName -sys systemName
   ```

   Use the same values for *resourceName* and *systemName* as in the previous step.

HP 3PAR RemoteCopy

This section describes the known issue in the Cluster Server agent for HP 3PAR RemoteCopy.

HP 3PAR RemoteCopy resource failed to come online due to certificate exception file path when HP 3PAR CLI used (4101785).

Symptom: HP 3PAR RemoteCopy resource failed to come online due to certificate exception file path when HP 3PAR CLI is used.

This issue occurs on the Linux operating systems.

```
Error: CLI Server Certificate

Issuer: CN=hpe3par02.sample.host.veritas.com

Subject: CN=hpe3par02.sample.host.veritas.com

SHA1 fingerprint: 94CF38E5553BB8515E53B748AAB03F9C88DDDD42

Validity: Not before: Jan  3 08:22:00 2023 GMT

Not after: Dec 31 08:22:00 2032 GMT

Warning: Self signed certificate

Warning: subject CN ("hpe3par02.sample.host.veritas.com") does not match
the system name ("10.210.231.20")
Continue connecting (yes/no)?
```

Workaround: Perform the following steps.

To export TPDCERTDIR environment variable

1. Stop VCS engine using `hastop` command.
2. Define TPDCERTDIR environment variable in `/opt/VRTSvcs/bin/custom_vcsenv` VCS environment variable file. Create the `/opt/VRTSvcs/bin/custom_vcsenv` file if not present.

   For example, define the variables as:

   ```
   TPDCERTDIR=/root/.hpe3par; export TPDCERTDIR
   ```

   TPDCERTDIR: Directory in which to save certificate exception file.
3. Start the VCS engine using `hastart` command.
4. Bring the resource online.

   ```
   # hares -online RemoteCopyResource -sys system
   ```

Limitations

This section describes the limitations of the agents in this release.

SAN HANA agent

The SAP HANA agent has the following limitations:

- SystemD support is not enabled for SAP HANA Scale-Out system.
- In case of SAP HANA System Replication, when the primary and secondary instances are offline simultaneously, the SAPHDB agent cannot determine the replication status. Therefore, the agent brings the SAP HANA instance up with the last known replication status.

SAP liveCache 7.7 agent

On SAP liveCache 7.7, the intentional offline functionality might not work because the `lcinit` and `lccluster` scripts do not get executed.

Documentation

The following sections contain useful information about the Cluster Server Agent Pack documentation.

Locating and viewing documentation

The latest version of the Agent Pack documentation is available in PDF format on the Veritas Services and Operations Readiness Tools (SORT) Web site here: https://sort.veritas.com/agents.

You can also find the documentation for each agent in the `docs` directory after you download the agent.

Getting help

Visit https://www.veritas.com/support/en_US.html for product assistance. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and our customer email notification service. If you encounter an error when using a product, include the error number preceding the message when contacting Technical Services. You can also use the error number to search for information in TechNotes or documents on the Web site.