Cluster Server Agent for NetApp SnapMirror with Clustered Data ONTAP Configuration Guide

Windows

7.0

April 2019

VERITAS™

Veritas InfoScale™ Availability Agents

Last updated: 2019-04-03

Legal Notice

Copyright © 2019 Veritas Technologies LLC. All rights reserved.

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

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

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

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

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

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

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

http://www.veritas.com

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:

xyz@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

Contents

Chapter 1 Introducing the agents for cluster-mode SnapMirror 6

About the cluster-mode SnapMirror agent 6
About the cluster-mode NetApp Filer agent 7
Supported software 7
Typical cluster-mode SnapMirror setup in a VCS cluster 7
Cluster-mode SnapMirror agent functions 8
About the online function of the cluster-mode SnapMirror agent 9
Cluster-mode Filer agent functions 10

Chapter 2 Installing and removing the agent for cluster-mode SnapMirror 12

Before you install the agent for cluster-mode SnapMirror 12
Installing the agent for cluster-mode SnapMirror 13
Removing the agent for cluster-mode SnapMirror 14

Chapter 3 Configuring the agent for cluster-mode SnapMirror 16

Configuration concepts for cluster-mode SnapMirror and Filer agents 16
Cluster-mode SnapMirror agent resource type definition 16
Cluster-mode SnapMirror agent attribute definitions 17
Cluster-mode SnapMirror agent sample configurations 19
Cluster-mode Filer agent resource type definition 24
Cluster-mode Filer agent attribute definitions 24
Cluster-mode Filer agent sample configuration 25
Before you configure the agent for cluster-mode SnapMirror 25
About cluster heartbeats 26

Chapter 4 Testing VCS disaster recovery support with cluster-mode SnapMirror 27

How VCS recovers from various disasters in an HA/DR setup with cluster-mode SnapMirror 27
Failure scenarios in global clusters 28
Testing the global service group migration 31
Testing disaster recovery after host failure 32
Testing disaster recovery after site failure 32
Performing failback after a node failure or an application failure 33
Performing failback after a site failure 34

Chapter 1

Introducing the agents for cluster-mode SnapMirror

This chapter includes the following topics:

- About the cluster-mode SnapMirror agent
- About the cluster-mode NetApp Filer agent
- Supported software
- Typical cluster-mode SnapMirror setup in a VCS cluster
- Cluster-mode SnapMirror agent functions
- About the online function of the cluster-mode SnapMirror agent
- Cluster-mode Filer agent functions

About the cluster-mode SnapMirror agent

The VCS agent for NetApp SnapMirror with Clustered Data ONTAP provides application failover support and recovery in environments that use SnapMirror to replicate data between NetApp filers. You can use this agent in global clusters that run VCS. This agent works with the NetApp Filer with Clustered Data ONTAP agent for certain functions.

Note: The NetApp SnapMirror features and NetApp Filer devices in Clustered Data ONTAP environments are henceforth referred to as cluster-mode SnapMirror and cluster-mode Filer.

The agent performs the following tasks:

- Monitors and manages the state of a volume for which SnapMirror replication is configured on the filers.
- Ensures that at any given time, only one host has safe exclusive access to the configured filer volume.
- Determines the current role of the filer volume with respect to replication, and promotes a read-only target to a read-write source during a wide-area failover.

The cluster-mode SnapMirror agent supports only the iSCSI and FC/FCoE protocols.

The agent supports only data protection relationships, but not others like vault and load-sharing.

The agent does not support the following configurations:

- Qtree replication
- Multi-pathing
- Fire drill

About the cluster-mode NetApp Filer agent

The cluster-mode NetApp Filer agent monitors the local NetApp filer and determines it's connectivity with the VCS node. This agent is configured as a resource of type NetappFilerCM.

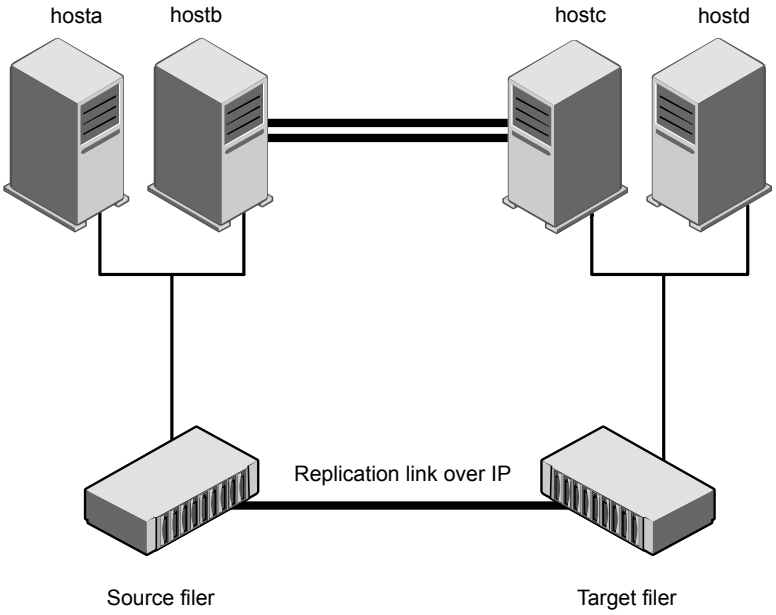
Supported software

For information on the software versions that the agent for cluster-mode SnapMirror supports, see the Veritas Services and Operations Readiness Tools (SORT) site: https://sort.veritas.com/agents.

Typical cluster-mode SnapMirror setup in a VCS cluster

The following figure depicts a typical cluster setup in a cluster-mode SnapMirror environment.

Figure 1-1 Typical clustering setup for the agent



Clustering in a cluster-mode SnapMirror environment typically consists of the following hardware infrastructure:

- One or more source hosts are connected by an ethernet cable to a NetApp device. The cluster-mode SnapMirror agent supports the iSCSI and FC/FCoE transport protocols.
- One or more target hosts are attached to a second filer with similar characteristics as the source hosts. The volume is a target for cluster-mode SnapMirror.
- The network heartbeat between the two data centers is used to determine their health; the heartbeat could be LLT or TCP/IP.
- In a global cluster environment, you must attach all hosts in the same cluster to the same filer.

Cluster-mode SnapMirror agent functions

This agent monitors and manages the state of the replicated cluster-mode NetApp SnapMirror volumes that are attached to VCS nodes. It brings resources online, takes them offline, and performs various monitoring actions.

Table 1-1 Agent functions

Function	Description
Online	Creates a lock file on the local host to indicate that the resource is online. Depending on whether the filer is a source or a target and on the state of the specified volume on the filer, the agent performs the online function. See "About the online function of the cluster-mode SnapMirror agent" on page 9.
Offline	Removes the lock file, but does not perform any filer operations. Taking the resource offline is not an indication of a pending role swap.
Monitor	Checks whether the lock file exists and acts accordingly: ■ If the lock file exists, it reports the status of the resource as online. ■ If the lock file does not exist, it reports the status of the resource as offline.
Open	Removes the lock file on the system on which this function is called. The agent prevents potential concurrency violation if the group fails over to another node. **Note:** The agent does not remove the lock file if the agent was started after a `hastop -force` command.
Clean	Performs the same operation as the offline function.

About the online function of the cluster-mode SnapMirror agent

The online function checks the state of the specified volume on the local filer device. The volume on the local filer is of the RW type when it is the replication source. The volume is of the DP type when it is the replication target.

The agent performs the following online operations:

- If the volume type on the local filer device is RW, the agent creates a lock file to indicate that the resource can come online.
- If the filer is a target, the agent attempts to reverse the direction of replication. To reverse the replication, the agent promotes the local filer to a source and the original source to a target as follows:

- Updates the destination volume
- Quiesces the replication
- Breaks off the SnapMirror connection
- Reverses the direction of replication.
- Resynchronizes the local filer with the new target filer
- Sets the SnapMirror schedule and policy on the remote filer, which is the new target

- If the original source is down, the agent attempts a takeover to enable local write access as follows:
  - Quiesces the replication
  - Breaks off the SnapMirror connection
- If the original source comes online, you must resynchronize the data manually.
- If read-write access is enabled successfully, the online function creates a lock file.

Cluster-mode Filer agent functions

This agent monitors and manages the state of the cluster-mode NetApp Filer devices that are attached to VCS nodes.

Table 1-2 Agent functions

Function	Description
Online	Checks whether the local filer is accessible and if so, the agent creates the resource lock file.
Offline	Removes the lock file and takes the filer resource offline without taking the corresponding array down.
Monitor	Checks whether the resource lock file exists and if so, checks whether the filer is accessible. If both the conditions are met, it reports the resource as online.
Open	Removes the lock file on the system on which this function is called. The agent prevents potential concurrency violation if the group fails over to another node. **Note:** The agent does not remove the lock file if the agent was started after a `hastop -force` command.

Table 1-2 Agent functions *(continued)*

Function	Description
Clean	Performs the same operation as the offline function.

Chapter 2

Installing and removing the agent for cluster-mode SnapMirror

This chapter includes the following topics:

- Before you install the agent for cluster-mode SnapMirror
- Installing the agent for cluster-mode SnapMirror
- Removing the agent for cluster-mode SnapMirror

Before you install the agent for cluster-mode SnapMirror

Before you install the VCS agent for cluster-mode SnapMirror, ensure that you install and configure VCS on all nodes in the cluster.

Set up replication and the required hardware infrastructure.

Note: For VCS 6.0, 6.0.1, 6.0.2, and VCS 7.0, make sure that the Microsoft Visual C++ 2010 SP1 (x64) and the Microsoft Visual C++ 2010 SP1 (x86) re-distributable packages are installed on the systems where you need to install the agent pack.

The SnapMirrorCM agent only supports HTTP as the transport protocol; make sure that HTTP is enabled on the NetApp filer.

The SnapMirrorCM agent requires some specific VRTSPerl modules for its operation, which are not available with InfoScale 7.3.1 on Windows. Make sure to install the

VRTSPerl_7_3_10001_3969020 patch to get the required modules. The patch is available at:

https://sort.veritas.com/patch/detail/14619

See “Typical cluster-mode SnapMirror setup in a VCS cluster” on page 7.

Installing the agent for cluster-mode SnapMirror

You must install the cluster-mode SnapMirror agent on each node in the cluster. In global cluster environments, install the agent on each node in each cluster.

To install the VCS agent for cluster-mode SnapMirror from the agent pack release

1. Log on to any node in the cluster.

   Ensure that the logged on user has the domain administrative privileges.

2. Download the agent pack from the Veritas Services and Operations Readiness Tools (SORT) site: https://sort.veritas.com/agents.

   You can download the complete agent pack `zip` file or the individual agent `zip` file.

3. Uncompress the file to a temporary location.

4 If you downloaded the complete agent pack `zip` file, navigate to the appropriate directory:

Windows Server 2008 R2 x64	`cd1\windows\w2k8r2x64\vcs\replication\ntap_agent\`*`agent_version`*`\pkgs`
Windows 2012 x64	`cd1\windows\w2k12x64\vcs\replication\ntap_agent\`*`agentversion`*`\pkgs`
Windows Server 2012 R2 x64	`cd1\windows\w2k12r2x64\vcs\replication\ntap_agent\`*`agent_version`*`\pkgs`
Windows Server 2016 x64	`cd1\windows\w2k16\vcs\replication\ntap_agent\`*`agent_version`*`\pkgs`

5 Double-click **vrtsvcsntapcm.msi**.

Follow the instructions on the wizard to complete the installation of the agent.

The installer for cluster-mode SnapMirror agent installs the binaries for both, the cluster-mode SnapMirror and cluster-mode Filer agents.

The installer logs are created at the location specified in the `%TEMP%` environment variable.

Removing the agent for cluster-mode SnapMirror

Note: Do not attempt to remove the agent if the service groups that access the shared storage are online.

To remove the agent for cluster-mode SnapMirror that was installed from an agent pack release

1 Open the Programs and Features window, select Cluster Server Agent for NetApp SnapMirror with Clustered Data ONTAP (or `vrtsvcsntapcm.msi`), and click **Uninstall**.

2 Follow the wizard instructions to complete the uninstallation.

Note: When you uninstall the agent pack, all the agent binaries for cluster-mode SnapMirror are removed. If you need the agent binaries that were part of the base release, you must manually repair the base release.

Chapter 3

Configuring the agent for cluster-mode SnapMirror

This chapter includes the following topics:

- Configuration concepts for cluster-mode SnapMirror and Filer agents
- Before you configure the agent for cluster-mode SnapMirror

Configuration concepts for cluster-mode SnapMirror and Filer agents

In a NetApp Clustered Data ONTAP environment, you can configure SnapMirror resources with or without Filer resources for high availability using VCS.

For SnapMirror resources with Filer resources, Veritas recommends the following configuration:

- Configure the SnapMirror resource and the Filer resource in a separate service groups.
- Configure the Filer service group as a child of the SnapMirror service group and set the dependency as `online-local-firm`.

Cluster-mode SnapMirror agent resource type definition

The SnapMirrorCM resource type represents the cluster-mode NetApp SnapMirror agent in VCS.

```
type SnapMirrorCM (
 static int ActionTimeout = 120
 static int NumThreads = 1
 static int OfflineMonitorInterval = 30
```

```
 static int OpenTimeout = 180
 static int AgentReplyTimeout = 30
 static i18nstr ArgList[] = { VolumeName, LocalFilerName, LocalFilerPword,
  RemoteFilerName, RemoteFilerPword,   LocalFilerUserName,
  RemoteFilerUserName, VServer, CModeCluster, AutoTakeover, SplitTakeover }
 str VolumeName
 str LocalFilerName
 str LocalFilerUserName = root
 str LocalFilerPword
 str RemoteFilerName
 str RemoteFilerUserName = root
 str RemoteFilerPword
 str VServer
 str CModeCluster
 boolean AutoTakeover = 0
 int SplitTakeover = 0
)
```

Cluster-mode SnapMirror agent attribute definitions

The following VCS agent attributes are required for cluster-mode SnapMirror configurations.

Table 3-1 Required attributes for the cluster-mode SnapMirror agent

Attribute	Description
Name: **LocalFilerName** Type: string Dimension: scalar	The DNS resolvable name of the local NetApp filer. You must use the same value for the LocalFilerName as in the NetAppSnapMirror configuration. If the filer name is not fully qualified in the NetAppSnapMirror configuration, do not use the fully qualified name to set this attribute. For example, if the filer name is defined as **netapp3.example.com** in the configuration, use the same filers name to set the attribute.
Name: **LocalFilerUserName** Type: string Dimension: scalar	The local NetApp filer user who has permissions to perform SnapMirror actions using ONTAP SDK.
Name: **LocalFilerPword** Type: string Dimension: scalar	A valid encrypted password for the user on the local filer. If you enter the password from the command line, run the `vcsencrypt` command to encrypt the password. Do not encrypt passwords when entering them from the GUI.

Table 3-1 Required attributes for the cluster-mode SnapMirror agent *(continued)*

Attribute	Description
Name: **RemoteFilerName** Type: string Dimension: scalar	The DNS resolvable name of the remote NetApp filer. You must use the same value for the RemoteFilerName as in the NetAppSnapMirror configuration. If the filer name is not fully qualified in the NetAppSnapMirror configuration, do not use the fully qualified name to set this attribute. For example, if the filer name is defined as **netapp3.example.com** in the configuration, use the same filer name to set the attribute.
Name: **RemoteFilerUserName** Type: string Dimension: scalar	The remote NetApp filer user who has permissions to perform SnapMirror actions using ONTAP SDK.
Name: **RemoteFilerPword** Type: string Dimension: scalar	A valid encrypted password for the root user on the remote filer. If you enter the password from the command line, run the `vcsencrypt` command to encrypt the password. Do not encrypt passwords when entering them from the GUI.
Name: **VolumeName** Type: string Dimension: scalar	Specifies the name of the replicated volume on the filer. You must use same case for the volume name as on the filer, because the attribute value is case-sensitive.
Name: **VServer** Type: string Dimension: scalar	Specifies the Vserver name of the SnapMirror relationship in cluster mode.
Name: **CModeCluster** Type: string Dimension: scalar	Specifies the cluster name of the SnapMirror relationship in cluster mode.
Name: **AutoTakeover** Type: boolean Dimension: scalar	Used to determine whether or not the cluster-mode SnapMirror resource should be brought online when the remote filer is not reachable. ■ False: If the remote filer is unreachable, no action is taken. ■ True: If the remote filer is unreachable, the resource is brought online. Default value: False

Table 3-1 Required attributes for the cluster-mode SnapMirror agent *(continued)*

Attribute	Description
Name: **SplitTakeover** Type: integer Dimension: scalar	Used to determine whether or not the cluster-mode SnapMirror resource should be brought online when the replication state is broken-off. ■ 0 (zero): Indicates that the resource is not be brought online if the replication state is broken-off. ■ 1: Indicates that the resource is brought online if the replication state is broken-off. ■ Other values of the attribute are reserved for future use by the agent.

Cluster-mode SnapMirror agent sample configurations

A resource of the SnapMirrorCM type may be configured with the NetappFilerCM resource type as follows in `main.cf`:

```
include "types.cf"

cluster pr_clus1 (
 UserNames = { a = bkkE }
 ClusterAddress = "10.209.56.97"
 Administrators = { a }
 )

remotecluster dr_clus1 (
 ClusterAddress = "10.209.56.117"
 )

heartbeat Icmp (
 ClusterList = { dr_clus1 }
 Arguments @dr_clus1 = { "10.209.56.117" }
 )

system DL380G9-20-VM2 (
 )

group ClusterService (
 SystemList = { DL380G9-20-VM2 = 0 }
 AutoStartList = { DL380G9-20-VM2 }
 )
```

```
IP csg_ip (
 Address = "10.209.56.97"
 SubNetMask = "255.255.252.0"
 MACAddress @DL380G9-20-VM2 = "00:50:56:8E:27:CD"
 )

NIC csg_nic (
 MACAddress @DL380G9-20-VM2 = "00:50:56:8E:27:CD"
 )

Process wac (
 StartProgram @DL380G9-20-VM2 = "\"C:\\Program Files
   \\Veritas\\Cluster Server\\bin\\wac.exe\""
 StopProgram @DL380G9-20-VM2 = "\"C:\\Program Files
   \\Veritas\\Cluster Server\\bin\\wacstop.exe\""
 MonitorProgram @DL380G9-20-VM2 = "\"C:\\Program Files
   \\Veritas\\Cluster Server\\bin\\wacmonitor.exe\""
 )

csg_ip requires csg_nic
wac requires csg_ip


// resource dependency tree
//
// group ClusterService
// {
// Process wac
//     {
//     IP csg_ip
//         {
//         NIC csg_nic
//         }
//     }
// }


group filer_sg (
 SystemList = { DL380G9-20-VM2 = 0 }
 AutoStartList = { DL380G9-20-VM2 }
 )
```

```
 NetappFilerCM filer_res (
  LocalFilerName = "10.209.92.170"
  LocalFilerUserName = vrpadmin
  LocalFilerPword = CODoGOpOLoQIdIEiF
  )



 // resource dependency tree
 //
 // group filer_sg
 // {
 // NetappFilerCM filer_res
 // }


group netapp_sg (
 SystemList = { DL380G9-20-VM2 = 0 }
 ClusterList = { pr_clus1 = 0, dr_clus1 = 1 }
 AutoStartList = { DL380G9-20-VM2 }
 )

 MountV mount_res (
  MountPath = E
  VolumeName = vol1
  VMDGResName = dg_res
  )

 SnapMirrorCM res1 (
  VolumeName = bck2
  LocalFilerName = "10.209.92.170"
  LocalFilerUserName = vrpadmin
  LocalFilerPword = frgRjrSroRtlGlhLi
  RemoteFilerName = "10.209.92.171"
  RemoteFilerUserName = vrpadmin
  RemoteFilerPword = codOgoPolOqiDieIf
  VServer = SAN_IAFAS3240
  )

 VMDg dg_res (
  DiskGroupName = windg
  )
```

```
 requires group filer_sg online local firm
 dg_res requires res1
 mount_res requires dg_res


 // resource dependency tree
 //
 // group netapp_sg
 // {
 // MountV mount_res
 //     {
 //     VMDg dg_res
 //         {
 //         SnapMirrorCM res1
 //         }
 //     }
 // }


group netapp_sg2 (
 SystemList = { DL380G9-20-VM2 = 0 }
 AutoStartList = { DL380G9-20-VM2 }
 )

 MountV mount_res (
  MountPath = F
  VolumeName = vol2
  VMDGResName = dg_res1
  )

 SnapMirrorCM snapmirror_res2 (
  VolumeName = remvol
  LocalFilerName = "10.209.92.170"
  LocalFilerUserName = vrpadmin
  LocalFilerPword = EQFqIQrQNqSKfKGkH
  RemoteFilerName = "10.209.92.171"
  RemoteFilerUserName = vrpadmin
  VServer = SAN_IAFAS3240
  CModeCluster = IAFAS3240
  )
                VMDg dg_res1 (
  DiskGroupName = windg1
  )
```

```
 requires group filer_sg online local firm


 // resource dependency tree
 //
 // group netapp_sg2
 // {
                  MountV mount_res1
                    {
                      VMDg dg_res1
                       {

 //            SnapMirrorCM snapmirror_res2
 // }
```

A resource of the NetAppSnapMirrorCM type may be configured without the NetAppFilerCM resource as follows in `main.cf` (partial code snippet):

```
group Snapmirror_sg (
     SystemList = { DL380G9-47-VM14 = 0 }
     ClusterList = { drsite1 = 1, prsite1 = 0 }
     AutoStartList = { DL380G9-47-VM14 }
     )

     MountV mount_res (
           MountPath = E
           VolumeName = vol1
           VMDGResName = dg_res
           )

     SnapMirrorCM res1 (
           VolumeName = vol15gb
           LocalFilerName = "10.209.92.170"
           LocalFilerUserName = vrpadmin
           LocalFilerPword = bncNfnOnkNphChdHe
           RemoteFilerName = "10.209.92.171"
           RemoteFilerUserName = vrpadmin
           RemoteFilerPword = JVKvNVwVSvXPkPLpM
           VServer = SAN_IAFAS3240
           CModeCluster = IAFAS3240
           )
```

```
VMDg dg_res (
      DiskGroupName = windg
      DGGuid = 4f693034-de74-42e1-8e72-a99b2219cf88
      )

mount_res requires dg_res
dg_res requires res1


// resource dependency tree
//
//   group Snapmirror_sg
//   {
//   MountV mount_res
//       {
//       VMDg dg_res
//           {
//           SnapMirrorCM res1
//           }
//       }
//   }
```

Cluster-mode Filer agent resource type definition

The NetappFilerCM resource type represents the cluster-mode NetApp Filer agent in VCS.

```
type NetappFilerCM (
 static i18nstr ArgList[] = { LocalFilerName, LocalFilerPword,
  LocalFilerUserName }
 static int ToleranceLimit = 1
 str LocalFilerName
 str LocalFilerUserName = root
 str LocalFilerPword
)
```

Cluster-mode Filer agent attribute definitions

The following VCS agent attributes are required for cluster-mode Filer configurations.

Table 3-2 Required attributes for the cluster-mode Filer agent

Required Attribute	Description
Name: **LocalFilerName** Type: string Dimension: scalar	The DNS resolvable name of the local NetApp filer. You must use the same value for the LocalFilerName as in the NetAppSnapMirror configuration. If the filer name is not fully qualified in the NetAppSnapMirror configuration, do not use the fully qualified name to set this attribute. For example, if the filer name is defined as **netapp3.example.com** in the configuration, use the same filers name to set the attribute.
Name: **LocalFilerUserName** Type: string Dimension: scalar	The local NetApp filer user who has permissions to perform SnapMirror actions using ONTAP SDK.
Name: **LocalFilerPword** Type string: Dimension: scalar	A valid encrypted password for the user on the local filer. If you enter the password from the command line, run the `vcsencrypt` command to encrypt the password. Do not encrypt passwords when entering them from the GUI.

Cluster-mode Filer agent sample configuration

A resource of the NetappFilerCM type may be configured with the as follows in `main.cf`:

```
NetappFilerCM filer_res (
  LocalFilerName = "10.209.92.170"
  LocalFilerUserName = vrpadmin
  LocalFilerPword = CODoGOpOLoQIdIEiF
  )
```

Before you configure the agent for cluster-mode SnapMirror

Before you configure the agent, review the following information:

- Verify that you have installed the agent on all systems in the cluster.
- Verify the hardware setup for the agent.
  See "Typical cluster-mode SnapMirror setup in a VCS cluster" on page 7.
- Make sure that the cluster has an effective heartbeat mechanism in place.

See “About cluster heartbeats” on page 26.

You can automate the mounting of filer volumes through VCS. Configure a resource of type MountV as the parent of the SnapMirrorCM resource. You must also configure the filer to export the volumes to all the nodes in the cluster.

About cluster heartbeats

In a global cluster, VCS sends ICMP pings over the public network between the two sites for network heartbeating. To minimize the risk of split-brain, VCS sends ICMP pings to highly available IP addresses. VCS global clusters also notify the administrators when the sites cannot communicate.

Chapter 4

Testing VCS disaster recovery support with cluster-mode SnapMirror

This chapter includes the following topics:

- How VCS recovers from various disasters in an HA/DR setup with cluster-mode SnapMirror
- Testing the global service group migration
- Testing disaster recovery after host failure
- Testing disaster recovery after site failure
- Performing failback after a node failure or an application failure
- Performing failback after a site failure

How VCS recovers from various disasters in an HA/DR setup with cluster-mode SnapMirror

This topic lists various failure scenarios and describes how VCS responds to the failures in the following DR cluster configurations.

Global clusters

When a site-wide global service group or system fault occurs, VCS failover behavior depends on the value of the ClusterFailOverPolicy attribute for the faulted global service group. The VCS agent for cluster-mode SnapMirror ensures safe and exclusive access to the configured cluster-mode SnapMirror devices.

See "Failure scenarios in global clusters" on page 28.

Refer to the *Cluster Server Administrator's Guide* for more information on the DR configurations and the global service group attributes.

Failure scenarios in global clusters

The following table lists the failure scenarios in a global cluster configuration and describes the behavior of VCS and the agent in response to the failure.

Table 4-1 Failure scenarios in a global cluster configuration with the VCS agent for cluster-mode SnapMirror

Failure	Description and VCS response

Application failure	Application cannot start successfully on any hosts at the primary site.
	VCS response at the secondary site:
	■ Causes global service group at the primary site to fault and displays an alert to indicate the fault.
	■ Does the following based on the ClusterFailOverPolicy global service group attribute:
	  ■ Auto or Connected—VCS automatically brings the faulted global group online at the secondary site.
	  ■ Manual—No action. You must bring the global group online at the secondary site.
	Agent response: The SnapMirrorCM agent first executes the update operation to switch the source and destination. To make local device RW enabled, the agent changes the SnapMirror replication to the broken-off state. Then, it reverses the direction of replication by using the reverse-resync operation.
	See "Performing failback after a node failure or an application failure" on page 33.

Host failure	All hosts at the primary site fail.
	VCS response at the secondary site:
	■ Displays an alert to indicate the primary cluster fault.
	■ Does the following based on the ClusterFailOverPolicy global service group attribute:
	  ■ Auto—VCS automatically brings the faulted global group online at the secondary site.
	  ■ Manual or Connected—No action. You must bring the global group online at the secondary site.
	Agent response:
	The SnapMirrorCM agent first executes the update operation to switch the source and destination. To make local device RW enabled, the agent changes the SnapMirror replication to the broken-off state. Then, it reverses the direction of replication by using the reverse-resync operation.
	See "Performing failback after a node failure or an application failure" on page 33.

Table 4-1 Failure scenarios in a global cluster configuration with the VCS agent for cluster-mode SnapMirror *(continued)*

Failure	Description and VCS response

Site failure	All hosts and the storage at the primary site fail.
	
	If the primary filer is down, the SnapMirrorCM agent sets the replication state to UNHEALTHY.
	
	VCS response at the secondary site:
	
	■ Displays an alert to indicate the cluster fault.
	■ Does the following based on the ClusterFailOverPolicy global service group attribute:
	  ■ Auto—VCS automatically brings the faulted global group online at the secondary site.
	  ■ Manual or Connected—No action. You must bring the global group online at the secondary site.
	
	The SnapMirrorCM agent takes action based on the AutoTakeover attribute value as follows:
	
	■ **True**: Changes the SnapMirror relationship status to broken-off, promotes the local device to the RW state, and brings the SnapMirror resource online.
	■ **False**: Does not change the state of the local device, but faults the resource and logs a message stating that administrator intervention is required.
	
	See "Performing failback after a site failure" on page 34.

Replication link failure	Replication link between the arrays at the two sites fails. VCS response: No action. **Note:** Currently, the cluster-mode SnapMirror agent cannot monitor the SnapMirror replication link status.

Table 4-1 Failure scenarios in a global cluster configuration with the VCS agent for cluster-mode SnapMirror *(continued)*

Failure	Description and VCS response

Network failure	The network connectivity and the replication link between the sites fail.
	
	VCS response at the secondary site:
	
	■ VCS at each site concludes that the remote cluster has faulted.
	■ Does the following based on the ClusterFailOverPolicy global service group attribute:
	  ■ Manual or Connected—No action. You must confirm the cause of the network failure from the cluster administrator at the remote site and fix the issue.
	  ■ Auto—VCS brings the global group online at the secondary site which may lead to a site-wide split brain. This causes data divergence between the devices on the primary and the secondary arrays.
	  When the network (WAC and replication) connectivity is restored, you must manually resync the data.
	
	  Note: Veritas recommends that the value of the ClusterFailOverPolicy attribute is set to Manual for all global groups to prevent unintended failovers due to transient network failures.
	
	To resynchronize the data after the network link is restored:
	
	■ Take the global service group offline at both the sites.
	■ Manually resynchronize the data.
	  Depending on the site whose data you want to retain, use the appropriate API for NetApp SnapMirror with Clustered Data ONTAP.
	
	The SnapMirrorCM agent takes action based on the AutoTakeover attribute value as follows:
	
	■ **True**: Changes the SnapMirror relationship status to broken-off, promotes the local device to the RW state, and brings the SnapMirror resource online.
	■ **False**: Does not change the state of the local device, but faults the resource and logs a message stating that administrator intervention is required.

Table 4-1 Failure scenarios in a global cluster configuration with the VCS agent for cluster-mode SnapMirror *(continued)*

Failure	Description and VCS response

Storage failure	The array at the primary site fails.
	If the primary filer is down, the SnapMirrorCM agent sets the replication state to UNHEALTHY.
	VCS response at the secondary site:
	■ Causes the global service group at the primary site to fault and displays an alert to indicate the fault.
	■ Does the following based on the ClusterFailOverPolicy global service group attribute:
	  ■ Auto or Connected—VCS automatically brings the faulted global service group online at the secondary site.
	  ■ Manual—No action. You must bring the global group online at the secondary site.
	The SnapMirrorCM agent takes action based on the AutoTakeover attribute value as follows:
	■ **True**: Changes the SnapMirror relationship status to broken-off, promotes the local device to the RW state, and brings the SnapMirror resource online.
	■ **False**: Does not change the state of the local device, but faults the resource and logs a message stating that administrator intervention is required.

Testing the global service group migration

After you configure the Cluster Server agent for cluster-mode SnapMirror, verify that the global service group can migrate to hosts across the sites. Depending on your DR configuration, perform one of the following procedures.

To test the global service group migration in global cluster setup

1. Fail over the global service group from the primary site to the secondary site.

   Perform the following steps:

   ■ Switch the global service group from the primary site to any node in the secondary site.

   ```
   hagrp -switch global_group -any -clus cluster_name
   ```

   VCS brings the global service group online on a node at the secondary site.

   ■ Verify that the volumes at the secondary site are write-enabled and the mirror state is SNAPMIRRORED.

2. Fail back the global service group from the secondary site to the primary site.

   Perform the following steps:

- Switch the global service group from the secondary site to the primary site.

  ```
  hagrp -switch global_group -any -clus cluster_name
  ```

  VCS brings the global service group online at the primary site.
- Verify that the volumes at the secondary site are write-enabled and the mirror state is SNAPMIRRORED.

Testing disaster recovery after host failure

Review the details on host failure and how VCS and the Cluster Server agent for cluster-mode SnapMirror behave in response to the failure.

See "Failure scenarios in global clusters" on page 28.

To test disaster recovery for host failure in global cluster setup

1. Halt the hosts at the primary site.

   The value of the ClusterFailOverPolicy attribute for the faulted global group determines the VCS failover behavior.

   - Auto—VCS brings the faulted global service group online at the secondary site.
   - Manual or Connected—You must bring the global service group online at the secondary site.

     On a node in the secondary site, run the following command:

     ```
     hagrp -online -force global_group -any
     ```

2. Verify that the global service group is online at the secondary site.

   ```
   hagrp -state global_group
   ```

3. Verify that the volumes at the secondary site are write-enabled and the mirror state is SNAPMIRRORED.

Testing disaster recovery after site failure

Review the details on site failure and how VCS and the Cluster Server agent for cluster-mode SnapMirror behave in response to the failure.

See "Failure scenarios in global clusters" on page 28.

To test disaster recovery for site failure in global cluster setup

1. Halt all nodes and the arrays at the primary site.

If you cannot halt the array at the primary site, then disable the replication link between the two arrays.

The value of the ClusterFailOverPolicy attribute for the faulted global group determines the failover behavior of VCS.

- Auto—VCS brings the faulted global group online at the secondary site.
- Manual or Connected—You must bring the global group online at the secondary site.
  On a node in the secondary site, run the following command:

  ```
  hagrp -online -force global_group -any
  ```

2. Verify that the volumes at the secondary site are write-enabled and the mirror state is BROKEN-OFF.
3. Verify that the global service group is online at the secondary site.

   ```
   hagrp -state global_group
   ```

Performing failback after a node failure or an application failure

Review the details on node failure and application failure and how VCS and the agent for cluster-mode SnapMirror behave in response to these failures.

See “Failure scenarios in global clusters” on page 28.

After the nodes at the primary site are restarted, you can perform a failback of the global service group to the primary site. Perform the procedure that applicable to your DR configuration.

To perform failback after a node failure or an application failure in global cluster

1. Switch the global service group from the secondary site to any node in the primary site.

   ```
   hagrp -switch global_group -any -clus cluster_name
   ```

   VCS brings the global service group online at the primary site.
2. Verify that the volumes at the primary site are write-enabled and the mirror state is SNAPMIRRORED.

Performing failback after a site failure

After a site failure at the primary site, the hosts and the storage at the primary site are down. VCS brings the global service group online at the secondary site and the cluster-mode SnapMirror agent write enables the volumes at the secondary site. The mirror state is BROKEN-OFF.

Review the details on site failure and how VCS and the agent for cluster-mode SnapMirror behave in response to the failure.

See "Failure scenarios in global clusters" on page 28.

When the hosts and the storage at the primary site are restarted and the replication link is restored, the mirror state becomes BROKEN-OFF at both the sites. The volumes are write-enabled at both sites. You can now perform a failback of the global service group to the primary site.

To perform failback after a site failure in global cluster

1. Take the global service group offline at the secondary site. On a node at the secondary site, run the following command:

   ```
   hagrp -offline global_group -any
   ```

2. Resync the devices using the snapmirror-resync ONTAP API and pass the appropriate values to the `destination-location` parameter.

   The volumes are write-enabled at the primary site and write-disabled at the secondary site. The mirror state is SNAPMIRRORED.

3. Bring the global service group online at the primary site. On a node in the primary site, run the following command:

   ```
   hagrp -online global_group -any
   ```