Symantec High Availability Solution– DR Configuration with non-shared disks managed using SFW

Windows Server 2008 (x64), Windows Server 2008 R2 (x64)

6.0.1

February 2013

Symantec

Contents

Chapter 1

Configuring application monitoring in a disaster recovery setup

This chapter includes the following topics:

About configuring a disaster recovery setup for application monitoring

A Disaster Recovery (DR) configuration enables you to continue application monitoring at a different geographical location, in event of a calamity at the current location. A DR setup for application monitoring continuity requires you to configure application monitoring at both, the primary and the secondary site. This sets up the VCS clusters at both the sites. The cluster at the primary site provides data and services during normal operation, and the cluster at the secondary site provides data and services if the primary site fails. To provide the application monitoring continuity, VCS continuously monitors and communicates events between the cross-site clusters.

This technote describes how to plan and configure a disaster recovery setup in a VMware environment with non-shared disks using SFW storage. It provides the configuration steps for both,

- Configuring DR using Veritas Volume Replicator (VVR)- Replicating application data across sites over IP
- Configuring DR using hardware replication- Replicating the storage disks across sites

How the solution works

Configuring disaster recovery setup in a VMware environment with non-shared disks using SFW involves configuration of Veritas Volume Replicator (VVR) to replicate the application data or the configuration of hardware replication solution to replicate the storage disks.

In a typical configuration, a VCS cluster is configured at both, the primary and the disaster recovery site and the application is installed and configured on all the VCS cluster systems. The application data is saved on the non-shared virtual disks (VMware Virtual Machine Disk (VMDK) or the Raw Device Mapping (RDM) disk files) and depending on the configuration either the application data is replicated on to the disks at the secondary site or the entire data disks are replicated to the secondary site.

Note: VMware Virtual Machine Disk (VMDK) and the Raw Device Mapping (RDM) disk files are supported in case of DR configuration using VVR. For configuring DR using hardware replication only the Raw Device Mapping (RDM) disk files are supported.

In case of VVR configuration, the replication is monitored by the VCS agent for VVR. Similarly, in case of hardware replication the replication is monitored by the VCS agent for the respective hardware used.

Note: Currently, only the Hitachi True Copy (HTC) and EMC SRDF/Star solution is supported.

As part of the VCS cluster configuration, an application dependency (service) group is configured. Similarly, as part of the VVR or hardware replication configuration a replication dependency group is configured. A dependency is set between the application and replication dependency (service) groups.

The application dependency group is online on the primary site and the replication dependency group is online on both the sites.

If an application or a system fails, the application is failed over to another system within the current primary site. If the entire primary site fails, the application is brought online at the secondary site (which then becomes the new primary) and the replicated data or the replicated disks are used.

Pre-requisites

Review the following pre-requisites before you begin to configure the disaster recovery setup:

Task	Description
Verify the hardware and software prequisites	Review the product installation requirements for your systems. For the detailed information on requirements refer to the following product documentations: ■ *Veritas Storage Foundation™ and High Availability Solutions Installation and Upgrade Guide* ■ *Symantec High Availability Console Installation and Upgrade Guide*
Configure the network and manage storage	Configure the storage disks to save the application data. The application monitoring configuration in a VMware environment with non shared disks requires you to use the RDM or VMDK disk formats. During a failover, these disks can be deported from a system and imported to another system. **Note:** For configuring DR using hardware replication only RDM disk formats are supported. For the detailed information on managing the storage disks refer to *Symantec High Availability Solutions Guide for VMware*
Verify the requirements for configuring VVR	For configuring DR using VVR, ensure that the VVR replication related pre-requisites are performed. For details refer to the high availability and disaster recovery solutions guide for the respective application.

Verify the requirements for configuring hardware replication	For configuring DR using hardware replication, ensure that the requirements for the hardware replication are performed. For details refer to the high availability and disaster recovery solutions guide for the respective application.

Configuring DR- Using VVR

Table 1-1 describes the tasks to set up a typical DR configuration in a VMware environment, that involves VMware non-shared disks managed using SFW.

Table 1-1 Tasks for configuring a DR setup

Task	Description
Install the Symantec High Availability Console	At both the sites, install the Symantec High Availability Console to enable integration with vSphere Client and provides access control for vCenter Server users to perform the following tasks: ■ Install the Symantec High Availability guest components ■ Manage the Symantec High Availability guest components licenses ■ Configure and control application monitoring For details refer to the *Symantec High Availability Console Install and Upgrade Guide*.
Install the Symantec High Availability Guest Components	Use the product installer or the CLI to install SFW HA as part of the Symantec High Availability guest components installation. You must install this on all the systems where you want to configure application monitoring. **Note:** During the installation, you must select the VCS option to configure Global Cluster Option (GCO). GCO enables you to link the clusters located in different geographies and provides wide-area failover. For configuring DR using VVR, you must also select the SFW option to install VVR. For details refer to the *Veritas Storage Foundation and High Availability Solution Install and Upgrade Guide*.
Install application	At both the sites, install on the systems where you want to configure application monitoring. For details refer to the respective application configuration guides.

Table 1-1 Tasks for configuring a DR setup *(continued)*

Task	Description
Configure SSO	At both the sites, configure SSO between the guest systems and the Console Server. SSO configuration involves specifying the system administrator account to set up a permanent authentication for the system user account. It is required to perform all operations on the system. For details refer to the *Symantec High Availability Solutions Guide for VMware*.
Configure application for high availability at both the sites	From the Symantec High Availability tab, configure application monitoring using the **Configure application for high availability** link. For details refer to the respective application configuration guides.
At the disaster recovery site take the storage component (MountV resource) offline.	Use the Veritas Cluster Server Java Console to view the component dependency (resource dependency) for the configured application (service group) and take the storage component (MountV resource) offline. For more details refer to the *Veritas Cluster Server Administrator's Guide*.
At both the sites configure the VCS ClusterService group	Use the Veritas Cluster Server Configuration wizard (VCW) to configure the VCS ClusterService group. Based on the systems you select, VCW identifies that the VCS cluster is already configured. It thus proceeds to configure the ClusterService group (CSG). The ClusterService group contains components (resources) to configure the Wide-area connector (WAC) process, which is used in global clusters. For more details on configuring a ClusterService group, refer to the *Veritas Cluster Server Administrator's Guide*.
At both the sites, create the Replicated Data Sets (RDS)	Use the VEA Console to launch the Setup Replicated Data Set Wizard. Use this wizard to create the Replicated Data Sets (RDS) and start replication between the primary and secondary sites.

Table 1-1 Tasks for configuring a DR setup *(continued)*

Task	Description
At the primary site, create a replication dependency (service) group	Use the Configuration Wizard from the Java Console and select the "VvrRvgVMNSGroup" template to create a replication dependency group (service group). For more details on configuring a ClusterService group, refer to the *Veritas Cluster Server Administrator's Guide*.
Modify the created replication dependency group	Using Java Console, modify the replication dependency group as follows: ■ From the replication dependency group, select and delete the VMNSDg component (resource). ■ From the application dependency group select the VMNSDg and VMwareDisks components. Remove these components from the application dependency group and paste them in the replication dependency group. ■ Set the dependencies between the components in both, the application dependency group and the replication dependency group. For more details refer to the sample dependency diagram. See "Sample dependency- VVR based replication" on page 23. ■ Review the attribute values of all the components in the replication dependency group. Modify the attribute values as required.
Add the RVGPrimary component (agent resource) to the application dependency group, at the primary site	Using Java Console, add the RVGPrimary component to the application dependency group and specify its attribute definitions. For more details refer to the *Veritas Volume Replicator Administrator's Guide*. After you add the component, you must set its dependency order. For more details refer to the sample dependency diagram. See "Sample dependency- VVR based replication" on page 23.
At the secondary site, create a replication service group	Use the Configuration Wizard from the Java Console and select the "VvrRvgVMNSGroup" template to create a replication dependency group (service group).
Modify the replication dependency group that is created	Using Java Console, modify the replication dependency group created on the secondary site. Perform the steps as that performed on the primary site.

Table 1-1 Tasks for configuring a DR setup *(continued)*

Task	Description
Add the RVGPrimary component (agent resource) to the application dependency group, at the secondary site	Using Java Console, add the RVGPrimary component to the application dependency group and specify its attribute definitions. After you add the component, you must set its dependency order. For more details refer to the sample dependency diagram. See "Sample dependency- VVR based replication" on page 23.
Set the dependency between the application the replication groups	Using Java Console, set the dependency between the application the replication group at the respective sites. For more details refer to the sample dependency diagram. See "Sample dependency- VVR based replication" on page 23.
Add the remote cluster at the primary site	Using Java Console, add the secondary site cluster to the primary site. For more details refer to the *Veritas Cluster Server Administrator's Guide*
Configure the Global Cluster Option	Configure the Global Cluster Option for Wide-Area Failover to link the clusters (add the remote cluster to a local cluster) and convert the application service group to a global service group. For more details on configuring the Global Cluster Option for Wide-Area Failover, refer to the *Veritas Cluster Server Administrator's Guide.*
Verify application failover in both, local and disaster recovery clusters	Use Java Console to verify the application failover within the local and disaster recovery clusters. This completes the disaster recovery cluster configuration. For more details refer to *Veritas Cluster Server Administrator's Guide.*

Configuring DR- Using hardware replication

Table 1-2 describes the tasks to set up a typical DR configuration in a VMware environment, that involves VMware non-shared disks managed using SFW.

Table 1-2 Tasks for configuring a DR setup

Task	Description
At both the sites, install the Symantec High Availability Console	Install the Symantec High Availability Console to enable integration with vSphere Client and provides access control for vCenter Server users to perform the following tasks: ■ Install the Symantec High Availability guest components ■ Manage the Symantec High Availability guest components licenses ■ Configure and control application monitoring For details refer to the *Symantec High Availability Console Install and Upgrade Guide*.
At both the sites, install the Symantec High Availability Guest Components	Use the product installer or the CLI to install SFW HA as part of the Symantec High Availability guest components installation. You must install this on all the systems where you want to configure application monitoring. **Note:** During the installation, you must select the VCS option to configure Global Cluster Option (GCO). GCO enables you to link the clusters located in different geographies and provides wide-area failover. For details refer to the *Veritas Storage Foundation and High Availability Solution Install and Upgrade Guide*.
Install application at the primary site	Install the on the systems where you want to configure application monitoring. For details refer to the respective application configuration guides.
Configure SSO	At both the sites, configure SSO between the guest systems and the Console Server. SSO configuration involves specifying the system administrator account to set up a permanent authentication for the system user account. It is required to perform all operations on the system. For details refer to the *Symantec High Availability Solutions Guide for VMware*.

Table 1-2 Tasks for configuring a DR setup *(continued)*

Task	Description
At the primary site map the hardware replication LUNs	Connect the replication LUNs and the Command Device Disk (incase of HTC hardware replication)/Gatekeeper Device Disk (in case of SRDF hardware replication) to the ESX hosts at the primary site. Also, expose these LUNs to the systems on which you plan to configure application monitoring. You must expose these LUNs to the virtual machines in the "Physical" compatibility mode.
At the primary site configure application for high availability	From the Symantec High Availability tab, configure application monitoring using the **Configure application for high availability** link. For details refer to the respective application configuration guides.
Modify the VMwareDisks resource attribute	From the application dependency group created at the primary site, modify the "DisksPaths" attribute of the VMwareDisks resource. Specify the "Value" as the Command Device Disk path (in case of HTC based replication)/Gatekeeper Device Disk path (in case of SRDF based replication) and the "Key" as the SCSI-Port.
Reverse the replication from the secondary site to the primary site	Execute the action on the secondary site to establish reverse replication (secondary to primary). For more details refer to the respective hardware product documentation.

Table 1-2 Tasks for configuring a DR setup *(continued)*

Task	Description
At the secondary site install the application and create the application dependency group	Perform the following tasks to install the application and create the application dependency group at the secondary site: ■ Install on the systems where you want to configure application monitoring. For details refer to the respective application configuration guides. ■ Map the hardware replication LUNs Connect the replication LUNs and the Command Device Disk (incase of HTC hardware replication)/Gatekeeper Device Disk (in case of SRDF hardware replication) to the ESX hosts at the secondary site. Also, expose these LUNs to the systems on which you plan to configure application monitoring. You must expose these LUNs to the virtual machines in the "Physical" compatibility mode. ■ Modify the VMwareDisks resource attribute From the application dependency group created at the secondary site, modify the "DisksPaths" attribute of the VMwareDisks resource. Specify the "Value" as the Command Device Disk path (in case of HTC based replication)/Gatekeeper Device Disk path (in case of SRDF based replication) and the "Key" as the SCSI-Port.
Reset the replication direction	Execute the action on the primary site to establish replication from primary to secondary. For more details refer to the respective hardware product documentation.
At both the sites modify the application dependency group	At both the sites modify the application dependency group to include the hardware replication agent resource. Using Java Console create a component (resource) for the hardware replication (HTC or SRDF) and set its dependency between the VMNSDG and the VMwareDisks components. See "Sample dependency- Hardware replication setup" on page 26.

Table 1-2 Tasks for configuring a DR setup *(continued)*

Task	Description
At both the sites configure a VCS ClusterService group	Use the Veritas Cluster Server Configuration wizard (VCW) to configure the VCS ClusterService group. Based on the systems you select, VCW identifies that the VCS cluster is already configured. It thus proceeds to configure the ClusterService group (CSG). The ClusterService group contains components (resources) to configure the Wide-area connector (WAC) process, which is used in global clusters. For more details on configuring a ClusterService group, refer to the *Veritas Cluster Server Administrator's Guide*.
Add the remote cluster at the primary site	Using Java Console, add the secondary site cluster to the primary site. For more details refer to the *Veritas Cluster Server Administrator's Guide*.
Configure the Global Cluster Option	Configure the Global Cluster Option for Wide-Area Failover to link the clusters (add the remote cluster to a local cluster) and convert the application service group to a global service group. For more details on configuring the Global Cluster Option for Wide-Area Failover, refer to the *Veritas Cluster Server Administrator's Guide*.
Verify application failover in both, local and disaster recovery clusters	Use Java Console to verify the application failover within the local and disaster recovery clusters. This completes the disaster recovery cluster configuration. For details refer to *Veritas Cluster Server Administrator's Guide*.

Appendix A

Sample configuration- DR setup using VVR

This appendix includes the following topics:

Sample configuration

The following sample configuration depicts a VCS cluster configuration with a single system at both the sites. The application dependency group is configured to monitor the application state in case of a disaster at the primary site.

```
include "types.cf"

cluster VXDRCLS1 (
 UserNames = { "username@domain" = "admin" }
 ClusterAddress = "VirtualIPAddress"
 Administrators = { "username@domain" }
 Operators = { "username@domain" }
 SecureClus = 1
 )

remotecluster VXDRCLS2 (
 ClusterAddress = "VirtualIPAddress"
 )

heartbeat Icmp (
 ClusterList = { VXDRCLS2 }
 Arguments @VXDRCLS2 = { "VirtualIPAddress" }
```

```
 )

system VXDRHOST1 (
 )

system VXDRHOST2 (
 )

group ClusterService (
 SystemList = { VXDRHOST1 = 0, VXDRHOST2 = 1 }
 AutoStartList = { VXDRHOST1, VXDRHOST2 }
 Administrators = { "username@domain" }
 Operators = { "username@domain" }
 )

 IP csg_ip (
  Address = "IPAdress"
  SubNetMask = "SubNetMask"
  MACAddress @VXDRHOST1 = "00:5B:HB:SX:9H:99"
  MACAddress @VXDRHOST2 = "00:G0:X6:9N:03:9C"
  )

 NIC csg_nic (
  MACAddress @VXDRHOST1 = "00:5d:H6:8M:03:99"
  MACAddress @VXDRHOST2 = "00:5f:5N:8D:03:9C"
  )

 Process wac (
  StartProgram @VXDRHOST1 = "\"C:\\Program Files\\Veritas\
  \Cluster Server\\bin\\wac.exe\""
  StartProgram @VXDRHOST2 = "\"C:\\Program Files\\Veritas\
  \Cluster Server\\bin\\wac.exe\""
  StopProgram @VXDRHOST1 = "\"C:\\Program Files\\Veritas\
  \Cluster Server\\bin\\wacstop.exe\""
  StopProgram @VXDRHOST2 = "\"C:\\Program Files\\Veritas\
  \Cluster Server\\bin\\wacstop.exe\""
  MonitorProgram @VXDRHOST1 = "\"C:\\Program Files\\Veritas\
  \Cluster Server\\bin\\wacmonitor.exe\""
  MonitorProgram @VXDRHOST2 = "\"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 FS_SG (
 SystemList = { VXDRHOST1 = 0, VXDRHOST2 = 1 }
 ClusterList = { VXDRCLS2 = 1, VXDRCLS1 = 0 }
 Administrators = { "username@domain" }
 Operators = { "username@domain" }
 )

 FileShare FS-SG-FileShareRes-1 (
  PathName = "\\"
  ShareName = VOL1
  LanmanResName = FS_SG-LanmanRes_1
  MountResName = FS_SG-MountVRes_1
  )

 FileShare FS-SG-FileShareRes-2 (
  PathName = "\\"
  ShareName = VOL2
  LanmanResName = FS_SG-LanmanRes_1
  MountResName = FS_SG-MountVRes_2
  )

 IP FS_SG-IPRes_1 (
  Address = "IPAddress"
  SubNetMask = "Subnetmask"
  MACAddress @VXDRHOST1 = 00-5H-G6-64-03-99
  MACAddress @VXDRHOST2 = 00-59-L9-F4-03-9C
```

```
 )

Lanman FS_SG-LanmanRes_1 (
 VirtualName = FSVS11070
 IPResName = FS_SG-IPRes_1
 )

MountV FS_SG-MountVRes_1 (
 MountPath = "I:"
 VolumeName = VOL1
 VMDGResName = FS_SG-VMNSDgRes_1
 )

MountV FS_SG-MountVRes_2 (
 MountPath = "J:"
 VolumeName = VOL2
 VMDGResName = FS_SG-VMNSDgRes_1
 )

NIC FS_SG-NICRes_1 (
 MACAddress @VXDRHOST1 = 00-50-56-84-03-99
 MACAddress @VXDRHOST2 = 00-50-56-84-03-9C
 )

RVGPrimary FS_SG-RVGPrimaryRes_1 (
 RvgResourceName = VVR_SG-VvrRvg_1
 )

requires group VVR_SG online local hard
FS-SG-FileShareRes-1 requires FS_SG-MountVRes_1
FS-SG-FileShareRes-1 requires FS_SG-LanmanRes_1
FS-SG-FileShareRes-2 requires FS_SG-MountVRes_2
FS-SG-FileShareRes-2 requires FS_SG-LanmanRes_1
FS_SG-IPRes_1 requires FS_SG-NICRes_1
FS_SG-LanmanRes_1 requires FS_SG-IPRes_1
FS_SG-MountVRes_1 requires FS_SG-RVGPrimaryRes_1
FS_SG-MountVRes_2 requires FS_SG-RVGPrimaryRes_1


// resource dependency tree
//
// group FS_SG
// {
```

```
// FileShare FS-SG-FileShareRes-1
//     {
//     MountV FS_SG-MountVRes_1
//         {
//         RVGPrimary FS_SG-RVGPrimaryRes_1
//         }
//     Lanman FS_SG-LanmanRes_1
//         {
//         IP FS_SG-IPRes_1
//             {
//             NIC FS_SG-NICRes_1
//             }
//         }
//     }
// FileShare FS-SG-FileShareRes-2
//     {
//     MountV FS_SG-MountVRes_2
//         {
//         RVGPrimary FS_SG-RVGPrimaryRes_1
//         }
//     Lanman FS_SG-LanmanRes_1
//         {
//         IP FS_SG-IPRes_1
//             {
//             NIC FS_SG-NICRes_1
//             }
//         }
//     }
// }


group VVR_SG (
 SystemList = { VXDRHOST1 = 0, VXDRHOST2 = 1 }
 Administrators = { "username@domain" }
 Operators = { "username@domain" }
 )

 IP VVR_SG-IPRes_1 (
  Address = "IPAddress"
  SubNetMask = "Subnetmask"
  MACAddress @VXDRHOST1 = 00-50-H6-84-D3-99
  MACAddress @VXDRHOST2 = 00-5F-56-84-N3-9C
  )
```

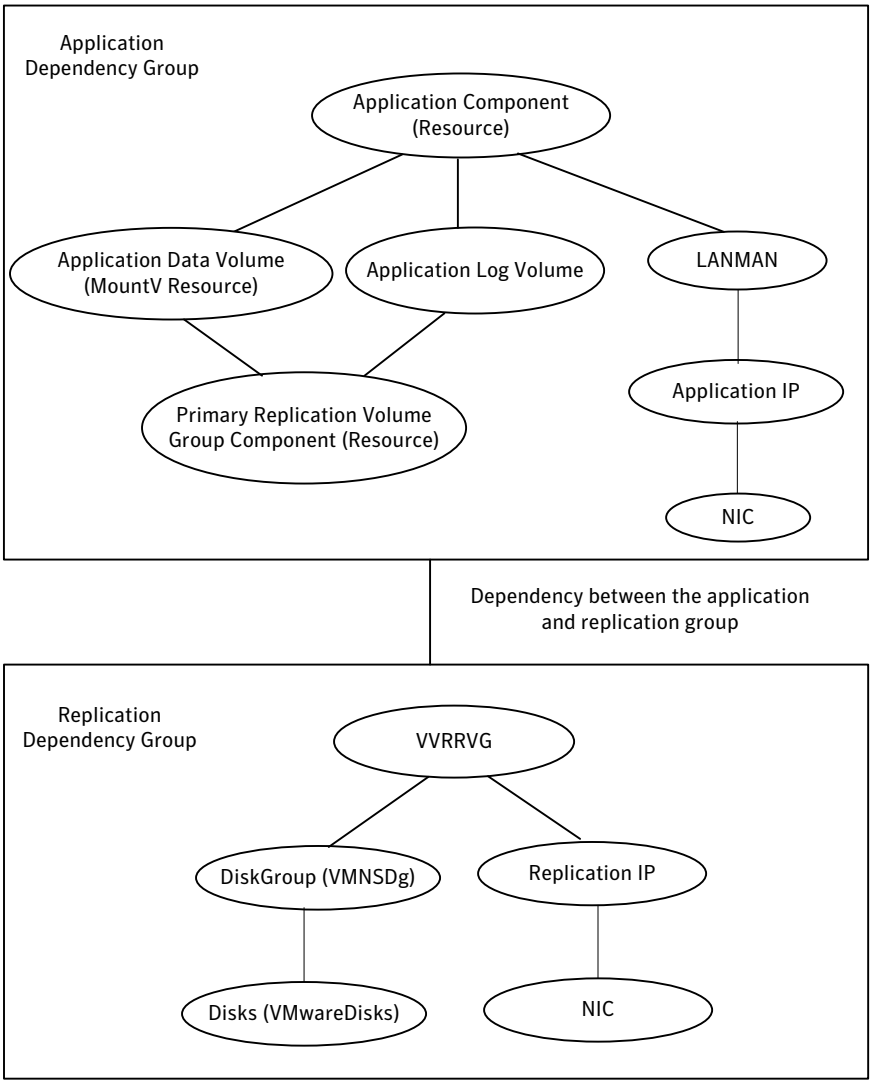
```
NIC VVR_SG-NICRes_1 (
 MACAddress @VXDRHOST1 = 00-H0-56-8Y-03-99
 MACAddress @VXDRHOST2 = 00-50-J6-84-M3-9C
 )

VMNSDg FS_SG-VMNSDgRes_1 (
 DiskGroupName = FS_DG
 DGGuid = c9528a9a-5c0a-4f9a-97cd-69f21dca4fb4
 )

VMwareDisks FS_SG-VMwareDisksRes_1 (
 ESXDetails = { "10.209.111.241" = "root=drfPspSrhJejFjg" }
 DiskPaths = {
   "6000C295-d580-0dd8-0c4c-9fffe4a9e849:[Host241-Storage2]
    VxDRHost1/VxDRHost1_1.vmdk" = "0:1",
   "6000C297-d2cd-ab58-206e-488839a69ed3:[Host241-Storage2]
    VxDRHost1/VxDRHost1_2.vmdk" = "0:2" }
 )

VvrRvg VVR_SG-VvrRvg_1 (
 RVG = FS_RVG
 VMDgResName = FS_SG-VMNSDgRes_1
 IPResName = VVR_SG-IPRes_1
 )

VVR_SG-IPRes_1 requires VVR_SG-NICRes_1
FS_SG-VMNSDgRes_1 requires FS_SG-VMwareDisksRes_1
VVR_SG-VvrRvg_1 requires FS_SG-VMNSDgRes_1
VVR_SG-VvrRvg_1 requires VVR_SG-IPRes_1


// resource dependency tree
//
// group VVR_SG
// {
// VvrRvg VVR_SG-VvrRvg_1
//     {
//     VMNSDg FS_SG-VMNSDgRes_1
//         {
//         VMwareDisks FS_SG-VMwareDisksRes_1
//         }
//     IP VVR_SG-IPRes_1
```

```
//          {
//          NIC VVR_SG-NICRes_1
//          }
//      }
// }
```

Sample dependency- VVR based replication

Figure A-1 represents the sample dependency between the application group dependency and the replication group dependency

Figure A-1 Sample dependency between the application and replication group dependency



Appendix B

Sample configuration- DR setup using hardware replication

This appendix includes the following topics:

Sample dependency- Hardware replication setup

Figure B-1 represents the sample dependency between the application group dependency in a hardware based replication setup