APPENDIX B

High Availability and Disaster Recovery Certification Test Plan

The HA/DR certification test plan validates that the Security Manager application is highly available and can survive various hardware and software failures. The test plan also covers maintenance activities, such as manually switching the application between servers.

Note Security Manager client sessions require active users to log in again after an application failover. This behavior is equivalent to stopping and starting Security Manager services running on the server.

The following test case categories are contained in this appendix:

Manual Switches

This section covers two different types of manual switches. In a single cluster with two servers, you can switch between the two servers in the cluster (intracluster switch); in a dual cluster configuration with a single server in each cluster, you can switch between clusters (intercluster switch).

This section contains the following topics:

IntraCluster Switch

Test Case Title: Manual application switch within a cluster.

Description: The application is manually switched to a different server in the same cluster using VCS.

Test Setup: A dual node cluster (Figure 1-1 on page 12) in a single cluster configuration.

Step 1 Ensure that the APP service group is running on the primary server. Using the VCS Cluster Explorer, select the **APP** service group. From the shortcut menu, select **Switch To**, and choose the secondary server. Alternatively, issue the following command:

```
C:\> hagrp -switch APP -to secondary_server_name
```

Step 2 From the Resource view of the APP service group, observe that the resources in the service group go offline on the primary server and then come online on the secondary server. Or issue the following command to observe the status of the APP service group.

```
C:\> hagrp -state APP
```

Step 3 From a client machine, launch the Security Manager client, using the virtual hostname or IP address in the Server Name field of the login dialog box. Verify that you can log in to the application successfully.

InterCluster Switch

Test Case Title: Manual application switch between clusters.

Description: The application is manually switched to a server in a different cluster using VCS.

Test Setup: A dual cluster configuration as shown in Figure 1-2 on page 14 with a single server in each cluster.

Step 1 Using the VCS Cluster Explorer, select the **APP** service group. From the shortcut menu, select **Switch To**, then **Remote Switch(...)**, to open the Switch global dialog box. In the dialog box, specify the remote cluster and, if desired, a specific server in the remote cluster. Alternatively, issue the following command:

```
C:\> hagrp -switch APP -any -clus secondary_cluster_name
```

Step 2 From the Resource view of the APP service group, observe that the resources in the service group go offline in the primary cluster. Select the root cluster node in the tree and use the Remote Cluster Status view to see that the APP service group goes online on the remote cluster. Or issue the following command to observe the status of the APP service group.

```
C:\> hagrp -state APP
#Group       Attribute            System                        Value
APP          State                csm_primary:<Primary Server>  |OFFLINE|
APP          State                localclus:<Secondary Server>  |ONLINE|
```

Step 3 From a client machine, launch the Security Manager client by entering the appropriate hostname or application IP address used in the secondary cluster in the Server Name field of the Login dialog box. Verify that you can successfully log in to the application.

Step 4 Log out of the Security Manager client, and then switch the APP service group to the primary cluster using either the VCS Cluster Explorer or the following command:

```
C:\> hagrp -switch APP -any -clus primary_cluster_name
```

Ethernet/Network Failures

HA/DR configurations have two types of server Ethernet connections. The first are the Ethernet connections used for network communications (public interfaces); the second are Ethernet interfaces dedicated for intracluster communications (private interfaces). This section covers failure test cases for each type of Ethernet interface.

Network Communication Failures

This section describes the tests used to verify that VCS can detect failure of the network Ethernet ports used for network communications. This section contains the following topics:

Network Ethernet Failure on Secondary Server, Single Cluster

Test Case Title: A failure occurs in the network Ethernet connection on the secondary server in a single cluster configuration.

Description: This test case verifies that VCS can detect a failure on the network Ethernet port on the secondary server and then recover after the failure is repaired.

Test Setup: A dual node cluster (Figure 1-1 on page 12) in a single cluster configuration with a single network connection per server.

Step 1 Verify that the application is running on the primary server.

Step 2 Log in to the application from a client machine.

Step 3 Remove the Ethernet cable from the network port on the secondary server to isolate the server from communicating with the switch/router network. Wait for at least 60 seconds for VCS to detect the network port failure. Verify that VCS detects a failure of the NIC resource on the secondary server by running the following command:

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A <PrimaryServer>       RUNNING              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APP             <SecondaryServer>    Y          N               OFFLINE|FAULTED

-- RESOURCES FAILED
-- Group           Type                 Resource             System
C  APP             NIC                  NIC                  <SecondaryServer>
```

Step 4 Restore the Ethernet cable to the network port on the secondary server. Verify that VCS detects that the failure was cleared by running the following command:

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APP             <SecondaryServer>    Y          N               OFFLINE
```

Network Ethernet Failure on Primary Server, Single Cluster

Test Case Title: A failure occurs in the network Ethernet connection on the primary server in a single cluster configuration.

Description: This test case verifies that VCS can detect a failure on the network Ethernet port of the primary server and automatically switch the application to the secondary server. After the problem is fixed, you can switch the application back to the primary server manually.

Test Setup: A dual node cluster (Figure 2-2 on page 23) with a single network connection per server.

Step 1 Verify that the application is running on the primary server.

Step 2 Remove the Ethernet cable from the network port on the primary server to isolate the server from communicating with the switch/router network. Verify that VCS detects a failure of the NIC resource and automatically switches the APP service group to the secondary server:

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               OFFLINE|FAULTED
B  APP             <SecondaryServer>    Y          N               ONLINE

-- RESOURCES FAILED
-- Group           Type                 Resource             System
C  APP             NIC                  NIC                  <PrimaryServer>
C  APP             IP                   APP_IP               <PrimaryServer>
```

Step 3 Verify that you can log in to the application while it is running on the secondary server.

Step 4 Replace the Ethernet cable on the network port of the primary server and manually clear the faulted IP resource on the primary server:

```
C:\> hares -clear APP_IP -sys primary_server_name
```

Step 5 Manually switch the APP service group back to the primary server.

```
C:\> hagrp -switch APP -to primary_server_name
```

Network Ethernet Failure on Secondary Server, Dual Cluster

Test Case Title: A failure occurs in the network Ethernet connection on the secondary server in a dual cluster configuration.

Description: This test case verifies that VCS can detect a failure on the network Ethernet port and then recover after the failure is repaired.

Test Setup: A dual cluster configuration (Figure 1-2 on page 14) with a single node in each cluster and a single Ethernet network connection for each server.

Step 1 Verify that the APP service group is running on the primary cluster/server.

Step 2 Log in to the Security Manager from a client machine.

Step 3 Remove the Ethernet cable from the network port on the server in the secondary cluster. This isolates the server from communicating with the switch/router network and interrupts replication. From the primary server, verify that replication was interrupted (disconnected) by running the following command:

```
C:\> vxprint -Pl
Diskgroup = datadg

Rlink      : rlk_172_6037
info       : timeout=500 packet_size=1400
             latency_high_mark=10000 latency_low_mark=9950
             bandwidth_limit=none
state      : state=ACTIVE
             synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
             remote_host=172.25.84.34
             remote_dg=datadg
             remote_rlink=rlk_172_32481
             local_host=172.25.84.33
protocol   : UDP/IP
flags      : write attached consistent disconnected
```

Step 4 Run the following command from the primary server to verify that communication with the secondary cluster was lost:

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APPrep          <PrimaryServer>      Y          N               ONLINE
B  ClusterService  <PrimaryServer>      Y          N               ONLINE

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_secondary        ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_secondary   LOST_CONN

-- REMOTE SYSTEM STATE
-- cluster:system                    State                Frozen
N  csm_secondary:<SecondaryServer>   RUNNING              0
```

```
-- REMOTE GROUP STATE
-- Group           cluster:system       Probed     AutoDisabled    State
O  APP csm_secondary:<SecondaryServer>  Y          N               OFFLINE
```

Step 5 Reattach the network Ethernet cable to the secondary server and verify that replication resumed.

```
C:\> vxprint -Pl

Diskgroup = datadg

Rlink      : rlk_172_6037
info       : timeout=29 packet_size=1400
             latency_high_mark=10000 latency_low_mark=9950
             bandwidth_limit=none
state      : state=ACTIVE
             synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
             remote_host=172.25.84.34
             remote_dg=datadg
             remote_rlink=rlk_172_32481
             local_host=172.25.84.33
protocol   : UDP/IP
flags      : write attached consistent connected
```

Step 6 Verify that communications to the secondary cluster has been restored.

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0
-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APPrep          <PrimaryServer>      Y          N               ONLINE
B  ClusterService  <PrimaryServer>      Y          N               ONLINE

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_secondary        ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_secondary   RUNNING

-- REMOTE SYSTEM STATE
-- cluster:system                   State                Frozen
N  csm_secondary:<SecondaryServer>  RUNNING              0

-- REMOTE GROUP STATE
-- Group           cluster:system       Probed     AutoDisabled    State
O  APP csm_secondary:<SecondaryServer>  Y          N               OFFLINE
```

Step 7 If replication has not recovered you may need to manually clear the IP resource if it has faulted and then start the APPrep service group on the secondary as follows:

```
C:\> hares -clear APP_IP
C:\> hagrp -online APPrep -sys secondary_server_name
```

Network Ethernet Failure on Primary Server, Dual Cluster

Test Case Title: A failure occurs in the network Ethernet connection on the primary server.

Description: This test case verifies that VCS can detect a failure on the primary server network Ethernet port and can recover by starting the application on the secondary server. After the Ethernet connection is restored, you can manually fail over back to the original primary server, retaining any data changes that were made while running on the secondary.

Test Setup: A dual cluster configuration (Figure 1-2 on page 14) with a single node in each cluster.

Step 1 Verify that the **APP** service group is running on the primary cluster.

Step 2 Remove the network Ethernet cable from the port on the server in the primary cluster to isolate the server from communicating with the switch/router network. VCS should detect this as a failure of the IP and NIC resources. Verify that VCS detected the failure and brought down the APP service group.

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A <PrimaryServer>       RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               OFFLINE
B  APPrep          <PrimaryServer>      Y          N               OFFLINE|FAULTED
B  ClusterService  <PrimaryServer>      Y          N               ONLINE

-- RESOURCES FAILED
-- Group           Type                 Resource             System
C  APPrep          IP                   APP_IP               <PrimaryServer>
C  APPrep          NIC                  NIC                  <PrimaryServer>

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_secondary        DOWN

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_secondary   FAULTED

-- REMOTE SYSTEM STATE
-- cluster:system       State                Frozen
N  csm_secondary:<SecondaryServer> FAULTED              0

-- REMOTE GROUP STATE
-- Group          cluster:system                  Probed     AutoDisabled    State
O  APP            csm_secondary:<SecondaryServer> Y          N               OFFLINE
```

Step 3 Start the APP service group on the secondary cluster using the following command on the secondary server:

```
C:\> hagrp -online -force APP -sys secondary_server_name
```

Step 4 From your client machine, log in to Security Manager to verify that it is operational. Change some data so that you can verify that changes are retained when you switch back to the primary server.

Step 5 Reconnect the network Ethernet cable to the primary cluster server.

Step 6 Clear any faults on the IP resource and turn on the **APPrep** service from the primary server:

```
C:\> hares -clear APP_IP
C:\> hagrp -online APPrep -sys primary_server_name
```

Step 7 Convert the original primary RVG to secondary and synchronize the data volumes in the original primary RVG with the data volumes on the new primary RVG using the fast failback feature. Using the Cluster Explorer for the secondary cluster, right-click the RVGPrimary resource (**APP_RVGPrimary**), select **actions**, then select **fbsync** from the Actions dialog box, and then click **OK**. Alternatively, you can issue the following command:

```
C:\> hares -action APP_RVGPrimary fbsync 0 -sys secondary_server_name
```

Step 8 Using the VCS Cluster Explorer on the secondary cluster, select the **APP** service group. From the short-cut menu, select **Switch To**, then **Remote Switch(...)**, to open the Switch global dialog box. In the dialog box, specify the primary cluster and the primary server. Alternatively, issue the following command:

```
C:\> hagrp -switch APP -any -clus primarycluster
```

Step 9 Log in to the application to verify that the changes you made on the secondary server were retained.

Cluster Communication Failure

Test Case Title: Failures occur in the Ethernet used for cluster communication.

Description: The dedicated Ethernet connections used between servers in the cluster for intracluster communication fail. The test verifies that the cluster communications continue to function when up to two of the three redundant communication paths are lost.

Test Setup: A dual-node cluster (Figure 1-1 on page 12) in a single cluster configuration, with two dedicated cluster communication Ethernet connections and a low-priority cluster communication connection configured on the network Ethernet connection.

Note In addition to the commands given in this test case, you can monitor the status of the cluster communications from the Cluster Explorer by selecting the root node in the tree and selecting the System Connectivity tab.

Step 1 Issue the following command to verify that all systems are communicating through GAB.

Note Group Membership Services/Atomic Broadcast (GAB) is a VCS protocol responsible for cluster membership and cluster communications.

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen   e8cc02 membership 01
Port h gen   e8cc01 membership 01
```

Step 2 Remove the Ethernet cable from the first dedicated Ethernet port used for cluster communication on the primary server.

Step 3 Issue the following command to view the detailed status of the links used for cluster communication and verify that the first dedicated cluster communication port is down.

Note The asterisk (*) in the output indicates the server on which the command is run. The server where the command is run always shows its links up, even if one or more of those ports are the ones that are physically disconnected.

```
# lltstat -nvv
LLT node information:
    Node           State    Link  Status  Address
   * 0 <PrimaryServer>   OPEN
                                 Adapter0   UP    00:14:5E:28:52:9C
                                 Adapter1   UP    00:14:5E:28:52:9D
                                 Adapter2   UP    00:0E:0C:9C:20:FE
     1 <SecondaryServer> OPEN
                                 Adapter0   DOWN
                                 Adapter1   UP    00:14:5E:28:27:17
                                 Adapter2   UP    00:0E:0C:9C:21:C2
...
```

Step 4 If you configured a low-priority heartbeat link on the network interface, remove the Ethernet cable from the second dedicated Ethernet port used for cluster communication on the primary server.

Step 5 Issue the following command to verify that all systems are communicating through GAB. Also confirm that both servers in the cluster are now in a Jeopardy state, since each server has only one heartbeat working.

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen   e8cc02 membership 01
Port a gen   e8cc02   jeopardy ;1
Port h gen   e8cc01 membership 01
Port h gen   e8cc01   jeopardy ;1
```

Step 6 Issue the following command to view the detailed status of the links used for cluster communication and verify that the second dedicated Ethernet port for cluster communications on the primary server is down.

```
# lltstat -nvv
LLT node information:
    Node           State    Link  Status  Address
   * 0 <PrimaryServer>   OPEN
                                 Adapter0   UP    00:14:5E:28:52:9C
                                 Adapter1   UP    00:14:5E:28:52:9D
                                 Adapter2   UP    00:0E:0C:9C:20:FE
     1 <SecondaryServer> OPEN
                                 Adapter0   DOWN
                                 Adapter1   UP    00:14:5E:28:27:17
                                 Adapter2   DOWN
```

Step 7 Replace the Ethernet cable on the second dedicated Ethernet port for cluster communications on the primary server.

Step 8 Verify that the Jeopardy condition was removed by issuing the following command:

```
# gabconfig -a
GAB Port Memberships
===============================================================
Port a gen   e8cc02 membership 01
Port h gen   e8cc01 membership 01
```

Step 9 Replace the Ethernet cable on the first dedicated Ethernet port for cluster communications on the primary server.

Server Failures

This section covers causing server failures by removing the power from the server to cause a failure. Four cases are covered:

- Standby Server Failure, Single Cluster, page B-10
- Primary Server Failure, Single Cluster, page B-11
- Standby Server Failure, Dual Cluster, page B-12
- Primary Server Failure, Dual Cluster, page B-14

Standby Server Failure, Single Cluster

Test Case Title: The standby server in a single cluster configuration fails.

Description: This test case verifies that the application running in the primary server is unaffected and that after the standby server is repaired, the application can successfully rejoin the cluster configuration.

Test Setup: A dual node cluster (Figure 2-2 on page 23) with two dedicated cluster communication Ethernet connections and a low-priority cluster communication connection on the network Ethernet connection.

Step 1 Verify that the application is running on the primary server in the cluster.

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APP             <SecondaryServer>    Y          N               OFFLINE
```

Step 2 Remove the power for the secondary server and verify that VCS detected the failure and that the application continues to operate on the primary server.

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0
A  <SecondaryServer>    FAULTED              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
```

Step 3 Reapply power and boot the secondary server. After the server recovers, verify that it rejoined the cluster in a healthy state by running the following command. The output should be identical to the output in Step 1.

```
C:\> hastatus -sum
```

Primary Server Failure, Single Cluster

Test Case Title: The primary server in a single cluster fails.

Description: This test case verifies that if a primary server fails, the application starts running on the secondary server and that after the primary server is restored, the application can be reestablished on the primary server.

Test Setup: A dual node cluster (Figure 1-1 on page 12).

Step 1 Verify that the APP service group is running on the primary server in the cluster by examining the output of the following command:

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APP             <SecondaryServer>    Y          N               OFFLINE
```

Step 2 Remove the power from the primary server and verify that VCS detected the failure and that the APP service group automatically moved to the secondary server.

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      FAULTED              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <SecondaryServer>    Y          N               ONLINE
```

Step 3 Verify that you can successfully log in to Security Manager from a client machine.

Step 4 Restore the power to the primary server and verify that the server can rejoin the cluster in a healthy condition. Run the following command. The output should be identical to the output in Step 1.

```
C:\> hastatus -sum
```

Step 5 Manually switch the APP service group back to the primary server.

```
C:\> hagrp -switch APP -to primary_server_name
```

Standby Server Failure, Dual Cluster

Test Case Title: The standby server in a dual cluster configuration fails.

Description: This test case verifies that an application running in the primary cluster is unaffected by a standby server failure and that after the standby server is repaired, the application can successfully rejoin the dual cluster configuration.

Test Setup: A dual cluster configuration, with replication (Figure 1-2 on page 14), with a single node in each cluster.

Step 1 Verify that the APP and ClusterService service groups are running in the primary cluster by running the following command on the primary server:

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APPrep          <PrimaryServer>      Y          N               ONLINE
B  ClusterService  <PrimaryServer>      Y          N               ONLINE

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_secondary        ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_secondary   RUNNING

-- REMOTE SYSTEM STATE
-- cluster:system                  State                Frozen
N  csm_secondary:<SecondaryServer> RUNNING              0

-- REMOTE GROUP STATE
-- Group          cluster:system                  Probed     AutoDisabled    State
O  APP            csm_secondary:<SecondaryServer> Y          N               OFFLINE
```

Step 2 Remove the power from the secondary server and verify that the primary cluster detects a loss of communication to the secondary cluster:

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APPrep          <PrimaryServer>      Y          N               ONLINE
B  ClusterService  <PrimaryServer>      Y          N               ONLINE

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_secondary        ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_secondary   LOST_CONN

-- REMOTE SYSTEM STATE
-- cluster:system                  State                Frozen
N  csm_secondary:<SecondaryServer> RUNNING              0

-- REMOTE GROUP STATE
-- Group          cluster:system                  Probed     AutoDisabled    State
O  APP             csm_secondary:<SecondaryServer> Y          N               OFFLINE
```

Step 3 Restore the power to the secondary server. After the server restarts, verify that the primary cluster reestablished communications with the secondary cluster by running the following command. The output should be identical to the output in Step 1.

```
C:\> hastatus -sum
```

Step 4 Verify that the replication is operational and consistent by running the following command:

```
C:\> vxprint -Pl
Diskgroup = BasicGroup

Diskgroup = datadg

Rlink      : rlk_172_6037
info       : timeout=16 packet_size=1400
             latency_high_mark=10000 latency_low_mark=9950
             bandwidth_limit=none
state      : state=ACTIVE
             synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
             remote_host=172.25.84.34
             remote_dg=datadg
             remote_rlink=rlk_172_32481
             local_host=172.25.84.33
protocol   : UDP/IP
flags      : write attached consistent connected
```

Primary Server Failure, Dual Cluster

Test Case Title: The primary server in a dual cluster configuration fails.

Description: This test case verifies that if a primary server fails, the application starts running on the secondary server and that after the primary server is restored, the application can be reestablished on the primary server.

Test Setup: A dual cluster configuration, with replication (Figure 1-2 on page 14), with a single node in each cluster.

Step 1 Verify that the APP and ClusterService service groups are running in the primary cluster by running the following command from the secondary server:

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <SecondaryServer>    Y          N               OFFLINE
B  APPrep          <SecondaryServer>    Y          N               ONLINE
B  ClusterService  <SecondaryServer>    Y          N               ONLINE

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_primary          ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_primary     RUNNING

-- REMOTE SYSTEM STATE
-- cluster:system       State                Frozen
N  csm_primary:<PrimaryServer> RUNNING              0

-- REMOTE GROUP STATE
-- Group           cluster:system              Probed     AutoDisabled    State
O  APP             csm_primary:<PrimaryServer> Y          N               ONLINE
```

Step 2 Remove the power from the primary server to cause a server failure. Verify that the secondary cluster reported a loss of connectivity to the primary cluster.

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <SecondaryServer>    Y          N               OFFLINE
B  APPrep          <SecondaryServer>    Y          N               ONLINE
B  ClusterService  <SecondaryServer>    Y          N               ONLINE

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_primary          ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_primary     LOST_CONN
```

```
-- REMOTE SYSTEM STATE
-- cluster:system              State                Frozen
N  csm_primary:<PrimaryServer> RUNNING              0

-- REMOTE GROUP STATE
-- Group           cluster:system              Probed     AutoDisabled    State
O  APP             csm_primary:<PrimaryServer> Y          N               ONLINE
```

Step 3 Confirm that the state of the replication is disconnected. You can see this state from the **flags** parameter in the output of the following command:

```
C:\> vxprint -Pl
Diskgroup = BasicGroup

Diskgroup = datadg

Rlink      : rlk_172_32481
info       : timeout=500 packet_size=1400
             latency_high_mark=10000 latency_low_mark=9950
             bandwidth_limit=none
state      : state=ACTIVE
             synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
             remote_host=172.25.84.33
             remote_dg=datadg
             remote_rlink=rlk_172_6037
             local_host=172.25.84.34
protocol   : UDP/IP
flags      : write attached consistent disconnected
```

Step 4 Start the application on the secondary server by using the following command.

```
C:\> hagrp -online -force APP -sys secondary_server_name
```

Step 5 Log in to the application and change some data so that you can verify later that changes made while the application operating on the secondary server can be retained when you revert to the primary server.

Step 6 Restore power to the primary server and allow the server to fully start up.

Step 7 Verify the status of the replication to show that the replication is connected; however, the two sides are not synchronized.

```
C:\> vxprint -Pl
Diskgroup = BasicGroup

Diskgroup = datadg

Rlink      : rlk_172_32481
info       : timeout=500 packet_size=1400
             latency_high_mark=10000 latency_low_mark=9950
             bandwidth_limit=none
state      : state=ACTIVE
             synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
             remote_host=172.25.84.33
             remote_dg=datadg
             remote_rlink=rlk_172_6037
             local_host=172.25.84.34
protocol   : UDP/IP
flags      : write attached consistent connected dcm_logging failback_logging
```

Step 8 Convert the original primary RVG to secondary and synchronize the data volumes in the original primary RVG with the data volumes on the new primary RVG using the fast failback feature. Using the Cluster Explorer for the secondary cluster, right-click the RVGPrimary resource (**APP_RVGPrimary**), select **actions**, then select **fbsync** from the Actions dialog box, and then click **OK**. Alternatively you can issue the following command:

```
C:\> hares -action APP_RVGPrimary fbsync 0 -sys secondary_server_name
```

Step 9 Verify that the current secondary (former primary) is synchronized with the current primary (former secondary) by looking for the keyword **consistent** in the **flags** parameter of the output of the following command:

```
C:\> vxprint -Pl
Diskgroup = BasicGroup

Diskgroup = datadg

Rlink      : rlk_172_32481
info       : timeout=29 packet_size=1400
             latency_high_mark=10000 latency_low_mark=9950
             bandwidth_limit=none
state      : state=ACTIVE
             synchronous=off latencyprot=off srlprot=off
assoc      : rvg=CSM_RVG
             remote_host=172.25.84.33
             remote_dg=datadg
             remote_rlink=rlk_172_6037
             local_host=172.25.84.34
protocol   : UDP/IP
flags      : write attached consistent connected
```

Step 10 Using the VCS Cluster Explorer on the secondary cluster, select the **APP** service group. From the shortcut menu, select **Switch To**, then **Remote Switch(...)** to open the Switch global dialog box. In the dialog box specify the primary cluster and the primary server. Alternately issue the following command, where *primarycluster* is the name of the primary cluster:

```
C:\> hagrp -switch APP -any -clus primarycluster
```

Step 11 Log in to the application to verify that the changes you made on the secondary server were retained.

Application Failures

This section covers test cases where the Security Manager application fails. Two cases are covered: a single cluster configuration and a dual cluster configuration. This section contains the following topics:

Application Failure, Single Cluster

Test Case Title: The application fails on the primary server in a single cluster configuration.

Description: This test case verifies that VCS detects an application failure and that VCS automatically moves the application to the secondary server.

Test Setup: A dual node cluster (Figure 1-1 on page 12) using the default application failover behavior.

Step 1 Verify that the APP service group is running on the primary server in the cluster by running the following command:

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A <PrimaryServer>       RUNNING              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               ONLINE
B  APP             <SecondaryServer>    Y          N               OFFLINE
```

Step 2 On the server where Security Manager is running, stop the application by issuing the following command:

```
C:\> net stop crmdmgtd
```

Step 3 Verify that VCS detects that Security Manager failed on the primary server and starts the application on the secondary server.

```
# hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               OFFLINE|FAULTED
B  APP             <SecondaryServer>    Y          N               ONLINE

-- RESOURCES FAILED
-- Group           Type                 Resource             System
C  APP             CSManager            APP_CSManager        <PrimaryServer>
```

Step 4 Manually clear the fault on the APP service group.

```
C:\> hagrp -clear APP -sys primary_server_name
```

Step 5 Manually switch the APP service group back to the primary server.

```
C:\> hagrp -switch APP -to primary_server_name
```

Application Failure, Dual Cluster

Test Case Title: The application fails on the primary server in a dual cluster configuration.

Description: This test case verifies that VCS detects an application failure.

Test Setup: A dual cluster configuration, with replication (Figure 1-2 on page 14), with a single node in each cluster. Likewise, the assumption is that the default application failover behavior has not been modified (that is, failover between clusters requires manual intervention).

Step 1 Verify that the APP and ClusterService service groups are running in the primary cluster by running the following command from the primary server:

```
C:\> hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <SecondaryServer>    RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <SecondaryServer>    Y          N               OFFLINE
B  APPrep          <SecondaryServer>    Y          N               ONLINE
B  ClusterService  <SecondaryServer>    Y          N               ONLINE

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_primary          ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_primary     RUNNING

-- REMOTE SYSTEM STATE
-- cluster:system       State                Frozen
N  csm_primary:<PrimaryServer> RUNNING              0

-- REMOTE GROUP STATE
-- Group           cluster:system              Probed     AutoDisabled    State
O  APP             csm_primary:<PrimaryServer> Y          N               ONLINE
```

Step 2 On the server where Security Manager is running, stop the application by issuing the following command:

```
C:\> net stop crmdmgtd
```

Step 3 Verify that VCS detects that the application failed and stops the APP service group. Issue the following command and observe the output.

```
# hastatus -sum
-- SYSTEM STATE
-- System               State                Frozen
A  <PrimaryServer>      RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State
B  APP             <PrimaryServer>      Y          N               OFFLINE|FAULTED
B  APPrep          <PrimaryServer>      Y          N               ONLINE
B  ClusterService  <PrimaryServer>      Y          N               ONLINE

-- RESOURCES FAILED
-- Group           Type                 Resource             System
C  APP             CSManager            APP_CSManager        <PrimaryServer>

-- WAN HEARTBEAT STATE
-- Heartbeat       To                   State
L  Icmp            csm_secondary        ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State
M  csm_secondary   RUNNING

-- REMOTE SYSTEM STATE
```

```
-- cluster:system                  State                Frozen
N  csm_secondary:<SecondaryServer> RUNNING              0

-- REMOTE GROUP STATE
-- Group          cluster:system                  Probed     AutoDisabled    State
O  APP            csm_secondary:<SecondaryServer> Y          N               OFFLINE
```

Step 4 Manually clear the fault on the APP service group.

```
C:\> hagrp -clear APP
```

Step 5 Put the APP service group online on the primary server to restart the application.

```
C:\> hagrp -online APP -sys primary_server_name
```