Maintenance Activities

This chapter describes maintenance activities related to Security Manager when it is used in an HA/DR configuration. This chapter containing the following topics:

Customizing VCS Behavior

VCS supports an extensive number of variables to control VCS behavior, such as responses to resource failures. If you followed the default installation as described in this document, here are some of the resulting failover behaviors. You should review these and other behavior controls as described in *Veritas Cluster Server User's Guide*.

- If Security Manager fails, VCS does not try to restart the application on the same server; instead, VCS fails it over to the standby server in the cluster. However, you can use a resource-level attribute, RestartLimit, to control the number of times the agent tries to restart the resource before declaring the resource as faulted.
- When first trying to bring the Security Manager application online on a given server, VCS will attempt to bring the resource online only once. The OnlineRetryLimit resource-level attribute specifies the number of times the online entry point is retried if the initial attempt fails.
- By default, VCS runs the Security Manager application monitor script every 60 seconds. This means that it can take up to 60 seconds to detect an application failure. The MonitorInterval is a resource-level attribute that can be adjusted.
- If you are using dual clusters, failover between the clusters is a manual operation by default. This avoids having both clusters running the application simultaneously. If communication between the clusters is lost (which can readily happen if no redundant paths exist between geographically separated data centers), VCS cannot determine whether the remote cluster failed or a communication problem exists. If you

prefer automatic failover between clusters, you can configure it with the ClusterFailOverPolicy attribute on the APP service group.

Security Certificates for SSL

Security Manager allows configuring the use of Secure Socket Layer (SSL) encryption between the server and the client browser or application. SSL encryption requires the creation and placement of a digital certificate on the server. Part of the identity information contained in the digital certificate is the Common Name (CN) or “Host Name” as shown on the Common Services web GUI. In a HA/DR configuration where there are multiple servers and corresponding hostnames you may want to take special steps to ensure that you maintain a certificate that matches the hostname or IP address used to access the application.

In the case of a single cluster, you access the application with a single virtual IP address or virtual hostname. In this case you should create a certificate with the CN equal to the virtual IP address or virtual hostname. Because the virtual IP or virtual hostname address is valid regardless of the server in the cluster running the application, you do not need to update the digital certificate files in the event of a failover.

However, in the case of a dual geographic cluster configuration, each cluster has its own IP address or hostname associated with the application. As a result, if the digital certificate file has been created to match one cluster, it will not match when the application fails over to the other cluster. In this case you might want to update the digital certificate files to match the other cluster in the event of an inter-cluster failover.

Note If you use a virtual hostname to access the application, you can avoid having to update the certificates for an inter-cluster failover by instead using DNS updating. In the event of an inter-cluster failover, DNS is updated with the new IP address associated with the virtual hostname. Because clients are using the same virtual hostname in all cases to access the application, there is no need to update the certificate files.

The Security Manager Agent for VCS can automatically copy digital certificate files stored on a non-shared, non-replicated local directory prior to starting the application. However, you need to place the appropriate files in this directory on each server in the clusters. The directory is specified to the agent using the CertificateDir parameter.

In the case of a geographic redundancy (DR) configuration where there is a single server at each site, a simpler option is available. You can configure the agent to regenerate the certificate files based on the hostname of the server. This works because there are no virtual IP addresses or virtual hostnames involved. To configure the agent for this behavior, specify the keyword regen for the value of the CertificateDir parameter.

When Security Manager is installed, it creates by default a self-signed certificate matching the local hostname of the server. If appropriate for your configuration, to generate a self-signed certificate matching a virtual IP address or virtual hostname, follow this procedure:

Step 1 Log in to the web browser interface of the server (http://<*hostname or IP address*>:1741).

Step 2 Access the self-signed Certificate Setup screen as follows:

a) On the Cisco Security Management Suite homepage, click **Server Administration**.

b) From the menu on the Server Admin page, select **Server** > **Single Server Management** > **Certificate Setup**.

Step 3 Populate the fields of the certificate and specify either the virtual IP address or virtual hostname in the CN field, then click Apply.

The following certificate-related files are generated in the NMSROOT\MDC\Apache\conf\ssl directory:

- server.key
- server.crt
- server.pk8
- server.csr
- openssl.conf
- chain.cer

If you are using a single cluster, no further action is required. However, if you are using a dual geographic cluster configuration with multiple servers in each cluster, you should copy the certificate-related files listed above to a non-shared, non-replicated local directory on each server in the cluster. You should then do the same procedure for the secondary cluster, except this time specify the virtual IP address or virtual hostname of the secondary cluster. When you define the CSManager resource, specify the selected non-shared, non-replicated local directory for the **CertificateDir** attribute. The agent then automatically copies the certificate files to the appropriate working directory after a failover, prior to starting the application.

Manually Starting, Stopping, or Failing Over Security Manager

In a non-HA/DR configuration, you normally start and stop Security Manager with the Windows Services application or its command-line equivalents, net start and net stop. However, in an HA/DR configuration, you must not use this approach. Specific scripts are provided for starting and stopping Security Manager in an HA/DR configuration. These scripts perform additional procedures necessary if you start Security Manager on a different server. These scripts and others make up the Security Manager agent for VCS. The agent enables VCS to control and monitor Security Manager. If you are not using VCS, you can use these scripts to manually start and stop Security Manager.

The section contains the following topics:

VCS Case

If you are using VCS, you should use the VCS controls to manually start, stop, or fail over the Security Manager service group (APP). In VCS terminology, start and stop are referred to as online and offline, respectively. You can bring online, bring offline, or fail over the Security Manager service group using the VCS GUI or the VCS command-line interface. Appendix B, High Availability and Disaster Recovery Certification Test Plan, has examples for performing such operations.

Caution If you manually stop Security Manager outside of VCS (such as by using net stop), VCS views this as an application failure and tries to initiate recovery.

Non-VCS Case

If you are not using VCS, you can use the online and offline scripts provided with Security Manager to start and stop Security Manager. These scripts can be found at:

$NMSROOT\MDC\athena\ha\agent\Veritas60 (for Veritas 6.0.1)

$NMSROOT\MDC\athena\ha\agent\Veritas602 (for Veritas 6.0.2)

$NMSROOT\MDC\athena\ha\agent\Veritas61 (for Veritas 6.1)

$NMSROOT\MDC\athena\ha\agent\Veritas70 (for Veritas 7.0)

$NMSROOT\MDC\athena\ha\agent\Veritas72 (for Veritas 7.2)

$NMSROOT\MDC\athena\ha\agent\Veritas74 (for Veritas 7.4)

Windows Server 2012, 2012R2 Syntax for Veritas 6.0.1, Veritas 6.0.2, Veritas 6.1, Veritas 7.0, Veritas 7.2, and Veritas 7.4:

```
perl online.pl CSManager <PathName> <EventIPAddress> [ <CertificateDir>|regen ]
```

For example:

```
perl online.pl CSManager F:\Progra~1\CSCOpx 192.0.2.1
```

Note You must select the Run as administrator option when opening the Command Prompt.

Syntax	Description
<*PathName*>	The Security Manager installation path (for example, “F:\Program Files\CSCOpx”). If the installation path contains spaces, enclose the argument in quotes.
<*EventIPAddress*>	The IP address that the Security Manager application uses for client/server and server/device communications.
<*CertificateDir*>	Optional. Allows you to specify a nonshared, non-replicated local directory where SSL certificate files are kept. If specified, the script copies these files to the appropriate directory under the installation directory for use by the application. If the keyword regen is used, the script regenerates the SSL certificate based on the local hostname of the server. Regardless of the value used for this parameter, if the hostname of the server matches that of the Security Manager application files, no actions are taken on the certificates. See also Security Certificates for SSL, on page 2.

The offline script syntax for Windows Server 2012 , 2012R2 is shown below:

Windows Server 2012 , 2012R2 Syntax for Veritas 6.0.1, Veritas 6.0.2 and Veritas 6.1:

```
perl offline.pl CSManager <PathName> <EventIPAddress>
```

For example:

```
perl offline.pl CSManager F:\Progra~1\CSCOpx 192.0.2.1
```

Note You must select the Run as administrator option when opening the Command Prompt.

Syntax	Description
<*PathName*>	The Security Manager installation path (for example, “F:\Program Files\CSCOpx”). If the installation path contains spaces, enclose the argument in quotes.
<*EventIPAddress*>	The IP address that the Security Manager application uses for client/server and server/device communications.

For ease of use, you might want to create an online and offline batch file (for example, online.bat and offline.bat), which includes the appropriate attributes for your configuration.

To perform a manual failover, you can use VEA or the command line to transfer the primary role within your replicated volume group. If both the primary and secondary server are functioning, you can migrate the primary role to the secondary (effectively reversing the direction of replication) or, if the primary server has failed and is unavailable, you can have the secondary server take over the primary role (with or without fast-failback). Refer to the Veritas Volume Replicator administrator’s guide for details.

The following is an outline of the manual failover procedure for a disaster recovery configuration using replication between two servers:

Step 1 Stop Security Manager on the primary server using the offline.pl script.

Step 2 Unassign the drive letter from the volume used for Security Manager on the primary server.

Step 3 Migrate ownership from the primary server to the secondary server using the VEA GUI.

Step 4 Assign the drive letter for the volume used for Security Manager on the secondary server.

Step 5 Start Security Manager on the secondary server using the online.pl script.

Note If you are migrating/failing-over to the secondary server for the first time, you must upgrade the file permissions for the casusers group. This is a one-time activity. For more information, see Updating Permissions on the Working Volume.

Integrating Cisco Secure ACS with Security Manager

As described in the Installation Guide for Cisco Security Manager, you can integrate Cisco Secure ACS with Security Manager to provide enhanced authorization for Security Manager users. In an HA/DR configuration,

you need to add each Security Manager server involved in the configuration as a AAA client in ACS. When you specify the server in ACS, specify the fixed IP address associated with server's physical hostname.

If you are using an HA/DR configuration for Security Manager with ACS integration, you should also deploy multiple ACS servers to avoid having ACS become a single point of failure. If you only have one ACS server and it fails, you cannot log in to Security Manager without taking corrective action to either restore ACS or reset the Security Manager server to use local authentication. ACS supports the deployment of a primary ACS along with multiple secondary ACSs, where database replication is used to keep the secondary ACSs synchronized with the primary ACS. Security Manager supports specifying up to three ACSs, so if the first ACS is unavailable, it tries the second, and finally the third, if necessary.

Note Beginning with Cisco Security Manager 4.21, Cisco Identity Services Engine (ISE) can be used for authentication purposes, in the place of earlier ACS server.

Upgrading Security Manager

Security Manager upgrades come in various forms:

- Major releases (change in the first number of the release, for example, 3.x to 4.x)
- Minor releases (change in the second digit of the release, for example, 3.1 to 3.2)
- Maintenance releases (change in the third digit of the release, for example, 3.1 to 3.1.1)
- Service packs (identified by a service pack identifier, such as SP2 for Security Manager 3.1)

When you upgrade Security Manager in an HA/DR configuration, the main difference is whether it is necessary to upgrade just the primary server with the active instance of Security Manager or to also upgrade the secondary servers, which have only a spare copy of Security Manager for establishing the correct registry configuration necessary for Security Manager to run on the server. If an upgrade modifies the registry, you must perform the upgrade on all servers in the HA/DR configuration. Normally service packs do not affect the registry, so it is sufficient to install the service pack just on the primary server. For major, minor, or maintenance releases, normally you should upgrade all servers. However, check the readme file or release notes for exceptions to these guidelines.

When upgrading a secondary server, you must mount the spare copy of the Security Manager to the standard $NMSROOT (such as F:\Program Files\CSCOpx) path used on all servers in the configuration and then install the regular upgrade. This ensures that the registry settings are correct for running the upgraded version of Security Manager on any secondary server.

Before you upgrade, stop VCS on all servers (using **hastop -all -force** on any server in the cluster stops VCS on all servers in the cluster and leaves the application and its resources operational). If you are upgrading on all servers and your configuration uses replication, you should pause or stop the replication during the upgrade and then synchronize the secondary servers after the upgrade is complete.

Backing Up Security Manager

An HA/DR deployment configuration of Security Manager does not replace the need for backing up Security Manager regularly. The HA/DR configuration protects you against loss of data or application downtime due

to hardware failures; however, it does not protect you against user actions such as accidentally or maliciously modifying or deleting important information maintained in Security Manager. Therefore, you should continue to back up the Security Manager database and information files; you can use the backup feature in Security Manager.

You should back up only the primary active instance of Security Manager, not the spare instances associated with secondary servers. Security Manager can be restored on any server in the HA/DR configuration or any server that has the compatible Security Manager application installed.

Uninstalling Security Manager

To uninstall Security Manager from all servers in the HA/DR configuration, follow these steps:

Step 1 Make sure Security Manager is running on the primary server in the primary cluster.

Step 2 Using the Cluster Explorer, right-click the **APP_CSManager** resource and uncheck the **critical** check box. You are prompted to switch to read/write mode, so click **Yes** when this dialog box appears.

Step 3 Right-click the **APP_CSManager** resource and select **Offline** on the primary server. Wait for Security Manager to go offline.

Step 4 Perform required maintenance activities, as needed.

Step 5 Start the daemon manager manually on the server, using the **net start crmdmgtd** command.

Step 6 The **APP_CSManager** will come online; check the **critical** check box.

Step 7 Delete the APP_CSManager resource and then save the VCS configuration.

Step 8 If you are using replication, stop replication using the VEA GUI.

Step 9 To uninstall Security Manager on the primary server, choose **Start** > **All Programs** > **Cisco Security Manager** > **Uninstall Cisco Security Manager**.

Step 10 On the secondary server, import the disk group if not already done, which contains the cscopx_spare volume, using either the VEA GUI or the command line.

Step 11 Assign the selected drive letter to the cscopx_spare volume using either the VEA GUI.

Step 12 To uninstall Security Manager on the primary server, choose **Start** > **All Programs** > **Cisco Security Manager** > **Uninstall Cisco Security Manager**.

Step 13 Repeat Steps 10 through 12 on any other secondary servers or the primary server in a secondary cluster.

Note If you do not plan to re-install Security Manager, you should also delete service groups in VCS associated with Security Manager and the Replicated Volume Group if using replication. You should also delete any unneeded volumes and disk groups as well.

Migrating a Non-HA Security Manager to HA

If you have an existing Security Manager installed in a regular non-HA configuration, this section addresses how to migrate that instance to an HA configuration. Use the following steps to perform the migration:

Step 1 Perform a backup of the existing Security Manager instance as described in the *User Guide for CiscoWorks Common Services 3.2*. See the section entitled *Backing Up Data* in the *Configuring the Server* Chapter available here: http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.2/user/guide/admin.html

Step 2 Create the desired Security Manager HA or DR deployment environment as described in this document.

Step 3 Restore the backup taken from the original Security Manager instance to the primary server in the HA or DR deployment environment as described in the User Guide for CiscoWorks Common Services 3.2. See the section entitled "Restoring Data" available at the link above.

Step 4 Manually synchronize the database passwords in the registry on any secondary servers with the passwords on the primary server. On the primary server, use the registry editor (**Start** > **Run** > **regedit**) to find and note the values for the CWEPWD registry entries under folders cmf, vms, rmeng, and aus under HKEY_LOCAL_MACHINE\SOFTWARE\OBDC\OBDC.INI. Edit the CWEPWD registry values on any secondary machine to match those on the primary.