Installing the Cisco Security Management Suite High Availability Solution

This chapter explains how to install Security Manager in an HA or DR deployment configuration. You should perform these tasks in order, although some tasks are optional or might not apply depending on your specific configuration.

This chapter contains the following topics:

Making Ethernet Connections

To make the Ethernet connections required by your HA or DR configuration, follow these steps:

Step 1 Make the Ethernet connections between the servers and switches according to Figure 2-1 or Figure 2-2, depending on your cluster configuration.

Note Use of a second Ethernet connection to the router/switch network for each server is optional, but it adds an extra level of redundancy in the event of a NIC or local Ethernet switch failure. Veritas Cluster Server (VCS) includes the IPMultiNicPlus agent. This agent allows setting up multiple NIC cards on a server which provides redundant access for the server to the router/switch network. If a NIC card fails, a cable is removed, or some other failure occurs, VCS can detect the failure and reassign the working virtual IP address to another working NIC card on the

server. See the Veritas Cluster Server Bundled Agents Reference Guide for details on the IPMultiNicPlus agent. The examples in this document only show the case of a single NIC card for network access.

You can also used vendor specific NIC teaming (IEEE 802.3ad link aggregation) solutions as an alternative.

Step 2 In the case of a dual-node cluster, make the Ethernet cluster communication connections between the servers according to Figure 2-2. When connecting directly between servers, you might not have to use a crossover Ethernet cable, depending on whether the interfaces support automatic crossover detection. Most newer Ethernet interfaces support this feature and allow using a straight-through cable when directly connecting to another server.

Installing Microsoft Windows Server

Install the supported Microsoft Windows operating system:

Microsoft Windows Server 2012, Standard and Datacenter Edition

Microsoft Windows Server 2012 R2, Standard and Datacenter Edition

We recommend that you use the same operating system on all servers.

Note Symantec Veritas Storage Foundation HA for Windows version 6.0.1 / 6.0.2 / 6.1 requires that you install the operating system in the same path on all systems. For example, if you install Windows on C:\WINDOWS of one node, installations on all other nodes must be on C:\WINDOWS. Make sure that the same drive letter is available on all nodes and that the system drive has adequate space for the installation.

Connecting the Servers to External Storage

If you are using a dual-node cluster, shared external storage is required. You may use any storage hardware in *Hardware Compatibility List for Veritas Storage Foundation & High Availability Solutions for Windows*. Either internal or external storage can be used for a single-node cluster.

Installing Symantec Veritas Products

Install and configure the Symantec Veritas products and components. The products and components required vary depending on whether a single local cluster, dual geographic clusters, or replication without clustering configuration is used. Some components are optional, such as the GUI for Volume Manager (Veritas Enterprise Administrator). See Table 3-1.

Table 3-1 Veritas Software Components

Veritas Product/Component	Single Local Cluster	Dual Geographic Clusters	Replication without Clustering
Storage Foundation for Windows	—	—	Required
Symantec Veritas Storage Foundation HA for Windows version 6.0.1 / 6.0.2 / 6.1	Required	Required	—
Volume Replicator Option	Not Required	Required	Required
Global Cluster Option	Not Required	Required	—
Dynamic Multipathing Option	See Note[1]	See Note[1]	See Note[1]
Veritas Enterprise Administrator (GUI)[2]	Required	Required	Required
Cluster Manager (GUI) [2]	Optional	Optional	—

1. Required only if you are using external storage with multiple host bus adapters providing multiple paths between the server and disk storage
2. Can be installed either on the server or a separate client machine.

See the applicable Veritas release notes and installation guides for prerequisites and instructions for installing the Veritas software.

Note One important prerequisite is that you configure the servers as part of a Windows Server domain.

Mirroring the Boot Disk (Optional)

Mirroring the boot disk is optional; however, it provides an extra level of protection for a given server. If the boot disk fails, the machine can be recovered quickly by booting from the mirrored alternate boot disk. Mirroring is accomplished by placing the boot disk in a dynamic disk group under Veritas Volume Manager control and then adding a mirror.

See the section called “Set up a Dynamic Boot and System Volume” in the Symantec Veritas Storage Foundation HA for Windows version 6.0.1 / 6.0.2 / 6.1 administrator’s guide for details on this procedure.

Veritas Volume Manager Configuration Tasks

In this section, you configure the necessary disk group and volumes required for the Security Manager application. The configuration varies depending on whether the server involved is the primary server or a secondary server and whether or not replication is involved. You can perform Volume Manager tasks with the VEA GUI or through the command line. For details on using VEA or the command line for these steps, see the Symantec Veritas Storage Foundation HA for Windows version 6.0.1 / 6.0.2 / 6.1 administrator's guide.

This section contains the following topics:

Primary Server (without Replication)

Use this procedure to configure the disk group and volumes required for Security Manager on the primary server in a single-cluster configuration where replication is not involved. In a single-cluster configuration, external shared storage is used, which is accessible to all servers in the cluster.

To configure the disk group and volumes, follow these steps:

Step 1 Create a disk group with the following characteristics:

- Group Name: **datadg**
- Type: **Dynamic (Cluster)**
- Number of Disks: If using software RAID, include at least two disks in the group for mirroring; otherwise, a single logical disk (using hardware RAID) is sufficient. The disks used for this disk group must be accessible to all nodes in the cluster.

Note The use of software RAID 5 is not recommended.

Step 2 Create a volume in the **datadg** disk group with the following characteristics:

- Volume Name: **cscopx**
- Assigned Drive Letter: **<Selected Drive Letter>**

Note You can choose any available drive letter; however, the drive letter must be the same on all systems.

- File Type: **NTFS**

Primary Servers (with Replication)

Use this procedure to configure the disk group and volumes required for Security Manager on the primary servers in a dual geographic configuration where replication is running between the two clusters. Perform this procedure on the primary server in both the primary and secondary cluster. For each cluster you can use either a single-node cluster or a cluster with multiple nodes using shared storage; however, this document does not cover the case of a multi-node cluster in a dual geographic configuration.

To configure the disk group and volumes, follow these steps:

Step 1 Create a disk group with the following characteristics:

- Group Name: **datadg**
- Type: **Dynamic (Cluster)** (when using VCS), **Dynamic (Secondary)** (when not using VCS)
- Number of Disks: If using software RAID, include at least two disks in the group for mirroring; otherwise, a single logical disk (which uses hardware RAID) is sufficient. If this is a multi-node cluster, the disks used for this disk group must be accessible to all nodes in the cluster.

Note The use of software RAID 5 is not recommended.

Step 2 Create a volume in the **datadg** disk group with the following characteristics:

- Volume Name: **cscopx**
- Assigned Drive Letter: **<Selected Drive Letter>** (for the primary cluster), **None** (for the secondary cluster)
- File Type: **NTFS** (for the primary cluster), None (for the secondary cluster)
- Volume Logging: **None**

Step 3 Create a volume in the **datadg** disk group for use as a storage replicator log (SRL) with the following characteristics:

- Volume Name: **data_srl**
- Assigned Drive Letter: **None**
- File Type: **Unformatted**
- Volume Logging: **None**

Note For information on choosing the proper size of the SRL, see the Volume Replicator administrator's guide.

Secondary Servers and the Primary Server in a Secondary Cluster

Use this procedure to configure the disk group and volumes required for installing Security Manager on secondary servers and on the primary server in a secondary cluster. You must install Security Manager on all secondary servers, as well as the primary server in a secondary cluster. In these cases, you install Security Manager on a spare volume, which is mounted temporarily before installation, then dismounted and not used again until you want to uninstall Security Manager from the server or you want to upgrade Security Manager. You must mount the temporary volume on the same drive letter as the one used for the primary server in the primary cluster and you must use the same installation path (for example, F:\Program Files\CSCOpx) during the installation.

To configure the disk group and volumes, follow these steps:

Step 1 If you are not creating the spare volume on an existing disk group, create a disk group with the following characteristics:

- Group Name: **datadg_spare**
- Type: **Dynamic (Secondary)**
- Size: **5GB** (The volume only needs to be large enough to install Security Manager)
- Number of Disks: Since this disk group is not used to store application data, a single, nonredundant disk is sufficient.

Step 2 Create a volume in the disk group with the following characteristics:

- Volume Name: **cscopx_spare**
- Assigned Drive Letter: **<Selected Drive Letter>**

Note You **must** use the same drive letter that is used for the cscopx drive on the primary server.

- File Type: **NTFS**

Installing Security Manager

The Security Manager installer detects the presence of Symantec Veritas Storage Foundation HA for Windows version 6.0.1 / 6.0.2 / 6.1 and asks you whether you want to install Security Manager in an HA/DR configuration. If you select this option, the only additional information to specify beyond a regular installation is the database password. In a non-HA/DR installation, the database password is autogenerated. However, since the database password must be the same on all servers in the HA/DR configuration, the installer prompts you to specify the password. You must use this same password on all servers in the HA/DR configuration.

The HA/DR installation installs the Cisco Security Manager agent for VCS, so VCS recognizes a new **CSManager** resource type and can control and monitor Security Manager.

The HA/DR installation also configures the Security Manager and related services in Windows for a Startup Type of Manual instead of Automatic, because the Veritas cluster server instead controls the starting and stopping of Security Manager on each server in the HA/DR configuration. Otherwise, the Security Manager application would try to start on all servers in the HA/DR configuration after any server reboot, when Security Manager should run only on one server at any time.

You must install Security Manager on each server in the HA/DR configuration. However, only the primary instance of Security Manager is used and protected in the HA/DR configuration. Other installations are performed to enable the primary instance to run on any of the secondary servers in the configuration.

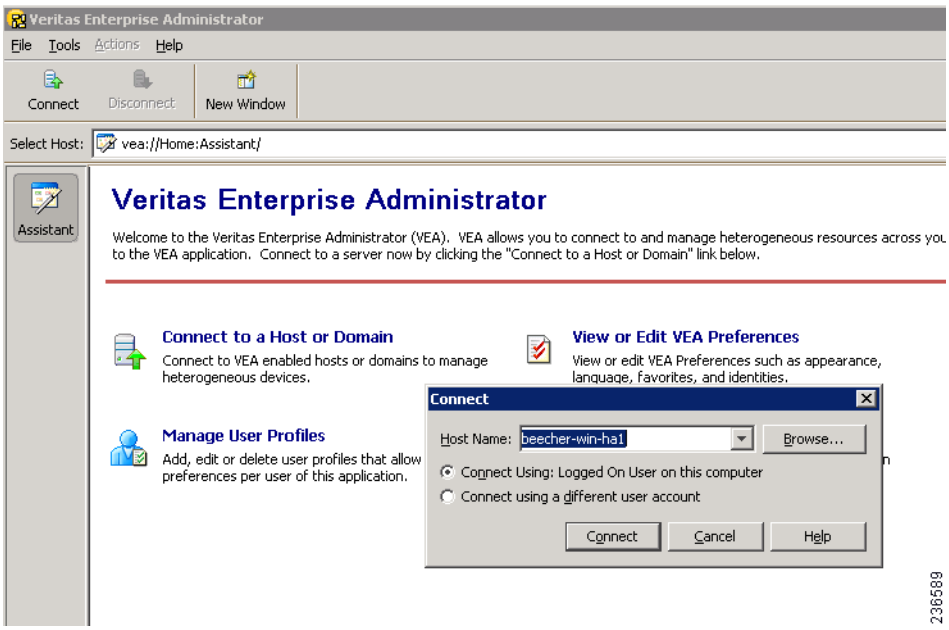
This section contains the following topics:

Installing Security Manager on the Primary Server

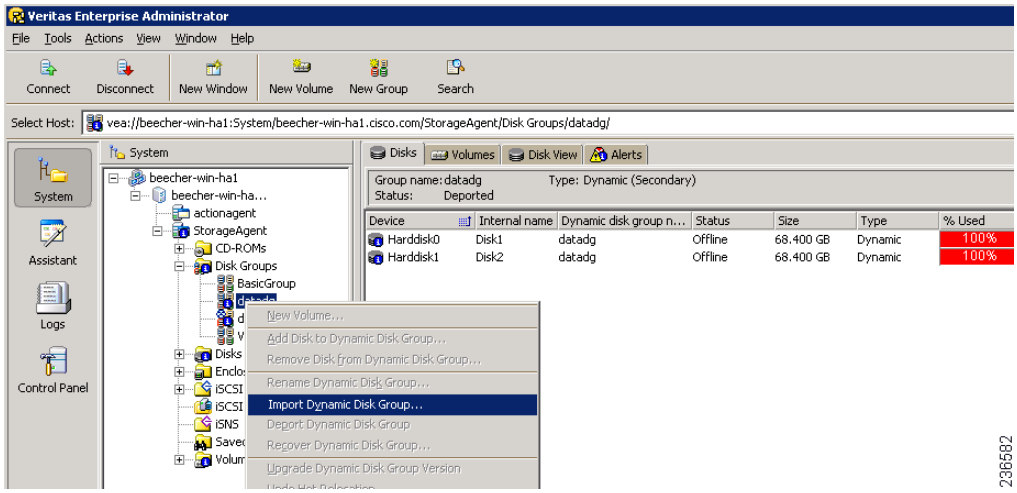
Use this procedure to install the primary instance of Security Manager that is used in production and is protected by the HA/DR configuration.

To install Security Manager on the primary server, follow these steps:

Step 1 On the primary server in the cluster, open the Veritas Enterprise Administrator (VEA GUI) application and login.



Step 2 Right-click the **datadg** disk group and select **Import Dynamic Disk Group**.



Step 3 Make sure the **Import as dynamic disk group** option is selected, and then click **OK**.

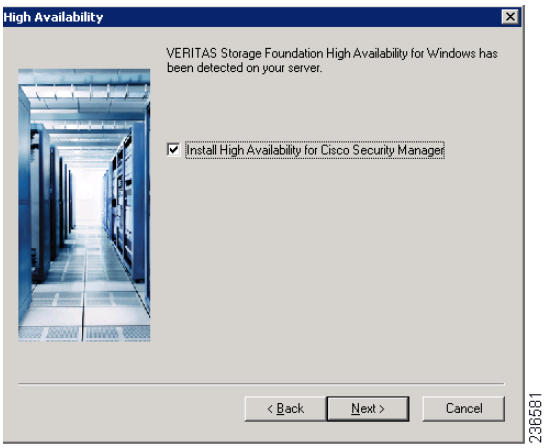
Step 4 Expand the **Volumes** folder under System.

Step 5 Right-click the **cscopx** volume and choose **File System > Change Drive Letter and Path**.

Step 6 Assign the desired drive letter to the **cscopx** volume and then click **OK**. Refer to the Local Redundancy Configuration Worksheet, page 2-5, or Geographic Redundancy (DR) Configuration Worksheet, page 2-7, for drive assignment.

Step 7 Install Security Manager according to the Security Manager Installation Guide, while noting the following HA specific items.

a. When prompted whether to install Security Manager for HA, indicate yes by checking the box.



b. When prompted for the installation directory, specify: *<Selected Drive Letter>:\Program Files\CSCOpx*.

c. When prompted to specify the database password, choose an appropriate password and remember it; you will use this password for all Security Manager servers in the HA/DR configuration.

Note Near the end of the Security Manager installation, you might see a message that you are using a multihomed server and that you must update the gatekeeper.cfg file. You can ignore this message, because the agent scripts used in the HA/DR configurations modify this file.

Step 8 After Security Manager has been installed, reboot the server.

Step 9 After the system reboots, open the VEA GUI and check to see if the shared disk group is Imported. If the disk group status is Offline, repeat Step 2 through Step 6 to import the disk group and assign the same drive letter used during installation.

Step 10 Start Security Manager using the online.pl script. For more information, see Manually Starting, Stopping, or Failing Over Security Manager, page 4-3.

Note It is necessary to start Security Manager to complete configuration of the Windows registry entries needed for Security Manager to correctly operate.

Step 11 Allow 5 to 10 minutes for Security Manager to complete startup, then log in to the application's web interface using the following URL: **http://<server hostname or IP address>:1741**. Verify that you can successfully log in.

Tip Alternatively, you can use the **pdshow** command to verify that the Cisco Security Manager services are running successfully.

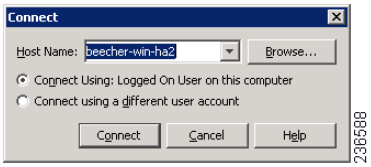
Step 12 Log out of the application's web interface, then stop Security Manager using the offline.pl script. For more information, see Manually Starting, Stopping, or Failing Over Security Manager, page 4-3.

Installing Security Manager on Secondary Servers

Use this procedure to install Security Manager on secondary servers. Installing Security Manager on secondary servers is similar to installing it on a primary server, with one important difference. You install Security Manager onto a spare volume (**cscopx_spare**) associated with the specific secondary server, which is used again only if you want to upgrade or uninstall Security Manager. This spare volume must be large enough to hold the Security Manager application with an empty database (~2 GB). You can create the spare volume on the **datadg** disk group if enough space is available or, preferably, on a separate disk group.

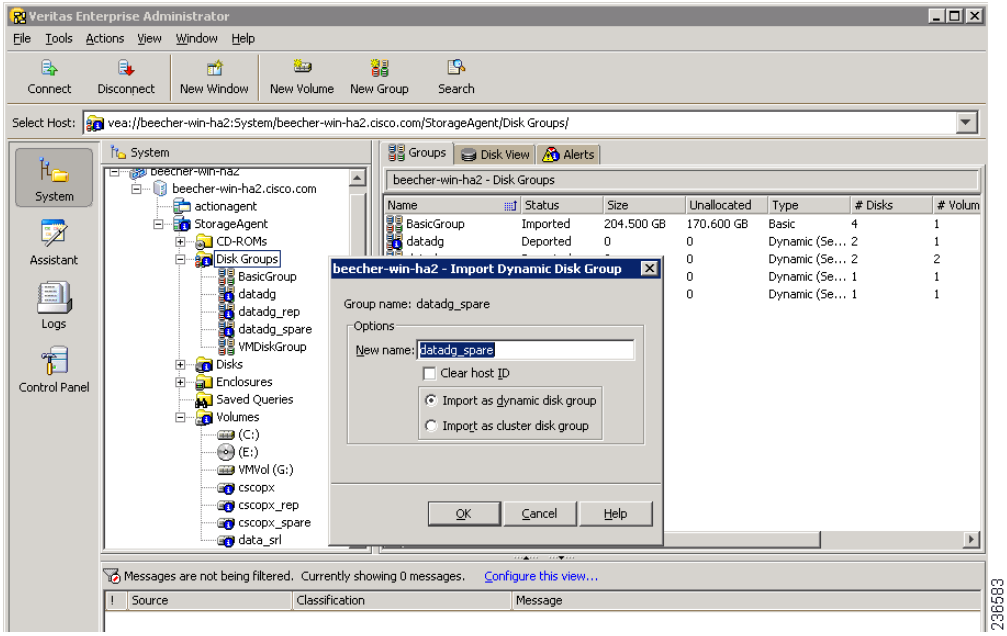
To install Security Manager on a secondary server, follow these steps:

Step 1 On the secondary server, open the Veritas Enterprise Administrator (VEA GUI) application and log in.



Step 2 Right-click the **datadg_spare** disk group and select **Import Dynamic Disk Group**.

Step 3 Make sure the **Import as dynamic disk group** option is selected, and then click **OK**.



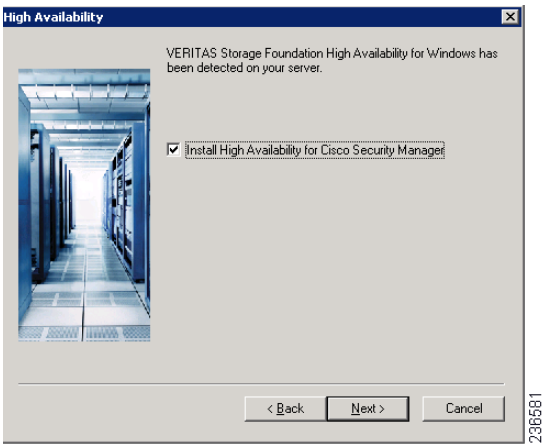
Step 4 Expand the **Volumes** folder under System.

Step 5 Right-click the **cscopx_spare** volume and choose **File System > Change Drive Letter and Path**.

Step 6 Assign the desired drive letter to the **cscopx_spare** volume and then click **OK**. Refer to the Local Redundancy Configuration Worksheet, page 2-5, or Geographic Redundancy (DR) Configuration Worksheet, page 2-7, for drive assignment.

Step 7 Install Security Manager according to the Security Manager Installation Guide, while noting the following HA-specific items.

a. When prompted whether to install Security Manager for HA, indicate yes by checking the box.



b. When prompted for the installation directory, specify: *<Selected Drive Letter>:\Program Files\CSCOpx*.

c. When prompted to specify the database password, choose the same password you chose for the primary server.

Note Near the end of the Security Manager installation, you might see a message that you are using a multihomed server and that you must update the gatekeeper.cfg file. You can ignore this message, because the online script used in the HA/DR configurations modifies this file.

Step 8 After Security Manager has been installed, reboot the server.

Step 9 After the system reboots, open the VEA GUI and check to see if the shared disk group is Imported. If the disk group status is Offline, repeat Step 2 through Step 6 to import the disk group and assign the same drive letter used during installation.

Step 10 Start Security Manager using the online.pl script. For more information, see Manually Starting, Stopping, or Failing Over Security Manager, page 4-3.

Note It is necessary to start Security Manager to complete configuration of the Windows registry entries needed for Security Manager to correctly operate.

Step 11 Allow 5 to 10 minutes for Security Manager to complete startup, then log in to the application's web interface using the following URL: **http://<server hostname or IP address>:1741**. Verify that you can successfully log in.

Tip Alternatively, you can use the **pdshow** command to verify that the Cisco Security Manager services are running successfully.

Step 12 Log out of the application's web interface, then stop Security Manager using the offline.pl script. For more information, see Manually Starting, Stopping, or Failing Over Security Manager, page 4-3.

Step 13 After installation is complete, unassign the drive letter from the spare volume.

Manually Starting Services in Secondary HA Server

If in Security Manager version 4.10, one or more services do not start up in secondary HA server in DR mode, follow these steps:

Step 1 Run the following command to reset the casuser password:

***<NMSROOT>*\setup\support\resetcasuser.exe**

Example: `C:\Progra~2\CSCOpx\setup\support\resetcasuser.exe`

Step 2 Of the two options displayed, on screen, choose option 2 -Enter casuser password. You will be prompted to enter a password for casuser and then to reenter the password for confirmation.

Step 3 If local security policy is configured, add the casuser account to the 'Log on as a service' operation in the local security policy.

Note The following five permissions are assigned and set, automatically, at the time of Security Manager installation:
Access this computer from network- casusers, Deny access to this computer from network-casuser, Deny logon locally-casuser, Log on as a batch job-casuser casusers, and Log on as a service- casuser.

Step 4 Run the following command to apply the casuser permission to NMSROOT:

C:\Windows\System32\cacls.exe "*<NMSROOT>*" /E /T /G Administrators:F casusers:F

Example: `C:\Windows\System32\cacls.exe "C:\Progra~2\CSCOpx" /E /T /G Administrators:F casusers:F`

Step 5 Run the following command to set the casuser to database services.

<NMSROOT>*\bin\perl *<NMSROOT>*\bin\ChangeService2Casuser.pl casuser *<casuserpassword>

Example: `C:\Progra~2\CSCOpx\bin\perl C:\Progra~2\CSCOpx\bin\ChangeService2Casuser.pl casuser admin123`

Veritas Volume Replicator Tasks

Use this procedure to configure replication for a dual geographic cluster configuration where replication is running between the clusters.

To configure replication, follow these steps:

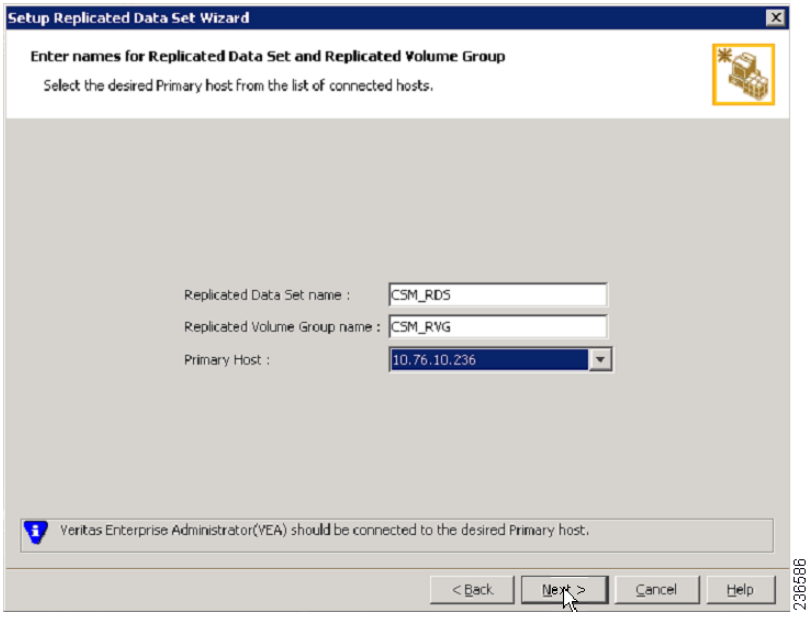
Step 1 Using VEA GUI, connect to the primary and secondary hosts.

Step 2 Make sure that the *datadg* disk group is imported on both the primary and secondary server.

Step 3 Choose **View > Connection > Replication Network**.

Step 4 Select **Replication Network** from the tree, select the **Setup Replicated Data Set** wizard from the toolbar, and then specify the following on the first panel of the wizard:

- Replicated Data Set Name: **CSM_RDS**
- Replicated Volume Group name: **CSM_RVG**
- Select the primary host from the drop-down list.



Step 5 Click **Next**, and on the Select Dynamic Disk Group and volumes to be replicated panel of the wizard, specify the following:

- Dynamic Disk Group: **datadg**
- Volumes: **cscopx**

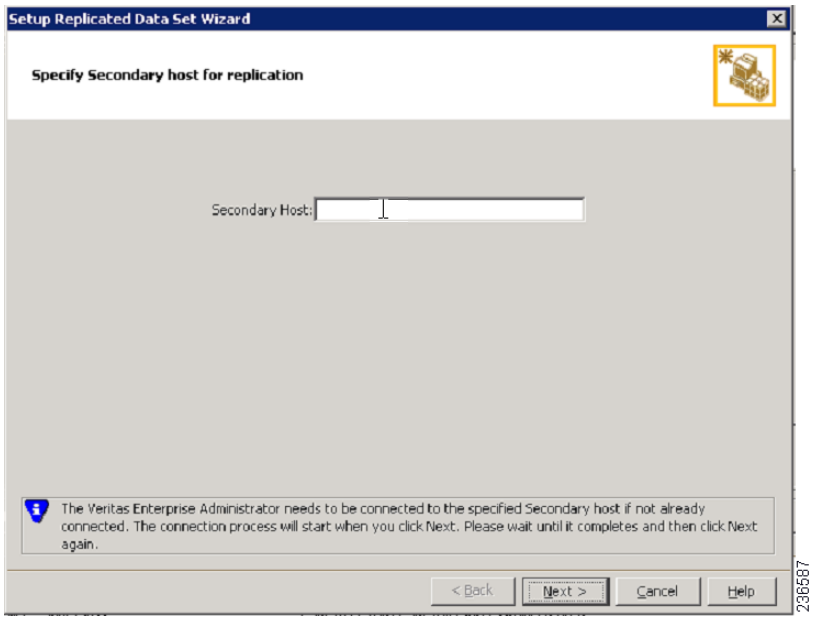
Step 6 Click **Next**. If data_srl is the only other available volume, it will automatically be selected as the storage volume for the replicator log. If more than one additional volume is available, the Storage Replicator Log panel appears. Specify the following:

- Volume for the Replicator Log: **data_srl**

Step 7 Click **Next**, review the summary information, and then click **Create Primary RVG** to create the RVG.

Step 8 After successfully creating the Primary RVG, click **Yes** when prompted to add a secondary host to the RDS.

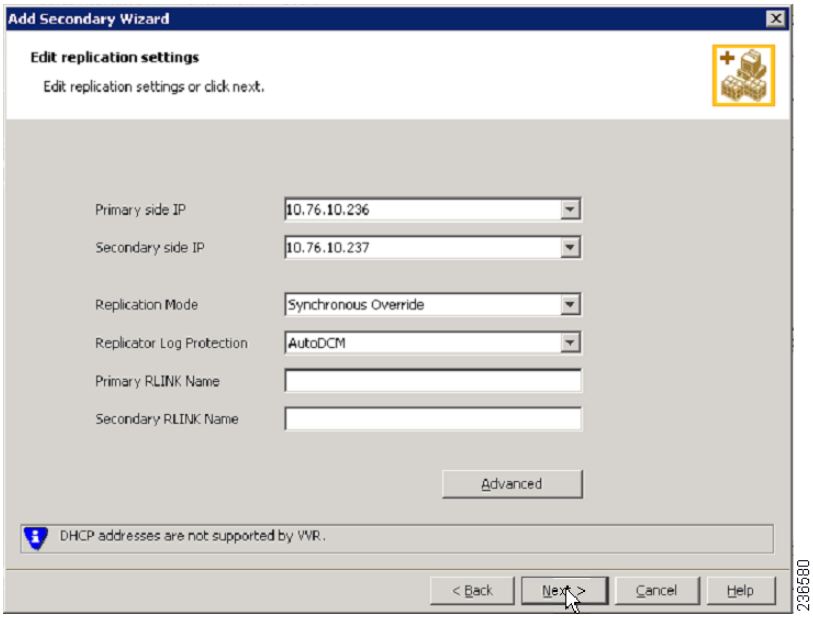
Step 9 On the Specify Secondary host for replication panel, enter the name or IP address of the secondary host in the Secondary Host field.



Step 10 Click **Next** and on the edit replication settings panel specify the following:

Note For the primary and secondary side IP addresses you can specify the fixed IP addresses of the NIC cards. However, if you use Veritas Cluster Server, you must go back later and update the IP address to use virtual IP addresses under VCS control. Do this from VEA by selecting the secondary RVG in the tree and then choosing **Actions > Change Replication Settings**.

- Primary side IP: <IP address of the primary server>
- Secondary side IP: <IP address of the secondary server>
- Replication Mode: **Synchronous Override**
- Replicator Log Protection: <Choose from **Off**, **Fail**, **DCM**, **AutoDCM** (Default), **Override**>. See the Volume Replicator administrator's guide for descriptions of each choice.



Step 11 Click **Next** to start replication with the default settings. Select **Synchronize Automatically** and make sure Start Replication is checked.

Step 12 Click **Next** to display the Summary page, and then click **Finish**.

Updating Permissions on the Working Volume

When Security Manager is installed, it creates a special local user (casuser) and group (casusers) for running Security Manager. To run the protected instance of Security Manager on secondary servers, you must add the local casusers group permissions to the cscopx volume.

This section contains the following topics:

Updating Permissions when using Shared Storage

To add the local casusers group permissions for a secondary server when using shared storage, follow these steps:

Step 1 If it is running on the primary server, stop Security Manager using the offline.pl script. For more information, see Manually Starting, Stopping, or Failing Over Security Manager, page 4-3.

Step 2 Deport the **datadg** disk group from the primary server.

Step 3 Import the **datadg** diskgroup onto the secondary server.

Step 4 Assign the primary volume (cscopx) to the selected drive letter using either the VEA GUI or the command line.

Step 5 From Windows Explorer, right-click the **<Selected Drive Letter>:\Program Files\CSCOpx** folder and choose the **Sharing and Security** menu item.

Step 6 The folder properties dialog box appears. Select the **Security** tab, and then click **Add**.

Step 7 In the Select Users or Groups dialog box, click **Location**, and then select the local server from the selection tree.

Step 8 Enter **casusers** in the enter object names text box, and then click **Check Names**. The text box should then display *<ServerName>\casusers*. Click **OK**.

Step 9 Making sure casusers is selected, check the **Full Control** check box under Allow to grant the casusers group full control.

Step 10 Click **Advanced**.

Step 11 Under Advanced Settings, check the **Replace permission entries on all child objects with entries shown here that apply to child objects** check box.

Step 12 Click **Apply** and wait for the permissions to propagate to all child objects under the CSCOpx directory.

Step 13 When propagation is complete, click **OK**.

Step 14 Click **OK** to close the CSCOpx Properties dialog box.

Step 15 Unassign the drive letter from the cscopx volume.

Step 16 Deport the datadg disk group from the secondary server.

Step 17 Import the datadg diskgroup onto the primary server.

Step 18 Assign the primary volume (cscopx) to the selected drive letter using either the VEA GUI or the command line.

Updating Permissions when using Replication

To add the local casusers group permissions for a secondary server when using replication, follow these steps:

Step 1 If it is running on the primary server, stop Security Manager using the offline.pl script. For more information, see Manually Starting, Stopping, or Failing Over Security Manager, page 4-3.

Step 2 Unassign the drive letter from the cscopx volume.

Step 3 Migrate the replication primary to the secondary.

Step 4 Assign the selected drive letter to the cscopx volume on the secondary server.

Step 5 From Windows Explorer, right-click the **<Selected Drive Letter>:\Program Files\CSCOpx** folder and choose the **Sharing and Security** menu item.

Step 6 The folder properties dialog box appears. Select the **Security** tab and click **Add**.

Step 7 In the Select Users or Groups dialog box click **Location**, and select the local server from the selection tree.

Step 8 Enter **casusers** in the enter object names text box, and then click **Check Names**. The text box should then display *<ServerName>\casusers*. Click **OK**.

Step 9 Making sure casusers is selected, check the **Full Control** check box under Allow to grant the casusers group full control.

Step 10 Click **Advanced**.

Step 11 Under the Advanced Settings, check the **Replace permission entries on all child objects with entries shown here that apply to child objects** check box.

Step 12 Click **Apply** and wait for the permissions to be propagated to all child objects under the CSCOpx directory.

Step 13 When propagation is complete, click **OK**.

Note While the permissions are being updated you may encounter an error dialog with the title "Error Applying Security" with the message "An error occurred applying security information to: <*Selected Drive Letter*>:\Program Files\CSCOpx\log\dcr.log. Access is denied." You can safely ignore this error and click **Continue** on the error dialog to complete the process of updating permissions.

Step 14 Click **OK** to close the CSCOpx Properties dialog box.

Step 15 Unassign the drive letter from the cscopx volume.

Step 16 Migrate the replication back to the primary server.

Step 17 Assign the selected drive letter to the cscopx volume on the primary server.

Veritas Cluster Server Tasks

This section describes the process for setting up and configuring the Veritas cluster(s). There are two specific scenarios described:

Single Local Cluster (Dual-Node) Configuration, page 3-16

Dual Geographic Cluster Configuration, page 3-24

Single Local Cluster (Dual-Node) Configuration

This section covers the setup and configuration of a single, local cluster with two nodes in the cluster (primary and secondary).

This section contains the following topics:

Creating the Cluster

To create the cluster, follow these steps:

Step 1 Create a cluster using the VCS Cluster Configuration wizard, where:

- Cluster Name = CSManager_Primary
- Cluster ID = 0

Include the primary and secondary servers in the definition of the cluster. Part of the cluster definition in the wizard is to specify the NICs for the private network. VCS uses a private network for communications between cluster nodes for cluster maintenance. You can also assign one of the network Ethernet interfaces to act as low-priority cluster communications interface in case all the dedicated cluster communication interfaces fail.

Step 2 To start the Cluster Manager, choose **Start > All Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** and log in to the cluster.

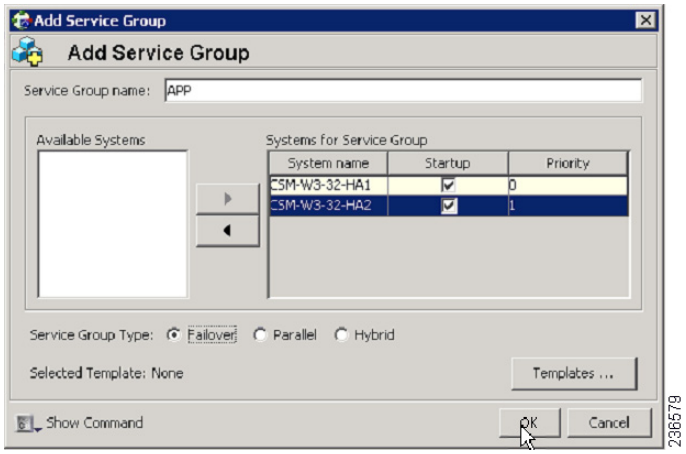
Step 3 Using the Cluster Manager, import the **CSManager** resource type by choosing **File > Import Types**. Browse to the CSManagerTypes.cf file located under $VCS_ROOT\cluster server\conf\config and click **Import**.

Creating the Application Service Group

To create the application service group, follow these steps:

Step 1 Right-click the **CSManager** resource and select **Add Service Group**.

Add a service group called **APP**, and include both servers for this service group with the Startup option checked for each server and the service group type of Failover.

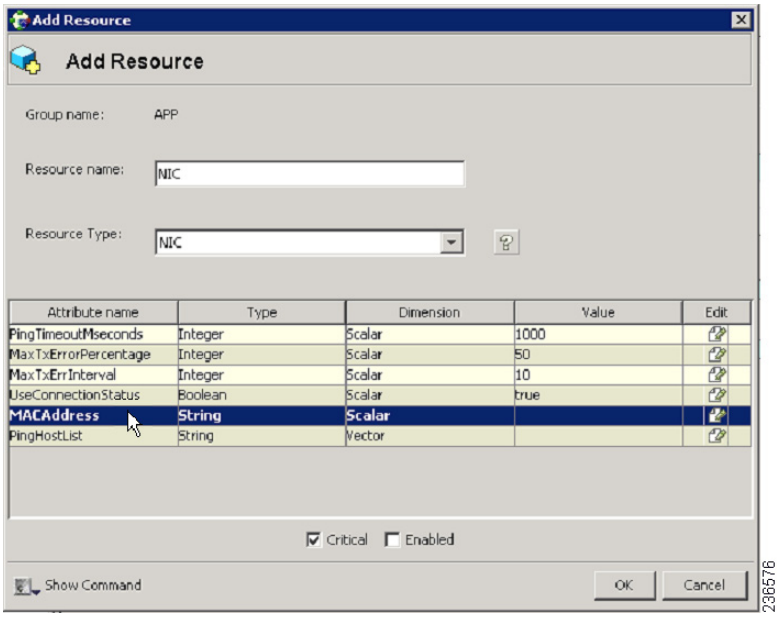


Step 2 Right-click the **APP** service group and select **Add Resource**.

Add the NIC resource and check the **Critical** and **Enabled** check boxes.

- Resource name = **NIC**
- Resource Type = **NIC**
- MACAddress = <MAC address of the NIC used for accessing the Security Manager application>, which is defined uniquely for each server in the cluster.

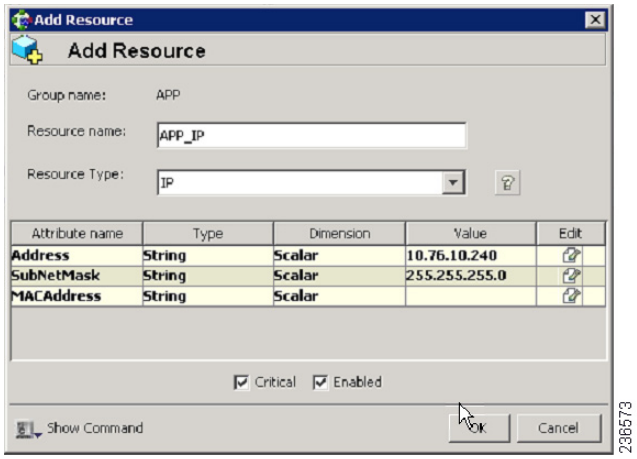
Note You can find the MAC address associated with each Ethernet interface using the DOS-level command **ipconfig -all**.



Step 3 Right-click the **APP** service group and select **Add Resource**.

Add the IP resource and check the **Critical** and **Enabled** check boxes.

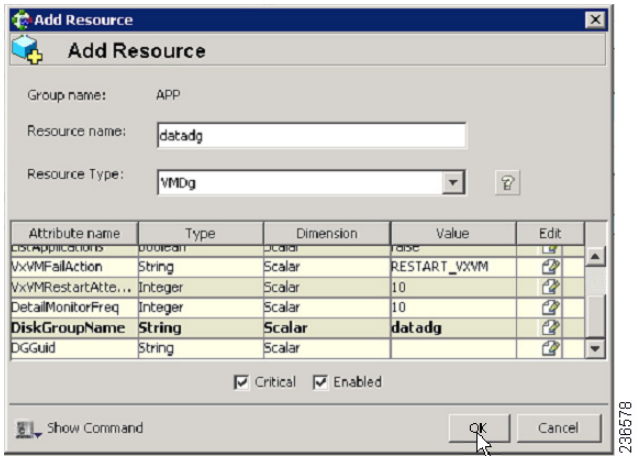
- Resource name = **APP_IP**
- Resource Type = **IP**
- Address = <Virtual IP address allocated for use by the Security Manager application> (defined as a Global attribute)
- SubNetMask = <subnet mask> (defined as a Global attribute)
- MACAddress = <MAC Address of the NIC used for accessing the Security Manager application>, (defined for each server in the cluster)



Step 4 Right-click the **APP** service group and select **Add Resource**.

Add the VMDg Resource and check the **Critical** and **Enabled** check boxes.

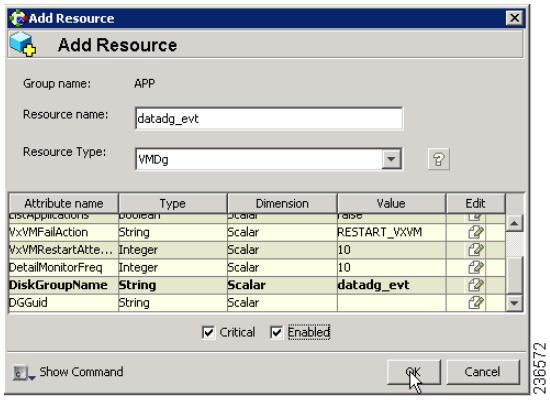
- Resource name = **datadg**
- Resource Type = **VMDg**
- DiskGroupName = **datadg**
  (defined as a Global attribute)



Step 5 Right-click the **VMDg** resource group and select **Add Resource**.

Add the datadg_evt resource and check the **Critical** and **Enabled** check boxes.

- Resource name = **datadg_evt**
- Resource Type = **VMDg**
- DiskGroupName = **datadg_evt**
  (defined as a Global attribute)



Step 6 Right-click the **APP** service group and select **Add Resource**.

Add the MountV Resource and check the **Critical** and **Enabled** check boxes.

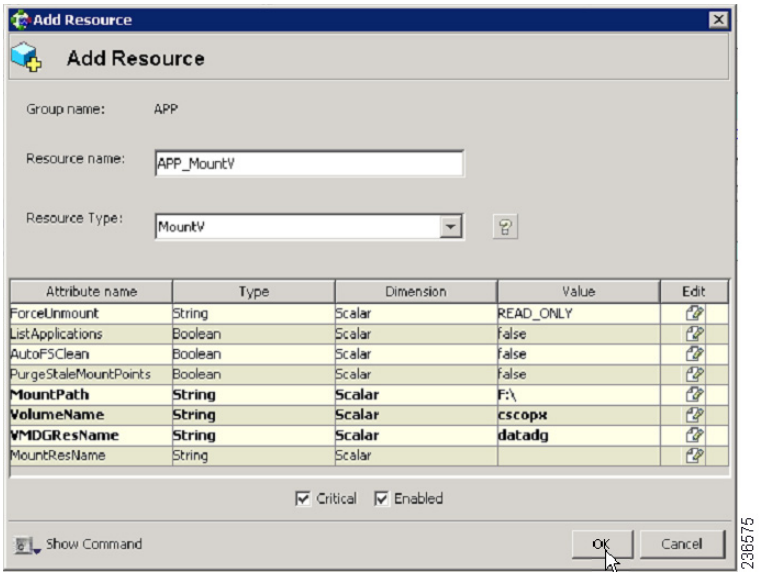
- Resource name = **APP_MountV**
- Resource Type = **MountV**

- MountPath = <Selected Drive Letter>:\
  (defined as a Global attribute)
- VolumeName = **cscopx**
  (defined as a Global attribute)
- VMDGResName = **datadg**
  (defined as a Global attribute)
- ForceUnmount = {NONE, READ-ONLY, ALL}

  Defines whether the agent unmounts the volume forcibly when it is being used by other applications. The following choices are available:

  - NONE: The agent does not unmount the volume if an application is accessing it.
  - READ-ONLY: The agent unmounts the volume if applications are accessing it in a read-only mode.
  - ALL: The agent unmounts the volume regardless of the type of access an application has.

  The default is NONE. If the volume cannot be unmounted, automatic failover to the secondary server might be prevented, so you might want to select a value of READ-ONLY or ALL.



Step 7 Right-click the **MountV** resource group and select **Add Resource**.

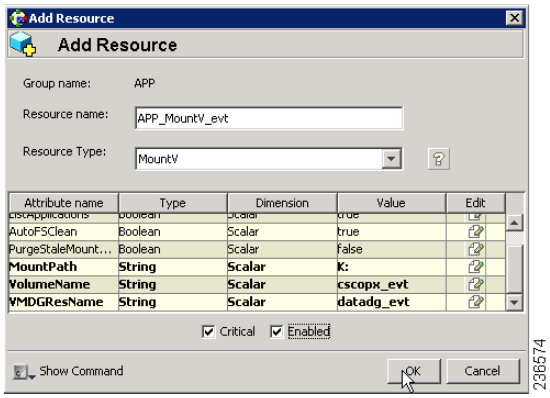
Add the MountV_evt Resource and check the **Critical** and **Enabled** check boxes.

- Resource name = **APP_MountV_evt**
- Resource Type = **MountV**
- MountPath = <Selected Drive Letter>:\
  (defined as a Global attribute)
- VolumeName = **cscopx_evt**
  (defined as a Global attribute)
- VMDGResName = **datadg_evt**
  (defined as a Global attribute)
- ForceUnmount = {NONE, READ-ONLY, ALL}

Defines whether the agent unmounts the volume forcibly when it is being used by other applications. The following choices are available:

- NONE: The agent does not unmount the volume if an application is accessing it.
- READ-ONLY: The agent unmounts the volume if applications are accessing it in a read-only mode.
- ALL: The agent unmounts the volume regardless of the type of access an application has.

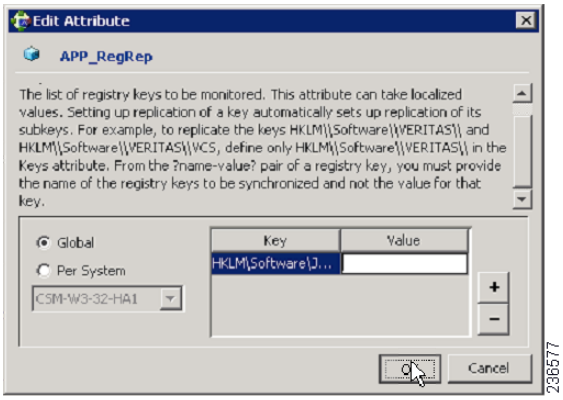
The default is NONE. If the volume cannot be unmounted, automatic failover to the secondary server might be prevented, so you might want to select a value of READ-ONLY or ALL.



Step 8 Right-click the **APP** service group and select **Add Resource**.

Add the RegRep resource and check the **Critical** and **Enabled** check boxes.

- Resource name = **APP_RegRep**
- Resource Type = **RegRep**
- MountResName = **APP_MountV**
  (defined as a Global attribute)
- ReplicationDirectory = **\REGREP\DEFAULT**
  (defined as a Global attribute)
- Keys (defined as a Global attribute)
  Key = **HKLM\Software\JavaSoft\Prefs\vms**
  Value = <blank>

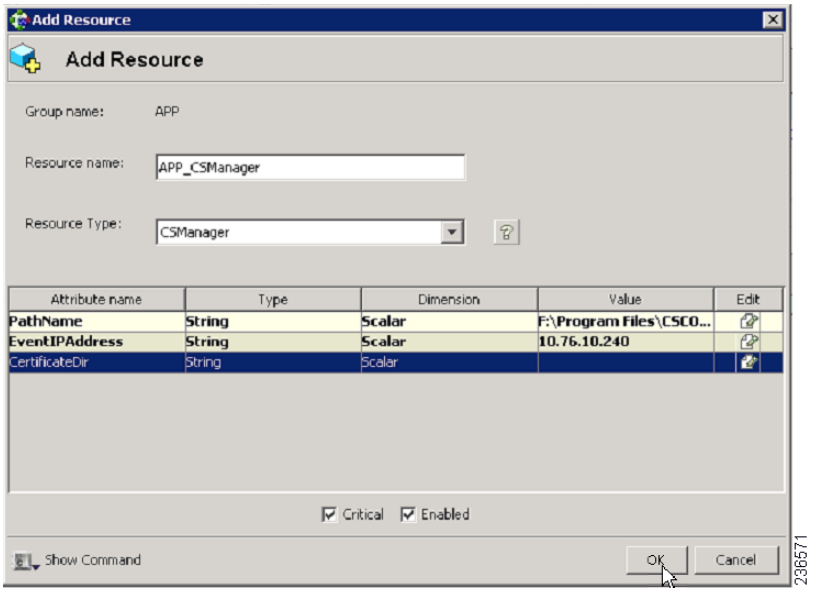


Note Security Manager stores client user preferences in the server registry under HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\vms. The registry replication agent (RegRep) monitors changes to the specified registry location on the active server and synchronizes these changes to a secondary server in the event of a failover.

Step 9 Right-click the **APP** service group and select **Add Resource**.

Add the CSManager resource and check the **Critical** and **Enabled** check boxes.

- Resource name = **APP_CSManager**
- Resource Type = **CSManager**
- PathName = **<Selected Drive Letter>:\Program Files\CSCOpx** (defined as a Global attribute)
- EventIPAddress = The same IP address as used in APP_IP (defined as a Global attribute)
- CertificateDir = See Security Certificates for SSL, page 4-2, for an explanation of this attribute.



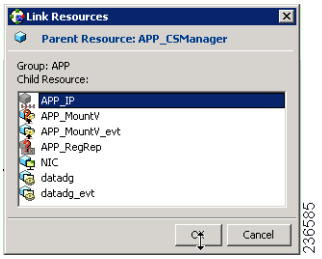
Step 10 Link the resources as defined in the following table (see Figure A-1 on page A-2).

Parent Resource	Child Resource
APP_CSManager	APP_RegRep
APP_CSManager	APP_IP
APP_IP	NIC
APP_RegRep	APP_MountV
APP_RegRep	APP_MountV_evt
APP_MountV	datadg
APP_MountV_evt	datadg_evt

To link resources, follow these steps:

a. Right-click the parent resource, and then select **Link**.

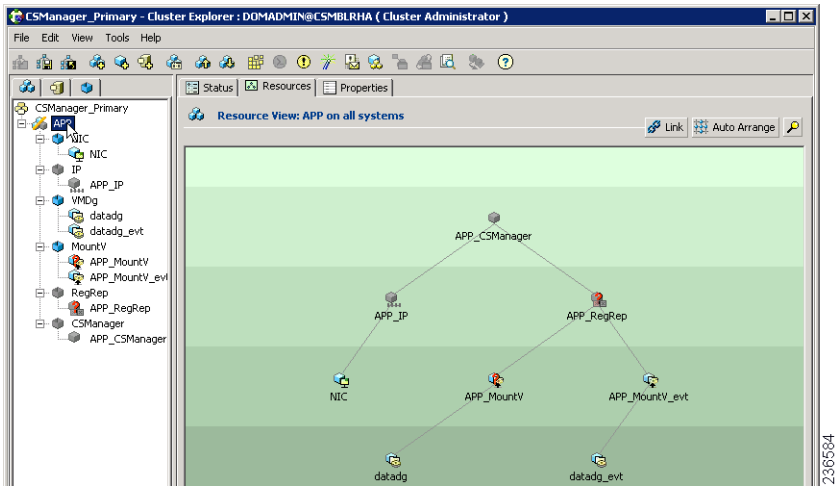
The Link Resources dialog box appears.



b. Select the child resource, and then click **OK**.

The selected resources are linked.

When all links have been made, your resource view should look like the following:



Creating the ClusterService Group (Optional)

You can optionally configure a ClusterService group to run the following optional components:

- Cluster Manager (Web Console)
- Notification

You can use the VCS Configuration wizard to configure these components. See the Veritas Cluster Server administrator's guide for details. The notification service is useful because it can notify you of events happening in the cluster either through email or SNMP traps.

Dual Geographic Cluster Configuration

This section covers the setup and configuration of two clusters geographically separated with a single node in each cluster.

Note You can also create dual geographic cluster configurations with multiple nodes within one or both clusters.

This section contains the following topics:

Creating the Primary and Secondary Clusters

To create the primary and secondary clusters, follow these steps:

Step 1 Create a cluster on the primary server (in the primary cluster) using the VCS Cluster Configuration wizard, where:

- Cluster Name = CSManager_Primary
- Cluster ID = 0

Step 2 Create a cluster on the primary server (in the secondary cluster) using the VCS Configuration wizard, where:

- Cluster Name = CSManager_Secondary
- Cluster ID = 1

Step 3 In the primary cluster, start the Cluster Manager by choosing **Start > All Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** and log in to the cluster.

Step 4 Using the Cluster Manager, import the **CSManager** resource type by choosing **File > Import Types**. Browse to the CSManagerTypes.cf file located under $VCS_ROOT\cluster server\conf\config and click **Import**.

Step 5 Repeat Steps 3 and 4 for the secondary cluster.

Creating the ClusterService Group

To create the ClusterService group, follow these steps:

Note Perform these steps on both the primary and secondary clusters.

Tip You can use the VCS Configuration wizard as an alternate method to the procedures in this section for creating the ClusterService group and wac resource for intercluster communications. You can also configure the optional Cluster Manager (Web Console) and Notification components with the VCS Configuration wizard. See the Veritas Cluster Server administrator's guide.

Step 1 Right-click the **CSManager** resource and select **Add Service Group**.

Add a service group called **ClusterService**.

Step 2 Right-click the **ClusterService** service group and select **Add Resource**.

Add the NIC resource:

- Resource name = **NIC**
- Resource Type = **NIC**
- MACAddress = <MAC Address of the NIC card>

Note You can find the MAC address associated with each Ethernet interface using the DOS-level command **ipconfig -all**.

Step 3 Right-click the **ClusterService** service group and select **Add Resource**.

Add the IP resource

- Resource name = **VCS_IP**
- Resource Type = **IP**
- Address = <Virtual IP address allocated for the cluster>
- SubNetMask = <subnet mask>
- MACAddress = <MAC Address of the corresponding NIC card>

Step 4 Right-click the **ClusterService** service group and select **Add Resource**.

Add the wac resource:

- Resource name = **wac**
- Resource Type = **Process**
- StartProgram = **C:\Program Files\Veritas\Cluster Server\bin\wac.exe**
- StopProgram = **C:\Program Files\Veritas\Cluster Server\bin\wacstop.exe**
- MonitorProgram = **C:\Program Files\Veritas\Cluster Server\bin\wacmonitor.exe**

Step 5 Link the resources as defined in the following table (see Figure A-4 on page A-4).

Parent Resource	Child Resource
wac	VCS_IP
VCS_IP	NIC

To link resources, follow these steps:

a. Right-click the parent resource, and then select **Link**.

The Link Resources dialog box appears.

b. Select the child resource, and then click **OK**.

The selected resources are linked.

Creating the Replication Service Group

To create the replication service group, follow these steps:

Note Perform these steps on both the primary and secondary clusters.

Step 1 Right-click the **CSManager** resource and select **Add Service Group**.

Add a service group called APPrep.

Step 2 Right-click the **APPrep** service group and select **Add Resource**.

Add the Proxy resource:

- Resource name = **VVR_NIC_Proxy**
- Resource Type = **Proxy**
- TargetResName = **NIC**

Step 3 Right-click the **APPrep** service group and select **Add Resource**.

Add the IP resource:

- Resource name = **VVR_IP**
- Resource Type = **IP**
- Address = <Virtual IP address allocated for replication>
- SubNetMask = <subnet mask>
- MACAddress = <MAC address of the corresponding NIC card>

Step 4 Right-click the **APPrep** service group and select **Add Resource**.

Add the VMDg resource:

- Resource name = **datadg**
- Resource Type = **VMDg**
- DiskGroupName = **datadg**

Step 5 Right-click the **APPrep** service group and select **Add Resource**.

Add the VvrRvg resource:

- Resource name = **APP_RVG**
- Resource Type = **VvrRvg**
- RVG = **CSM_RVG**
- VMDGResName = **datadg**
- IPResName = **VVR_IP**

Step 6 Link the resources as defined in the following table (see Figure A-3 on page A-3).

Parent Resource	Child Resource
VVR_IP	VVR_NIC_Proxy
APP_RVG	VVR_IP
APP_RVG	datadg

To link resources, follow these steps:

a. Right-click the parent resource, and then select **Link**.

The Link Resources dialog box appears.

b. Select the child resource, and then click **OK**.

The selected resources are linked.

Creating the Application Service Group

To create the application service group, follow these steps:

Note Perform these steps on both the primary and secondary clusters.

Step 1 Add a service group called APP.

Step 2 Right-click the **APP** service group and select **Add Resource**.

Add the RVG primary resource:

- Resource name = **APP_RVGPrimary**
- Resource Type = **RVGPrimary**
- RvgResourceName = **APP_RVG**

Step 3 Right-click the **APP** service group and select **Add Resource**.

Add the MountV resource:

- Resource name = **APP_MountV**
- Resource Type = **MountV**
- Mount Path = <Selected Drive Letter>:\

- Volume Name = **cscopx**
- VMDg Resource Name = **datadg**

Step 4 Right-click the **APP** service group and select **Add Resource**.

Add the RegRep resource and check the **Critical** and **Enabled** check boxes.

- Resource name = **APP_RegRep**
- MountResName = **APP_MountV**
- ReplicationDirectory = **\REGREP\DEFAULT**
- Keys = **HKLM\Software\JavaSoft\Prefs\vms**

Note Security Manager stores client user preferences in the server registry under HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\vms. The registry replication agent (RegRep) monitors changes to the specified registry location on the active server and synchronizes these changes to a secondary server in the event of a failover.

Step 5 Right-click the **APP** service group and select **Add Resource**.

Add the Proxy resource:

- Resource name = **APP_NIC_Proxy**
- Resource Type = **Proxy**
- TargetResName = **NIC**

Step 6 Right-click the **APP** service group and select **Add Resource**.

Add the IP resource:

- Resource name = **APP_IP**
- Resource Type = **IP**
- Address = <Virtual IP address allocated for the application>
- SubNetMask = <subnet mask>
- MACAddress = <MAC address of the corresponding NIC card>

Step 7 Right-click the **APP** service group and select **Add Resource**.

Add the CSManager resource:

- Resource name = **APP_CSManager**
- Resource Type = **CSManager**
- PathName = **<*Selected Drive Letter*>:\Program Files\CSCOpx**
- EventIPAddress = The same IP address as you used in APP_IP
- CertificateDir = See Security Certificates for SSL, page 4-2, for an explanation of this attribute.

Step 8 Link the resources as defined in the following table (see Figure A-2 on page A-3).

Parent Resource	Child Resource
APP_MountV	APP_RVGPrimary
APP_RegRep	APP_MountV
APP_CSManager	APP_RegRep

Parent Resource	Child Resource
APP_IP	APP_NIC_Proxy
APP_CSManager	APP_IP

To link resources, follow these steps:

a. Right-click the parent resource, and then select **Link**.

   The Link Resources dialog box appears.

b. Select the child resource, and then click **OK**.

   The selected resources are linked.

Creating the Cluster Level Configuration

To create the cluster level configuration, follow these steps:

Step 1 Link the APP service group as the parent of the APPrep service group with an online local firm dependency. Perform this step on both the primary and secondary clusters.

Step 2 Under the cluster properties specify the cluster address, which is the same IP address that you used in the VCS_IP resource.

Step 3 From the primary cluster, choose **Edit > Add/Delete Remote Cluster** to use the Remote Cluster Configuration wizard to add the secondary cluster.

Step 4 From the primary cluster, choose **Edit > Configure Global Groups** to use the Global Group Configuration wizard to configure the APP service group as a global group.

See Figure A-5 on page A-4.