



# APPENDIX **E**

## Veritas Cluster Server

---

This module provides basic guidelines for the Veritas Cluster Server (hereafter VCS) configuration in an SM cluster installation. It assumes basic knowledge of the VCS environment; it does not replace the VCS user guide. This module does not cover installation of the cluster or of the SM cluster agents.

This module lists the software and hardware system requirements for the VCS. It also gives a systematic explanation on how to configure the SM cluster using the VCS configuration tools. Most of the examples are taken from the use of the Java Veritas Manager GUI, although the operations can also be done via the Veritas command-line utilities.

The SM supports Veritas Cluster Server version 3.5 and 4.1 on Solaris machines and Veritas Cluster Server version 2.2 and 4.1 on Red-Hat Linux machines.

Veritas Software was acquired by Symantec. Currently, the cluster solution is still called the Veritas Cluster Server.

- [Information About Veritas Cluster Servers, page E-1](#)
- [How to Configure the SM Cluster Resources, page E-5](#)
- [How to Add SM Cluster Resources, page E-8](#)
- [Useful Operations, page E-15](#)
- [Linking the Resources, page E-19](#)
- [Verifying that the Service Group is Online, page E-20](#)
- [SNMP Support, page E-20](#)
- [How to Configure the SnmpConsole Attribute, page E-23](#)

## Information About Veritas Cluster Servers

- [Veritas Cluster Server System Requirements, page E-2](#)
- [Veritas Cluster Server Nodes on Remote Sites, page E-2](#)
- [Replication Configuration Guidelines, page E-3](#)

## Veritas Cluster Server System Requirements

For your convenience, the following Veritas Cluster Server System Requirements have been taken from the Veritas site:

<http://www.veritas.com>

- Supported Platforms:
  - Sun Solaris 8, 9, 10
  - Red Hat Linux 3.0, 4.0
- Networking:
  - Public Network: 10 MB/100 MB/Gigabit Ethernet
  - Private Network: 10 MB/100 MB/Gigabit Ethernet
- Ethernet Controllers:
  - Requires at least three independent Ethernet connections per system
- Memory:
  - Each VERITAS Cluster Server system requires at least 128 MB of RAM (256 MB of RAM is recommended)
- Supported Server Hardware:
  - Please refer to <http://support.veritas.com> or contact your VERITAS sales representative for the latest list of certified server hardware.
    - Sun Solaris 8, 9, 10
    - Red Hat Linux 2.1, 3.0, 4.0
- Supported Storage Hardware:
  - Please refer to <http://support.veritas.com> or contact your VERITAS sales representative for the latest list of certified storage hardware.
    - Sun
    - Red Hat Linux

## Veritas Cluster Server Nodes on Remote Sites

The heartbeat links use the Low Latency Transport (LLT) Ethernet/dlpi protocol. It uses Ethernet broadcasts and must be on the same broadcast network. A separate layer-2 switch per heartbeat link is supported. The distance limitation is based on performance. A number of factors govern cluster distance. The primary factors for LLT are network connectivity and latency. Direct L2 low latency connections must be provided for LLT with a maximum round-trip time of 500 milliseconds. Large campus clusters or metropolitan area clusters must be very carefully designed to provide two completely separate paths for heartbeat to prevent a single fiber optic or fiber bundle failure from removing the heartbeat links.

Although the database replication network uses IP as its transport, it must have two separate connection paths between the nodes that provide at least 10Mbps for the subscriber data replication.

When planning an SM Cluster setup where the nodes are at a distance from each other, please consult the Veritas support.

## Replication Configuration Guidelines

- [Replication Scheme Setup, page E-3](#)
- [Replication Network Configuration, page E-3](#)
- [Veritas Cluster Server Configuration Guidelines, page E-5](#)

### Replication Scheme Setup

After the replication network has been setup (as described in the [Replication Network Configuration, page E-3](#) section), the replication scheme needs to be set to the database. Setting the replication scheme is performed using the **p3db** CLU:

```
>p3db --set-rep-scheme
```

This operation configures the database to send every subscriber-data update to the peer machine.

If the setup operation fails because there might be an existing replication scheme already set, run the following CLU to drop the previous replication scheme and then set the new scheme:

```
>p3db --drop-rep-scheme
```

By configuring and running the VCS agent of the replication agent or by running the **p3db --rep-start** CLU, the replication agent starts its work.

### Replication Network Configuration

The configuration of the replication private network between the two SMs of the cluster must be carefully planned. This section discusses some of the guidelines for performing the configuration.

The TimesTen replication agent uses hostnames to implement fail-over between the two replication NICs. The agent uses the first IP address of the hostname supplied to the agent to connect to the other agent. If the connection fails and cannot be reconstructed on the first IP, the replication agent tries the next IP addresses assigned to this hostname, and so on.

Editing the `/etc/hosts` file to assign hostnames to IP addresses.

You **must** use the predefined hostnames `SM_REP1` and `SM_REP2` as the hostnames for replication.

**Note**

---

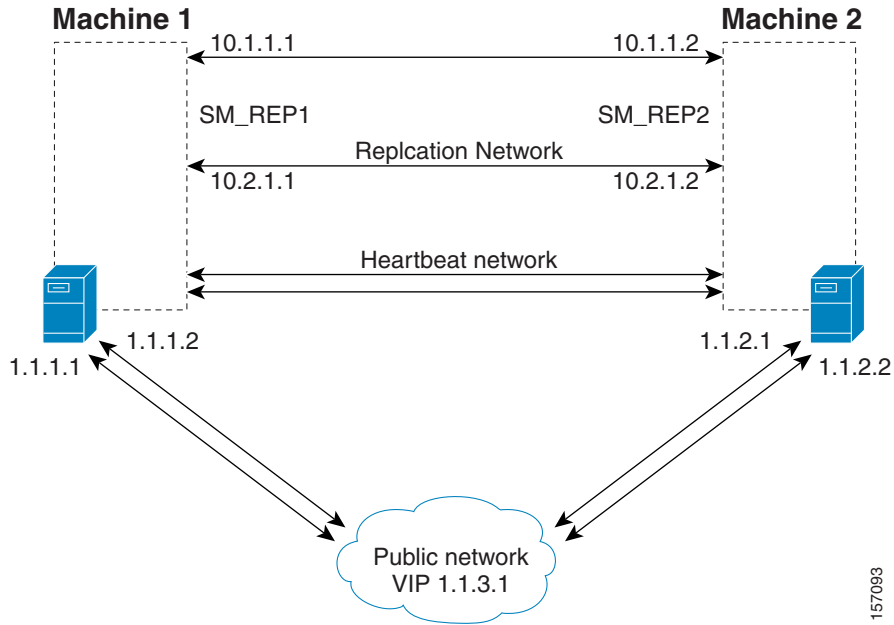
Verify in the OS configuration files that the `/etc/hosts` file is used before using a name server.

---

**Example:**

The following figure shows an example of a replication network.

**Figure E-1 Veritas Network Replication Configuration**



To configure the replication network shown by the above figure, do the following:

- Configure the IP addresses of each of the replication NICs, each one in a different network. In this example, the IP addresses of the Machine1 replication NICs are 10.1.1.1 and 10.2.1.1.
- Assign a hostname *SM\_REP1* to both of the local replication NIC IP addresses. In this example, the hostname *SM\_REP1* is assigned to the IP addresses of the replication NICs on Machine1. In the */etc/hosts* file, be sure to also assign the local hostname (Machine1) to the local replication NICs. Ensure that there are no empty lines between the lines containing the local hostname.
- Assign a hostname *SM\_REP2* to both of the remote replication NIC IP addresses. In this example, the hostname *SM\_REP2* is assigned to the IP addresses of the replication NICs of Machine2
- The */etc/hosts* file on Machine1 should appear as follows:

```
127.0.0.1 localhost
1.1.1.1 Machine1 loghost
10.1.1.1 Machine1 SM_REP1 REP_1_NIC_1
10.2.1.1 Machine1 SM_REP1 REP_1_NIC_2
10.1.1.2 SM_REP2 REP_2_NIC_1
10.2.1.2 SM_REP2 REP_2_NIC_2
```

- The */etc/hosts* file on Machine2 should appear as follows:

```
127.0.0.1 localhost
1.1.2.1 Machine2 loghost
10.1.1.2 Machine2 SM_REP2 REP_2_NIC_1
10.2.1.2 Machine2 SM_REP2 REP_2_NIC_2
10.1.1.1 SM_REP1 REP_1_NIC_1
10.2.1.1 SM_REP1 REP_1_NIC_2
```



**Note**

Make sure the system uses the */etc/hosts* file before it performs DNS or any other name service operation.

## Veritas Cluster Server Configuration Guidelines

The following procedures assume that the following operations were performed before starting the VCS configuration:

- Installation of the VCS on both machines. As part of this installation:
  - Each machine was given a hostname, which is used as the *system* name for the VCS configuration.
  - The machines are configured to recognize each other's hostname.
- An IP address was allocated for the cluster (hereafter, *the cluster's IP*).
- The SM and the TimesTen database were installed on both machines.
- The SM VCS agents were installed on each machine.
- The VCS manager Java console was installed on the administrator PC.

Note that in an SM cluster, two SM machines are connected to each other in a fully redundant way. The connection uses four cables: two for the VCS heartbeat mechanism, and two for the TimesTen database replication mechanism. Each machine is connected to the network via one of two redundant NICs. To access the cluster, you should use the *cluster IP address*, which is a virtual IP managed by the VCS. For management operations, you should use the local IP address of each machine.

## How to Configure the SM Cluster Resources

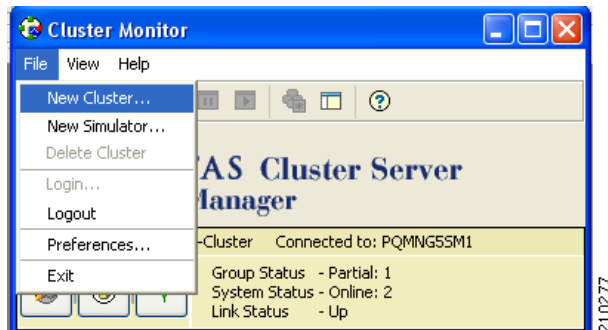
To configure the VCS with the SM cluster resources, perform the procedures described in the following sections.

- [Adding Clusters, page E-6](#)
- [Adding Service Groups, page E-7](#)
- [Setting Auto-start, page E-8](#)

## Adding Clusters

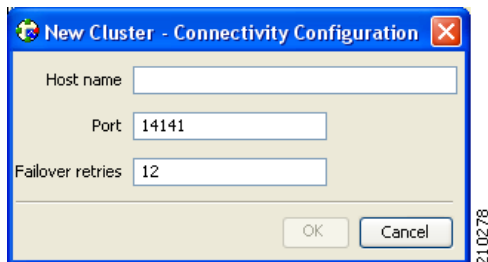
- Step 1** Open the VCS cluster manager Java console by choosing **Start >Programs >Veritas Cluster Manager >Cluster Manager (Java console)**.
- Step 2** Add a new cluster by choosing **File >New Cluster**

**Figure E-2 Cluster Monitor: New Cluster**



- Step 3** Configure the cluster

**Figure E-3 Adding a Cluster**



- Cluster Alias—cluster name
- Host Name—one of the machine's IP addresses or hostname.

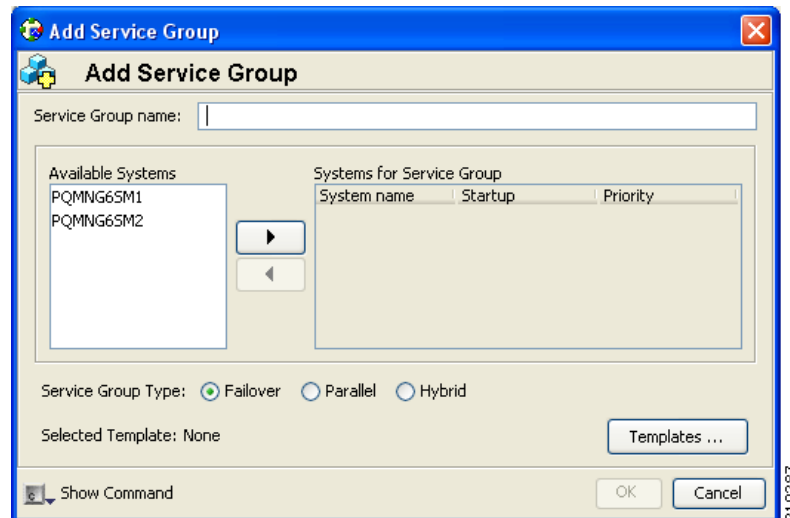
- Step 4** Log in to the cluster.

## Adding Service Groups

- Step 1** In the cluster explorer, from the service group tab, right-click the cluster, and choose **Add Service Group**.

The Add Service Group window appears.

**Figure E-4** Adding a Service Group



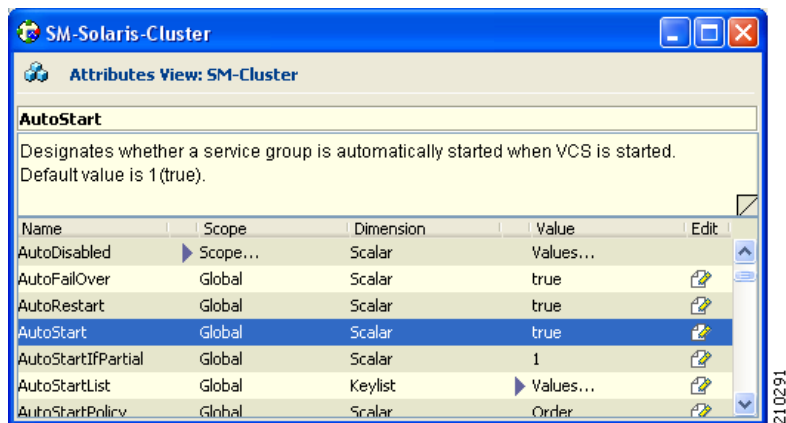
- Step 2** Enter a name for the service group.
- Step 3** Add the two machines as part of the service group and define their priority in the cluster.
- Step 4** Click **OK**.

## Setting Auto-start

This section describes how to set the auto-start parameters that define which machine will start after a boot of both nodes. If these parameters are not set, then at boot of both nodes the cluster will stay offline.

- Step 1** From the service group display, click **Show All Attributes**.
- Step 2** Make sure that both nodes are defined in the AutoStartList.

**Figure E-5 AutoStart List**



- Step 3** Specify which node will start by defining the **AutoStartPolicy** parameter.
- Step 4** Make sure that the AutoStart parameter is set to **true** (if **false**, both nodes will come up as standby).

## How to Add SM Cluster Resources

This section describes how to add the various SM cluster resources.

- [Adding Resources - General Guidelines, page E-9](#)
- [Adding Network NICs, page E-10](#)
- [Adding Network VIPs, page E-12](#)
- [Adding SM Resources, page E-13](#)
- [Adding TimesTen Daemon Resources, page E-14](#)
- [Adding TimesTen Replication Agent Resources, page E-15](#)



## Adding Resources - General Guidelines

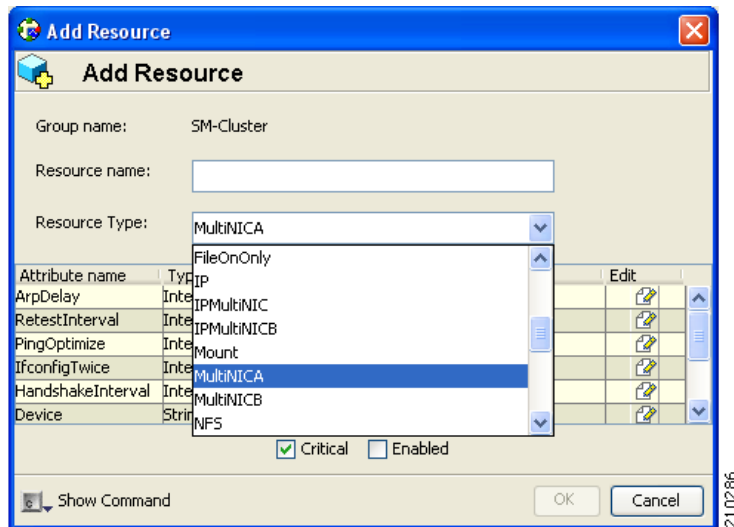
- Step 1** From the right-click menu of the service group, click **Add Resource**.

**Figure E-6** Adding Resources - General Guidelines



The Add Resource screen appears.

**Figure E-7** Adding Multi NICA Resource: Select MultiNICA



- Step 2** On the Add Resource screen, from the Resource Type drop-down list choose the resource type and give the resource a name.
- Step 3** Configure any required attributes.
- Step 4** When you are finished, click **OK**.

## Adding Network NICs

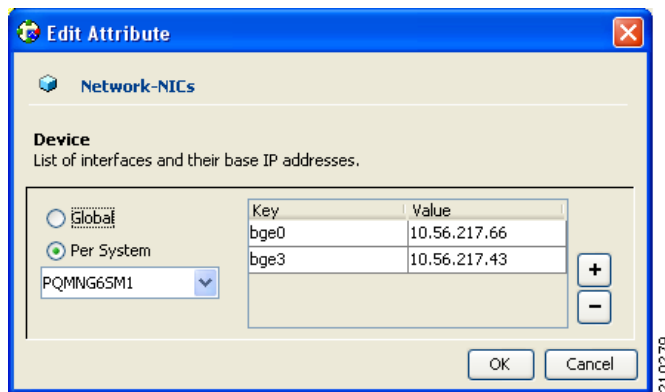
- Step 1** Decide which two network interfaces to use for the network connection.
- Step 2** Add a MultiNICA resource called *Network-NICs* to the service group.
- Step 3** Define the Device and NetMask parameters.
- Device—Write the names of the Network NICs in the KEY column and their corresponding IP addresses in the VALUE column.



**Note** Use the LOCAL option and configure each machine separately, because the IP addresses are different in each machine.

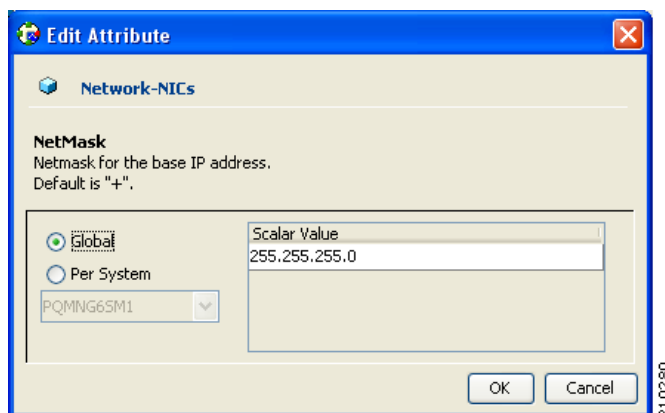
- In the following example, **bge0** and **bge3** are the network NICs.

**Figure E-8** Adding Network NIC: Device Attribute



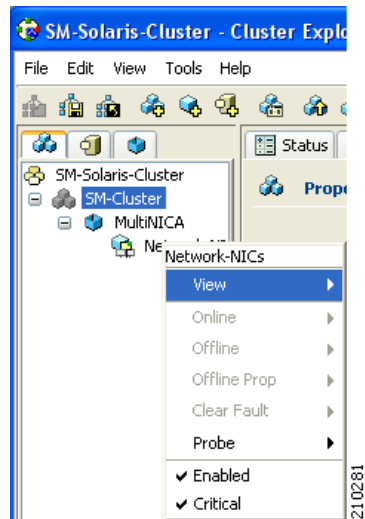
- NetMask—Assign a relevant network mask. For example, 255.255.255.255 can be defined as a network mask.

**Figure E-9** Adding Network NIC: NetMask Attribute



**Step 4** Click the **Enabled** and **Critical** attributes of the resource.

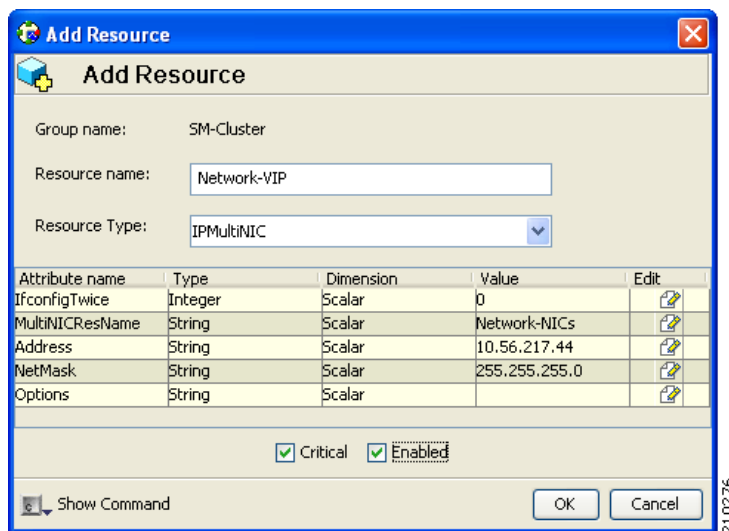
**Figure E-10** Adding Network NIC: Setting Attributes



## Adding Network VIPs

- Step 1** Decide on the IP address of the cluster.
- Step 2** Add an IPMultiNIC resource called *Network-VIP* to the service group.
- Step 3** Define the Address, Net-mask, and MultiNICAResName parameters.
- Address—Type the Cluster IP address.
  - Net-mask—Type the network-mask you want to use for this IP.
  - MultiNICAResName—Type *Network-NICs* to specify the relevant NICs.

**Figure E-11** Adding Network VIP Resource

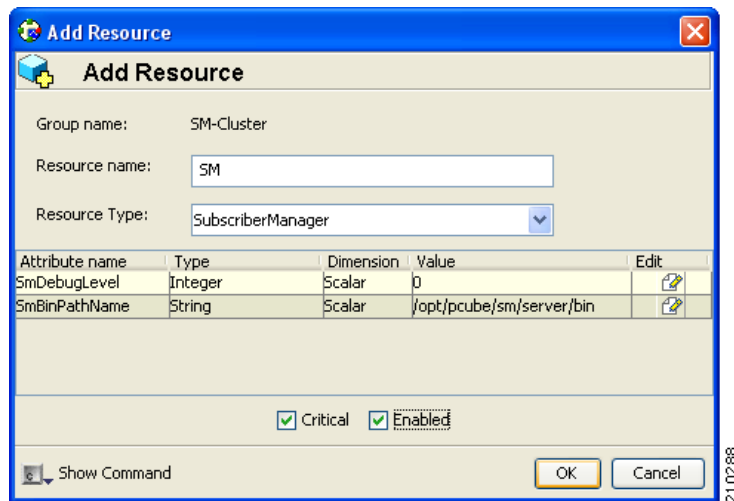


- Step 4** Check the **Enabled** and **Critical** check boxes.  
See [Figure E-10](#)

## Adding SM Resources

- Step 1** Import the SubscriberManager agent's type from file `/opt/VRTSvcs/bin/SubscriberManager/SubscriberManager.cf`.
- Step 2** Add a SubscriberManager resource called *SM* to the service group.
- Step 3** Define the `SmBinPathName` and `SmDebugLevel` parameters.
- `SmBinPathName`—Type the path to the bin directory under the SM installation directory; for example, `/opt/pcube/sm/server/bin/`.
  - `SmDebugLevel`—Type a number between 1 and 4 to view debug messages, type 0 to disable debug messages.

**Figure E-12** Adding SM Resource



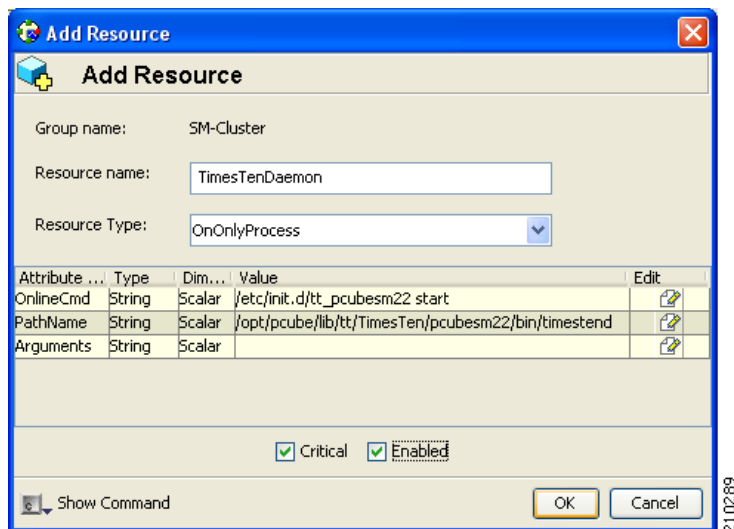
210286

## Adding TimesTen Daemon Resources

- Step 1** Import the OnOnlyProcess agent's type from file `/opt/VRTSvcs/bin/OnOnlyProcess/OnOnlyProcess.cf`.
- Step 2** Add an OnOnlyProcess resource called *TimesTenDaemon* to the service group.
- Step 3** Define the OnlineCmd, PathName, and Arguments parameters.
- OnlineCmd—Type the TimesTen Daemon start command: `/etc/init.d/tt_pcubesm22 start`.
  - PathName—Type the TimesTen Daemon process path; for example, `/opt/pcube/lib/tt/TimesTen/pcubesm22/bin/timestend`.
  - Arguments—To view the arguments, run the following command of the machine:  

```
ps -eaf | grep timestend
```
  - For example, the arguments can be: `-initfd 13`

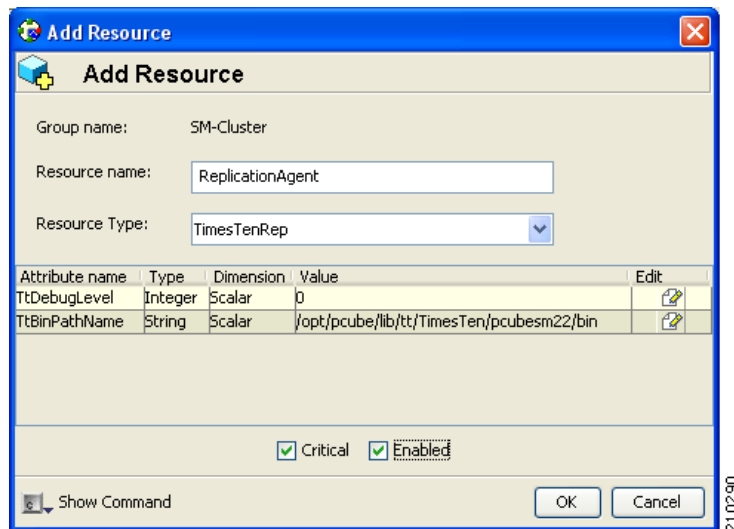
**Figure E-13** Adding TimesTenDaemon Resource



## Adding TimesTen Replication Agent Resources

- Step 1** Import the TimesTenRep agent's type from file `/opt/VRTSvcs/bin/TimesTenRep/TimesTenRep.cf`.
- Step 2** Add a TimesTenRep resource called `ReplicationAgent` to the service group.
- Step 3** Define the `TtBinPathName` and `TtDebugLevel` parameters.
- `TtBinPathName`—Type the TimesTen bin directory path; for example, `/opt/pcube/lib/tt/TimesTen/pcubesm22/bin`.
  - `TtDebugLevel`—Type a number in the range of 1-4 for viewing debug messages; enter 0 for disabling the debug messages.

**Figure E-14** Adding TimesTen Replication Agent



## Useful Operations


The following sections are useful operations for the management of the VCS.

- [Logging into the Cluster, page E-16](#)
- [Saving the Configuration, page E-16](#)
- [Closing the Configuration, page E-16](#)
- [Importing Types, page E-17](#)

## Logging into the Cluster

After you add a cluster, you are required to log in to the cluster.

---

**Step 1** Click the  icon.

A login window appears.


**Step 2** Log in with the initial user and password.  
The initial user is *admin* , the initial password is *password* .

---

## Saving the Configuration

Before exiting the VCS make sure to save your configuration; otherwise, your configuration will be lost.

---


**Step 1** Click the  icon, or choose **File >Save Configuration**.

---

## Closing the Configuration

Before exiting the VCS, make sure your configuration is closed. Some operations (like rebooting the system) could fail or cause a configuration conflict if performed while the configuration is in read/write mode.

---

**Step 1** Click the  icon, or choose **File >Close Configuration**.

Before exiting the VCS, make sure your configuration is closed. Some operations (like rebooting the system) could fail or cause a configuration conflict if performed while the configuration is in read/write mode.

---



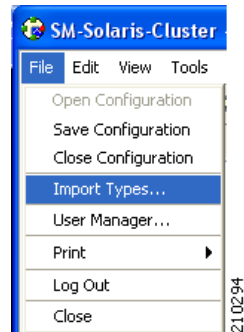
## Importing Types

To configure the SM Veritas agents, you first have to import the type file of these agents.

**Step 1** From the File menu, choose **Import Types**.

A navigation window appears:

**Figure E-15** *Importing Types*

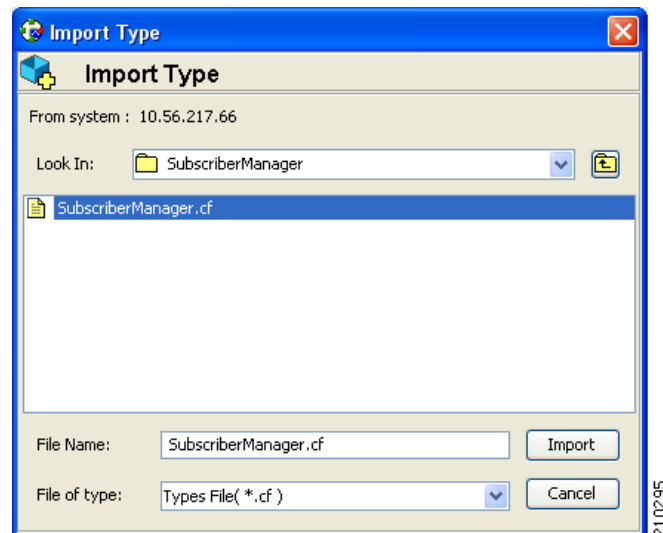


The window allows you to navigate through one of the cluster-system's file system.

**Step 2** Go to the agent directory under `/opt/VRTSvcs/bin/<agent-dir>`.

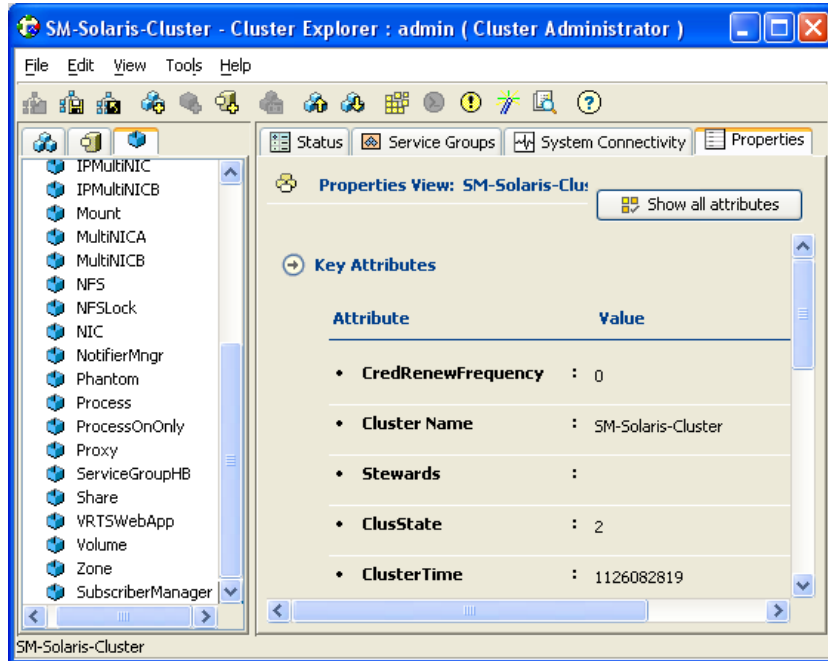
In the agent directory there is a file with a `.cf` extension.

**Figure E-16** *Importing Types: Select File*



- Step 3** Select the file with the **.cf** extension.  
The resource parameters are shown in the following window.

**Figure E-17** *Importing Types: Resource Parameters*



210206

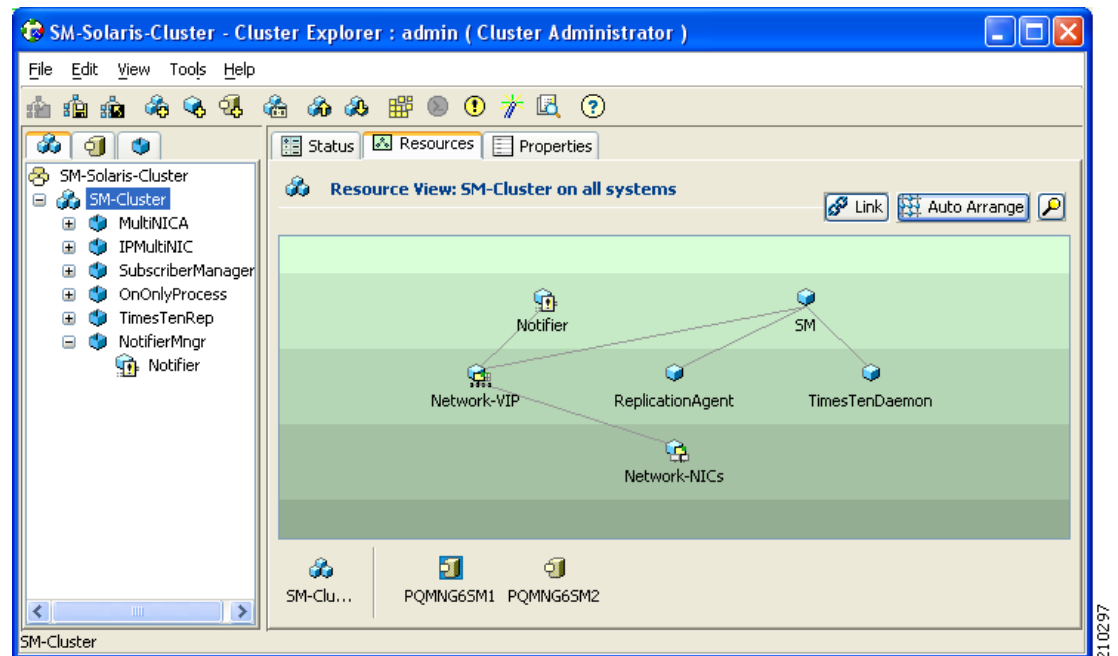
# Linking the Resources

Linking the resources defines the order of becoming online and going offline.

- Step 1** Select the service group and enter the **Resources** tab.
- Step 2** To link two resources, click once on one resource, pull the line to the second resource, and click once over the icon of the second resource.

The final links should look like those in the following figure.

**Figure E-18** *Linked Resources*



210297

## Verifying that the Service Group is Online

**Step 1** Check that all of the resources are online/offline according to the system and the resource type.

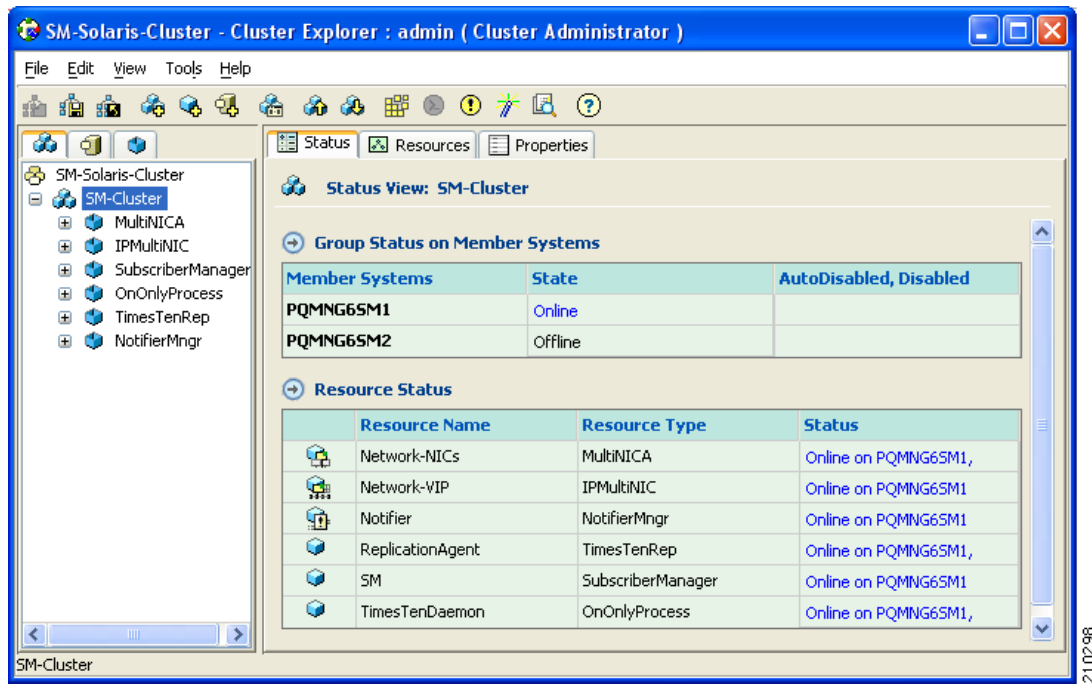


**Note**

The TimesTen Daemon, the NICs, and the TimesTen Replication Agent should all be online on all of the systems.

The state should be similar to the following figure.

**Figure E-19** Verifying Service Group is Online



## SNMP Support

VCS provides a method for notifying the user of important events such as a resource or system fault. For this purpose, VCS supplies a NotifierMngr agent that enables the reception of messages from VCS and the delivery of those messages to SNMP consoles. This section describes configuring NotifierMngr in order to enable SNMP support.

- [Configuring NotifierMngr, page E-21](#)
- [Adding NotifierMngr Resource, page E-21](#)
- [Configuring the NotifierMngr Attributes, page E-22](#)

## Configuring NotifierMngr

Add and configure NotifierMngr using either the command line or the Cluster Manager Java Console.

When started from the command line, Notifier is a process that VCS does not control.

For best results, use the NotifierMngr agent bundled with VCS to configure Notifier as part of a highly available service group, which can then be monitored, brought online, and taken offline.

The following sections describe the configuration process using the Cluster Manager Java Console.

## Adding NotifierMngr Resource

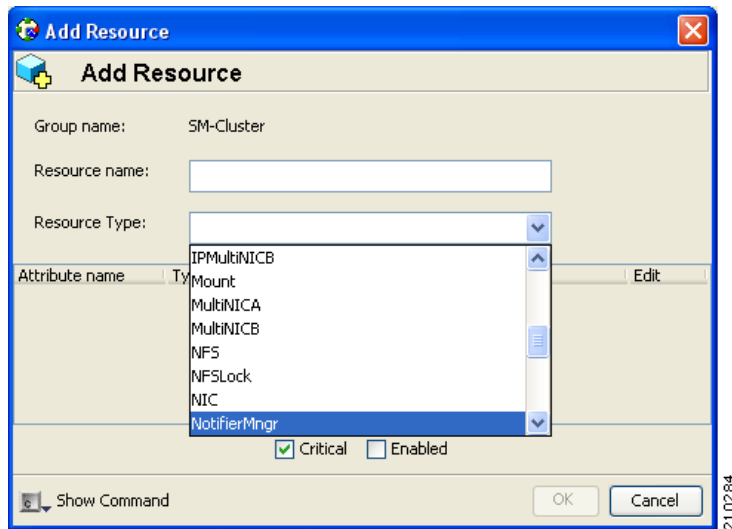
- Step 1** Add a NotifierMngr resource called *Notifier* to the service group.

**Figure E-20** Adding Notifier Manager Resource: Add Resource



The Add Resource screen appears.

**Figure E-21** Adding Notifier Manager Resource: Select NotifierMngr



- Step 2** From the Add Resource screen, choose **NotifierMngr** as the resource type.

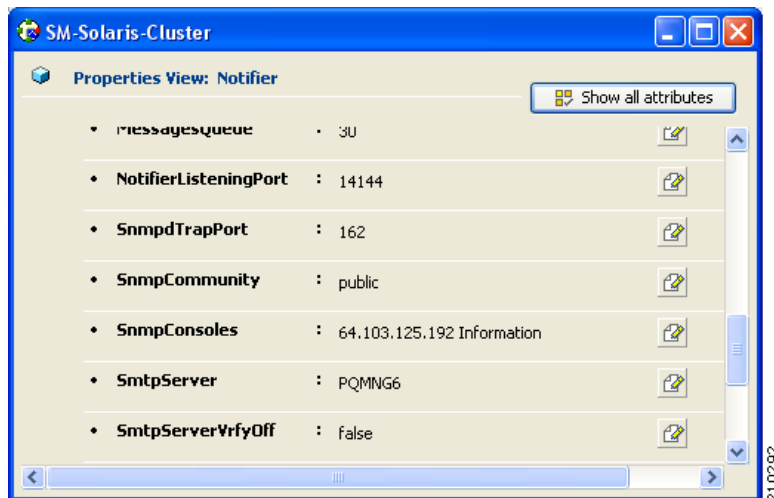
## Configuring the NotifierMngr Attributes

After adding the NotifierMngr resource, configure its attributes.

**Step 1** Select NotifierMngr as the resource type.

The following screen appears.

**Figure E-22** Configuring Notifier Manager Attributes



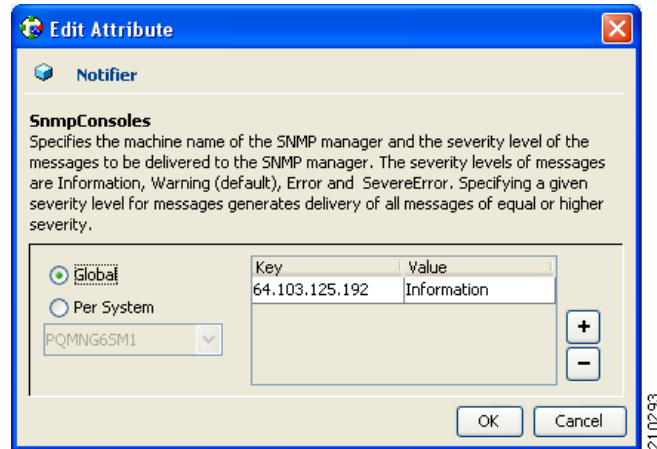
**Step 2** Define the SnmpConsoles, SnmpdTrapPort, and SnmpCommunity parameters.

- SnmpConsoles—Specify the machine name of the SNMP manager and the severity level of messages to be delivered to the SNMP manager. The severity levels of messages are Information, Warning, Error, and SevereError. Specifying a given severity level for messages generates delivery of all messages of equal or higher severity.
- SnmpdTrapPort—Specify the port to which the SNMP traps are sent. The value specified for this attribute is used for all consoles if more than one SNMP console is specified. The default is **162**.
- SnmpCommunity—Specify the community ID (a string scalar) for the SNMP manager. The default is **public**.

# How to Configure the SnmpConsole Attribute

The SnmpConsole attribute specifies the IP addresses to which you want the SNMP traps to be sent. You can specify different trap severity for each IP address:

**Figure E-23** Configuring SNMP Console Attributes



## Linking to IPMultiNIC

### Viewing Traps

After adding and configuring NotifierMgr, it will send traps according to the configured severity to the destinations configured by the SnmpConsole Attribute.

View these traps using SNMP trap viewer/MIB Browser (for example, AdventNet MibBrowser).

For a complete list of traps/severities, please see Chapter 10 of the VERITAS Cluster Server User Guide.

- 
- Step 1** Using the resources viewer, connect the *Notifier* to the *Network-VIP* resource so that it will be online after the VIP.

For more information, see [Figure E-14](#) in Adding TimesTen Replication Agent Resources.

---

