

Chapter 17

Configuring NIC Host Redundancy

Typically, you use network information collector (NIC) replication rather than NIC host redundancy to maintain high availability for NIC. NIC replication lets you share system load between NIC hosts and is simpler to configure and maintain than NIC redundancy. NIC redundancy is provided for backward compatibility. For information about NIC replication, see *Chapter 9, Locating Subscriber Information with the NIC*.

Topics include:

- Overview of NIC Host Redundancy on page 271
- Before You Configure NIC Host Redundancy on page 272
- Configuring NIC Host Redundancy on page 272
- Configuring Monitors on page 275
- Optimizing Performance of the NIC Proxy for NIC Host Redundancy on page 280
- Viewing Log Files for NIC Hosts and Monitors from the Solaris CLI on page 282
- Clearing Persistent Data and Logs for NIC Hosts and NIC Monitors on page 282

Overview of NIC Host Redundancy

NIC host redundancy is available only on installations on Solaris platforms. You configure NIC host redundancy from the SDX Configuration Editor and from the local configuration tool for NIC monitors. You cannot configure NIC host redundancy from the CLI.

In NIC host redundancy, two NIC hosts with the same configuration act as a redundant pair. One host assumes the active role, and the other the passive role. If the active host fails, the passive host writes its Common Object Request Broker Architecture (CORBA) object reference to the directory and assumes the active role. The former active host reassumes the active role only when the current active host fails. Each pair of redundant hosts constitutes a *community*.

You can also add a *monitor*, which tracks the redundant components, to that community. The SRC software includes a NIC monitor component; you can install one NIC monitor on a machine. You can then add that monitor to the directory and use it in a host redundancy configuration.

The monitor acts on behalf of a client or server that is not part of the community. If the client or server cannot communicate with the active host in the community but the hosts can communicate with each other, the monitor prompts the passive host to assume control. Without the monitor, the passive host would not assume control, and the host would be unavailable.

The members in the community exchange keepalive messages to monitor each other's availability. If a member does not receive a keepalive message from another member during the specified time, the first member assumes that the second member is unavailable.

For an example of NIC host redundancy, see the network configuration for the OnoPopAllRealms distributed configuration shown in *Chapter 21, NIC Configuration Scenarios*. The monitor BOClient is installed on the same machine as the NIC proxy and tracks the communications between the hosts OnePopBO/One and OnePopBO/Two. If the monitor detects that the connection to the active host is unavailable, it prompts the passive host to assume control.

Before You Configure NIC Host Redundancy

If a directory does not support multimaster replication on the same machine as the NIC host, use NIC replication rather than NIC host redundancy. Without multimaster replication on the same machine, the NIC host must write its CORBA object references to the directory only when you start the NIC host, therefore a directory failure is unlikely to affect the operation of the NIC.

Before you configure NIC host redundancy, make sure that:

- NIC host software is installed on two separate machines for each set of NIC hosts to act as a redundant pair.
- Redundancy monitor software is installed on each system that is to act as a NIC monitor.

Usually, you install the monitor on the same machine as the SAE. A machine can support only one monitor.

Configuring NIC Host Redundancy

To configure NIC host redundancy, complete the following tasks:

1. Configuring Redundant Hosts on page 273
2. Configuring Communities on page 274

Configuring Redundant Hosts

If you use NIC host redundancy, configure two redundant hosts for each host.

To use SDX Configuration Editor to configure redundant hosts:

1. In the navigation pane, select a configuration file for the NIC.
2. Select the **Hosts** tab, expand a section for a host, and then expand the **Redundant Hosts** section.
3. Create a new instance of a redundant host.

4. In the Redundant Host section, edit the fields.
See *Redundant Hosts Fields* on page 273.
5. Repeat Steps 2 to 4 to create the other redundant hosts.
6. Select **File > Save**.
7. Right-click the configuration file, and select **SDX System Configuration > Export to LDAP Directory**.

Redundant Hosts Fields

In SDX Configuration Editor, you can modify the following fields in the Redundant Hosts section of the Hosts pane in a NIC configuration file.

Redundancy Community

- Path to the community to which the redundant host belongs.
- Value—Path to community
 - Path is relative to the Static Configuration object.
 - Subfolders in a path are separated by the forward slash (/).
- Example—/communities/nicsae

Hot Standby Agents

- List of paths to redundant agents for SAE plug-in agents supported by the redundant hosts.
- Value—Comma-separated list of paths to agents
 - Path is relative to the Static Configuration object.
 - Subfolders in a path are separated by the forward slash (/).
- Example—agents/IpVr/demo, agents/DnVr/demo

Hosted Agents

- List of paths to agents and redundant agents supported by the redundant hosts.
- Value—Comma-separated list of paths to agents
 - Path is relative to the Static Configuration object.
 - Subfolders in a path are separated by the forward slash (/).
- Example—agents/IpVr, agents/IpVr/demo, agents/DnVr, agents/DnVr/demo, agents/PoolVr

Configuring Communities

To use SDX Configuration Editor to configure a community for NIC host redundancy:

1. In the navigation pane, select a NIC configuration file.
2. Select the **Redundancy** tab, expand the **Communities** section, and create a new instance of a community.

The screenshot shows a software interface with a 'Communities' section. Under 'Communities', there is a 'Community (nicsae)' entry. Below this entry, there are two input fields: 'Community Members' and 'Keep Alive Time'. Above these fields, there are two buttons: 'Create a New Instance of' and 'Delete an Instance', each with a small checkmark icon.

3. In the Communities section, edit the values for the fields.
See *Communities Fields* on page 275.
4. Select **File > Save**.
5. Right-click the configuration file, and select **SDX System Configuration > Export to LDAP Directory**.

Communities Fields

In SDX Configuration Editor, you can modify the following fields in the Communities section of the Redundancy pane in a NIC configuration file.

Community Members

- List of community members—either two redundant hosts or two redundant agents plus an optional monitor.
- Value—Text string
 - For hosts—Name of the redundant host in the format `<primaryHostName> / <redundantHostName>`
 - For agents—Name of the redundant host that supports the redundant agent in the format `<primaryHostName> / <redundantHostName>`
 - For monitor—Name of the monitor; must match the name specified in the monitor process (see *Configuring a Monitor Process* on page 277)
- Example—`DemoHost/One, DemoHost/Two, DemoMonitor`

Keep Alive Time

- Maximum time after which a host or agent in the community must receive an availability message from the other host or agent. If the secondary host or agent does not receive a message during this time, it assumes that the primary host or agent is unavailable and assumes control.
- Value—Number of seconds in the range 0–2147483647
- Example—`agents/IpVr/demo, agents/DnVr/demo`

By design, redundancy properties are not dynamically updated if their value changes in the directory. If you change the configuration for the redundancy communities while the two hosts are running but before you start the monitor, the configuration perceived by the monitor is different from the one perceived by the hosts.

Configuring Monitors

You can add NIC monitors to track redundant components.

Complete the following tasks to configure NIC monitors:

1. Configuring Operating Parameters for Monitors on page 276
2. Configuring a Monitor Process on page 277
3. Configuring JacORB Properties on Redundant NIC Hosts on page 278
4. Starting NIC Hosts on page 279
5. Starting NIC Monitors on page 279

Configuring Operating Parameters for Monitors

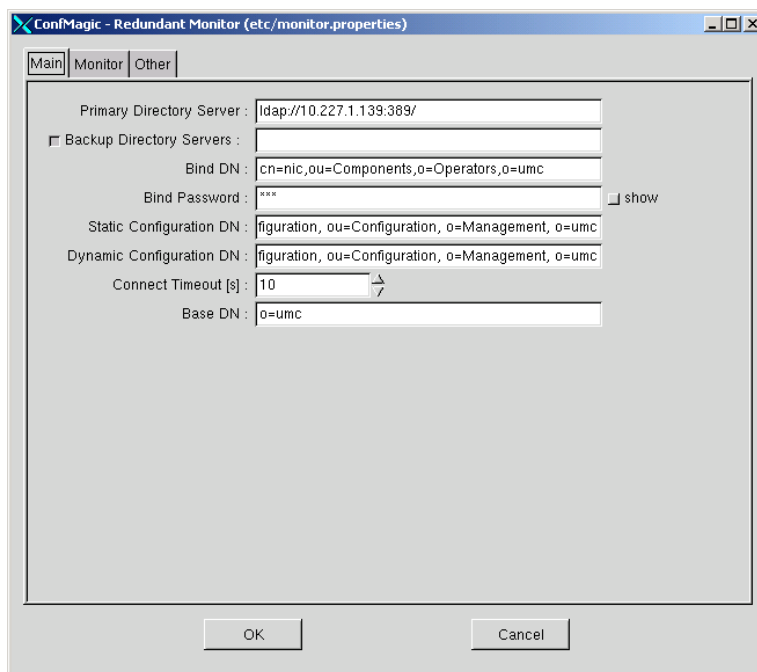
You must configure operating parameters for each monitor in your NIC configuration. The operating parameters define how the monitor interacts with other SRC components, such as the directory.

To configure the operating parameters:

1. Log in as **root**.
2. Start the local configuration tool in the directory where you installed the redundancy monitor software.

/opt/UMC/monitor/etc/config

The Redundant Monitor window appears.



3. In the Redundant Monitor window, edit or accept the default values for the fields.

See *JRE Properties for a Redundant Monitor* on page 277 and Chapter 11, *Configuring NIC on a Solaris Platform*.

4. Click **OK**.

JRE Properties for a Redundant Monitor

In the local configuration tool, you can set the value for the Redundant Monitor Java in the Monitor tab.

Redundant Monitor Java

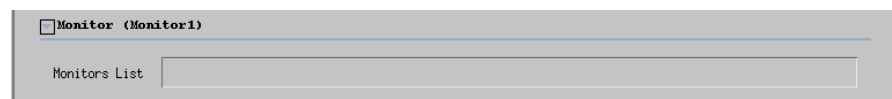
- Path to the JRE.
- Value—Path (absolute or relative) to the directory that contains the JRE
- Example—`../jre/bin`

Configuring a Monitor Process

You configure a monitor by adding it to a monitoring process, referred to as a monitor.

To use SDX Configuration Editor to configure a monitoring process:

1. In the navigation pane, select a NIC configuration file.
2. In the Redundancy tab, expand the **Monitors** section, and create a new instance of a monitor (monitoring process).



3. In the Monitor section, specify the monitors that this monitoring process supports.

See *Monitor Field* on page 278.

4. Select **File > Save**.
5. Right-click the configuration file, and select **SDX System Configuration > Export to LDAP Directory**.

Monitor Field

In SDX Configuration Editor, you can modify the following field in the Monitor section of the Redundancy pane in a NIC configuration file.

Monitor List

- List of monitors that the monitoring process will support.
- Value—Comma-separated list of monitors; each monitor has the format `< monitorName > :/communities/ < communityName >`
 - `< monitorName >` —Name of monitor; must match the name specified in the community (see *Configuring Communities on page 274*)
 - `< communityName >` —Name of community; must match the name specified in the configuration for the community (see *Configuring Communities on page 274*)
- Example—`DemoMonitor:/communities/Demohost, nicSaeDemoMonitor:/communities/nicsaeDemo`

Configuring JacORB Properties on Redundant NIC Hosts

If the system on which a NIC hosts resides uses an object request broker (ORB) different from the one provided in the SRC software distribution, it is important to configure some JacORB properties on each NIC host to enable the ORB to correctly determine when connections between redundant NIC hosts are unavailable. If you do not configure these properties properly, the ORB relies on the TCP default socket timeout (usually 8 minutes) to determine when a connection between redundant NIC hosts is unavailable or cannot be established. Using high values for these properties affects overall system availability.

To configure the JacORB properties:

1. With a text editor, open the *jacorb.properties* file.
2. Ensure that the property `jacorb.connection.client_idle_timeout` is uncommented, and set this property to a value between 5,000 and 30,000 milliseconds.

See *JacORB Properties for Timeouts on page 279*.

3. (JRE 1.4 only) If the default value is not appropriate for your network configuration, change the value of the property `net.juniper.smgmt.socket_factory.timeout.connect`.

See *JacORB Properties for Timeouts on page 279*.

4. Save and close the *jacorb.properties* file.
5. Repeat Steps 1 to 4 for each NIC host.

JacORB Properties for Timeouts

In the *jacorb.properties* file, you can modify the following timeout properties.

jacorb.connection.client_idle_timeout

- Time after which the ORB assumes that an existing connection between two machines has become unavailable.
- Value—Number of milliseconds in the range 5000–30000
- Default—30000
- Example—`jacorb.connection.client_idle_timeout = 10000`

net.juniper.smgmt.socket_factory.timeout.connect

- Time after which the ORB assumes that a new connection cannot be established between two machines.
- Value—Number of milliseconds in the range 0–2147483647
- Default—5000
- Example—`net.juniper.smgmt.socket_factory.timeout.connect = 10000`

Starting NIC Monitors

You must start each NIC monitor before its associated components can begin operating.

To start a monitor:

1. On the machine on which the monitor is installed, log in as `root` or as an authorized nonroot admin user.
2. Start the monitor from its installation directory:

`/opt/UMC/monitor/etc/monitor start`

After you have started a monitor, you can view log files of its operation and stop the host or monitor.

Starting NIC Hosts

You must configure operating parameters for each NIC host and then start each NIC host before its associated components can begin operating.

For information about how to configure NIC host parameters and how to start NIC hosts see *Chapter 11, Configuring NIC on a Solaris Platform*.

Verifying That a Monitor Is Running

To verify that the monitor is running:

1. On the host on which the monitor is installed, log in as **root** or as an authorized nonroot admin user.
2. Display the status of the monitor from its installation directory.

```
/opt/UMC/monitor/etc/monitor status
```

Stopping a Monitor

To stop the monitor:

1. On the host on which the monitor is installed, log in as **root** or as an authorized nonroot admin user.
2. Stop the monitor from its installation directory.

```
/opt/UMC/monitor/etc/monitor stop
```

Optimizing Performance of the NIC Proxy for NIC Host Redundancy

If you configure NIC host redundancy and the NIC proxy submits resolution requests to the NIC host at a high rate, the NIC proxy may take a significant amount of time to start communicating with a NIC host when that host makes the transition from the passive role to the active role. In this case, you will notice that many resolution requests are failing, and the NIC log files will indicate that the NIC proxy is sending requests to the former active NIC host.

This time delay occurs because the ORB tries to connect the NIC proxy to the former active NIC host for each outstanding resolution request. When the connection attempt fails, the ORB tries several times to reconnect the devices and waits for a specified interval of time between each attempt. To accelerate this process, modify the ORB properties that control these actions.

Depending on which NIC proxies are affected, you can modify the properties for one Web application only or for all Web applications in a JRE. For information about configuring the properties of an ORB other than JacORB, see the documentation for the ORB, and use the property descriptions below as a guideline.

To configure the properties for JacORB:

1. Access the directory that contains the *jacorb.properties* file.
 - To configure the properties for one Web application only:
cd <webAppDirectory>/WEB-INF/lib
 - To configure the properties for all Web applications in the JRE:
cd <jreInstallDirectory>/jre/lib
2. With a text editor, open the *jacorb.properties* file.
3. Modify the values of the properties *jacorb.retries* and *jacorb.retry_interval*.
 See *JacORB Properties for Retry Intervals* on page 281.
4. Save and close the *jacorb.properties* file.

JacORB Properties for Retry Intervals

In the *jacorb.properties* file, you can modify the following properties for retry intervals.

jacorb.retries

- Number of times that the ORB tries to connect the NIC proxy to the NIC host.
- Value—Integer in the range 0–2147483647
- Guidelines—If you notice that many resolution requests are failing and the NIC log files indicate that the NIC proxy is sending requests to the former active NIC host, reduce the value of this property.
- Default—5
- Example—*jacorb.retries* = 1

jacorb.retry_interval

- Time between the ORB's attempts to connect the NIC proxy to the NIC host.
- Value—Number of milliseconds in the range 0–2147483647
- Guidelines—If you notice that many resolution requests are failing and the NIC log files indicate that the NIC proxy is sending requests to the former active NIC host, reduce the value of this property.
- Default—500
- Example—*jacorb.retry_interval* = 200

Viewing Log Files for NIC Hosts and Monitors from the Solaris CLI

To view the log files for the UNIX processes associated with NIC hosts and monitors:

1. Access the log directory.

```
cd /opt/UMC/nic/var/log
```

or

```
cd /opt/UMC/monitor/var/log
```

2. Display the file.

```
more nic_info.log
```

or

```
more moninfo.log
```

Clearing Persistent Data and Logs for NIC Hosts and NIC Monitors

You can clear the log files for a NIC host or monitor and delete the persistent data that the NIC host or monitor writes to files or devices by using the **stdout** and **stderr** options. Clearing these types of data does not remove data about NIC hosts or monitors from the directory.

To delete persistent data and clear log files for a NIC host or monitor:

1. On the machine where you installed the NIC host or monitor, log in as **root** or as another authorized user.
2. Stop the NIC host or monitor.

```
/opt/UMC/nic/etc/nichost stop  
/opt/UMC/monitor/etc/monitor stop
```

3. Delete the data.

```
/opt/UMC/nic/etc/nichost clean  
/opt/UMC/monitor/etc/monitor clean
```

The system responds with a status message.

4. Restart the NIC host.

```
/opt/UMC/nic/etc/nichost start  
/opt/UMC/monitor/etc/monitor start
```