CA Spectrum®

Alarm Notification Manager User Guide

Release 9.4

ca® technologies

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

CA Technologies Product References

This document references the following CA Technologies products:

- CA Spectrum®
- CA Spectrum® Alarm Notification Manager (SANM)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction 7

Chapter 2: Creating and Editing Alarm Notification Policies 11

Chapter 3: Associating Policies with Applications 19

Chapter 4: Monitoring SANM Processes 25

Chapter 1: Introduction

This section contains the following topics:

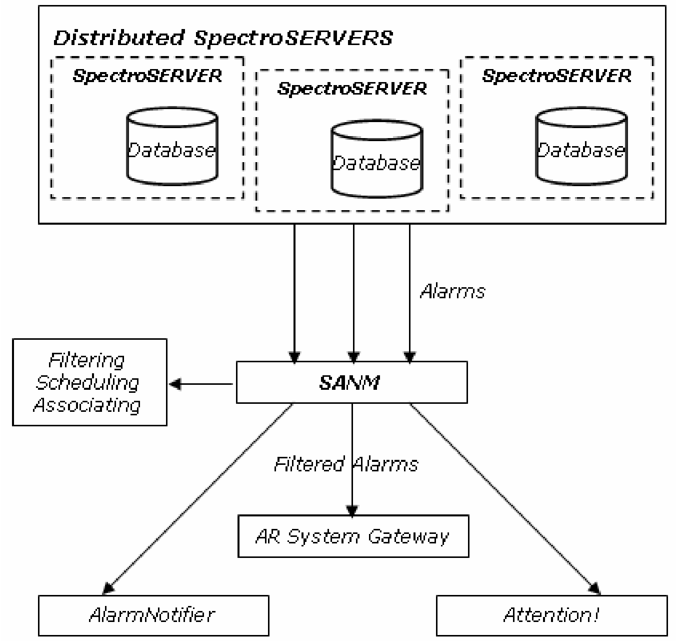
About SANM

The Alarm Notification Manager (*SANM*) is a CA Spectrum component that enhances the functionality of CA Spectrum alarm-processing applications. Multiple alarm-processing applications are available for CA Spectrum, including AlarmNotifier and Attention!. These applications respond to CA Spectrum alarms by sending email notifications, creating trouble tickets, and more. SANM lets you create and associate alarm notification policies with applications.

How CA Spectrum Monitors Alarms

CA Spectrum, alarm-processing applications, and SANM work together in the alarm monitoring process.

The following diagram shows the alarm monitoring process:



The following workflow describes how CA Spectrum monitors alarms:

1. CA Spectrum polls the modeled network elements and updates the status of each element in the SpectroSERVER database.
2. CA Spectrum generates an alarm when it receives a trap from the network, or when it detects a critical status change in a network model. In the OneClick Console, the model icon changes from green to another color that indicates the alarm severity level.
   - CA Spectrum posts specific information for each alarm on the Alarm Details tab of the Component Detail pane.
   - CA Spectrum posts alarm event information to the Events tab of the Component Detail panel.
3. Data about alarms that CA Spectrum has generated is passed to SANM. SANM lets you create and associate alarm notification policies with alarm processing applications. In addition, the SANM Schedule subview lets you schedule application and policy associations and automates the association process.
4. SANM passes the alarm information to alarm processing applications only when the alarm types specified in the policies occur.

AlarmNotifier

Alarms that SANM filters are sent to AlarmNotifier. When both SANM and AlarmNotifier are installed, AlarmNotifier gains some capabilities:

- You can apply the SANM alarm-filtering policies to individual instances of AlarmNotifier.
- AlarmNotifier can generate alarm notifications from all landscapes of a distributed SpectroSERVER environment.
- Additional commands are available to acknowledge and clear alarms from AlarmNotifier.
- A new startup command lets you start multiple instances of AlarmNotifier. You can associate each instance with a different SANM alarm notification policy.
- Other new startup commands let you create summary or detailed trace files.
- AlarmNotifier scripts include new parameters that contain information about troubleshooting alarms.
- The AlarmNotifier resource file includes new parameters to obtain more information about alarms.
- SANM lets you automatically associate a different policy with AlarmNotifier at a specified time.

Attention!

Attention! is a client-server network monitoring and notification system. The Attention! application alerts system managers to critical system and network events. Supported alert formats include alphanumeric paging, telephone calls, email, PA announcements, electronic message boards, and custom notifications. You can use SANM as a foundation for integration between CA Spectrum and Attention!.

The Alarm Resource File

The alarm resource file, .alarmrc, contains operating parameters that define SANM defaults. You can modify these parameters to customize SANM alarm management.

You can find the alarm resource file in the <*$SPECROOT*>/Notifier directory. For more information, see the *Alarm Notifier User Guide*.

We recommend creating a backup copy of the file before you modify it.

If you reinstall CA Spectrum or upgrade the version, the installation saves your resource file, .alarmrc, to a backup directory. Versions of the resource file that you saved with another name are preserved in the <*$SPECROOT*>/SANM directory. That directory also contains the default resource file that is included with the reinstallation or upgrade.

Chapter 2: Creating and Editing Alarm Notification Policies

This section contains the following topics:

Create an Alarm Notification Policy

An alarm notification policy specifies the alarm types that an alarm-processing application receives and filters the unwanted alarms. You can create alarm notification policies to determine which applications receive alarms of the types you select.

Follow these steps:

1. Click the Locater tab in the Navigation panel of the OneClick Console.
2. Select All Applications under SANM, and click (Launch the selected search).

   The Select Landscapes to Search dialog opens.
3. Select the landscapes to include in your search, and click OK.

   The available applications and the policy that they are using appear in the Contents panel on the right. The policy details appear in the Component Detail panel below the Contents panel.

   Note: Run AlarmNotifier at least once. Otherwise, the search returns no models. The AlarmNotifier file is located in the <*$SPECROOT*>/Notifier directory.
4. In the Component Detail panel, click the link to create or set policy under General Information.

   The Select Policy dialog opens.
5. Click Create.

   The Create SANM Policy dialog opens.

6. Enter the policy name in the Name text box.

7. (Optional) Create one or more filters to associate with the new policy.

   Note: We recommend assigning policy names that indicate when the policy is used. For example, use a name like 'ciscoRtrPM' so that you can identify Cisco router policies in a collection.

8. Click OK.

   The new policy is created.

Define a Filter For a Policy

You can define alarm notification policy filters that refine notification policies. A filter must be associated with a policy. Filters include parameters to include or exclude alarms by severity and by device type. You can set filters for alarms of specified types, on specified landscapes, or in specified topologies.

Follow these steps:

1. Click the Locater tab in the Navigation panel of the OneClick Console.

2. Select All Applications under SANM and click (Launch the selected search).

   The Select Landscape to Search dialog opens.

3. Select the landscapes you want to include in your search and click OK.

   The available applications and the policy they are using appear in the Contents and Component Detail panels on the right.

4. In the Component Detail panel, click the create/set policy link in the General Information subview.

   The Select Policy dialog opens.

5. Click Create.

   The Create SANM Policy dialog opens.

6. Click the Add button.

   The Add Filter dialog opens.

7. Enter the following information:

   Name

   Defines the new filter name.

   Notes

   (Optional) Describes the filter.

Age Time

(Optional) Indicates the time for which the filter holds the alarm. The alarm passes to the alarm processing application after the age time.

Notification Data

(Optional) Defines the data that is sent with the alarm notification.

8. Define parameters for your filter:

   a. (Optional) Select the Landscapes tab to define the landscapes for the filter. To define the landscape, select servers in the Include and Exclude lists. You can move servers between the Include and Exclude lists by using the arrow buttons provided.

      Note: OneClick combines the Landscapes and Servers parameters of the legacy SANM UI into a single parameter, Landscapes.

   b. (Optional) Select the Severity tab to define the alarm severity to include or exclude. To define the severity, select alarm severity levels from the Include and Exclude lists.

   c. (Optional) Select the Device Type tab to specify the device types for the filter, as follows:

      - Select an option to see the lists of device types to Include or Exclude.
      - Enter a device type and click Add to add it to the included or excluded list.

        Note: Enter the name of an existing device type, or the name of a device type that you plan to create.

      - Click Browse to select from a list of existing device types.
      - Select a device type and click Remove to remove it from the list.
      - Select a device type and click Modify to edit that device type.

   d. (Optional) Select the Collections tab to specify the collection of policies for the filter. Alarms on devices that are in these collections are filtered. The steps to include, exclude, add, remove, modify, and browse for containers are the same as for the previous tab.

   e. (Optional) Select the Topology tab to specify the topology containers for the filter. Alarms on devices that are in these topologies are filtered. The steps are the same as for the previous tabs.

   f. (Optional) Select the Alarm Type tab to include or exclude alarms of specific types.

   g. (Optional) Select the Model Type tab to include or exclude models of specific types.

   h. (Optional) Select the Location tab to specify location containers for the filter.

      Alarms on devices that are in these locations are filtered.

i. (Optional) Select the Organization tab to specify the organization containers for the filter.

   Alarms on devices that are in these organizations are filtered.

j. (Optional) Select the IP Address/Range tab to specify the Internet Protocol (IP) addresses for the filter.

   SANM only passes alarms that are generated within the specified network, subnet, or IP address range to the alarm processing application.

k. (Optional) Select the Model Name tab to specify the model names for the filter.

9. Click OK.

   The new filter is defined.

   Note: If you create a filter with multiple parameters, you create an AND condition. As a result, all of the parameters must return TRUE for the filter to return any results. To create an OR condition, create two filters, each with a different filter parameter.

10. Enter a name for the new policy in the Name field of the Create SANM Policy dialog, and click OK.

    Note: We recommend assigning policy names that indicate when the policy is used. For example, use a name like 'ciscoRtrPM' so that you can identify Cisco router policies in a collection.

    The new policy is created.

Add a Filter to an Existing Policy

You can add a filter to an existing policy.

Follow these steps:

1. Click the Locater tab in the Navigation panel of the OneClick Console.

2. Select SANM, All Policies and click (Launch the selected search).

   The Select Landscapes to Search dialog opens.

3. Select the landscapes that you want to include in your search and click OK.

   The existing polices display in the Contents panel on the right.

4. Select the policy for which you want to add a filter.

   The policy details display in the Component Detail panel.

5. Expand the Filters menu under the Information tab in the Component Detail panel.

6. Click (Opens a dialog to add a filter to this policy).

   The Add a Filter dialog opens.

7. Enter the filter information as explained in Define a New Filter (see page 12) and save the information.

   The filter is added to the policy.

Change the Filter Order

You can change the order in which the filters that are associated with a policy are processed.

This feature applies only to Notification Data. For instance, if Notification Data on filter 1 has jack@xyz.com, and filter 2 has jill@xyz.com, the alarm notifier returns jack@xyz.com:jill@xyz.com. If you change the order, the output is jill@xyz.com:jack@xyz.com.

Follow these steps:

1. Click the Locater tab in the Navigation panel of the OneClick Console.

2. Select SANM, All Policies, and click (Launch the selected search).

   The Select Landscape to Search dialog opens.

3. Select the landscapes to include in your search, and click OK.

   The existing policies appear in the Contents panel on the right.

4. Select a policy whose filter order you want to change.

   The policy details appear in the Component Detail panel below the Contents panel.

5. Expand the Filters menu under the Information tab and click (Opens a dialog to set the Notification data order).

   The Set Order dialog opens.

6. Select a filter.

7. Use the arrow buttons to move the filter up or down in the order, and click OK.

   The filter is processed according to the new order.

Edit a Filter

Edit a filter to change the values of filter parameters. You can add, edit, and delete the filter parameters.

Follow these steps:

1. Click the Locater tab in the Navigation panel of the OneClick Console.
2. Select SANM, All Policies, and click (Launch the selected search).

   The Select Landscape to Search dialog opens.
3. Select the landscapes that you want to include in your search, and click OK.

   The existing policies appear in the Contents panel.
4. Select the filter in the filter table and click (Opens a dialog to edit the selected filter).

   The filter opens for editing.
5. Edit the Name, Notes, Age Time, Notification Data fields as required.
6. Click each parameter tab to add, edit and delete the corresponding parameter values, as explained in Define a New Filter (see page 12).

   Note: If you delete all values of a parameter, the filter no longer includes that parameter.
7. Select the Show only filtered by parameters check box if you want to view only the parameters included in the filter.
8. Click OK.

   The filter is edited.

Add Filter Parameters

You can add parameters to a filter to increase the level of filtering.

Note: You can add a parameter to a filter by adding a value to that parameter. That is, if a parameter was not included when you created the filter, defining a value for that parameter adds that parameter to the filter.

Follow these steps:

1. Open the filter for editing (see page 16).
2. Click the tab of the parameter that you want to add to the filter.
3. Add one or more values to the parameter, as explained in Define a New Filter (see page 12).
4. Click OK.

   The parameter is added to the filter.

Delete a Filter

You can delete a filter that is no longer required.

To delete a filter, select the filter in the filter table and click ✖ (Permanently deletes the selected item).

The filter is deleted.

Add a Model or Alarm to a Policy

You can add a model or an alarm to a policy.

Follow these steps:

1. Click the Explorer tab in the Navigation panel of the OneClick Console.

   The model or alarm details display in the Contents panel on the right.
2. Right-click the model or alarm and select Add to, SANM Policy, Add.

   The Select Policy dialog opens.
3. Select a policy and click OK.

   The Select Write Option dialog opens.

   Note: To remove the item, select Remove.
4. Select an option.

   The model or alarm is added to the selected policy.

Editing an Alarm Notification Policy

You can edit a policy before or after you save it, regardless of whether it is associated with an application. If the policy is associated with an application, SANM begins enforcing the new policy as soon as you save your changes.

Important! The Archive Manager must be running and connected to the SpectroSERVER for modified policies to take immediate effect.

Chapter 3: Associating Policies with Applications

This section contains the following topics:

The Association Process

After you create an alarm notification policy, you associate the policy with one or more alarm processing applications. An association between a policy and an application remains in effect until you associate another policy with that application or delete the associated policy.

SANM enforces a rule that an application can have only one associated policy at a time. To let an application to process different alarms at different times, associate the policies with the applications manually at run time. Or use the Schedule subview to schedule the associations automatically at a specified date and time. To run the same application with different policies, start multiple instances of the application, each with a unique name. Then associate the different policies with the application instances.

To change the policy that is associated with an application, associate a policy, such as the default policy, with that application. If you instead delete the associated policy, SANM associates the default policy with the application. Editing a policy that is associated with multiple alarm processing applications changes the policy for all of the applications. Reassociating the policy with each application is not required.

The SANM Default Policy

SANM associates a default policy with each application when you start the application for the first time, or when you delete a policy associated with that application. You can also explicitly associate the default policy with an application.

The default policy is a null policy; it does not filter alarms. That is, applications that are associated with the default policy receive all alarm notifications that occur in every landscape in the landscape map of the SpectroSERVER to which SANM is connected.

You can modify the default policy to add filters, but SANM continues to associate it with applications by default.

If you delete a policy that is associated with an application, SANM associates the default policy with that application. Therefore, before you delete a policy, check whether the default policy has been modified. If you delete a policy that is associated with an application, or if you modify the default policy, SANM displays a warning.

You can avoid associating the default policy associated with an application when you delete the associated policy. First associate a different policy with the application. The current policy is automatically deleted.

Associate a Policy with an Application

You can associate a policy with an application in OneClick.

Follow these steps:

1. Click the Locater tab in the Navigation panel of the OneClick Console.
2. Select SANM, All Applications and click (Launch the selected search).

   The Select Landscape to Search dialog opens.
3. Select the landscapes to include in your search, and click OK..

   The existing applications appear in the Contents panel on the right.
4. Click the Create/Set Policy link.

   The Select Policy dialog opens.
5. Select a policy and click OK.

   The policy is associated with the application.

The Schedule Subview

The Schedule subview automates the association process and lets you implement alarm notification policies according to a schedule. For example, if you want an alarm application to take action in response to an alarm during the evening, you can create a special evening policy and can schedule the association of this policy with the application for 6 PM every day. You can then schedule the association of a different daytime policy with the same application for 7 AM every day. The Schedule subview lets you perform scheduled associations. You can avoid manually associating a new policy each time you want a change in alarm filtering.

You can verify the results of operations that were performed by the Schedule subview on the Events tab in OneClick.

Schedule an Association

You can schedule a policy association with an application in OneClick.

Follow these steps:

1. Click the Locater tab in the Navigation panel of the OneClick Console.
2. Select SANM, All Applications and click (Launch the selected search).

   The Select Landscape to Search dialog opens.
3. Select the landscapes to include in your search, and click OK..

   The existing applications display in the Contents panel on the right.
4. Select the SANM application whose policy you want to schedule.
5. In the Component Detail panel, expand the Scheduled Policies menu under the Information tab and click (Opens a dialog to schedule a policy to the current policy).

   The Select Policy And Schedule dialog opens.
6. Select a policy, select a schedule, and click OK.

   Note: You can create custom policies and schedules by clicking the Create buttons.

   The scheduled policy displays in the Scheduled Policies table.

Additional Utilities

AlarmNotifier includes three utilities that you can use to manage existing alarms:

- assignticket
- clearticket
- updatealarm

assignticket Utility

The assignticket utility is used to populate the Trouble Ticket ID field of an alarm with the name of the person to whom the ticket is assigned.

Run this utility using the following syntax:

```
assignticket modelhandle alarmid assignee [username]
```

modelhandle

Indicates the handle of the model where the alarm was raised.

alarmid

Indicates the ID of the alarm to which to write.

assignee

Indicates the name of the user to whom the ticket is assigned.

username

(Optional) Specifies the name of the CA Spectrum user account to use to connect to the SpectroSERVER.

clearticket Utility

Use the clearticket utility to clear an alarm.

Run this utility using the following syntax:

```
clearticket -mh model_handle -ai alarm_ID -su username
```

-mh *model handle*

Indicates the handle of the model where the alarm exists.

-ai *alarm_ID*

Indicates the ID of the alarm to clear.

-su *username*

Specifies the name of the user account to use to connect to the SpectroSERVER.

updatealarm Utility

Use the updatealarm utility to set the value of any attribute on any alarm.

Run this utility using the following syntax:

```
updatealarm modelhandle alarmid attrid attrvalue [username]
```

modelhandle

Indicates the handle of the model where the alarm was raised.

alarmid

Indicates the ID of the alarm to which to write.

attrid

Indicates the ID of the attribute to which to write.

attrvalue

Indicates the value to write to the attribute.

username

(Optional) Specifies the name of the user account to use to connect to the SpectroSERVER.

Chapter 4: Monitoring SANM Processes

This section contains the following topics:

SANM Events

The Events tab in OneClick lists events that occur on a SpectroSERVER. When a user performs a SANM operation, the results of the operation appear on the Events tab with other CA Spectrum events. The following information about an event is listed:

- Date and time of the operation
- Application name and policy name
- User's host and user name
- Explanation of the event
- Event code

Note: For more information about using the Events tab, see the *Operator Guide*.

SANM Event Codes

Each SANM event code corresponds to a SANM operation. Use the following SANM event codes to locate SANM operation entries or to filter out all entries that are not specific to SANM operation.

00d70000

Application registered with SANM

00d70001

Application unregistered with SANM

00d70002

Association created

00d70004

Scheduled association created

00d70006

Policy created

00d70008

Policy modified

00d7000a

Application created

00d7000b

Application creation failed

Tracing Policies

To collect information about how a policy is working for a SANM-enabled application, at application startup you can enable the creation of a detailed or summary trace file for that application.

- **Detailed trace file**: Indicates the filters in a policy alarm that did not match when they were evaluated against that policy.
- **Summary trace file**: Indicates the time when an alarm notification is passed to the associated application when that application is started. A summary trace file does not include information about alarms that do not meet the criteria that are specified in a policy.

Use a record of policy-based actions by SANM as a decision-making tool. The results may confirm that you have the correct policy in place for an application, or they may compel you to refine your policy. For example, you can discover that you are inadvertently excluding alarms that should be passed to an application.

The Summary Trace File

The summary trace file includes a summary of all alarm notifications (set, cleared, updated) sent to the application, as follows:

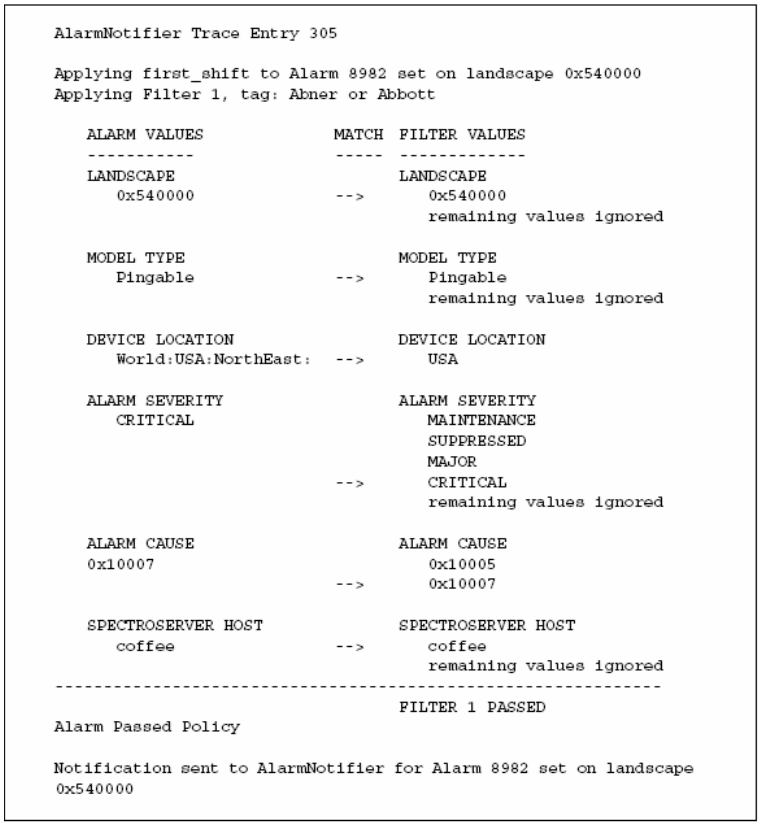
```
05/24/2000 15:48:44 SANM Trace Entry 1

Notification sent to AlarmNotifier for Alarm 52 set on landscape 0x540000

05/24/2000 15:48:44 SANM Trace Entry 2

Notification sent to AlarmNotifier for Alarm 21 updated on landscape 0x540000

05/24/2000 15:48:44 SANM Trace Entry 3

Notification sent to AlarmNotifier for Alarm 26 cleared on landscape 0x540000
```

The summary trace file does not indicate the alarms that failed the policy.

The Detailed Trace File

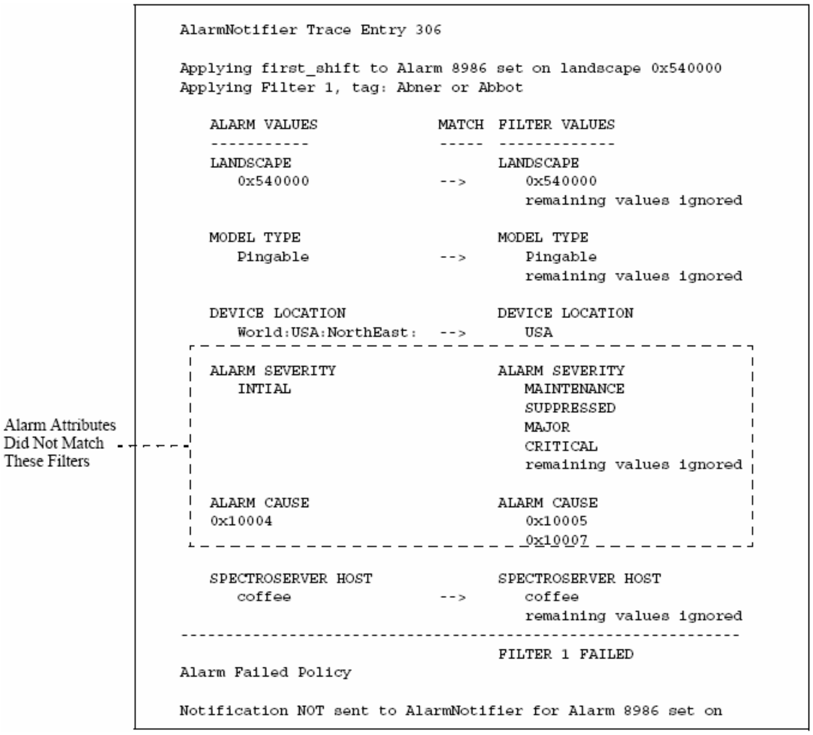
A detailed trace file includes entries for alarms that meet and that do not meet the criteria of a policy. An alarm entry includes the alarm attribute values, which that are compared to the filter parameter values. An arrow symbol under MATCH between ALARM VALUES and FILTER VALUES indicates a match. The arrow is absent if the values do not match.

The following is an example of a trace file that indicates that an alarm passed a policy:



```
AlarmNotifier Trace Entry 305

Applying first_shift to Alarm 8982 set on landscape 0x540000
Applying Filter 1, tag: Abner or Abbott

   ALARM VALUES             MATCH  FILTER VALUES
   -----------              -----  -------------
   LANDSCAPE                       LANDSCAPE
      0x540000              -->       0x540000
                                      remaining values ignored

   MODEL TYPE                      MODEL TYPE
      Pingable              -->       Pingable
                                      remaining values ignored

   DEVICE LOCATION                 DEVICE LOCATION
      World:USA:NorthEast:  -->       USA

   ALARM SEVERITY                  ALARM SEVERITY
      CRITICAL                        MAINTENANCE
                                      SUPPRESSED
                                      MAJOR
                            -->       CRITICAL
                                      remaining values ignored

   ALARM CAUSE                     ALARM CAUSE
   0x10007                            0x10005
                            -->       0x10007

   SPECTROSERVER HOST              SPECTROSERVER HOST
      coffee                -->       coffee
                                      remaining values ignored
--------------------------------------------------------------
                                   FILTER 1 PASSED
Alarm Passed Policy

Notification sent to AlarmNotifier for Alarm 8982 set on landscape
0x540000
```

The following is an example of a trace file that indicates that an alarm failed a policy:



```
AlarmNotifier Trace Entry 306

Applying first_shift to Alarm 8986 set on landscape 0x540000
Applying Filter 1, tag: Abner or Abbot

   ALARM VALUES            MATCH  FILTER VALUES
   -----------             -----  -------------
   LANDSCAPE                      LANDSCAPE
      0x540000             -->       0x540000
                                     remaining values ignored

   MODEL TYPE                     MODEL TYPE
      Pingable             -->       Pingable
                                     remaining values ignored

   DEVICE LOCATION                DEVICE LOCATION
      World:USA:NorthEast: -->       USA

   ALARM SEVERITY                 ALARM SEVERITY
      INTIAL                         MAINTENANCE
                                     SUPPRESSED
                                     MAJOR
                                     CRITICAL
                                     remaining values ignored

   ALARM CAUSE                    ALARM CAUSE
   0x10004                           0x10005
                                     0x10007

   SPECTROSERVER HOST             SPECTROSERVER HOST
      coffee               -->       coffee
                                     remaining values ignored
-------------------------------------------------------------
                                  FILTER 1 FAILED
Alarm Failed Policy

Notification NOT sent to AlarmNotifier for Alarm 8986 set on
```

Alarm Attributes
Did Not Match
These Filters

Chapter 5: SANM and AlarmNotifier

This section contains the following topics:

AlarmNotifier Enhancements

AlarmNotifier gains capabilities when you install SANM on your system. These capabilities include additional startup options for specifying application names and for creating trace files, alarm acknowledge and alarm clear commands, and script and resource file parameters. SANM also lets AlarmNotifier operate in a distributed environment.

Start AlarmNotifier

AlarmNotifier is located in the <*$SPECROOT*>/Notifier directory. This directory contains the following files by default:

- .alarmrc
- AlarmNotifier
- ClearScript
- README
- SetScript
- UpdateScript

AlarmNotifier includes the following additional files and directory:

AlarmAck

Acknowledges an alarm.

AlarmClear

Clears an alarm.

Trace

Displays trace files.

To start AlarmNotifier, use the following AlarmNotifier command in the <*$SPECROOT*>/Notifier directory:

```
AlarmNotifier [-r resourcefile] [-n application][-tl summary|details [-tn tracefile]
[-ts size]]
```

-r *resourcefile*

Lets you specify a resource file other than the default resource file .alarmrc.

-n *application*

Lets you override the application name value that is specified by the APPLICATION parameter in the resource file. You can specify a different name for an AlarmNotifier application instance. This option lets you start multiple instances of AlarmNotifier and associate each of them with a different SANM alarm-filtering policy. If a name is not assigned to the APPLICATION parameter in the resource file, use the -n option at start-up to specify an application name.

-tl summary | details

Lets you activate tracing at a specified level, summary or detailed. The default format for an AlarmNotifier trace file is the application name together with the date when the trace file was created.

-tn *tracefile*

Lets you specify a trace file name other than the default name, which is provided when only the -tl option is used. Use this option with the -tl option.

When using the trace file option, the output file is written by default to the <*$SPECROOT*>/Notifier/trace directory. To explicitly name an output file and path, use the [-tn filename] option. If <*filename*> is a relative path, trace output is written to a file that is relative to the current directory. If <*filename*> is an absolute path, trace output is written to the absolute path.

-ts *size*

Lets you specify the number of lines in the trace file. Use this option with the -tl option. The application writes this number of lines to the file and then wraps around to the beginning of the file. Entries are numbered sequentially, and an END OF TRACE line follows the last entry. The default number of lines in a trace file is 10000.

Access Alarm Management Parameters

The Alarm Management view lets you control some aspects of alarm management. Two parameters in this view, Generate Alarm Events and Add Events to Alarms, determine how the SpectroSERVER reacts to alarm updates.

You can view and modify alarm management parameters in OneClick to control some aspects of alarm management.

Follow these steps:

1. Open OneClick.
2. In the Navigation panel, select a VNM model in the Universe view.

   The corresponding details appear in the Contents panel and Component Detail panel on the right.
3. In the Component Detail panel, select the Information tab and open the Alarm Management menu.

   The following alarm management parameters affect alarm event updates:

   Generate Alarm Events

   > Enables the generation of alarm change events (which indicate that alarms are generated, updated, or cleared).
   >
   > **Default**: Enabled (Yes).
   >
   > **Important!** When Generate Alarm Events is enabled, always select the Store Event in Historical Database option for the event in the Event Configuration window. Otherwise, event information does not appear in the Events tab of the Component Detail pane as that event is not logged in the Historical database. In addition, always enable Generate Alarm Events when the Store Event in Historical Database option is selected. Otherwise, the Severity, Cleared On and the Cleared By fields are not updated in the Events tab.

   Add Events to Alarms

   > Controls whether alarm change events are added to each alarm. If disabled, alarm change events are not displayed in the Events tab of the Component Detail panel for the alarm. When enabled, adds any event that affects the alarm, thus incrementing the Occurrence counts. For example, events with different event types that generate the same alarm, such as alarm management or alarm clearing events, are also added.
   >
   > **Default**: Disabled (No).

   Note: For more information, see the *Distributed SpectroSERVER Administrator Guid*e.

Verify that Originating Event Data Is Saved

High traffic levels can prevent the Archive Manager from consistently providing the events that are associated with reported alarms. In such a case, you can still retrieve some basic information about the events that are associated with alarms. The SpectroSERVER stores this information by default.

Note: Only information about the first event that is associated with an alarm (the originating event) can be retrieved.

The Store_Originating_Event attribute (0x1296f) of the Alarm Management application model determines whether originating event information is available to the AlarmNotifier. Verify that the default setting, Yes (Enabled), is in force so that event information is available in failover situations.

Follow these steps:

1. Click the Locater tab in the Navigation panel of the OneClick Console.
2. Expand Application Models.
3. Double click By Name.
4. The Search box opens.
5. Type "AlarmMgmt" in the Model Name Contains field, and click OK.

   The Alarm Management model appears in the Results panel.
6. Select the AlarmMgmt model.

   The corresponding details appear in the Component Detail panel.
7. In the Component Detail panel, click the Attributes tab.
8. Type "Store" in the Search box to locate the Store_Originating_Event attribute.
9. Double-click it to verify the value in the right pane.

Alarm Acknowledgement

The AlarmAck command allows you to acknowledge alarms. This command can be used at any shell command prompt to acknowledge specific alarms, or it can be incorporated into a script. AlarmAck returns a value of 0 if the operation succeeds. Otherwise, it returns a non-zero value.

To acknowledge an alarm, run the AlarmAck command with the following syntax:

```
AlarmAck -a alarm -l landscape
```

-a *alarm*

Defines the alarm ID.

-l *landscape*

Defines the landscape handle for the landscape where the alarm was raised.

Note: Available only for distributed SpectroSERVER environments.

To acknowledge all alarms for a model, run the AlarmAck command with the following syntax:

```
AlarmAck -m modelhandle
```

-m *modelhandle*

Specifies the model handle for the model with the alarm conditions.

User-Clearable Alarms

The AlarmClear command clears user-clearable alarms. To determine whether an alarm is user-clearable, check the value of the UserClearable parameter in alarm notifications. AlarmClear can be launched from any shell command prompt to clear specific alarms, or you can incorporate it into a script. AlarmClear returns a value of 0 if the operation succeeds. Otherwise, it returns a non-zero value.

You can run the AlarmClear command to clear alarms using the following syntax:

```
AlarmClear -a alarm -l landscape
```

-a *alarm*

Defines the alarm ID.

-l *landscape*

Defines the landscape handle of the landscape where the alarm was raised.

SANM-Enabled Script Parameters

The SetScript, UpdateScript, and ClearScript scripts have additional parameters when they run on a computer where SANM is installed.

The following list describes the SANM-enabled script parameters:

FlashGreen

Displays in ClearScript notifications but not in SetScript or UpdateScript notifications.

When enabled, the cleared alarm exhibits the *flash green* condition: the flash green option for the model is enabled, and the GET_FLASH_GREEN parameter in the .alarmrc resource file is set to True. Even though SetScript and UpdateScript notifications do not display this field, the parameter is passed to these scripts, but it is invalid and has a default value of False.

Location

Identifies the location model that contains the network element whose alarm is set, updated, or cleared. The element must be modeled in the OneClick World topology view. You can find the location model that contains the model for the problematic network element in a colon-separated, hierarchical list of location models. For example, an alarm for a model that is contained in Room 222 on the first floor of the Boston building in the northeast region of the United States appears as follows:

USA:Northeast:BostonBldg:FirstFloor:Room222.

AlarmAge

Specifies the length of time that SANM retains an alarm from an instance of AlarmNotifier that is associated with that policy. The AlarmAge is set in the filters in an SANM policy. If the alarm must pass multiple filters with different ages, SANM uses the shortest, non-zero alarm age interval.

NotificationData

Lists notification data entries (names of persons) that SANM passes to an instance of AlarmNotifier that is associated with that policy. The entries are specified in the filters in an SANM policy. AlarmNotifier scripts can be configured to initiate email notifications to those persons in the notification data entries.

ProbableCause

Is the probable cause text associated with the alarm.

EventMessage

Is the message about the events that are associated with the alarm. This field is blank if the CA Spectrum alarm has no associated events, or if the event does not include alarm information.

Email Notifications

If you use an AlarmNotifier script to send an email notification, set the value for the VARFORMAIL parameter in the script. This parameter specifies to whom the email message is sent.

If you are using SANM-enabled AlarmNotifier, use the NotificationData parameter to set the value for VARFORMAIL. If you use NotificationData as the value for VARFORMAIL, email is sent to the persons who are specified in the NotificationData parameter in the SANM policy that is associated with the instance of AlarmNotifier that invokes the script. For example, if the Notification Data entry is formatted as "John: Mary or Sue: Lynn, Jeff", email is sent to John, Mary, Lynn, and Jeff, but not to Sue, because AlarmNotifier interprets the colon as an AND operator and does not act on the OR operator.

Other possible values for the VARFORMAIL parameter are RepairPerson or both. The RepairPerson option is the only option that is available for AlarmNotifier when it is not running with SANM. Both options indicate that the email notification is sent to the designated RepairPerson and to the person who is specified by the NotificationData parameter.

Note: For more information about configuring an AlarmNotifier script to send an email notification, see the *AlarmNotifier User Guide*.

Third-Party Applications

You can customize or replace the SetScript, ClearScript, or UpdateScript for integration with a third-party application. If you create your own script or executable, understand which arguments are passed from CA Spectrum to the receiving script or executable. The script or executable must receive all of the arguments that CA Spectrum passes to it in the correct order.

Note: Any CA Spectrum attribute of the model with the alarm can be passed to AlarmNotifier and can be used in a script. For more information, see the *AlarmNotifier User Guide*.

The following table shows the argument number, name, and format for each argument that is passed to each script when the USE_NEW_INTERFACE .alarmrc parameter is set to TRUE:

Argument	Name	Format
1	Date	mm/dd/yy
2	Time	hh:mm:ss
3	Model Type	Text
4	Model Name	Text
5	Alarm ID	Integer
6	Severity	Text
7	Cause	Text

Argument	Name	Format
8	Repair Screen	Text
9	Server	Text
10	Landscape	Hexadecimal
11	Model Handle	Hexadecimal
12	Model Type Handle	Hexadecimal
13	IP Address	xxx.xxx.xxx.xxx
14	Security String	Text
15	Alarm State	Text
16	Acknowledged	Text
17	Clearable	Text
18	Flash_Green	Text
19	Location	Text
20	Age	Integer
21	Notifdata	Text

The following table shows the argument number, name, and format for each argument that is passed to each script when the USE_NEW_INTERFACE .alarmrc parameter is set to FALSE:

Argument	Name	Format
1	Date	mm/dd/yy
2	Time	hh:mm:ss
3	Model Type	Text
4	Model Name	Text
5	Alarm ID	Integer
6	Severity	Text
7	Cause	Text
8	Repair Screen	Text
9	Status	Text
10	Server	Text
11	Landscape	Hexadecimal

Argument	Name	Format
12	Model Handle	Hexadecimal
13	Model Type Handle	Hexadecimal
14	IP Address	xxx.xxx.xxx.xxx
15	Security String	Text
16	Alarm State	Text
17	Acknowledged	Text
18	Clearable	Text
19	Flash_Green	Text
20	PCause	Text
21	Location	Text
22	Age	Integer
23	Notifdata	Text
24	EventMsg	Text

If USE_NEW_INTERFACE is set to TRUE, the Status, PCause, and EventMsg arguments are sent as environmental variables. The argument order is therefore affected. If USE_NEW_INTERFACE is set to FALSE, use the following syntax in your script to read data from the PCause and the EventMsg argument into a variable as follows:

```
<variablename>=`echo "$2" | tr '\350' '\012' | tr '\351' '"'`
```

This syntax is required to avoid problems when the script parses the extra data from new lines or other special characters.

Note: For more information about the USE_NEW_INTERFACE .alarmrc parameter, see the *AlarmNotifier User Guide*.

SANM-Enabled .alarmrc Parameters

The AlarmNotifier resource file, .alarmrc, has several additional parameters when you run AlarmNotifier on a computer that has SANM installed.

The following list describes the SANM-enabled parameters:

APPLICATION

Defines the application name that identifies this AlarmNotifier application. If you use multiple AlarmNotifier applications on your network, distinguish them with unique application names, such as AlarmNotifier1 or AlarmNotifier2. You can then use unique SANM alarm-notification policies with each application. If you use the n option when invoking AlarmNotifier, the APPLICATION parameter value is ignored.

Default: AlarmNotifier

GET_LOCATIONS

Lets you specify whether to notify you of the location of the device with the alarm. If you are not interested in location information, set this parameter to False. A False setting overrides any location that is specified as a filter parameter in an alarm-notification policy, reducing network traffic.

GET_PROBABLE_CAUSES

Lets you specify whether you want to receive the Probable Cause text that is associated with each alarm. If you are not interested in Probable Cause information, set this parameter to False, improving AlarmNotifier performance.

Default: True.

GET_EVENTS

Lets you specify whether to receive the Event message that is associated with an alarm. If you are not interested in event information, set this parameter to False. Excluding events reduces network traffic that AlarmNotifier generates and improves performance.

Default: True.

GET_FLASH_GREEN

Lets you specify whether to receive the Flash Green status for a model. ClearScript is the only script that displays the Flash Green status. When Flash Green is enabled for a model, the model continues to flash green after alarms are cleared. The flashing status signals that alarms have occurred even though they no longer exist. If the value of GET_FLASH_GREEN is set to False, the Flash Green status is always passed to the ClearScript as false. If set to True, the Flash Green status is correctly passed as either False or True.

Default: True.

MSG_TIMESTAMP_FORMAT

Sets the format for the timestamp on all SANM messages. The maximum length of the output string is 127 characters. Any characters other than the conversion strings are output as text in the timestamp. The default setting is %X %x:. The colon (:) is appended to the end of the timestamp. For example, to output the date/time for the current locale and the time zone name, the string %x %X %Z is entered as the value. If left blank, no timestamp is output on the messages. If an incorrect string is entered, that string displays as text in the output.

POLICY_LANDSCAPE

Lets you specify the landscape that AlarmNotifier uses for all SANM policy definitions. This parameter works with the POLICY_LANDSCAPE setting in the SANM .sanmrc file.

SHOW_ALL_EVENTS

Lets you specify whether to receive the most recent event or all events that were generated for an alarm. If set to False, AlarmNotifier only forwards the most recent event. For example, assume that an alarm was created based on an event, and then someone updated the status of that alarm. When the alarm status changed, another event that was related to that alarm was generated. In such a situation, AlarmNotifier only receives the status of that second event. The purpose of this type of filtering is to eliminate events that have already been forwarded. Filtering is especially important if the size of the message is relevant, for example, if the event message is sent as a page.

Default: False.

Chapter 6: Using SANM in a Distributed SpectroSERVER Environment

This section contains the following topics:

Landscapes and Alarm Monitoring

A Distributed SpectroSERVER (DSS) environment lets you divide network management tasks among several SpectroSERVERs. When you create a network model with multiple SpectroSERVERs, it is possible for SANM to access information from more than one SpectroSERVER simultaneously.

A landscape is the CA Spectrum term for a network domain that a single SpectroSERVER manages. When SANM operates in a distributed environment, it monitors alarms from all landscapes. Even though different landscapes can model each other in a DSS environment, SANM-enabled applications do not receive duplicate alarm information.

Because SANM evaluates alarms across VNMs in a DSS environment, you may want to limit the type of alarm notifications that you receive. In a DSS environment, limit the number of alarm notifications by carefully defining the parameters, Landscape, Subnet IP Address, and Device Location in the alarm notification policy.

SANM Policy Management Across Multiple Landscapes

Choose between two options for configuring SANM in a distributed environment. You can create SANM policies on any landscape and let SANM read all policies from all landscapes. Or you can create all SANM policies on one landscape and only let SANM read policies from that landscape. In either case, you can associate alarm-processing applications from any landscape with the SANM policies.

How to Create SANM Policies in a Single Landscape

If you set up a distributed environment so that all policies for all landscapes are defined and managed from a single SpectroSERVER, you can install alarm-processing applications on any of the SpectroSERVERs in the distributed environment. If the values in the application resource file are appropriate, the application finds the server that contains the SANM policy definitions and associates it with the appropriate policy. This configuration reduces the initial traffic on the network to associate alarm processing applications and SANM policies, and it also facilitates ongoing SANM policy management.

Note: You cannot migrate or move an SANM policy from one landscape to another. If you want to institute this configuration and already have policies defined on various landscapes, you must recreate these policies on the new landscape from which you will manage SANM policies.

To configure all SANM policies in one landscape, take the following steps:

1. Change the POLICY_LANDSCAPE parameter in the .alarmrc file to the landscape handle of the SpectroSERVER where SANM is installed, and where policies are created and managed.
2. Change the POLICY_LANDSCAPE parameter in the alarm-processing application resource file (.alarmrc, .arsgrc) to the landscape handle of the SpectroSERVER where SANM is installed. This parameter instructs the application where to look for defined policies.
3. Restart the SpectroSERVER where SANM is installed and restart the alarm-processing applications so that the changes to the resource file parameters are read.
4. Open SANM, All Policies on the Locater tab of OneClick, and click 🔍 (Launch the selected search).

   The only available policies are the policies that are created on this landscape. All alarm-processing applications whose POLICY_LANDSCAPE parameter is set to the landscape handle of this landscape are seen in the applications list.

How to Create SANM Policies on Multiple Landscapes

You can set up a distributed environment so that SANM policies can be defined and managed on any SpectroSERVER. Alarm-processing applications on any SpectroSERVER in the distributed environment have access to all of these policies.

To configure SANM policies in multiple landscapes, verify the following requirements:

- The POLICY_LANDSCAPE parameter in the .sanmrc file must have no associated value.
- The POLICY_LANDSCAPE parameter in the alarm-processing application resource file (.alarmrc, .arsgrc, etc.) must also have no associated value.

Then take the following steps:

1. Restart the SpectroSERVER where SANM is installed.
2. Restart the alarm-processing applications so that the changes to the resource file parameters are read.
3. Open OneClick. Verify that all policies that have been created within the distributed environment are available.
4. Verify that all alarm-processing applications in the distributed environment are available for association.

Methods for Determining Monitored Landscapes

You can use the following methods to determine which landscapes are monitored by SANM:

- Use the CA Spectrum Command Line Interface (CLI) application to connect to the SpectroSERVER to which SANM is connected. Then enter **show landscapes** on the command line.

  The CLI application displays a list of all landscapes that are modeled in that server.

  Note: For more information, see the *Command Line Interface User Guide*.

- Open any one of the detailed trace files that you specified for SANM-enabled applications. A trace file indicates the connection status of each landscape in the landscape map for the SpectroSERVER to which SANM is connected. Trace files are stored by default in a trace directory in the home directory of an SANM-enabled application.

Index