VMware Smart Service Assurance Manager Troubleshooting Guide

VMware Smart Assurance 10.0.0

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2019 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

1 Preface 4

- Purpose 4
- Audience 5
- VMware Smart Assurance Service Assurance Manager installation directory 5
- VMware Smart Assurance Service Assurance Manager 5
- Related documentation 6
- Suggestions for searching PDF files 7
- Conventions used in this document 7
- Pathname conventions 8
- Graphical conventions 8
- Manager 8
- Where to get help 8
- Your comments 9

2 Troubleshooting 10

- Configuration issues 10
- Adapter issues 17
- NOTIF issues 23
- Notification and event processing issues 24

3 Frequently Asked Questions 26

- Configuration queries 26
- Trap processing queries 28
- NOTIF queries 35
- Notification and Event processing queries 35
- Business Dashboard queries 38

Preface

1

As part of an effort to improve its product lines, VMware periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your VMware technical support professional if a product does not function properly or does not function as described in this document.

Note This document was accurate at publication time. Go to VMware Online Support docs.vmware.com to ensure that you are using the latest version of this document.

This chapter includes the following topics:

- Purpose
- Audience
- VMware Smart Assurance Service Assurance Manager installation directory
- VMware Smart Assurance Service Assurance Manager
- Related documentation
- Suggestions for searching PDF files
- Conventions used in this document
- Pathname conventions
- Graphical conventions
- Manager
- Where to get help
- Your comments

Purpose

This document contains troubleshooting instructions and frequently asked questions and troubleshooting tips on the VMware Smarts Service Assurance Manager.

Audience

This guide is intended for administrators who are responsible for deploying, installing, and configuring the Global Manager. IT managers who seek to understand the role of the Global Manager in the context of an VMware Smart Assurance solution may also find this guide useful.

In addition to the configuration guides for specific components, administrators should also read the VMware Smart Assurance Service Assurance Manager Deployment Guide and the VMware Smart Assurance System Administration Guide Guide.

VMware Smart Assurance Service Assurance Manager installation directory

In this document, the term BASEDIR represents the location where VMware Smart Assurance software is installed:

- For UNIX, this location is: /opt/InCharge/<*productsuite*>.

  For example, on UNIX operating systems, VMware Smart Assurance Service Assurance Manager is, by default, installed to /opt/InCharge/SAM/smarts.

  Optionally, you can specify the root of BASEDIR to be something other than /opt/InCharge (on UNIX), but you cannot change the <*product*> location under the root directory.

  The VMware Smart Assurance System Administration Guide provides more information about the directory structure of VMware Smart Assurance software.

VMware Smart Assurance Service Assurance Manager

The VMware Smart Assurance Service Assurance Manager includes the following products:

- Service Assurance Manager (Global Manager), includes Business Impact Manager (BIM) and Failover System
- Global Console
- Business Dashboard
- Companion UI
- SAM Native Adapters:
  - Service Assurance Manager Notification Adapters (E-Mail Notifier Adapter, Script Notifier Adapter, SNMP Trap Notifier Adapter, Log File Notifier Adapter)
  - Adapter Platform (Adapter Platform server, Syslog Adapter, SNMP Trap Adapter, sm_ems command-line interface)
  - VMware Smart Assurance Adapter for UIM/O
  - XML Adapter

Related documentation

In addition to this document, VMware Corporation provides a help system for command line programs as well as product documentation.

Help for command line programs

Descriptions of command line programs are available as HTML pages. The index.html file, which provides an index to the various commands, is located in the BASEDIR/smarts/doc/html/usage directory.

VMware Smart Assurance documentation

Readers of this guide may find the following related documentation helpful:

- Smarts Foundation EMC Data Access API (EDAA) Programmer Guide
- VMware Smart Assurance Common Information Model (ICIM) 1.11 Reference for Non-Service Assurance Manager Products
- VMware Smart Assurance Common Information Model (ICIM) Reference for Service Assurance Manager
- *VMware Smart Assurance Foundation Documentation Portfolio*
- VMware Smart Assurance System Administration Guide
- VMware Smart Assurance ASL Reference Guide
- VMware Smart Assurance Perl Reference Guide
- VMware Smart Assurance Dynamic Modeling Tutorial
- VMware Smart Assurance MODEL Reference Guide

VMware Smart Assurance Service Assurance Manager documentation

The following documents are relevant to users of the
VMware Smart Assurance Service Assurance Manager:

- VMware Smart Assurance Service Assurance Manager Release Notes
- VMware Smart Assurance Open Source License and Copyright Information
- VMware Smart Assurance Service Assurance Manager Introduction
- VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managers
- VMware Smart Assurance Service Assurance Manager Deployment Guide
- VMware Smart Assurance Service Assurance Manager Configuration Guide
- VMware Smart Assurance Service Assurance Manager Operator Guide

- VMware Smart Assurance Service Assurance Manager Dashboard Configuration Guide
- VMware Smart Assurance Business Impact Manager User Guide
- VMware Smart Assurance Failover System User Guide
- VMware Smart Assurance Service Assurance Manager Notification Adapters User Guide
- VMware Smart Assurance Service Assurance Manager Adapter Platform User Guide
- VMware Smart Assurance Adapter for Unified Infrastructure Manager/Operations Configuration Guide
- VMware Smart Assurance XML Adapter User Guide
- VMware Smart Assurance Notification Module User Guide
- VMware Smart Assurance Service Assurance Manager Troubleshooting Guide
- VMware Smart Assurance Companion UI Online Help
- VMware Smart Assurance Companion UI Open Source License and Copyright Information for GPLv3 as Included with a Distribution of SLES 11
- VMware Smart Assurance Service Assurance Manager Documentation Portfolio

  The VMware Smart Assurance Documentation Catalog provides documentation resources for other VMware Smart Assurance products.

Suggestions for searching PDF files

You can search across multiple PDF files by using the Adobe Acrobat Reader software:

1. If the documentation is not accessible to all users of the VMware Smart Assurance product, copy the contents of the BASEDIR/smarts/doc/pdf directory to a central location, such as a shared drive on your LAN, so that operators and others can view the documentation.
2. To search throughout the documentation library, open the Acrobat Reader software:
3. Select **Edit > Search**, and type a word or phrase.
4. Select **All PDF Documents** in, in the **Where would you like to search** option, and type the pathname of the location where the PDF documents reside.

   If you have more than one VMware Smart Assurance product installed, you can set up cross-product document searches by copying files from the BASEDIR/smarts/doc/pdf directory for each product into this common documentation directory path.

Conventions used in this document

VMware uses the following convention for special notices:

Note NOTICE is used to address practices not related to personal injury.

Typographical conventions

VMware uses the following type style conventions in this document:

Bold	Use for names of interface elements
Italic	Use for full titles of publications referenced in text
`Monospace`	Use for: ■ System output, such as an error message or script ■ System code ■ Pathnames, filenames, prompts, and syntax ■ Commands and options
`Monospace italic`	Use for variables.
`Monospace bold`	Use for user input.
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections — the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Pathname conventions

Directory pathnames are shown with forward slashes (/).

Graphical conventions

Under UNIX, the consoles appear with slight differences. For example, in views that display items in a tree hierarchy such as the Topology Browser, an open circle appears for UNIX.

Manager

Unless otherwise specified, the term Manager is used to refer to VMware Smart Assurance programs such as Domain Managers, Global Managers, and adapters.

Where to get help

VMware Smart Assurance support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about VMware products, go to VMware Online Support at:

docs.vmware.com

Technical support

Go to VMware Online Support. You will see several options for contacting VMware Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your VMware sales representative for details about obtaining a valid support agreement or with questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Provide your feedback of this document to:docs.vmware.com

Troubleshooting

2

This chapter includes the following topics:

- Configuration issues
- Adapter issues
- NOTIF issues
- Notification and event processing issues

Configuration issues

This section provides troubleshooting help for the following issues:

- Synchronizing Service Assurance Manager with other Domain Managers
- Out-of-memory issue
- Checking status of underlying domain managers
- Identifying a port number
- Refreshing the console
- Reattaching to a Manager
- Responding to disconnected Managers
- Support is absent for IPv6 literal addresses in URLs
- Web Console or viewlets running out-of-memory
- SelectiveGroup and HierarchicalGroup instances lost when HierarchicalGroupManager is deleted or purged
- Inability to load dynamic library causes ASL errors
- Unable to build hierarchical groups while running group driver
- Containment view missing from Presentation SAM

Synchronizing Service Assurance Manager with other Domain Manager s

Symptom

Unable to synchronize Service Assurance Manager with IP Availability Manager.

Recommended action

Run the following command to synchronize Service Assurance Manager with IP Availability Manager:

```
<basedir>/smarts/bin/dmctl -s <sam_server> invoke GA_DaemonDriver::<am_server>_Topo-Driver start
dmctl -s INCHARGE-SA invoke GA_DaemonDriver::INCHARGE-AM-PM_Topo-Driver start
```

Out-of-memory issue

Symptom

Subscriber queue keeps growing in the server for a client that has become inactive. The queue processing thread in the server gets blocked in the socket during a write-operation, when the client stops reading data off the socket. However, keepAlives continue to be sent, thus keeping the connection active.

Possible cause

The out-of-memory issue may be occurring because there is a finite amount of memory process that can be used. Hence, if you have a very large topology or lot of notifications in the SAM repository, then it would result in hitting the limit. Memory usage increases to the maximum during topology synchronization because new topology objects are created during synchronization.

Recommended action

The solutions recommended include:

- Refactoring of domains (short term solution): Redesign your deployment to deploy additional Global Managers in a hierarchical Service Assurance configuration. Instead of using one SAM, split them into two. For instance, if one SAM is configured with 20 underlying domains, then start two SAMs with 10 each. This reduces the topology size and notification flow. Additionally, you can choose to reduce the archive interval from 4 hours (default) to a shorter interval. Also, topology can be trimmed by avoiding import of unnecessary classes.
- Refine notification lists for users.
- Re-assess the topology synchronization configuration.
- Refine sets of trap and syslog notifications sent to SAM.
- Increase worker threads used for escalation.
- If you are on a lower version of SAM, migrate to a higher version. This is a good long term solution.

  The VMware Smart Assurance Service Assurance Manager Deployment Guide provides detailed guidelines and procedures for assessing and improving performance of your deployment.

Logs or information to collect

- Run <*BASEDIR*>/smarts/bin/sm_monitor against the domain for collecting data every few hours.
- Use the <*BASEDIR*>/smarts/bin/sm_getinfo utility to collect logs and configuration settings if you intend to raise an issue with support.

  The VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managers provides details on using the sm_getinfo utility to collect data to help in troubleshooting problems.

Checking status of underlying domain managers

Symptom

Unable to figure out the operational status of the underlying domain manager.

Recommended action

If you do not know the operational status of your underlying domain manager, use the brcontrol command or the Browse button in the Attach Manager dialog box to list the Managers and their status. The status listed for your Manager should be 'Running.' If your Manager is not running state, contact your administrator, consult the VMware Smart Assurance System Administration Guide, or refer to your specific product installation guide for instructions on starting the Manager.

For the brcontrolcommand, type one of the command lines shown in The brcontrol command.

Table 2-1. The brcontrol command

Operating system	Example
UNIX	<*BASEDIR*>/smarts/bin/brcontrol

Identifying a port number

Symptom

Unable to find the port number of a domain manager.

Recommended action

If you do not know the port number of a domain manager, use the brcontrolcommand or the Browse button in the Attach Manager dialog box to display the port number.

Refreshing the console

Symptom

Console display is distorted.

Recommended action

If your console does not display properly, you can force the console to redisplay. For example, if fragments of menus or fields from dialog boxes linger after the menus or dialog boxes close, you can redisplay the console.

To refresh a console, select **View** > **Refresh**.

Reattaching to a Manager

Symptom

Machine running Service Assurance Manager becomes unavailable.

Recommended action

Initially, when you log in to start a session, you specify the Manager to which you want to attach. Ordinarily, you do not have to attach again during your session.

If the machine running the Service Assurance Manager becomes unavailable, the Global Console polls the broker every 30 seconds and reattaches when the Manager is operational.
VMware Smart Assurance Service Assurance Manager Operator Guide includes instructions on manually attaching or reattaching to an VMware Smart Assurance Manager.

Note If a VMware Smart Assurance Manager disconnects, a Domain Disconnected message appears informing you that the Manager disconnected and that the console will reconnect when the domain becomes available.

Responding to disconnected Manager s

Symptom

Underlying Managers get disconnected from the Global Manager.

Recommended action

When underlying Managers disconnect from the Global Manager (for example, due to a network outage), the notifications from the unavailable sources are not updated in the console. The affected notifications, maps, and summaries no longer reflect the current conditions.

If a disconnect situation occurs, a Session Disconnected notification informs you that a specific Manager is disconnected and a similar entry is added to the audit log.

When the Manager reconnects, the Session Disconnected notification clears, and it is recorded in the audit log.

If you receive a Session Disconnected notification, your administrator should investigate it for a network connection failure or an operational problem. The Manager may need to be restarted.

Support is absent for IPv6 literal addresses in URLs

Symptom

Firefox and Mozilla web browsers support IPv6 literal addresses in URLs.

Recommended action

Use Firefox or Mozilla web browsers instead of Microsoft IE if you need to use an IPv6 literal address to access the Web Console or Business Dashboard.

Web Console or viewlets running out-of-memory

Symptom

Depending on the heap space configured for the web browser in which the Web Console or Business Dashboard runs, the Web Console or the viewlets in the Business Dashboard may run out-of-memory. By default, the Web Console and viewlets allocate less heap space than the Global Console. Less heap space may result in out-of-memory errors in the Web Console or viewlets. For example, an out-of-memory error may occur in a Web Console that heavily uses large map background images.

Recommended action

If the Web Console or viewlets run out-of-memory, adjust the maximum amount of heap space that the Java Plug-in uses for dynamic memory allocation. For example, by specifying -Xmx256M as a runtime parameter you can increase the heap space allocation to 256 MB. The number can be set larger or smaller than 256 MB, depending on the resources available on the client machine running the web browser. To increase the heap space for the Java Plug-in:

1 Launch the Java Plugin Control Panel. For instructions, see:

```
http://java.sun.com/j2se/1.5.0/docs/guide/deployment/deployment-guide/jcp.html.
```

2 In the **Java Plug-in Control Panel**, click the **Java** tab.

3 In the **Java** tab page, click **View** in the **Java Applet Runtime Settings** box.

4 The **Java Runtime Settings** dialog box appears.

5 In the **Java Runtime Settings** dialog box, in the **J ava Runtime Parameters** text entry field for your JRE, type the maximum heap-space runtime parameter (**-Xmx**) and a value for the parameter. For example:

```
-Xmx256M
```

6 **Save** your entry. Click **OK** to close the Java Runtime Settings dialog box. Then click **OK** to close the Java Control Panel.

   Close and restart any web browser running on the host machine.

SelectiveGroup and HierarchicalGroup instances lost when HierarchicalGroupManager is deleted or purged

Symptom

If the HierarchicalGroupManager instance is deleted or purged due to some reason, the group instances are not visible.

Recommended action

The HierarchicalGroupManager instance maintains relationships with HierarchicalGroups and SelectiveGroups. SelectiveGroups are created using SAM console and HierarchicalGroups are created from configuration files. Once HierarchicalGroupManager instance is purged, the group instances are not visible since the relationship information is lost even though group instances are present in the repository.

In case of HierarchicalGroup instances, use the following steps to recreate them:

1 In the Global Manager Administration Console, expand **INCHARGE-SA** > **ICS Configuration** and click **Business Templates**.

2 Click **Modify List** on the **Configure "Business Templates"** screen.

3 On the **Edit Business Template** dialog-box, select a template from **Selected Template Files** and remove it.

4 From **Available Template Files**, add the template you just removed.

5 Click **OK** on the **Edit Business Template** dialog-box.

6 Click **Apply** on the **Configure "Business Templates"** screen.

7 Start the group driver by running the following command:

```
dmctl -s INCHARGE-SA invoke GA_DaemonDriver::ICS-Group-Driver start
```

   For recreating SelectiveGroup instances, run the following command:

```
./sm_adapter -s INCHARGE-linux ics/ics-restore-selectivegroup.asl
```

Inability to load dynamic library causes ASL errors

Symptom

In a typical SAM configuration, when the server is started it does not contain the dynamic library to load all custom classes, for example, UIM_O_AdapterManager. In a custom hierarchical SAM configuration, this may result in generating ASL errors.

Recommended action

The following configuration must be made in the hierarchical SAM area to avoid the generation of ASL errors:

1 Copy dyn_uii.ldm and dyn_uii.mdl files from the Service Assurance Manager *<BASEDIR>*/smarts/model/ics files to the *<BASEDIR>*/smarts/local/model/top-sam folder. Here, top-sam is the custom folder created for the top-level SAM.

2 Restart the server.

Unable to build hierarchical groups while running group driver

Symptom

No map console groups are created running the GA_DaemonDriver using the dmctl -s INCHARGE-SA invoke GA_DaemonDriver::ICS-Group-Driver start command.

Recommended action

If there are multiple hosts configured across groups, there may be an issue while creating hierarchical groups in SAM. Delete the disjointed hosts from the topology and the current map console structure, and run the script.

Containment view missing from Presentation SAM

Symptom

Containment view is missing from Presentation SAM, but is available in Aggregation SAM. The problem occurs because the Presentation SAM topology driver is hanging.

Recommended action

To resolve this issue:

1 Run the following command to determine the state of the topology driver:

```
<BASEDIR>/smarts/bin/dmctl -s <Pres SAM> get GA_DaemonDriver::<AGG SAM>_Topo-Driver
```

2 Compare the state of the topology driver with that of the SAM domain. If the topology driver state is GA_DRIVER_RUNNING, but the SAM domain topology does not indicate that topology sync is occurring, then the topology driver is hanging. The topology driver must only be running during a SAM domain topology sync. When no topology sync is occurring, the topology driver must display the status as GA_DRIVER_STOPPED.

3 If the topology driver is hung, restart the Presentation SAM domain to resolve the issue.

The 'TimeOutTopo' flag in the dxa-sam.conf file helps detect if a a driver hanging and will stop the driver so that the next topology sync will proceed normally. By default the TimeOutTopo flag is disabled. To enable the flag:

4 Open the dxa-sam.conf configuration file for editing in sm_edit as follows:

```
<BASEDIR>/sm_edit conf/ics/dxa-sam.conf
```

5 Find the 'TimeOutTopo' line. Remove the comment hash character (#) from the start of the line to enable the functionality, and increase the timeout value (in seconds). For instance change the line #TimeOutTopo 60 to TimeOutTopo 600.

Note The increased value (600) specified in the example and can be configured to a different value. From SAM 8.1 Service Pack 1 (SP1) release, the TimeOutTopo value is set to 600 seconds by default and the dxa-sam.conf configuration file still contains the option of changing the time out value. For more information on the TimeOutTopo flag, see the VMware Smart Assurance Service Assurance Manager Configuration Guide. Earlier versions of SAM will not have a default value.

6 Run a reconfigure operation in Presentation SAM or restart the Presentation SAM domain for the changes to take effect in the active environment.

Adapter issues

This section provides troubleshooting help for the following issues:

- Notification adapter fails to start
- Notification adapter starts, but fails to connect to VMware Smart Assurance Manager
- Email not received from Email Notifier
- Email received from Email Notifier, but not for all events
- File notifier does not create a log file containing notifications
- Not all events are recorded in the file notifier output
- No traps delivered to destination by trap notifier
- Not all traps delivered to destination by SNMP Trap Notifier
- Script is not invoked for Script Notifier Adapter

Notification adapter fails to start

Symptom

Notification adapter appears not to start. The issue may be seen across Email Notifier Adapter, the Log File Notifier Adapter, the SNMP Trap Notifier Adapter, and the Script Notifier Adapter.

Recommended action

When a notification adapter appears not to start, check the status of its process or service.

For an adapter started with the sm_notify command

For an adapter started as a service

For UNIX

Type the command from the <*BASEDIR*>/smarts/bin directory:

```
./sm_service start <service_name> [<service_name> ...]
```

where <service_name> is the service you need to start.

Additionally, you can check the sm_notify_en_US_UTF-8.log present in the <*BASEDIR*>/local/logs folder or use the sm_getinfo utility to collect data to help troubleshoot the problem.

The VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managers provides details for using the sm_getinfo utility.

Notification adapter starts, but fails to connect to VMware Smart Assurance Manager

Symptom

Adapter starts successfully without any error, but cannot connect to an VMware Smart Assurance Manager. The issue may be seen across Email Notifier Adapter, the Log File Notifier Adapter, the SNMP Trap Notifier Adapter, and the Script Notifier Adapter.

Recommended action

When an adapter cannot connect to VMware Smarts Assurance Manager, it is usually for one of the following reasons:

- VMware Smart Assurance Manager is not running.
- Name of the VMware Smart Assurance Manager is not the same as the name specified in the adapter's configuration file.
- VMware Smart Assurance Manager cannot be reached from the host running the adapter.

Check the status of the VMware Smart Assurance Manager

Use the brcontrol command to check the status of the VMware Smart Assurance Manager. The syntax is:

```
<BASEDIR>/smarts/bin/brcontrol
```

By default, this command returns a list of VMware Smart Assurance Managers registered with the broker and their current state. The list indicates whether an VMware Smart Assurance Manager's state is RUNNING or DEAD. If the VMware Smart Assurance Manager is not running or included in the list, restart the VMware Smart Assurance Manager.

Check the name of the VMware Smart Assurance Manager in the configuration file

The configuration file of each adapter contains the name of the VMware Smart Assurance Manager to which it connects. This value in the configuration file can be overridden by using the **--server** option with the **sm_notify** command.

In cases where an adapter cannot connect, check that the **--server** option, if used, points to a valid VMware Smart Assurance Manager. If that is not the issue, check that the appropriate VMware Smart Assurance Manager is specified in the adapter's configuration file.

Adapters andVMware Smart Assurance Manager parameters lists the configuration file and parameter to check for each adapter.

Table 2-2. Adapters and VMware Smart Assurance Manager parameters

Adapter	Location and name (relative to *<BASEDIR>*/smarts/conf)	VMware Smart Assurance Manager parameter
Email Notifier Adapter	/notifier/mail-notify.conf	serverName
Log File Notifier Adapter	/notifier/file-notify.conf	serverName
SNMP Trap Notifier Adapter	/notifier/trap-notify.conf	serverName
Script Notifier Adapter	/notifier/script-notify.conf	serverName

Check communication to the VMware Smart Assurance Manager's host

If the adapter and the VMware Smart Assurance Manager run on different hosts, the adapter's host might not be able to communicate with the VMware Smart Assurance Manager's host. From the adapter's host, run the following command:

```
dmctl
--server=<InCharge_Manager> ping
```

The results of this command show whether the VMware Smart Assurance Manager is alive or unavailable.

Email not received from Email Notifier

Symptom

When the Email Notifier Adapter starts and connects to the Domain Manager, the intended recipient receives no email.

Recommended action

The issue is usually caused due to an incorrect configuration. The configuration file for the Email Notifier Adapter is mail-notify.conf. This file resides in the <*BASEDIR*>/smarts/notifier directory.

There are three parameters that specify where the Email Notifier Adapter delivers information. Parameters needed to receive email lists these parameters.

Table 2-3. Parameters needed to receive email

Parameter	Description
MailServer	Name for the mail server. For example: MailServer = "localhost"
SenderId	Email address associated with the adapter. Users can reply to this address. This address must be recognized by the mail server. For example: SenderId = "daemon@localhost"
Recipients	A comma-separated list of the recipients of the emails. The recipients in the list must be recognized by the mail server. For example: Recipients = "root@localhost,recipient@your_company.com"

Check the parameters in the configuration file and verify them with your email administrator. All three must have a valid value for the Email Notifier Adapter to work. For the changes to the configuration file to take effect, the adapter must be restarted.

Email received from Email Notifier, but not for all events

Symptom

Email Notifier Adapter does not seem to be sending messages for all of the correct events.

Recommended action

The issue could be that the subscription profile is incorrect or that you expect the adapter to be sending messages when notifications clear. To resolve the issue you can:

Modify the subscription profile

When the Email Notifier Adapter sends email, but does not send them for all expected events, the issue usually is improper subscriptions. “Specifying subscriptions in the configuration file” in the VMware Smart Assurance Service Assurance Manager Notification Adapters User Guide contains instructions on modifying the subscription profile for this adapter.

Change the Email Notifier Adapter to send notifications of cleared events

By default, the Email Notifier Adapter does not send messages when a notification clears. It only sends messages for new notifications or when the certainty of the notification changes.

To enable the Email Notifier Adapter to send CLEAR notifications, change the following in the file, <*BASEDIR*>/rules/notifier/mail/mail-filter.asl:

```
START () {
OMIT_CLEAR_EVENTS
}
to
START () {
// OMIT_CLEAR_EVENTS
}
```

After making changes to the file, restart the adapter for the changes to take effect.

File notifier does not create a log file containing notifications

Symptom

The Log File Notifier Adapter starts and connects to the VMware Smart Assurance Manager, but it does not appear to create the notification file.

Recommended action

Check to ensure the filename is the one you expect. The Log File Notifier Adapter's configuration file, file-notify.conf, contains the name of the notification file. The file-notify.conf file resides in the <*BASEDIR*>/smarts/conf/notifier directory. The parameter, fileName, defines the name of the notification file that the adapter creates for its output. The adapter always creates the notification file in the <*BASEDIR*>/smarts/local/logs directory. If you do not specify a value, the adapter creates a default file named <InCharge_Manager>-alarms.log.

Note Do not confuse this adapter's output file with its log file. The log file also appears in the <*BASEDIR*>/smarts/local/logs directory. You determine the log file's name when the adapter starts using the **--output** command option. The default name of the log file is sm_notify.log. Never use the same name for both the notification file and the Log File Notifier Adapter's log file.

Not all events are recorded in the file notifier output

Symptom

The Log File Notifier Adapter sends information to the notification file, but does not send it for all of the correct events.

Recommended action

The issue usually is caused due to improper subscriptions. “Specifying subscriptions in the configuration file” in the VMware Smart Assurance Service Assurance Manager Notification Adapters User Guide contains instructions on modifying the subscription profile for this adapter.

No traps delivered to destination by trap notifier

Symptom

The SNMP Trap Notifier Adapter starts and connects to the VMware Smart Assurance Manager and does not send the SNMP Traps.

Recommended action

The issue is usually the format of the parameter Destinations. The parameter, Destinations, is a table that contains the SNMP trap destinations. Each row in the table is surrounded by curly braces and consists of three different values: hostname or IP address, port number, and SNMP version. The values are separated by commas. There are two valid values for SNMP version: V1 and V2C. These values and the values for host name or IP address must be surrounded by quotation marks. The port number is an integer value with no quotation marks.

Each row in the table is separated from the next by a comma. Place a comma after the curly brace that marks the end of each row in the table except for the last. An outer set of curly braces defines the entire table.

For example, the Destinations parameter could appear as follows:

```
Destinations = {
{"localhost", 162, "V1"},
{"other-host", 30162, "V2C"},
{"195.67.23.103",21539, "V2C"}
}
```

Not all traps delivered to destination by SNMP Trap Notifier

Symptom

The SNMP Trap Notifier Adapter sends traps, but does not send them for the correct events.

Recommended action

The issue is usually improper subscriptions. “Specifying subscriptions in the configuration file” in the VMware Smart Assurance Service Assurance Manager Notification Adapters User Guide contains instructions on modifying the subscription profile for this adapter.

Script is not invoked for Script Notifier Adapter

Symptom

This issue applies to the Script Notifier Adapter, where scripts are not invoked for the adapter.

Recommended action

To ensure that the script is invoked for the Script Notifier Adapter:

1 Ensure your script is located in <*BASEDIR*>/smarts/local/actions, and that it is readable and executable.

2 Check the configuration file to see that you have altered the file to include the correct name for the script you want to invoke.

NOTIF issues

This section provides troubleshooting help for the following issues:

- Unable to startup NOTIF
- NOTIF Java errors in server log

Unable to startup NOTIF

Symptom

SAM or OI server logs indicate that NOTIF is active, but also indicate that NOTIF did not start. The following error message is generated:

```
Checking NOTIF settings for start flag...
Loading JVM interface...
Initializing JVM interface...
*** Notif start thread created; returning.
Program initialization call returned.
......<few more lines>.....
*** NOTIF DID NOT START!
com.vmware.smarts.notif.entryPoints.notifIcEntryPoint$notifNotEnable
Exception: com.smarts.remote.SmRemoteException
Started: Specified property not found in class
MR-PROPERTY_NOT_FOUND-Specified property not found in class
SAM will continue to run without Notif
```

Recommended action

Check for the following:

- If the value for SM_JAVA_ENABLED parameter is set to YES in the runcmd_env.sh file. The The runcmd_env.sh file is located in the <*BASEDIR*>/smarts/local/conf directory.

- All libraries and jars are present in the lib and classes folder, respectively.
- SM_LIB_PATH contains the entry for the <*BASEDIR*>/smarts/lib and <*BASEDIR*>/smarts/local/lib.

Logs or information to collect

- <server_name>.log
- Notif.<server_name>.audit.* files
- *.ncf files in server configuration directories in all the sitemod locations
- Use <*BASEDIR*>/smarts/bin/sm_getinfo utility to collect logs and configuration settings if you intend to raise an issue with support.

  The VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, and NPM Managers provides details on using the sm_getinfo utility to collect data to help in troubleshooting problems.

NOTIF Java errors in server log

Symptom

'ClassNotFound' errors observed in SAM or OI server log depending on where NOTIF is configured.

Recommended action

Check if jars in notif-init.asl are available in the <*BASEDIR*>/smarts/classes or <*BASEDIR*>/smarts/local/classes folder.

Logs or information to collect

- <server_name>.log
  - Notif.<server_name>.audit.0 files
    - Individual trap logs (if applicable)
    - *.ncf files in server config directories in all the sitemod locations

Notification and event processing issues

This section provides troubleshooting help for the following issues:

- Viewing subscriptions for an event
- Unsubscribing from disabled events

Viewing subscriptions for an event

Symptom

Unable to identify subscriptions for a given event, but able to view the bootstrap subscriptions.

Recommended action

Use the following command to view subscriptions associated with an event:

```
dmctl> exec dmdebug subscriptions[=all] [output=]
```

Unsubscribing from disabled events

Symptom

Unable to unsubscribe from Disabled events using the Service Assurance Manager.

Recommended action

To allow the Service Assurance Manager to subscribe to all problem events except for Disabled events, modify the DXA file which is used by the Service Assurance Manager to communicate with underlying domains. This file is available under:

<*BASEDIR*>/SAM/smarts/bin/sm_edit conf/ics/dxa-conn.conf

In this file change:

```
sub .*::.*::.*/p
```

to:

```
sub *::*::~Disabled/pg
```

Add, the ChoiceSubscription->glob = glob("*g*", Modifiers) line to the <*BASEDIR*>/SAM/smarts/bin/sm_edit rules/ics/ics-event-driver.asl file for the Service Assurance Manager not to filter the current Disabled events, for example:

```
ChoiceSubscription->symptoms = glob("*s*|*e*", Modifiers)
ChoiceSubscription->glob = glob("*g*", Modifiers)
ChoiceSubscription->quiet = TRUE
```

Frequently Asked Questions

3

This chapter includes the following topics:

- Configuration queries
- Trap processing queries
- NOTIF queries
- Notification and Event processing queries
- Business Dashboard queries

Configuration queries

This section answers the following frequently asked questions on SAM configuration:

- Editing .conf files
- Enabling SAM scheduling maintenance
- Obtaining information on users logged to domains
- Using ASL to create file outside of logs directory
- Accessing console message logs

Editing .conf files

Query

When do I edit the trapd.conf and trap_mgr.conf files?

Answer

Edit the trapd.conf file when you want to forward traps; use this file to specify where to forward what set of traps. Edit the trap_mgr.conf if you are configuring the Adapter Platform to send notifications on to the Global Manager.

Enabling SAM scheduling maintenance

Query

I am unable to turn on the SAM Scheduling maintenance feature as the interface is grayed out. The necessary script files under the actions directory are also unavailable. The user does not have a BIM license. Is a BIM license required for the maintenance feature?

Answer

A BIM license is not a prerequisite for running the maintenance feature. However, the MBIM server needs to be running, with SAM domain configured as its source. Also, SAM should be subscribed to the MBIM domain.

Obtaining information on users logged to domains

Query

I need details on the SAM-Presentation login information. Is there a flag or setting that we can set to obtain details of whose logged into the domains?

Answer

The SM_OKLOGIN_LOGLEVEL environment variable enables the logging of successful logins at FATAL severity, rather than INFORMATIONAL. SM_OKLOGIN_LOGLEVEL is a Boolean. Set SM_OKLOGIN_LOGLEVEL=1 in the runcmd_env.sh file, located in the <*BASEDIR*>/smarts/local/conf folder. You must restart the domain for the change to take affect.

Using ASL to create file outside of logs directory

Query

Can we use ASL to create or write a file (ACT_FILE) outside of the logs directory?

Answer

No, you cannot create or write a file (ACT_FILE) outside of the logs directory using ASL.

Accessing console message logs

The Global Console has two logs which are useful for troubleshooting:

- The Java console is the first tool to use for console debugging. It shows store exceptions, errors reading attributes, and stack traces.

  To collect the most information about potential console problems, specify the -Dcom.smarts.log.level=TRACE property.

Java console information can automatically be saved to a file on your local workstation by specifying the -Dcom.smarts.java.log=<*filename*> property. When specifying this property, the file is written to the <*BASEDIR*>/smarts/local/logs directory.

SM_WRITEABLE is an environment variable whose default value can be changed in the runcmd_env.sh. Use this console information to assist with debugging issues.

Note Before starting the console with the -Dcom.smarts.java.log=<*filename*> property , verify that the <*SM_WRITEABLE*>/logs directory exists under the <BASEDIR>/smarts/local folder.

- The message log shows everything the Manager sends to the console while the log window is activated (opened or minimized).

  This information can automatically be saved to a file on your local workstation by specifying the -Dcom.smarts.server.logMessages=true property. When specifying this property, the file is written to the <*SM_WRITEABLE*>/logs directory. Use this information to assist with debugging issues when the console stops responding.

  Note Before starting the console with the -Dcom.smarts.server.logMessages=true

  property, verify that the <*SM_WRITEABLE*>/logs directory exists under the <BASEDIR>/smarts/local folder.

  To access the log views, select **View** > **Java Console** or **View** > **Message Log**.

  In the Java console, the following warning is benign:

```
Warning: Could not get the full set of system properties.
```

Trap processing queries

This section answers the following frequently asked questions on trap processing:

- Difference between Notification Adapter and Adapter Platform
- Traps sent not reflected in Adapter Platform Server
- Check for agent sending traps
- Forwarding traps to servers
- Ensuring traps reach Adapter Platform
- Verifying trap forwarding
- Debugging SNMP Trap Notifier
- Debugging SNMP Trap Notifier
- Defining two SNMP traps in trap_mgr.conf file
- Number of traps adapter or exploder can process
- Improving performance of trap adapter and trap exploder

- Defining sm_adapter parameters
- Log levels defined

Difference between Notification Adapter and Adapter Platform

Query

Are SAM Notification Adapter and the Adapter Platform the same?

Answer

No. The VMware Smart Assurance Service Assurance Manager Notification Adapters convert SAM Notifications and log them either by writing to a file, emailing them, sending the notifications as traps, and so on. The Adapter Platform receives traps and processes them into notifications.

Traps sent not reflected in Adapter Platform Server

Query

When I send a trap, why don't I see it in the Adapter Platform server?

Answer

Check the following:

- Ensure that your trap OID, both generic and specific is configured within the trap_mgr.conf file. The file located under the <*BASEDIR*>/smarts/conf/icoi folder.
- Ensure that the agent sending the trap is in the Adapter Platform server topology.
- Ensure that you are giving the correct hostname and port to where your trap receiver is running.

Check for agent sending traps

Query

How do I check if the agent sending the trap is in the Adapter Platform server?

Answer

The IP address of the device sending the trap must be in the Adapter Platform server, and must be hosted by (with a HostedBy relationship) some unified computing system (UCS) for the trap notification to be created.

To check the HostedBy relationship, use your topology browser or use the following dmctl command:

```
dmctl -s <OI-Server> get IP::IP-<AgentIPAddress>::HostedBy
```

To use the topology browser, check under IP section, expand it, select your IP and see if that it has a HostedBy relationship.

The UnknownAgent is set to IGNORE by default. To create a trap notification in the Adapter Platform, the value for UnknownAgent must be set to CREATE in the trap configuration definition, else traps will be dropped.

Forwarding traps to servers

Query

How can I forward the Adapter Platform processed traps to the IP Availability Manager server?

Answer

Edit the trapd.conf file located under the <*BASEDIR*>/smarts/conf/icoi folder to include the IP address and Receiving Trap Port where the IP Availability Manager server is running in the FORWARD section. An example is provided below:

```
#           All generic traps (0 to 5) from network devices whose address
#           matches 193.20.*.* will be sent to obelix port 7000, surya port 162
#           and host 194.56.78.23 port 9000.
#
#     FORWARD: 193.20.*.* .* <0-5> * obelix:7000 surya 194.56.78.23:9000
```

Ensuring traps reach Adapter Platform

Query

How do I make sure that the traps are reaching the Adapter Platform?

Answer

Use one of the following methods:

- Shut down your the Adapter Platform.
- Start the default trap adapter with the same port as the Adapter Platform.
- Send your trap and check if the default trap adapter generates any output.

  The VMware Smart Assurance Service Assurance Manager Adapter Platform User Guide provides details on the procedures.

Verifying trap forwarding

Query

How do I verify that the traps are getting forwarded by the forwarder?

Answer

Use one of the following methods:

- Check the **<** *BASEDIR*>/conf/trapd/trapd.conf to see which HostName:Port the traps are forwarded.
- Start the default trap adapter on HostName with the specified Port. For example, sm_snmp -p 9987 trapd.
- Send a trap to the forwarder (default port: 9000) and check if you see any output of the trap sent to the HostName.

Debugging SNMP Trap Notifier

Query

How do I debug the SNMP Trap Notifier?

Answer

In the <*BASEDIR*>/smarts/local/rules/notifier folder, look up the notify.asl file. This is the main rule set. Additionally, you can also see the trap-notify.asl in the trap directory. If you set debug=TRUE in these files you will be able to get sufficient debugging information.

Trap exploder function

Query

Can I have the Trap Exploder send traps to both BGP and the Receiver?

Answer

Yes you can. Infact, you can send traps to any destination you like.

Defining two SNMP traps in trap_mgr.conf file

Query

Is it possible to define two SNMP traps in the trap_mgr.conf file - one to generate a notification and a second one to clear it?

Answer

Yes, it is possible to define two SNMP traps in the trap_mgr.conf file. As the trap is defined by the OID generic and specific, you can only have one definition for a particular combination. At times, the notify and clear are determined by the specific number, with one being notify and one being clear. If the status is contained in a varbind, you will need to use a single trap definition and then use the ASL option to set the action to notify or clear. An example is provided below:

```
-----------------------------------------------------
BEGIN_TRAP .1.3.6.1.4.1.9.5.* 6 1
        ClassName:        Host
        InstanceName:     $SYS$
        EventName:        lerAlarmOn
        Severity:         2
        EventText:        Fddi PORT Ler Flag set to TRUE for : fddi PORT SMT Index = $V1$ And fddi
PORT Index = $V2$
        Expiration:       600
        State:            NOTIFY
        EventType:        DURABLE
END_TRAP
BEGIN_TRAP .1.3.6.1.4.1.9.5.* 6 2
        ClassName:        Host
        InstanceName:     $SYS$
        EventName:        lerAlarmOn
        State:            CLEAR
END_TRAP
-----------------------------------------------------
```

Number of traps adapter or exploder can process

Query

What is the maximum number of traps per second that the trap adapter or exploder can process?

Answer

The number of traps that can be processed depends on the trap configuration, mainly hook scripts and the execution of the findComputerSystem call. The ideal rate without any kind of delay should be about 30-40 traps per second, with 4 threads. But on an average, the trap processing rate is around 15 traps per second. Again, these numbers are very subjective to the environment and the configuration.

Improving performance of trap adapter and trap exploder

Query

What is the best way to increase the performance of the trap adapter and trap exploder to better handle the traps hitting the exploder with more threads.

Answer

You can increase the performance of the trap adapter and trap exploder by:

- Keeping the number of threads for the Trap Exploder as default (1)
- Increasing the number of threads processing the traps for Trap Adapter

  You can specify these values in the trapd.conf and the trap_mgr.conf files for the Trap Exploder and Trap Adapter, respectively. The trapd.conf and trap_mgr.conf files files are available under the <*BASEDIR*>/smarts/conf/icoi/ folder.

  Find the line, #THREADS: 1 in the configuration files. The default value specified is 1. Retain the default entry for the trap exploder. For the trap adapter you can change the value for the threads to five.

Defining sm_adapter parameters

Query

Can you define the sm_adapter parameters: --loglevel and --errlevel? What are the allowed levels and what is expected to be seen when they are set.

Answer

Most messages printed by VMware Smart Assurance code use the exception logging mechanism with something like CI_ExException(...).log(), or SM_System logXXX() calls from ASL. The exception logging mechanism can send messages to one of two receivers, which could be the:

- Log file
- System error logger, which is the syslog mechanism on UNIX systems

  The second mechanism has the potential to cause problems. On UNIX systems, the syslog files are typically on small partitions, for example, /var/tmp. There have been cases where attempts to start VI failed because it uses /var/tmp for temporary files, and /var/tmp is filled with a huge log of messages from the VMware Smart Assurance server. Deleting the log file would temporarily solve the problem, but the system logger re-creates it and it will promptly start growing again. The exception logging mechanism is controlled by the severity level assigned to the message being logged. In the order from most to least severe, a message can have one of the following severity levels:

  Fatal, Error, Warning, Notice, Informational or Debug

  You can individually assign, to each of the two receivers, the minimum severity level for messages to be sent to that receiver. By default, the log file receives messages of severity Warning or above, and the system error logger receives messages of severity Error or above. Two standard options available with all VMware Smart Assurance main programs control these two levels:

- --errlevel: controls the minimum level for writing to the log file

- --loglevel: controls the minimum level for sending to the system logging facility

  If you use --help, you will see that there you can specify any of the listed severity levels as a value for either of these options, as well as a couple of additional levels that make sense to syslog, but which are synonyms for Fatal for the VMware Smart Assurance code. In addition, you can specify None to completely disable a particular receiver.

  If it is inconvenient to change your startup scripts, you can use the SM_MAIN_OPTIONS environment variable. Any standard option that appears in this variable becomes the default. You can override these default values on the command line. Thus, after setting:

- SM_MAIN_OPTIONS=--loglevel=None
- export SM_MAIN_OPTIONS

  any VMware Smart Assurance program you start will, by default will not send anything to the system error logging facility. To avoid having to actually look at the system log files always, you can set this in your .profile.

Log levels defined

Query

What do the log levels mean?

Answer

The log levels are defined below:

- \begin\item[FATAL]: Indicates a serious internal error. A FATAL error is raised only in circumstances where continued execution of the entire application is in question. Unless otherwise handled by an application code, a FATAL exception in any thread will cause the entire program to exit.
- \item[ERROR]: A serious error that indicates that a requested function cannot be accomplished. However, the application itself will normally be expected to continue. Unless otherwise handled by the application code, an ERROR exception in any thread causes that thread, but not the program as a whole, to exit.
- \item[WARNING]: Indicates that something unexpected happened. While the requested function was completed, it may not have been completed exactly as expected. Unhandled exceptions of this and lesser priority are logged but do not necessarily cause a thread to exit.
- \item[NOTICE]: Indicates that something unexpected happened that should be logged, but is not expected to interfere with normal functioning.
- \item[DEBUG]: A catch-all for debugging code.

- \end: Despite these intended meanings, an application may catch even a FATAL exception that it knows how to recover from and continue operation.

  There are a few exceptions to these definitions. For example, login failures are logged at FATAL level since they are considered important, even though they are completely recoverable as far as the application itself is concerned. There is an additional standard option, --tracelevel. An exception at this level or above causes a stack trace to be printed to the log file. This log tells you exactly where the exception was thrown, which may be more important that where it was caught and logged. By default, --tracelevel is set to Fatal.

NOTIF queries

This section answers the following frequently asked questions on NOTIF:

- Error messages in Adapter Platform log file

Error messages in Adapter Platform log file

Query

After enabling NOTIF, the following messages appear in the Adapter Platform log file:

- discardUnknownAgent.java. Got unknownAgentSetting: IGNORE
- discardUnknownAgent.java. Got ignoreUnknowns: true

Answer

Set the value for the environment variable, SM_JAVA_ENABLED to YES in the runcmd_env.sh file, available under the <*BASEDIR*>/smarts/local/conf/ directory.

Notification and Event processing queries

This section answers the following frequently asked questions on notification and event processing:

- Handling notification flooding
- Scenarios triggering NL_Delete
- Command to get queues
- Getting each notification to invoke the tool
- Identifying all subscriptions and subscribers to events
- Creating notifications using the Java API

Handling notification flooding

Query

For an ASL notification adapter subscribing to NL_Notify, NL_Change, NL_Clear, NL_Delete events, what happens if there is a flood of notifications? Is SAM able to queue them internally and make sure it passes all of them to the subscribing modules? Does it make sense to implement a queue-like data structure in the ASL adapter to first buffer the notifications before processing them.

Answer

There is no need to create your own queue. The SAM server creates the queues internally, and then feeds the alarms one at a time into the ASL script. Once the START rule is complete, then the next notification will be processed. So, if you do not write an efficient ASL script then it becomes a bottleneck and the queues in SAM build up, using up memory, and subsequent crash.

The only way that you can speed up the processing is by having multiple notification lists feeding multiple ASL scripts.

Scenarios triggering NL_Delete

Query

What are the scenarios in which NL_Delete will be triggered?

Answer

NL_Delete occurs when the event is archived or removed from the NL because of certain filtering actions.

Command to get queues

Query

What is the dmdebug command to get queues?

Answer

Run the following command to get queues:

```
dmctl> execute dmdebug --queues
```

This prints information about all server queues in the system into the server log file. An example for the queue output is provided below:

```
SubscriberFE                                        [0 worker(s)]
Current size 0, max 369; processed entries 21843
Size           0-0.00            0-0.00            0-0.00             0-0.00
Flow       21839+0.06        21803+0.05        21446+0.05         17895+0.06
Late      0.0000+0.00       0.0000+0.00       0.0000+0.00        0.0000+0.00
```

In the example, the first line gives you the name of the queue and the number of workers.

Note Subscriber Front Ends like the one cited here never have any workers, since they are not used as normal server queues.

The second line gives you the current size, and an exact maximum size. The total number of 'processed entries' indicates the total number of entries that have ever been pulled off the queue.

Getting each notification to invoke the tool

Query

We have escalation policies set to run automatic server tools which text, page or email various recipients. We noticed that sometimes we do not get paged or emailed. I did some testing and it seems that only the first notification of an event invokes the tool, until the notification is archived. Is anyone familiar with how to get each notification to invoke the tool with each notification?

Answer

You can do it with two escalation policies, and using a tag value in a user defined field.

- The first escalation policy triggers on the following conditions and executes the automatic tool:
  - STATUS == ACTIVE
  - USERDEFINED != TAG
- The second escalation policy triggers on the following conditions and clears out the tagged field:
  - STATUS == INACTIVE
  - USERDEFINED == TAG

    Then if the notification becomes active again, the criteria for the first escalation policy are met again and the automatic tool will be invoked again.

Identifying all subscriptions and subscribers to events

Query

Is it possible to identify if there is somebody who is subscribed for a given event or see all subscriptions, not just the bootstrap subscriptions?

Answer

Use the following command to see if anybody is associated with an event:

```
dmctl> exec dmdebug subscriptions[=all] [output=]
```

Creating notifications using the Java API

Query

We would like to create notifications in SAM directly from the Java API. Using the sm_ems command line interpreter is not an option. The device already exists within the IP/AM topology, but this is a Non-SNMP device. Messages are received through XML containing information on the notification details. It has to be through the Java API, and not use the ASL open adapter either as everything will run from a single adapter framework.

Answer

Use the dynamic model to define the new events that you want created. Then, you can use the Java API to toggle boolean flags. The VMware Smart Assurance MODEL Reference Guide and the VMware Smart Assurance Dynamic Modeling Tutorial provide examples of exporting new events.

If are using external instrumentation sources, you must use the "External" polling settings in AM/PM. To enable these, log into domain using the GUI, select the Domain Manager Administration Console > Polling and Thresholds. Once this is done, your instrumentation logic can set attributes in the instrumentation objects (follow the InstrumentedBy relationship in the Interface and IP objects).

Business Dashboard queries

This chapter includes information for troubleshooting the VMware Smart Assurance Business Dashboard and contains the following information:

- Business dashboard troubleshooting overview
- Debugging the Web Console
- Configuring the log file directories
- Configuring the log files
- Sun Java Console (Plug-in message log)
- Log file location
- Increasing the heap space

Note The information contained in this chapter should be checked against your installation before problems arise. Contact VMware Online support if it becomes necessary to clarify or resolve any questions or issues.

Business dashboard troubleshooting overview

When troubleshooting reasons why the Web Console stops responding, the following files and parameters are reviewed:

- Required files

  When troubleshooting issues, VMware always asks for the following files:

  - RPS files
  - Service Assurance Manager server log files
  - tomcat log files
  - sm_monitor log files
  - Console log files
  - ics.conf files

    The console log files include the VMware Smart Assurance Java Message log file, the Sun Java Plug-in Console log file, and the VMware Smart Assurance VMware Smart Assurance server messages received log file. By reviewing the console log files, VMware Smart Assurance can clearly determine if the console stopped responding because the system ran out of memory, or if the issue was the result of some other error. Using the server log file, VMware can review what occurred at the time the console stopped responding; for example, was the server busy or was there some other exception.

    From prior experience, a Web Console or Global Console stops responding as a result of the machine running out of memory.

- Debugging parameters

  To have debugging information entered in the log files, you must have the console debugging parameters set by default, before you use the console and the console stops responding. You need to verify that the debugging information is being entered into the log files before there is a problem. Having the debugging parameters set ensures that no critical information is lost.

- Primary Java log file

  The primary Java log file is the key tool used in diagnosing issues. This file gets overwritten at each startup time and is the file that saves the contents of the Console Java Log. Enable this file by typing the following command:

```
-Dcom.smarts.java.log=<
filename
>
```

- Asynchronous message log file

  This log file is controlled by versioning. This file can get very large if the server is processing numerous notifications. Enable the asynchronous message log file by typing the following command:

```
Dcom.smarts.server.logMessages=true
```

Debugging the Web Console

Query

How do I go about debugging the Web Console?

Answer

Web Console debugging parameters defines the parameters used to capture information when a Web Console stops responding.

Table 3-1. Web Console debugging parameters

Parameter	Description
-Xmx350m -Dsun.net.inetaddr.ttl=0	This parameter gets around the broker failover cache problem.
-Dcom.smarts.server.logMessages=true	This parameter logs all the asynchronous messages that the server sends to the console, primarily, notification adds/changes/deletes.
-Dcom.smarts.java.log=<name>-webconsole.log	This parameter saves the VMware Smart Assurance Java Message Log content. This content is lost when the console stops responding. This log file must be copied and saved before restarting the Web Console. Content included in this log file could provide information on why the console stopped responding. Restarting the Web Console overwrites this file.
-Dcom.smarts.log.level=TRACE	This parameter results in maximum information being entered in the Java Message Log.
Heap size	VMware has tested a heap size of 350 M

Note The parameters are configured in the Java Plug-in Control Panel.

Configuring the log file directories

Query

How do I set up the log file directories when the VMware Smart Assurance GUI is running as a Web Console in Internet Explorer?

Answer

You can set up the log file directories for the com.smarts.server.logMessages and com.smarts.java.log files when the GUI is running as a Web Console in Internet Explorer. The parameters can be enabled if they are set in the Java Control Panel in the workstations. To display the **Java Control Panel**, click **Settings** > **Control Panel** > **Java**.

Internet Explorer defaults the console's com.smarts.writeable parameter to the desktop location where log files are written. You can verify this in the Sun Java Console window (not the Smarts Java Log file).

To verify that the com.smarts.writeable parameter is configured correctly:

From Internet Explorer, click **Tools** > *Sun Java Console*.

The Java Console appears. An example of the type of information available from the Sun Java Console is:

```
Java Plug-in 1.4.2_06
Using JRE version 1.4.2_06 Java HotSpot(TM) Client VM
User home directory = C:\Documents and Settings\bm1.SMARTS
----------------------------------------------------
c: clear console window
f: finalize objects on finalization queue
g: garbage collect
h: display this help message
l: dump classloader list
m: print memory usage
o: trigger logging
p: reload proxy configuration
q: hide console
r: reload policy configuration
s: dump system and deployment properties
t: dump thread list
v: dump thread stack
x: clear classloader cache
0-5: set trace level to <n>
----------------------------------------------------
Properties: com.smarts.fixed, com.smarts.sitemod, com.smarts.writeable not found.
Defaulting com.smarts.fixed, com.smarts.sitemod, com.smarts.writeable paths to: C:\Documents and
Settings\bm1.SMARTS\Desktop
```

The Properties line defines the location of the com.smarts.writable path. In this example, the path has been defaulted to the desktop and the user ID has been defined by default as the user ID for the specific workstation (in the example, the user ID is: bm1.SMARTS).

Configuring the log files

Query

How do I retrieve the log files when running the Web Console?

Answer

To retrieve the log files when running the Web Console:

1 Verify that the log files have been configured.

   VMware Smart Assurance Service Assurance Manager Dashboard Configuration Guide provides additional information on configuring log file directories.

2 Create a new folder labeled “logs” on the workstation's desktop.

3 Click **Settings** > **Control Panel** > **Java**.

   The **Java Control Panel** appears.

4 Click **Advanced** and add a new Java Runtime Parameter. (For Java 1.5, click the Java tab and then click the View button to display the Java Runtime Settings window.) An example of the settings is:

   -Dcom.smarts.server.logMessages=true

   -Dcom.smarts.java.log=ZZZZ

   -Dcom.smarts.log.level=TRACE

5 Edit the -Dcom.smarts.java.log=ZZZZ to the name of your java log file.

   Note This log file does not get appended with versions. It needs to be saved before restarting the console. If the file is not saved before starting the console, the contents of the file are overwritten.

   After configuring the java log file location, when you run Internet Explorer, the log of server message log file and the java log file are written into the desktop's logs directory. The java log file lists trace level messages.

   Because the parameter was updated in the client’s Java Plug-in, you do not need to restart the tomcat application.

   You need to configure the log files location before a console stops responding so that information about the console not responding can be retrieved. Verify that the two debugging files (webconsole.log and server_Mesg_<*userid*>.log) get written to the logs directory.

Sun Java Console (Plug-in message log)

Query

How do I enable the Sun Java Plug-in and capture its content?

Answer

When the VMware Smart Assurance GUI is run as a Web Console, important debugging information is written to the Sun Java Plug-in Console. When the GUI stops responding but Internet Explorer continues to run (for example, if the web browser window goes blank), it is helpful to capture the contents of the Sun Java Plug-in console.

To enable the Sun Java Plug-in Console

To enable the Sun Java Plug-in Console:

1 From Settings, click **Control Panel**.

The **Control Panel** appears.

2 Double-click **Java**.

The **Java Control Panel** appears.

3 Click **Basic** (for Java 1.4.2) or click **Advanced** for Java 1.5.

4 Expand the **Java console** option.

5 Click the **Show Console** option.

By default, the Sun Java Plug-in Console displays as a window (typically in the upper-left corner of the screen) in Internet Explorer. You can also display the Sun Java Console by clicking the Internet Explorer's Tools menu and selecting the Sun Java Console.

Capturing the Sun Java Plug-in Console content

To capture the Sun Java Plug-in Console content:

1 From the Java Console, click **Copy**.

The content displayed in the Sun Java Console is copied to the clipboard.

2 Open a new file in a text editor and paste the clipboard contents into the new file.

3 Save the file and send the file to VMware along with other debugging information.

Note If you are reporting Web Console problems that did not cause the Web Console to stop responding, you should also copy, save, and send this log file.

Log file location

Query

Where do I find the log files for debugging issues related to the Web Console?

Answer

Log file location defines the log file locations.

Table 3-2. Log file location

File/ or log name	Location
rps file	<*BASEDIR*>/smarts/local/repos/icf directory. Run dmctl -s NA-SAM-PRES and invoke the ICF_PersistenceManager::ICF-PersistenceManager. Save this information before sending the rps file to ensure all notifications are saved to the rps.
SAM server log	<*BASEDIR*>/smarts/local/logs directory.
sm_monitor logs	<*BASEDIR*>/smarts/local/logs/SM_Monitor directory.
Tomcat logs	<*BASEDIR*>/smarts/jakarta-tomcat-5.0.16/logs directory from where tomcat started.
ics.conf file	<*BASEDIR*>/smarts/local/conf/ics directory.
Console logs	C:\Documents and Settings\<*username*>.SMARTS\Desktop\logs directory.

Increasing the heap space

Query

How do I increase the heap size for the Java Plug-in and for Java Web Start.

Answer

If the Web Console or viewlets run out of memory, adjust the maximum amount of heap space that the Java Plug-in uses for dynamic memory allocation. By specifying -Xmx256m as a runtime parameter, for example, you can increase the heap space allocation to 256 MB. The number can be set larger or smaller than 256 MB, depending on the resources available on the client machine running the web browser.

To increase the heap space for the Java Plug-in:

1 Launch the Java Control Panel. The Sun website provides instructions (http://java.sun.com).

2 In the Java Control Panel, click the Java tab.

3 In the Java Runtime Environment Settings section, click the View button. The Java Runtime Environment Settings dialog box appears.

4 In the Runtime Parameters field, type the maximum heap-space runtime parameter (-Xmx) and a value for the parameter. For example: -Xmx330m.

5 Click OK.

6 Click the Java Control Panel Apply button.

7 Terminate and restart any web browser running on the host machine.

For the Java Web Start, the heap space defaults to 350 megabytes.

Increasing Java Web Start heap space

To increase the heap space for the Java Web Start:

1 Using a text editor, open the <BASEDIR>/smarts/tomcat/webapps/webconsole/globalConsoleApp.jnlp file.

2 Locate the following line:

```
<j2se version="1.6.0+" max-heap-size="350M"/>
```

3 Change the max-heap-size variable value.

4 Save and close the file.