Troubleshooting
Avaya Aura™ System Manager 1.0

Avaya Aura™ System Manager 1.0
May 2009

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site: http://www.avaya.com/support

Licenses

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/ThirdPartyLicense/

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya Products should be reported to Avaya by sending mail to: securityalerts@avaya.com

Trademarks

Avaya, the Avaya logo, Avaya Aura™ System Manager are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions. All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya Inc. provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya Inc. provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Table of Contents

Overview

This Troubleshooting document provides information designed to help you resolve issues on Avaya Aura™ System Manager. This document provides a general approach for troubleshooting System Manager and describes how to use Avaya InSite Knowledgebase to look up procedures and specific solutions for a given symptom. General information on logs, alarms and security is given next.

URL: http://support.avaya.com
Click on Advanced Search. Select Product="System Manger". Select Document Type = "Problem Solution" for System Manager FAQ entries.

This document has troubleshooting advice for two audiences: 1) developers for Avaya products that are integrating with System Manager 1.0 and 2) users (Avaya customers).

System Manager is a management framework that is used to manage itself and other Avaya applications. Troubleshooting other Avaya applications is beyond the scope of this document. This document covers the general strategy for using System Manager as a starting point for troubleshooting other Avaya applications as well as for troubleshooting System Manager itself.

1. Alarm received at the Avaya Data Center
2. Use Services procedure to determine location and remote access steps the System Manager running on the customer premises
3. Follow procedure to have customer create temporary Services account
4. Log into the System Manager Common Console (https://<IMSMIPAddress>/IMSM/)
5. Use the left navigation bar to navigate to Monitoring

Alarms and Logs

System Manager generates alarms to notify users of system events. Alarms are grouped by categories. Each alarm category identifies the system component that generates the alarm. All alarms are generated from log messages based on mapping rules defined in the System Manager SPIRIT Agent configuration; there is no separate alarm generation facility. System Manager will forward alarms to Avaya Services SPIRIT Enterprise (if so configured). System Manager can also be configured to send SNMP traps to the customer NMS.

Since System Manager is a software-only offer, System Manager produces no alarms based on OS events. Currently System Manager does not generate any alarms for third party packages such as postgres and JBoss. Since none of these 3rd party packages produces logs in Avaya Common Log Format, the logs will not be registered in the System Manager Log Viewer either.

System Manager has a requirement for logs (and therefore alarm text) to be "helpful" and provide corrective action when possible. Therefore there is not much utility in providing a list of alarms in this document since no additional information will be known. Unhelpful logs/alarms should

have MRs written against them. However, certain common alarms or sequences of alarms may have a useful troubleshooting approach that is too lengthy to include in the alarm text itself. Those procedures will be document on InSite (and temporarily within this document as the System Manager team discovers repeated patterns of common alarms.)

Log File Types

Per the Avaya Common Log Format Specification, System Manager produces the following types of logs:

- Operational –viewable in the System Manager Log Viewer
- Audit—viewable in the System Manager Log Viewer
- Security—viewable in the System Manager Log Viewer
- Trace/Debug—NOT viewable in the System Manager Log Viewer. One must look on the local file system for these logs

Log File Locations

The majority of System Manager logs are found in /var/log/Avaya/mgmt/<domain>, where domain is an System Manager component. Each domain's directory will have audit, operational, debug and security log files. Not all domains implement auditable or security-related functionality, so those logs files will be empty. The spirit directory is for logs generated by the SPIRIT Enterprise components. The spiritlogs directory is a staging area for logs to be sent to the centralized System Manager log database and log viewer. The information in this directory is redundant with logs in other directories.

Other notable places to find logs:

- /opt/Avaya/SPIRIT/1.0.1/logging – SPIRIT Agent logs
- /opt/Avaya/install_logs – installation logs
- /opt/Avaya/JBoss/4.3.0/jboss-eap-4.3/jboss-as/server/avmgmt/log – JBoss logs for System Manager (not JON)

Security

Provides information on security issues, including:

- IP Port usage document is stored in COMPAS ID: 139536
- Additional Security information
- Additional security information and documentation about all Avaya products, including System Manager and the Avaya components that integrate with System Manager are available at the Avaya Security Advisories Website. For example, you can find information about the following:

- Avaya Product Security Vulnerability Response Policy
- Avaya Security Vulnerability Classification
- Security advisories for Avaya products
- Software patches for security issues

- Reporting a security vulnerability
- Automatic e-mail notifications of security advisories

You can also find additional information about security practices at the National Security Agency Security Configuration Guides Website.

Resolving General Issues

General Troubleshooting

How to find the detailed System Manager version

Description of Symptom

How does one determine the complete System Manager version string.

Cause

N/A

Proposed Solution

1) On an installed box: /opt/Avaya/Mgmt/<version>/installer_relno.txt

2) Through the Common Console UI: Settings -> Service Profile Management -> System Manager 1.0 -> applicationMetadata, versions_detail

What are the hardware requirements for System Manager?

Description of Symptom

What are the server requirements for System Manager?

Cause

N/A

Proposed Solution

4 Gigabytes of RAM, 3.0 GigaHz processor, at least 80 Gigabytes of disk with enough additional disk to hold logs records.

Release-to-release compatibility table. Can System Manager X.Y run on the same HW/OS as the previous release?

Description of Symptom

The Avaya CTO Manageability and Serviceability standards require a matric that shows if new releases of a product can run on previously supported hardware.

Cause

N/A

Proposed Solution

Since System Manager 1.0 is the first release, this table does not apply.

Information needed by support team to start Troubleshooting

Description of Symptom

Description of information is needed by support team in order to start trouble shooting.

Cause

N/A

Proposed Solution

1) Problem description
2) Steps through which problem can be reproduced.
3) The installer build in which the issue is occurring.
4) Java version used to do installation
5) Was it an upgrade? If yes, upgrade was done from which version? If not, was there any previous installation that has been manually cleaned?
6) Installation log files (refer section on Alarms and Logs for details on the location of the files)
7) Server log file (i.e., server.log) available at <JBOSS_HOME>/server/avmgmt/log.
8) The log of that domain available at /var/log/Avaya/mgmt/<domain-name>.

Installation

Installer throws error "Invalid encryption key"

Description: The user is prompted to enter an encryption key at the start of the installation. The encryption key is used to encrypt the passwords in the response file. No matter whatever encryption key is entered, installer always throw error "Invalid encryption key".
Cause(s): Java 1.4 is used to run installer
Proposed Solution: Make sure you use Java 1.6 or higher version. Check java version you are using by **java -version** command it should point to 1.6 or higher version.

Installer throws error "Encryption key is incorrect"

Description: : The user is prompted to enter an encryption key at the start of the installation. The encryption key is used to encrypt the passwords in the response file. Every time the installer is executed, it always throw an error "Encryption key is incorrect".

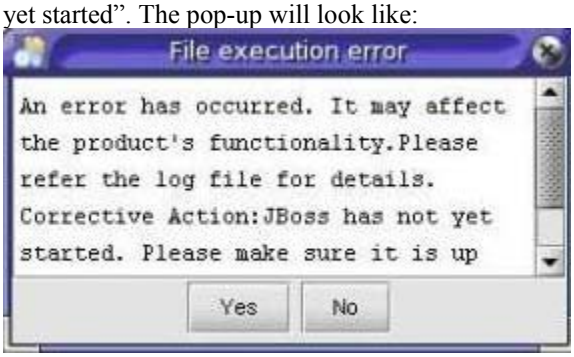
Cause(s): The script to run installer was executed first time with some other encryption key.

Proposed Solution: Follow below steps:

1. If there is any previous installation clean it. Follow details mentioned in section 2.1.9 if manual cleanup of previous installation is required.
2. Extract the installer zip in a new directory and run installer from the newly extracted files.

Received an error pop-up saying "JBoss has not yet started".

Description: An error pop-up is received during installation saying that "JBoss has not yet started". The pop-up will look like:



Cause(s): JBoss is taking more time to start then the specified sleep time

Proposed Solution: Follow below steps

- Keep installation on hold by not pressing "Yes"/"No".
- Check if there is a process for JBoss using following command **ps –aef | grep run.sh**
- If JBoss process exists, open a browser and hit the URL **https://<ip-address>/jmx-console** or **https://localhost/jmx-console** (user admin/admin credentials to access the page)
- Make sure jmx-console appears. If jmx-console is taking some time to come up, wait till it comes.
- Click yes in above mentioned pop-up.

Trust Management script failed during installation

Description: An error pop-up is received during installation with error that trust management script has failed

Cause(s): Either JBoss has not started till the time Trust management initializing scripts are not executed or Unlimited Strength JCE jar files are not replaced before installation.

Proposed Solution: Follow below steps

- Keep installation on hold by not pressing "Yes"/"No".
- Make sure that the JBoss is running using the details specified in section 2.1.3.
- Make sure that the Unlimited Strength JCE jar files specified in the installer user manuals pre-requisite section is present in **<JAVA_HOME>/jre/lib/security** (for JDK) and **<JRE_HOME>/lib/security** (for JRE).
- If CA Initializer has failed then run trust CA initializer in a new terminal window from the **$MGMT_HOME/trs/** directory using command **sh trust_ca_initializer_install.sh -RMIPORT 1399**.

- If Trust Initializer has failed then run trust initializer in a new terminal window from the **$MGMT_HOME/trs/** directory using command **sh trust_initializer_install.sh -RMIPORT 1399 -HTTPORT 8380 -TMCONFIGLOC $JBOSS_HOME/server/avmgmt/conf/tm**

The silent/unattended installation is failing due to pre-requisite check failures

Description: The silent/unattended installation fails due to failure of some pre-requisite checks and installation can't be continued.
Cause(s): This is as per design that unattended installation should not proceed if there are failure in pre-requisite checks.
Proposed Solution: Invoke the installer with the "***-p ignore***" argument. This will continue the installation even if there are failure in pre-requisite checks.

Installer execution gets stuck or hangs

Platform: Solaris
Description: Installer execution gets stuck or hangs
Cause(s):
Proposed Solution: Ensure that /etc/profile does not have an entry for **bash** command. If there is any such entry:

1. Remove the entry from the file
2. Clean the installation using steps specified in section 2.1.9
3. Execute the installer again.

How to do an installation on the second and subsequent nodes in a cluster setup?

Description: Need to do a cluster setup with Postgres as database. How to do installation on the second and subsequent node?
Cause(s):
Proposed Solution: For a cluster installation setup on the second or additional node, please make sure that you have unselected the Postgres pack in the packs selection panel. Follow the steps specified in installer user manual for the cluster information.

The installation failed. What should one do?

Description: Installation has failed and you would like to debug from the logs what were the reasons for failure
Cause(s):
Proposed Solution: Follow sequence of steps below

4. Check the installation logs for errors. The log file following the naming convention as integrated_management_system_manager_1_0_install-log_<yyyy>-<mm>-<dd>_<hh>.<mm>.<ss>.txt and should be present under "/tmp" (if installation was aborted) or <INSTALL_PATH> if the installation was completed.
5. Clean the failed installation by following the steps specified in section 2.1.9.
6. Follow the corrective actions specified in the install logs.
7. Run the installer again.

JON Server/Agent does not start

Description: JON Server/Agent is not getting started
Cause(s):
Proposed Solution: Follow below steps:

1. Ensure that the directory for jdk5/jre5 and its sub-directories and files have permissions 777. This can be done using command **ls –l <jdk5/jre5 location>**. Use command **chmod -R 777 <jdk5/jre5 location>** to assign permission recursively on the directory.
2. Restart the JON Server/Agent.

System Manager Console

Can't access System Manager console from remote machine

Description: The System Manager console is accessible from the local machine where System Manager is installed but not from the remote machine
Cause(s): The firewall is enabled on the machine where System Manager is installed and is stopping the user request.
Proposed Solution: Disable the firewall and try again.

The response time of all pages in System Manager console is high (i.e., > 10 seconds)

Description: Accessing any page of System Manager console is taking too much time to display the new page.
Cause(s):
Proposed Solution: Add the IP (if accessing using IP) or fully qualified host name (if accessing using hostname) to the "No proxy for…" setting of the browser.

Clicking any navigation menu link redirects to the login page

Description: When user clicks on any navigation menu link it redirects to the login page.
Cause(s): User session time out for that user.
Proposed Solution: Once user session timed out, user needs to re login. This will happen when user is not performing any operations till session time out on System Manager screen. The default session timeout is 20 minutes.

RBAC

Can't see 'Manage Roles' link in navigation tree

Description: The logged in user could not see the Manager Roles link in the navigation tree.
Cause(s): The logged in user does not have enough permissions to view RBAC pages.

Proposed Solution: The logged in user needs to be assigned appropriate permissions to the Role(s) the user has. At least one of the roles the user has should have view permission over all of the RBAC operation entries. Also, please make sure that the role has *view* permission on *UserManagement* operation entry in addition to RBAC pages as RBAC falls under UserManagement section.

Can't see some or any roles in the roles table

Description: When a user logs in to Panther and visit RBAC landing page, some or all the roles are not displayed in the roles table. Further, different users would see different roles in the roles table.
Cause(s): This is the intended behavior; the logged in user does not have enough permissions to view roles, even though he has permission to view the RBAC pages. Some have users may not have permission to view any roles or some users may have permissions to view only some roles.
Proposed Solution: If user need to see all the roles then modify a role that is assigned to this user and give view permission on all the roles. For this user need to select *'role'* as the '*resource type*' and select "*view*' from '*Actions*' list box and '*ALL'* from the radio buttons given below. Or if permission on selective roles need to be added in a role then click '*ADD*' button over the Groups and Resources table on Edit Role page and select the roles and assign view permission on this roles..

Import Roles link on landing page, Edit buttons, Duplicate button and Add button over permissions table in New Role page are disabled

Description: On the landing page of RBAC, Edit, Duplicate buttons, and Import Roles link are disabled even on clicking a row. Also, when you click on 'New' button and go to New Role page, the 'Add' button over the Permissions table is disabled.
Cause(s): This happens when GroupAndLookup Service is down and hence RBAC does not allow you to edit or duplicate a role, and even while creating a role, adding permissions over resources is disabled.
Proposed Solution: GroupAndLookup Service is necessary for effective use of RBAC. Make sure GroupAndLookup Service is deployed and running before using RBAC.

Only 'View' button is enabled on RBAC page

Description: After logging into RBAC landing page, most of the buttons and links are disabled, except 'View' button.
Cause(s): The user does not have permissions to add or change or duplicate or assign or unassign a role.
Proposed Solution: Edit any of the roles this user has got, and add corresponding permissions over the role.

Bulk Import of roles fail

Description: On the Import Roles page, when the user selects an xml file and click commit button the following errors happen:

1. *Failed To Import Roles*
2. *ConstraintViolationException: Could not execute JDBC Batch update*

Cause(s): One of the resource specified in some role is not present in the database (a resource can be a user, role, group, element, operation, alarm, scheduling job, etc), and so the constraint violation exception from DB.

Proposed Solution: Make sure that all the resources defined in the Bulk Import xml file are present in the database. Permission over resources that do not exist cannot be defined.

Assign Roles to Users and Un Assign Role from Users links are taking to error page.

Description: When a user selects some roles and clicks on either Assign Roles to Users or Un Assign Role from Users link the user is redirected to error page.

Cause(s): User Management Service is not installed.

Proposed Solution: Make sure that User Management Service is installed properly. User Management Service is required for RBAC to manage Role assignment/un assignment to or from users.

UPM

User is not able to change the user attribute

Description: User is not able to change user attribute.

Cause(s): User might not have appropriate permissions

Proposed Solution: Check user has a role which contains the appropriate permissions to change the user attributes.

User is not able to change the user address

Description: User is not able to change user address.

Cause(s): User might not have appropriate permissions.

Proposed Solution: User can't change the shared address from the user edit/new/view/duplicate page.

User is not able to see the any other record except than its own record

Description: User is not able to see the other user records.

Cause(s): User might not have appropriate permissions.

Proposed Solution: Check if user has appropriate role assigned to user. By default user has "end user" has role assigned to user which has permission to view/edit only own record.

Plug-in Framework

Getting validation failure error while deploying EPD/EP

Description: Getting validation failure error while deploying EPD/EP.

Cause(s): The EPD/EP is not as per the defined structure and xsd or the jar file is not packaged properly.
Proposed Solution: Make sure that the EPD/EP structure is as per guidelines and xsd. Also the jar file should be packaged using java utility.

Could not get database connection

Description: An error 'Unable to connect to database' is received while executing plug-in framework script.
Cause(s): The system is not able to parse the database connect string passed as the argument when executing plug-in scripts.
Proposed Solution: Make sure that the database URL is correct and is specified in quotes.

No suitable database driver found

Description: Executing plug-in framework script throws error that no suitable database driver is found.
Cause(s): The database driver was not found in the system's classpath.
Proposed Solution: Make sure that the database driver jar file is in the classpath.

Ear file not updated when an EP with jar or property file artifacts is deployed

Description: When an EP with jar or property file as artifact is deployed, the modified EAR file is not copied to the desired location (the deploy directory of the server instance).
Cause(s): This happens when system time is older then installer build time. In such setup when an EP with jar or properties file artifact is deployed, the ear of the corresponding application is modified. The modified date of ear is current date where as the ear in deploy directory has modified date as the installer build date. And the file is not replaced by plug-in framework.
Proposed Solution: Make sure that machine date/time is set to current date/time.

EP is not getting deployed.

Description: EP(s) fail to move into "DEPLOYED" state from "INIT" state.
Cause(s): The Plug-in Framework is not able to pick up the EP(s). This is due to EJB timer not running or EJB timer was not stopped properly when JBoss was restarted.
Proposed Solution: The EJB timer may not run if there is no Timers table created. Make sure that the timers table is there in the database to which JBoss makes a connection. If there are multiple EJB timer running linked to plug-in id, please restart the JBoss server.

SAL Enterprise/Agent

SAL Agent does not start

Environment: Solaris machine configured with zones
Description: SPIRIT Agent is not getting started
Cause(s): This can be due to port conflict. To confirm that it is the port conflict issue, make the following changes in $SPIRIT_HOME/wrapper.config file:

1. Set "wrapper.debug" to "true"
2. Set "wrapper.logfile.loglevel" to "ALL"
3. Restart the SPIRIT agent.

The log file $SPIRIT_HOME/logging/wrapper.log will get generated which will indicate that either of "wrapper.port" or "wrapper.jvm.port" is already in use.
Proposed Solution: To resolve the conflict issue

1. Modify **$SPIRIT_HOME/wrapper.config** as:
   - For changing the wrapper port add the entry "wrapper.port" with value greater than 32000 (this is the default value).
   - For changing the jvm add the entries "wrapper.jvm.port.min" and "wrapper.jvm.port.max" and set the values to anything greater than 32000 but excluding the port specified in above point. The default values for these entries are "31000" and "31999" respectively.
2. Restart the SPIRIT agent.

Login Troubleshooting

System Manager: Login: 404 Error after accepting Legal Page

Description of Symptom

HTTP Status 404 - /IMSM/%20%C2%A0
The requested resource (/IMSM/%20%C2%A0) is not available.

Cause

<cause, if known>

Proposed Solution

<steps to remedy the problem or further troubleshoot>

Specific Information required by support

<Information required by support if the person needs to contact support>

Troubleshooting FAQs

1. **What are the first steps to verify whether System Manager Installation is done properly and it's running?**

System Manager Installation can be done in two ways, through GUI or as unattended.

To ensure that you have successfully installed the System Manager, you must verify the following:

1. Ensure that the pre-requisites specified by System Manager are satisfied. After installation through GUI mode the installer displays a screen with the currents status. However, If the installation is done in unattended mode, the pre-requisite status is displayed on the console. The installer rollbacks if any pre-requisites fails (user can run installer with "-p ignore" option for ignoring pre-requisite failure error).
2. Complete the installation process successfully without any errors. While in GUI mode, if any error occurs during the installation, a pop-up screen appears. Whereas, if the installation is done in an unattended mode, the installer rollbacks the installation in case of error (user can run installer with "-c true" option to ignore error during installation.
3. Verify that the installation log file does not contain errors. After installation, the installer moves the file to the directory "$INSTALL_PATH/install_logs" , where $INSTALL_PATH is the path where installation is done (default to "/opt/Avaya"). And the installation log file should follow the naming convention as "system_manager_install-log_<date>_<time>.txt".
4. Complete the installation, and then verify that all the System Manager services for the installed components are running.
5. Login to System Manager UI and click on the navigation menu links, to verify that all links are operational without encountering any errors.

2. How can one tell if System Manager is running?

System Manager consists of Postgres, SPIRIT Agent, JBoss, JON Server, JON Agent, Apache, and Stunnel as a service.

To verify that all services are running, use the following commands or steps:

Postgres: service postgresql status

SPIRIT Agent: service spiritAgent status

JBoss: service jboss status

JON Server: service rhq-server status

JON Agent: service rhq-agent status

Apache: Run the command "ps –ef | grep apache". If apache is running then it will list out some process of apache.

Stunnel: service sysmgrstunnel status

3. How does one stop and start System Manager?

System Manager consists of Postgres, SPIRIT Agent, JBoss, JON Server, JON Agent, Apache, and Stunnel as a service. Stopping and starting System Manager specifies how to stop and restart each service.

Use the following command to stop or start services:

Stopping/Starting Postgres: service postgresql stop/start

Stopping/Starting SPIRIT Agent: service spiritAgent stop/start

Stopping/Starting JBoss: service jboss stop/start

Stopping/Starting JON Server: service rhq-server stop/start

Stopping/Starting JON Agent: service rhq-agent stop/start

Stopping/Starting Apache: service apachectl stop/start

Stopping/Starting Stunnel: service sysmgrstunnel stop/start

4. **System Manager doesn't seem to be shutting down. How does one kill it?**

   If you notice that the System Manager services like, Postgres, SPIRIT Agent, JBoss, JON Server, JON Agent, Apache, and Stunnel does not appear to be shutting down, even after issuing the stop command, then you have to manually suspend the service using the Kill command.

   Killing Postgres: Enter **ps -ef | grep postgres**. This command should display a list of all the Postgres processes that are currently running. And then Kill all those processes.

   Killing SPIRIT Agent: Enter **ps -ef | grep spirit**. This command should display a list of all the Spirit processes that are currently running. And then Kill all those processes.

   Killing JBoss:

   1. Enter **ps -ef | grep " -c avmgmt -b 0.0.0.0"**. This command should display a list of all the running JBoss processes. Now, kill these processes.
   2. After killing the Jboss processes, you must clear the JBoss pid file "/var/run/jboss.pid", and then restart again.

   Killing JON Server: Enter **ps -ef | grep JONServer**. This command should display a list of all the running JON Server processes. Now, kill these processes.

   Killing JON Agent: Enter **ps -ef | grep JONAgent**. This command should display a list of all the running Jon Agent process. Now Kill these processes.

   Killing Apache: Enter the **ps -ef | grep apache**. This command should display a list of all the running Apache process. Now Kill these processes.

   Killing Stunnel:

   - Enter **ps -ef | grep stunnel**. This command should display a list of all the running stunnel process. Now Kill these processes.
   - After killing the stunnel processes, you must clear the stunnel pid file "<STUNNEL_HOME>/stunnel.pid", and then restart again.

     Note: <STUNNEL_HOME> defaults to "/opt/Avaya/stunnel4.25/".

5. **What is the URL for accessing the Common Console?**

   To access the System Manger Common Console UI, type the URL: https://<IP/HOSTNAME>/IMSM.

   Where, "<IP/HOSTNAME>" is the IP or the hostname of the machine where System Manager is installed.

   After entering the valid login credentials, the System Manager UI, displays the Welcome page.

6. **What roles do technicians need to service a System Manager?**

7. **How can one use the Common Console to tell what release of System Manager one is using?**

   To identify the System Manager version, follow these steps:

   1. Login to System Manager UI Console.
   2. Go to “Settings -> Service Profile Management -> System Manager 1.0” screen.
   3. The value of attribute “version_detail” present under “applicationMetadata” specifies the current version of System Manager.

8. **If one can't log into the Common Console, how can one tell what release of System Manager one is using?**

   If you are unable to login to the System Manager UI console, verify the release of the System Manager, by logging in to the machine where System Manager is installed, and then view the file “$MGMT_HOME/installer_relno.txt”. This file contains the current version of System Manager.

   Note: $MGMT_HOME defaults to “/opt/Avaya/Mgmt/<release version>”.

9. **In what locations can one find log files and what kind of information goes in those log files?**

   Below are few directories that contain log files:

   <INSTALL_PATH>/install_logs/: The installer logs is stored in this directory. This log contains detail about installation, uninstallation, and rollback of System Manager.

   $JBOSS_HOME/server/avmgmt/log/server.log: This file contains log that are generated by System Manager JBoss server.

   $AVAYA_LOG: This directory contains sub-directory with name of each System Manager domains. Each sub-directory contains log of corresponding domains. Each domain log directory has different log files for trace, operational, audit, and security logs. Some domains may not generate audit or security logs, so it obvious that those domain log files will be empty.

   $AVAYA_LOG/spirt/: This directory contains logs generated by Spirit Enterprise.

   $AVAYA_LOG/spirtlogs/: This directory contains logs that need to be stored in a centralized System Manager log database and log viewer. The information in this directory can contain redundant logs which pertain to directories. Depending on the rule specified for generating alarms, an alarm may be generated by Spirit Agent for that log message.

   $SPIRIT_HOME/logging/: The directory contains logs generated by Spirit Agent.

   Backup/Restore Utility Log: These logs are generated on the database machine while the user performs backup/restore operations. The default path of the directory where the logs are generated is “/var/lib/pgsql/pem/log/”.

   Note:

   - <INSTALL_PATH> defaults to “/opt/Avaya/”.
   - $JBOSS_HOME defaults to “/opt/Avaya/JBoss/4.3.0/jboss-eap-4.3/jboss-as/”.
   - $AVAYA_LOG defaults to “/var/log/Avaya/mgmt/”.
   - $SPIRIT_HOME defaults to “/opt/Avaya/SPIRIT/<release version>”.

10. **Are there any log files one should not delete?**

    The log file can be deleted, but the user should not assume as general guidelines that the log file should not be in use while deleting the file. For example, the service/utility that logs into a particular file should not be running and using the file. For this you must first bring down the service, delete the file, and then restart the service.

11. **How does user change the log levels for various domains present on System Manager UI Console?**

The log level for any domain present on System Manager UI is controlled by the corresponding domain loggers/appenders. User may need to modify the log level of both domain logger and appender. This can be done through logging configuration UI or by directly modifying the logging configuration file.

For Modifying Log Level using the UI, follow these steps:

1. Login to System Manager UI Console.
2. Go to "Setting -> Logging Configuration". It should display the list of loggers.
3. Look for the domain logger that needs modification.
4. Select the logger and click 'Edit'. It should display the logger details and the appenders used by the logger. The details will be editable.
5. Select the domain appender and click 'Edit'. It should display the appender details in editable form.
6. Modify the log level of the appender as required and click 'Commit' to save changes. This will take user back to logger details screen.
7. Modify the log level of the logger and click 'Commit'.

For Modifying Log Level using the Command Line:

Modify the log level of domain loggers and appenders in the logging configuration file used by log4j. The file is located in "$JBOSS_HOME/server/avmgmt/conf/jboss-log4j.xml".

Note:

- $JBOSS_HOME defaults to "/opt/Avaya/JBoss/4.3.0/jboss-eap-4.3/jboss-as/".
- In both the case, the changes will be reflected in the system after some time when log4j picks the changes from the modified logging configuration file.
- If the change of log level is also required for the logs going in files tailed by Spirit Agent then while doing above changes for domain loggers/appenders, user should also modify the corresponding Spirit appenders displayed in the appenders list while modifying the domain logger. All domains use common Spirit appenders so any changes in Spirit appenders will be reflected for all domains.

12. How can one modify the log levels for Spirit Agent?

You can modify the log level for Spirit Agent by modifying the log levels of the loggers/appenders used by Spirit Agent. The log level for loggers/appenders are defined in the file "$SPIRIT_HOME/log4j.xml". After modifying the log levels, you must restart the Spirit Agent for the changes to be reflected in the system.

Note: $SPIRIT_HOME defaults to "/opt/Avaya/SPIRIT/<release version>".

13. The installation/uninstallation failed. How does one clean up before reinstalling?

If the installation/uninstallation fails, then you should follow these steps for performing a manual cleanup of installation:

1. Stop all the system manager services that are currently running (kill the services if can't be stopped).
2. Delete the installation directory where the installation was done (default "/opt/Avaya") if existing.
3. Delete the directory containing cert store (i.e., "/opt/cert-store/") if existing.
4. If old logs are not required then delete the logs directory $AVAYA_LOG if existing.
5. Delete the database backup/restore utility directory (default location is "/var/lib/pgsql/pem/") if existing.
6. Uninstall Postgres. For this run the command "rpm –qa | grep postgres". It will list all the Postgres rpm's that are currently installed in the system. Now run the command "rpm –e --nodeps <rpm name>" for each of the Postgres rpm's installed on the system.
7. Delete system user 'postgres' if existing by running the command "userdel postgres".
8. Delete the directory "/var/lib/pgsql" if existing.

9. Delete the scripts created by System Manager (i.e., avaya_mgmt.sh, jagent_mgmt.sh, jboss_mgmt.sh, jserver_mgmt.sh, spirit_mgmt.sh) if existing. These should be present under the directory "/etc/profile.d/".
10. Delete the entries of executing above scripts from file "/etc/profile" if existing.
11. Delete the services created by System Manager (i.e., apachectl, jboss, rhq-agent, rhq-server, spiritAgent, spiritAgentCLI, sysmgrstunnel) if existing. These should be present under the directory "/etc/init.d/".
12. Also delete the soft links of the above services (i.e., S56spiritAgent, S94apachectl, S94sysmgrstunnel, S95jboss. S98rhq-agent, S99rhq-server) from directory "/etc/rc.d/rc3.d/" and "/etc/rc.d/rc5.d/" if existing.
13. Delete the file "/var/run/jboss.pid" if existing.

Note: $AVAYA_LOG defaults to "/var/log/Avaya/mgmt/".

14. There are a bunch of unacknowledged alarms. How can they be purged?

The unacknowledged alarms can't be purged directly. For purging specific alarms you must change the state of the alarm to clear. To purge alarms, follow these steps:

1. Select the unacknowledged alarms and change the status to acknowledged.
2. Again select the acknowledged alarms and change the status to clear.

Use DRF functionality to purge alarms marked as clear. To purge alarm using DRF functionality, follow these steps:

1. Access DRF UI from "Settings -> Data Retention"
2. The UI will display some pre-defined rules for purging various items. Applying this rule purge the data which has age more than the number of days specified by the retention interval.
3. Applying rule "ClrdAlarmPurgeRule" will purge the alarms whose age current status is clear and age is more than the number of days specified by the retention interval (default to 120 days).
4. If user wants to purge the cleared alarms with some different age then user can modify the retention interval and apply the rule.

15. What user ID should be used to run System Manager? If System Manager is installed as root, can it be run under another ID?

Currently the System Manager cannot be accessed by any other user, if the installation of System Manager is performed through root. However, if the installation is performed by a non-root user, then it can be accessed only by the non-root user and root.

16. Login screen does not appear when running a browser from a remote box, but is accessible locally. What things need to be checked?

This problem occurs when firewall is enabled on the machine which blocks all the communication from external machines. But suggesting to disable the firewall is not a suitable solution for setups on field. And customers might be having different firewall rules. This need more analysis on which all ports need to be opened. This item should be included only once we have the details ready.

17. How to schedule System Manager backup?

To schedule System Manager backup:

1. Login to System Manager UI console.
2. Go to "Settings -> Backup and Restore".
3. Click on the button 'Backup'. This will take you to a screen where you can specify if you want to do local or remote backup.
4. Specify the details required for local or remote backup and click on the button 'Schedule'.
5. On the schedule backup screen specify the job name, schedule time, and repeat interval and click 'Commit'.

6. This should schedule a backup job as required.

18. A user forgot his password. How can it be reset?

If a user has forgotten the password, the password can be reset by the administrator as:

1. Logging to System Manager UI console.
2. Go to “User Management -> User Management”. It should display the list of the user present in the system.
3. Search for the user whose password needs to be reset.
4. Select the user and click ‘Edit’. It should display the user details. The details will be editable.
5. There will a link of “Change Password” under “Identity”. Administrator can specify new password here.

19. Is System Manager services restart is required when installing new or updated certificates?

Yes. When a new certificate is installed or an old certificate is updated, all System Manager services must be restarted again.

20. Information needed when a trouble ticket is escalated to the Tier 4 group.

Following information are required when escalating an issue::

1. Problem description.
2. Detailed steps to reproduce the problem if any.
3. The release version in which the issue is occurring.
4. Java version used to do installation and running System Manager
5. Details on if the system on which problem is happening is an upgrade from some previous release. If yes then from which release version upgrade has been done. If not then was there any previous installation that has been manually cleaned before doing the current installation.
6. Installation log files.
7. System Manager JBoss server log file available at “$JBOSS_HOME/server/avmgmt/log/server.log”.
8. The domain log available at “$AVAYA_LOG/<domain name>/”. Having domain log generated after changing the log level to finest will provide more details of the issue.

25. How does one stop and restart SPIRIT Agent?

Enter the following command/step for Stopping and Starting spirit agent:

Stopping/Starting SPIRIT Agent: service spiritAgent stop/start

26. How can one tell if SPIRIT Agent is running?

- Enter the following command/step, to verify that the status of the spirit agent:

SPIRIT Agent: service spiritAgent status