SOA Software: Troubleshooting Guide for Policy Manager and Network Director

SOA | software™

SOA Software Policy Manager

Troubleshooting Guide for Policy Manager and Network Director
1.1
October, 2013

Copyright

Trademarks

SOA Software, Inc.

SOA Software, Inc.
12100 Wilshire Blvd, Suite 1800
Los Angeles, CA 90025
(866) SOA-9876
www.soa.com
info@soa.com

Disclaimer

Contents

Chapter 1 | Introduction

Over the course of using Policy Manager, Network Director, Policy Manager for DataPower, or other SOA Software products such as Agents, you're likely to have to do some troubleshooting from time to time. Due to the relationship between the various containers and a selection of different type of web services, security, databases, and networks, there is a wide range of issues that might occur.

These products are deployed in a wide range of environments, and interface with a wide selection of products and versions, including operating systems, databases, servers, firewalls, security mechanisms, and others. It is important to take an orderly approach to installation, deployment, and troubleshooting.

If you encounter errors, check this publication and the resources referenced here.

This document also includes information about contacting technical support and the support process.

Finally, it includes some resource material such as firewall settings and database queries for your reference.

This chapter includes:

- Document Summary
- Customer Support
- Troubleshooting Resources and Tips
- Product Documentation

Document Summary

The table below provides a summary of the information in this publication and how it is organized.

This chapter…	Provides this information…
1: Introduction	General information about information resources available, information about working with Support, general information about basic troubleshooting tools.
2: Troubleshooting: Policy Manager	Troubleshooting information for Policy Manager
3: Troubleshooting: Network Director	Troubleshooting information for Network Director
4: Reference: Database Queries	Examples of database queries you can use to resolve issues or optimize.

Customer Support

This section provides information about working with SOA Software technical support, including:

- Contacting Technical Support
- Logging a Support Ticket

- Support Tickets: Customer Responsibilities
- Notes for Support Customers

Contacting Technical Support

If you experience an issue with an SOA product, you can contact SOA Support. SOA Software offers a variety of support services by email and phone. Support options and details are listed in the table below.

Support Option	Details
Email (direct)	support@soa.com
Phone	1-866-SOA-9876 (1-866-762-9876)
Email (via the website)	The Support section of the SOA Software website at https://support.soa.com/support provides an option for emailing product-related inquiries to our Support team. It also includes many product-related articles and tips that might help answer your questions.
Documentation Updates	We update our product documentation for each version. If you're not sure you have the latest documentation, send an email request to support@soa.com. Specify the product and version you're using.

For more information, visit https://support.soa.com/support/.

Logging a Support Ticket

There are two ways to log a support ticket:

- Submit a ticket directly from the SOA Software Support site at https://support.soa.com/support.
- Send an email to support@soa.com.

When you log a support ticket, provide clear and specific details about the issue you are having, with as much background information as possible. Include the appropriate log files based on the type of issue being reported.

To log an SOA support ticket

1 Log in to the SOA Support site, using the credentials provided to your organization, at this address:

```
http://support.soa.com
```

2 On the Support home page, click **Submit a Ticket**.

3 Under **Select Department**, choose the product you need help with and then click **Next**.

4 Select the Priority/Severity of the issue. For definitions and guidance, refer to the general support policy, available at: https://support.soa.com/docs/index.php?download=SupportOverview.doc.

5 Provide all the required information. The specific information required might vary depending on the product for which you're reporting an issue. For example, you might need to provide:

- Product version and update
- Database version
- Operating system (32/64-bit)

6 Provide a clear subject and description of the issue. If possible, include steps to reproduce your issue so that Support can troubleshoot it more effectively.

7 Attach log files, screen captures, or any other related files.

Support Tickets: Customer Responsibilities

When logging a support ticket, please bear in mind these additional points and customer responsibilities:

- Please make sure that the issue is related to the SOA product. In some cases, issues are caused by other factors such as network, firewall, or security certificates.
- In case of a Production Critical issue, you can contact SOA Support immediately and one of our knowledgeable support staff will help you troubleshoot your problem and collect information for further diagnosis. If you are reporting the issue by email, specify in the subject line that it is Production Critical. A production critical issue is defined as follows:
  - Actual or potential complete failure of traffic on a critical route due to failure of a system or network element.
  - Complete or partial loss of visibility/control of network elements.
  - Loss or impairment of control/monitoring equipment.
- Document the scenario/steps to reproduce the issue. If it's not possible to reproduce the issue, explain what was happening at the time you experienced the issue and what then occurred.
- Provide the appropriate log files from all SOA containers that are involved in the request flow.
- Collect any other information that you think will be useful for SOA engineers to understand and troubleshoot the issue.
- Report the issue to SOA Support using one of the options listed earlier in this chapter.

Notes for Support Customers

1 For the response time and actions taken based on ticket priority, refer to the Response Times table in the general Support Policy section of the Support Site.

2 If you urgently need a quick response (for example, in the case of a Production Critical issue), please call SOA Support, or submit a ticket and indicate it on the ticket.

3 If screen sharing or an online session is needed, please specify this in the ticket so that SOA Support can be prepared.

4 In the case of screen sharing or an online session, SOA Support may need to control the console to demonstrate how to resolve the issue.

5 If you allow SOA support to access your system directly, remember to also provide the needed access information such as VPN or authentication information.

Troubleshooting Resources and Tips

This section provides information on basic tools and resources you can use, and steps you can take, to help determine the exact cause of an issue or to provide more information to SOA Support. It includes the following subsections:

- Monitoring Tabs: Alerts and Logs

- Log Files
- Knowledge Base
- Release Notes
- Monitoring Tool
- Restarting the Container: General Information

Monitoring Tabs: Alerts and Logs

Monitoring information, including alerts and logs, is available at the following levels:

- For the entire organization
- For each container
- For each service
- For each contract

At each level, a monitoring tab gives you access to alerts, logs, and other information so that you can view the state of functions in real time.

Organization Monitoring Tab

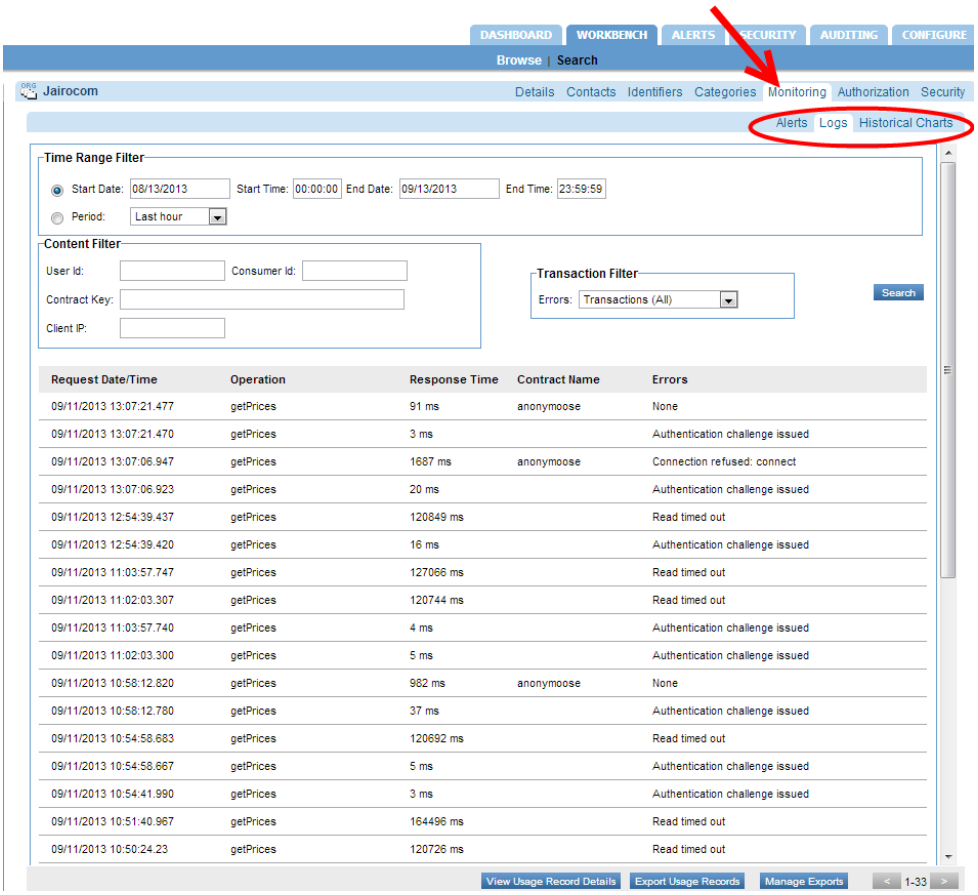
The highest level of monitoring information is available via the monitoring tab for an organization. This lets you view all logs and alerts sent by services and sub-organizations within the organization you are viewing.

This tab includes three types of alerts:

- Service Alerts
- SLA Alerts
- Container Alerts

If there is an error with one of your services, the monitoring tab is a good place to look first, to see if the alerts and log entries can help you identify the problem.

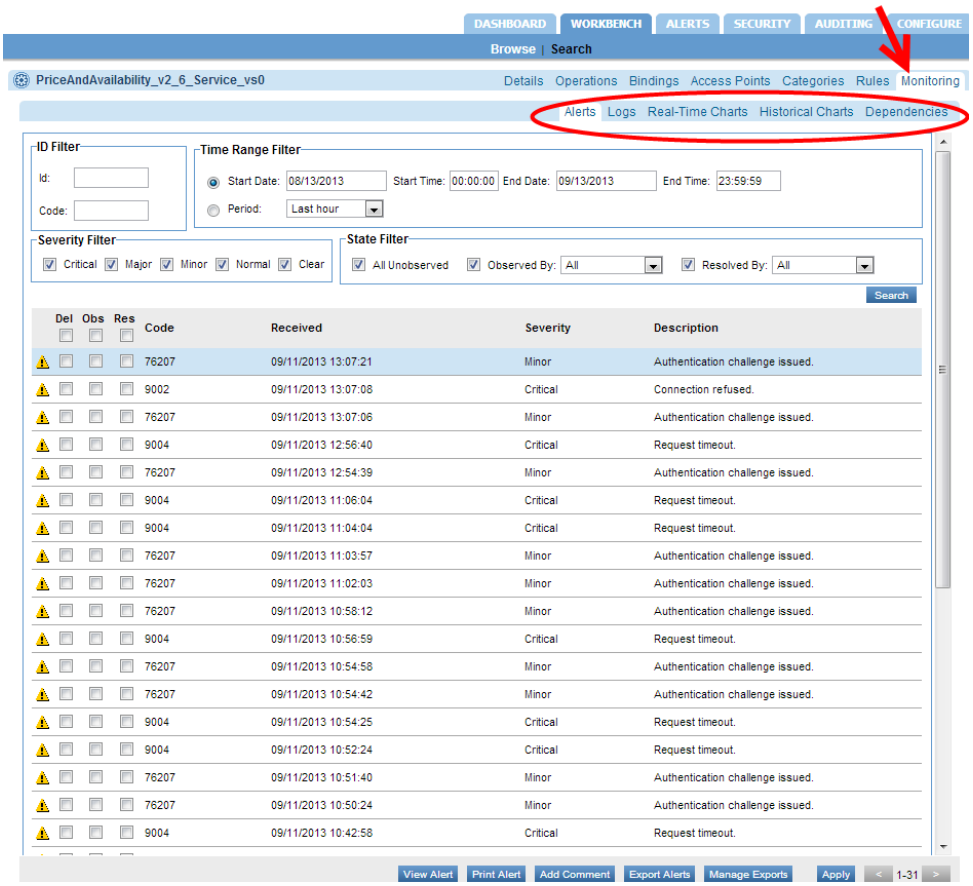
An example of the monitoring tab for an organization is shown below.



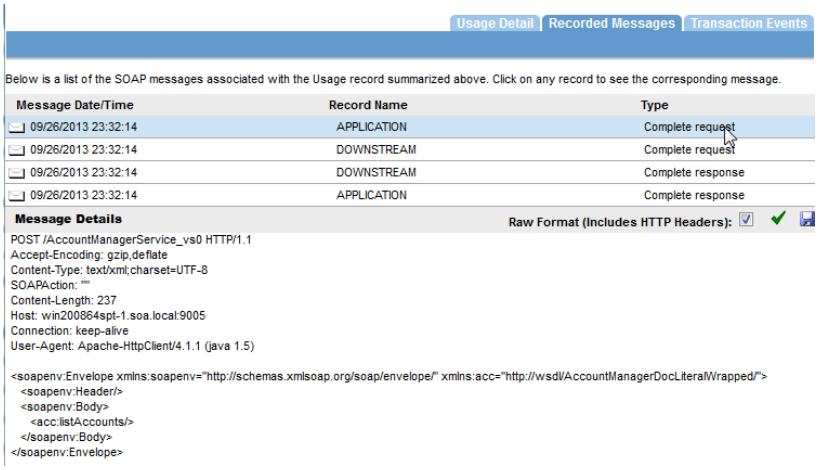
Service-Level Monitoring Tab

Each service also has its own monitoring tab, with alerts and logs relating only to that service and its operations, as shown below.

If the basic auditing policy is being used, the Monitoring -> Logs tab also shows usage data for the service. However, as a best practice this should only be used while troubleshooting or in non-production environments as the payload data is stored in the database.



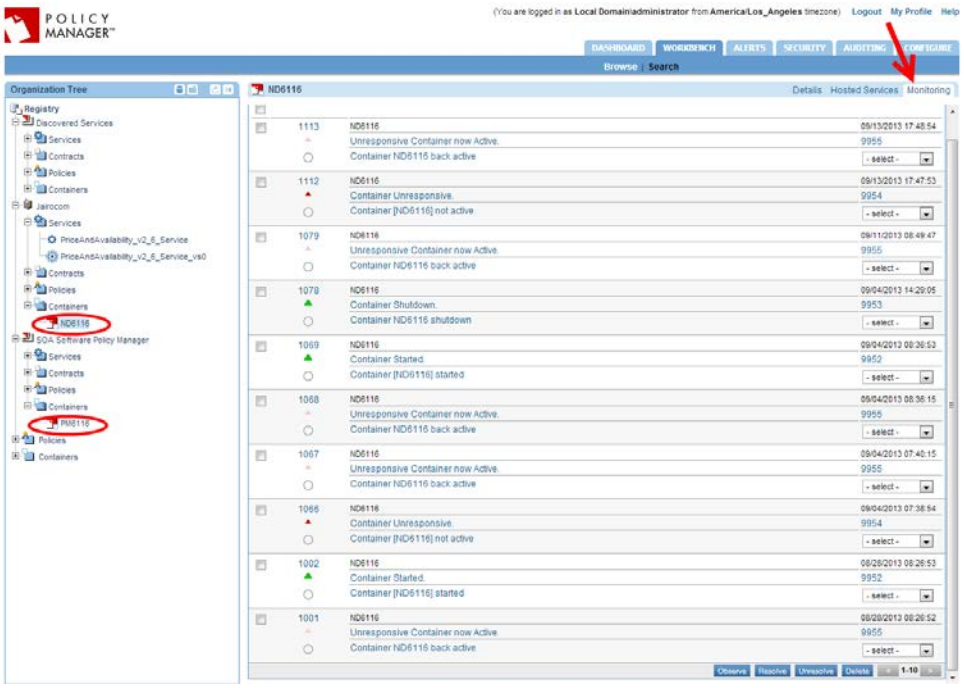
If the detailed auditing policy is being used, you can also view the request and response payload in the Logs tab. Double-click a specific message to see the Usage Data Details overlay. This includes usage detail, recorded messages, and transaction events. In the Recorded Messages tab you can see the individual request and response message. You can also choose to view Raw Format, which includes the HTTP headers. An example is shown below.



Monitoring Tab for the Container

If there is an issue with a specific container, alerts are displayed in the container's monitoring tab as well. You also see the container alerts when you log in to the Policy Manager console.

The example below shows the monitoring tab for a container.



In some cases the information on the monitoring tab can help you discover a deeper error occurring within the container or service.

The next step in troubleshooting an instance is to make use of the logging system.

Monitoring Tab for the Contract

A monitoring tab is also available for each contract, giving access to the logs applicable to the contract.

Log Files

By default, Policy Manager and Network Director only log errors (exceptions) that happen over the course of normal usage. If you are having any runtime processing errors or issues while performing some action in the Policy Manager console, applicable errors will generally be logged in the log file for the applicable container.

This section includes the following information about log files:

- File Location
- Modifying the Default Logging Behavior
- Turning Trace Logging On
- Determining Where to Look for Error Information

Note: There is another type of log that you can enable if needed. In the Policy Manager Admin Console, Configuration tab, choose the configuration category of com.soa.transport.jetty and enable the NCSA Access log (set the ncsa.access.log.enable property to **true**). Then, in the ncsa.access.log.filename field, specify the location for the log file. After that, access to any page in the Policy Manager Console or Admin Console generates an entry to the specified log file.

File Location

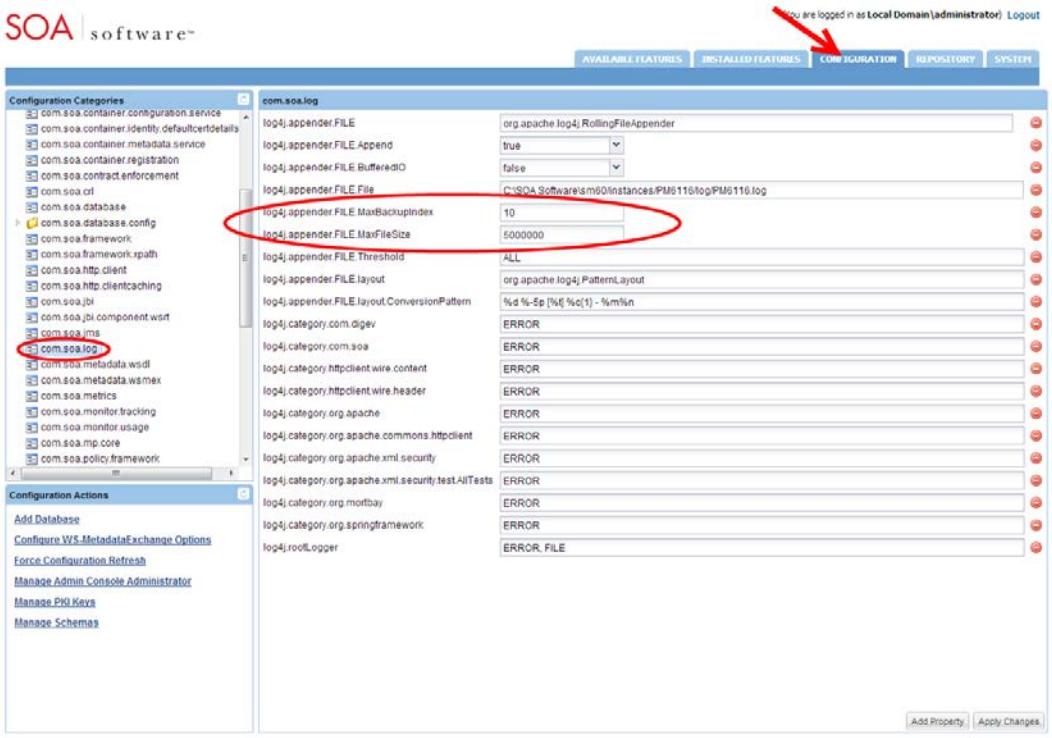
Each instance has its own set of logs at the following default location:

```
<installation directory>/sm60/instances/<instance name>/log
```

The default behavior for the logging system is to have a maximum of ten backup logs at 4.7 MB (5000000 bytes) each. When a log reaches 4.7 MB in size, the logging information rolls over into the next file. Once the total number of log files reaches 10, the oldest file is deleted when the new one starts.

Modifying the Default Logging Behavior

You can modify the default settings for logging behavior, along with the level of logging and other customization, in the Policy Manager Admin Console and in the Network Director Admin Console.



To modify the default logging behavior

1 Log in to the Policy Manager Admin Console or Network Director Admin Console.

2 Click the **Configuration** tab.

3 From the configuration categories on the left, find **com.soa.log**.

4 In the properties panel on the right, the two properties below control the number of backups and/or the maximum size for each log file. Modify as needed:

- log4j.appender.FILE.MaxBackupIndex: the number of backup files that are kept
- log4j.appender.FILE.MaxFileSize: the maximum size for each file

5 Click Apply Changes.

Turning Trace Logging On

If a problem with a container persists, you could enable trace logging in the Admin Console. Trace logging is enabled dynamically and does not require a container restart.

Depending on the category for which trace logging is enabled, detailed information is collected in the log file, including such activity as:

- Internal SOA to SOA container communication
- Database queries
- Incoming requests
- Certificate information
- Scheduled jobs

When the troubleshooting is complete, trace logging for the specific category should set back to the default setting of **error**.

A good practice is to figure what action is causing specific symptoms in the container, and turn on trace logging only while that action is occurring. For example, if a service detail page is coming up blank, you might want to see what Policy Manager is doing when you click on the service detail page. You would set the logging level to **trace**, click on the service detail page, and then change the level back to **error** and analyze the logs.

To turn trace logging on or off

1 Log in to the Policy Manager Admin Console or Network Director Admin Console.

2 Click the **Configuration** tab.

3 From the configuration categories on the left, find **com.soa.log**.

4 In the properties panel on the right, modify this property to enable or disable trace for all runtime activity on the container:

- To enable: log4j.category.com.soa: Switch from ERROR to TRACE
- To disable: log4j.category.com.soa: Switch from TRACE to ERROR

5 Click Apply Changes.

stdout.txt File

If there is an issue with the bundles not starting, you can check the stdout.txt file to get additional information for troubleshooting purposes.

This file is created whenever the container starts up. It is stored in the instances folder (instances/<container name>/log/stdout.txt).

Normally the file contains a one-line message stating that the bundles have started. However, if the bundles fail to load, the errors that occur during the container initialization process are recorded in this file. Errors relating to bundles loading do not appear in the Policy Manager log files, since logging of messages starts when the container has started.

Monitoring Tool

All Policy Manager 6.x containers include an optional Monitoring Tool to help troubleshoot issues related to the container resources. It is not installed by default but you can easily install it. You can use this tool to monitor and analyze the following:

- Incoming HTTP connections (com.soa.transport.httpclient)
- Database thread pool (com.soa.database.config.<db-config-id>-mon)
- Active/idle Policy Manager processes (com.soa.framework)
- Container memory usage (com.soa.vmstats)
- Outgoing HTTP connections (com.soa.transport.jetty)
- Monitoring queues (com.soa.usage)
- JMS connections (com.soa.transport.jms)

To install the monitoring tool

1 Log in to the Policy Manager Admin Console or Network Director Admin Console.

2 Click the Available Features tab.

3 From the **Filter** drop-down list at the top of the left panel, choose **Tool**.

4 Click the checkbox for the SOA Software Admin Monitoring Tool and click **Install Feature**.

5 Restart the container.

6 After restart, verify that the Monitoring tab is now present in the Admin Console, as shown below.

Note: This tool does not require additional machine or container resources to run. Before closing the tool, set the polling interval to 0.

Restarting the Container: General Information

Some types of changes that you might make will require restarting of the container before the changes go into effect. Other types of changes are effective immediately, without restarting the container.

In most cases, specific procedures and issue resolution notes in this document state whether you need to restart the container or not. In general, configuration changes do not require restart unless they include changes to the container listener or database. If you add or remove container features you'll need to restart the container for the changes to go into effect.

Examples of changes that require restart:

- Adding the monitoring tool in the Policy Manager Admin Console
- Changing database properties such as username, password, or hostname
- Changing the port number for the container listener (for Policy Manager versions 6.0 and prior)

Examples of changes that do not require restart:

- Increasing the log level to **TRACE**
- Adding an HTTP route configuration file to the /instances/<ND>/deploy folder
- Adding an identity system such as LDAP to the Policy Manager Workbench
- Changing the port number for the container listener (for Policy Manager version 6.1)

Determining Where to Look for Error Information

When trying to narrow down information for troubleshooting purposes, it might be useful to know what symptoms are likely to relate to which container types.

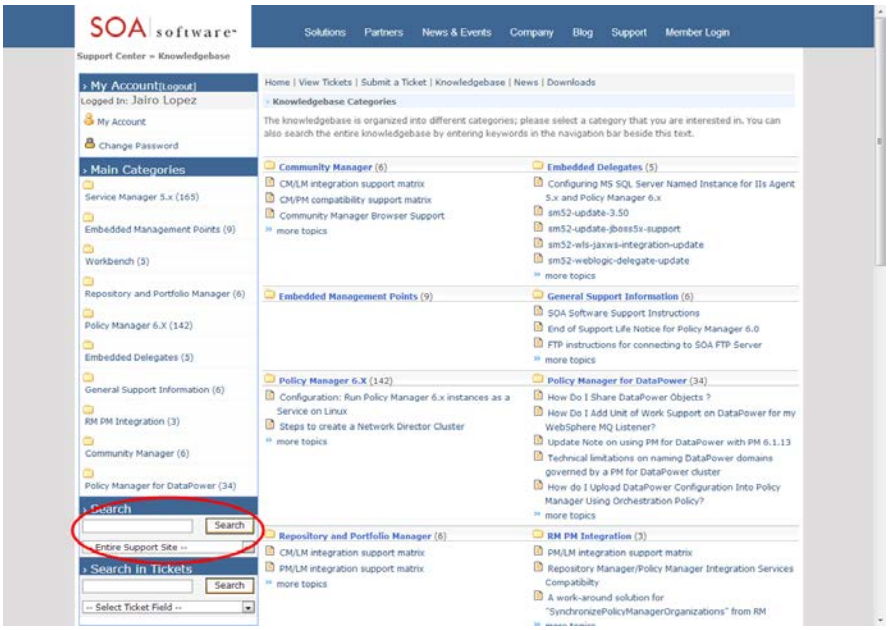
You might find info about these types of errors…	In this location…
Issues with the Policy Manager (for example, usage writer or container configuration), user interface issues, search results, and some database issues.	Policy Manager log files. These types of issues are generally a problem with the Policy Manager instance.
404 when invoking a service, bad context paths, virtual service authentication errors, authorization errors, or routing issues.	Network Director log files. Possibly also Policy Manager log files. These issues are likely to relate to the Network Director. However, since the Network Director communicates with the Policy Manage to retrieve information, in many cases the Policy Manager logs are helpful as well.
Container initialization.	stdout console or the stdout file. Any errors that occur during the container initialization process are written to stdout.

Knowledge Base

The SOA Software knowledge base, http://support.soa.com, includes many type of information such as:

- Configuration settings
- Specific problems and their resolution
- Supported versions
- Tuning information
- Known issues and workarounds
- Tips and tricks

The knowledge base home page is shown below.

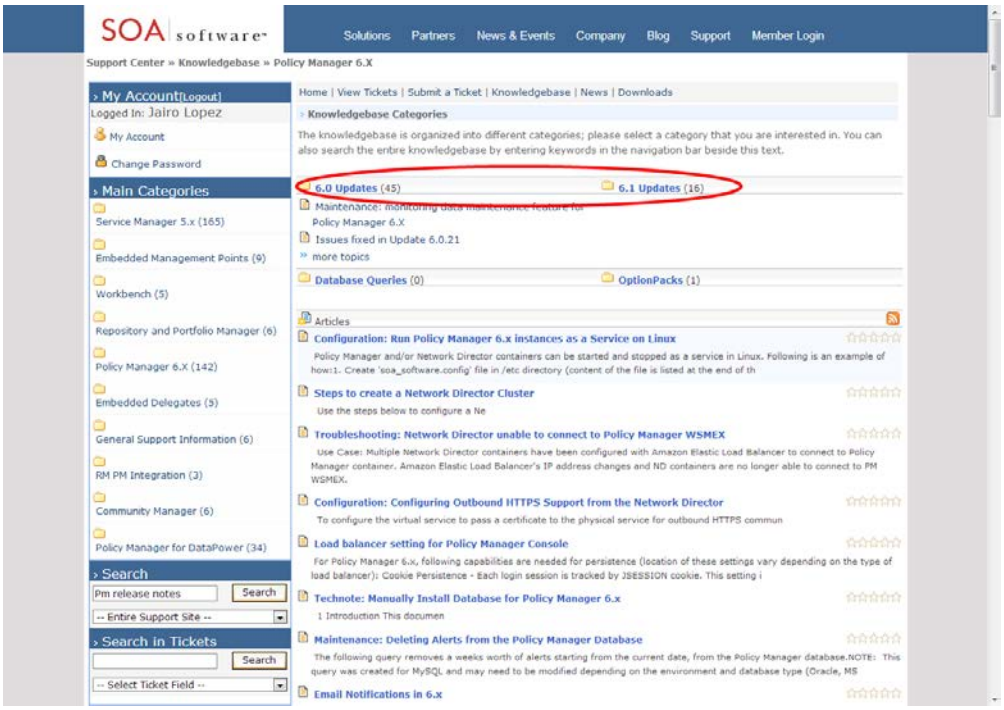


Release Notes

It's possible that you could encounter a bug that might have been resolved in a later version of the product. For this and other reasons, it's a good idea to check the release notes for versions later than yours.

The release notes for each product version include information about the bugs/issues that have been fixed in that version, as well as information about new product features and enhancements. You might find that the problem you encountered was resolved in a later version.

To view release notes, go to the knowledge base at http://support.soa.com. Click on the category for your product—for example, Policy Manager 6.x—and choose the applicable version update section, as shown below.



You will see a summary of the release notes for every version. Just browse through any versions newer than yours to see if the issue has been fixed in an upgrade.

In addition, a summary of the issues that were fixed in each update is included in a text file located in the ./sm60/docs directory.

Product Documentation

When you download your installation executable files, make sure you get and read the product documentation. The documentation for each product includes general information about installation and often includes troubleshooting information for the specific product.

Updates to documents are available from time to time on the Support site.

Chapter 2 | Troubleshooting: Policy Manager

This chapter includes information to help you troubleshoot issues that might come up with Policy Manager. The information is broken into two main sections, by role:

- Troubleshooting Issues: System Administrator
- Troubleshooting Issues: Policy Manager Administrator

Troubleshooting Issues: System Administrator

This section provides information about issues a System Administrator might encounter with Policy Manager. It includes:

- Database Issues
- Monitoring Issues
- Console Login Issues
- 404 Errors Returned for Configured Context Paths
- Unable to Access Policy Manager Container
- Email Configuration Issues
- Unable to start a Container

Database Issues

This section provides information about issues that might occur relating to your database, with suggestions and instructions to help you resolve the problem. It includes:

- Database Connections All In Use (Connection Pool Exhausted)
- Database Locks on soa_qrtz_locks Table
- Policy Manager Alert Code 92304, Retry Count Exceeded, when Database is Not Full
- Database Password Expired
- Database Thread Lock

Database Connections All In Use (Connection Pool Exhausted)

If database connections are all in use, virtual services on the Network Director might not be accessible. You might also see an out of memory error in the stdout log or console, and see the error message below in the log file:

```
SQLNestedException: Cannot get a connection, pool exhausted.
```

This can happen, in an environment with high traffic, if all database connections might be used by Policy Manager.

You can verify this with the monitoring tool for the Policy Manager container. If you see the error message listed above, the database connections are all in use.

Solution:

One resolution is to increase the maximum number of database threads. To do this, follow the steps below.

To increase the maximum number of database threads

1 Log in to the Policy Manager Admin Console.

2 Click the **Configuration** tab.

3 In the Configuration Categories section on the left, choose **com.soa.database.config**, and then select the applicable config ID.

4 Change the maxPoolSize value from **30** to **50**.

5 Click Apply Changes.

Note: The settings take effect immediately. You do not need to restart the container.

Database Locks on soa_qrtz_locks Table

If the DBA reports that there are database locks on the soa_qrtz_locks table with the Policy Manager database, it is probably because the Quartz scheduler is running on more than one Policy Manager instance.

The Quartz scheduler can only run on one Policy Manager instance. If your environment includes multiple Policy Manager instances, and more than one of them has the **org.quartz.scheduler.enabled** value set to **true**, it's likely that there will be issues with database locks on the soa_qrtz_locks table.

You'll need to determine which Policy Manager instance you want the Quartz scheduler to run on, and then disable it on any other Policy Manager instances.

Solution:

Verify that the Quartz scheduler is running on only one Policy Manager instance.

To set the Quartz scheduler to run on only one Policy Manager instance

1 Log in to the Policy Manager Admin Console for the instance of Policy Manager that you want the Quartz scheduler to run on.

2 Click the **Configuration** tab.

3 In the Configuration Categories section on the left, choose **com.soa.scheduler.quartz**, and then click the container.

4 On the right, make sure the **org.quartz.scheduler.enabled** value is set to **true**. If you change the value, click **Apply Changes**.

5 Log in to the Policy Manager Admin Console for the next instance of Policy Manager. Make sure the **org.quartz.scheduler.enabled** value is set to **false**. If you change the value, click **Apply Changes**.

6 Repeat Step 5 for all other Policy Manager instances.

Note: You do not need to restart the container after making these changes.

Policy Manager Alert Code 92304, Retry Count Exceeded, when Database is Not Full

Policy Manager alert code 92304 message text: **UsageWriter retry count has been exceeded**.

One possible cause for getting this alert code when the database is not full is that there is more than auditing policy applied to the service.

For example, you might have a detailed auditing policy attached and also have the recording component turned on for a pipeline policy.

If you have multiple auditing policies turned on you will typically see this alert. The database constraint does not allow duplicate monitoring of data.

Solution:

Verify that the service being called has only one auditing policy attached to it. If there is more than one, choose the auditing policy you most want to use and remove any others so there is just one auditing policy applied.

Database Password Expired

During the initial install, the database password is set up as part of configuring Policy Manager.

If the database password expires or is changed, Policy Manager cannot access the database.

Solution:

If the database password expires or is changed, you'll need to update it in Policy Manager.

Note: If the database password expires, contact the database administrator and if possible set the password to never expire. If this is not possible due to company security policies, follow the steps below to change the password.

To change the database password in Policy Manager

1 Log in to the Policy Manager Admin Console.

2 Click the **Configuration** tab.

3 In the Configuration Categories section on the left, choose **com.soa.database.config**, and then select the applicable config ID.

4 In the password field, specify the new password.

5 At the bottom right, click **Add Property**. The Add Configuration Property overlay appears.

6 Enter the following:

- Property Name: **encryptValues**
- Property Value: **false**

7 Click **Apply** to save the change and close the overlay.

8 Click Apply Changes.

9 Restart the Policy Manager instance.

Container Running Out of Memory

Note: This article applies to Policy Manager containers in version 6.1.6 update or later versions.

If the container is running out of memory, it could be because the automated rollup data deletion job is running, consuming memory.

By default, Policy Manager creates rollups for its own services, recording performance statistics for calls made to it, usually from Network Director.

The rollup data accumulates in the database over time if not cleaned out regularly. Automatic rollup data deletion jobs periodically clean out the accumulated data, but can slow down the system and even cause out of memory issues.

The automatic rollup data deletion job retrieves information older than a specified date, archives the data in the Export folder, and then deletes the archived information from the database. The job runs in the Policy Manager container. If there are a lot of calls to the Policy Manager at the time the job is running, you might see a condition where the Policy Manager container runs out of memory.

Solution:

If there are memory issues and you suspect the automated data deletion jobs are the cause, you can change the settings so that the data deletion job does not run automatically.

If your system is becoming slow, or you are getting memory errors, it might be because of the job that is required to process all the rollup data.

Typically, if there is a memory error, the container will consume all the CPU cycles and the memory usage for this process will be at 100%.

Some troubleshooting steps you can take:

- Add the monitoring tool. This will help you determine the issue. See *To install the monitoring tool* in Chapter 1.
- If the metrics are not important, you can disable the setting in the Policy Manager container's admin console so they are not generated (see *To disable unnecessary rollup data metrics* below).
- You can manually delete unnecessary data from the database (see *To manually delete unnecessary rollup data from the database* below). Some customers prefer not to have automatic rollup data deletion jobs scheduled so that they can choose the best time to run this maintenance task.

  Note: If you do this, you'll need to delete the data manually later.

- If you continue to experience memory issues after disabling the automated data deletion job, you can allocate more memory to the container Java process. The default is 1 GB, but you could increase the memory to 2 GB or more by changing to 64-bit JRE (see *Out of memory errors on the error log*).

To disable unnecessary rollup data metrics

1 Log in to the Policy Manager Admin Console.
2 Click the **Configuration** tab.
3 In the Configuration Categories section on the left, choose **com.soa.metrics**.
4 In the right pane, set the value of the **metrics.rollup.reporter.requireMetricsPolicy** property to **true**.
5 Click Apply Changes.

To turn off automatic monitoring data deletion jobs

1 Log in to the Policy Manager Admin Console.
2 Click the **Configuration** tab.
3 In the Configuration Categories section on the left, choose **com.soa.rollup.delete.old**.
4 Change one or more of the rollup enable properties from **true** to **false**.
5 Click Apply Changes.

Note: You must restart the Policy Manager container for the change to take effect.

To manually delete unnecessary rollup data from the database

To manually purge the rollup data from the database, run the queries below.

Note: Modify the date in the scripts below to reflect how much data you want to delete (the to_date value). Any information older than the date you specify is deleted.

Backing up before deletion—You can also back up the data before deletion, or you can export the monitoring data before deletion. For instructions on exporting, see the SOA Software knowledge base article:
https://support.soa.com/support/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=131.

Delete rollup (chart) data script:

```
delete from MO_ROLLUPDATA where INTVLSTARTDTS < to_date ('2013-12-01 00:00:00', 'YYYY-MM-DD
HH24:MI:SS')
delete from MO_ROLLUP15 where INTVLSTARTDTS < to_date ('2013-12-01 00:00:00', 'YYYY-MM-DD
HH24:MI:SS')
delete from MO_ROLL_ORG15 where INTVLSTARTDTS < to_date ('2013-12-01 00:00:00', 'YYYY-MM-DD
HH24:MI:SS')
delete from MO_ROLLUP_HOUR where INTVLSTARTDTS < to_date ('2013-12-01 00:00:00', 'YYYY-MM-DD
HH24:MI:SS')
delete from MO_ROLL_ORG_H where INTVLSTARTDTS < to_date ('2013-12-01 00:00:00', 'YYYY-MM-DD
HH24:MI:SS')
delete from MO_ROLLUP_DAY where INTVLSTARTDTS < to_date ('2013-12-01 00:00:00', 'YYYY-MM-DD
HH24:MI:SS')
delete from MO_ROLL_ORG_D where INTVLSTARTDTS < to_date ('2013-12-01 00:00:00', 'YYYY-MM-DD
HH24:MI:SS')
```

Monitoring Issues

This section provides information about issues that could affect your monitoring data, with suggestions and instructions to help you resolve the problem. It includes:

- No Data In Historical Charts
- Historical Charts Displayed for Some Increments but Not Others
- Historical Data Shows but Real-Time Data Does Not Show

No Data in Historical Charts

If you are seeing real-time charts, but there is no data in the historical charts, it might be because the MAX_ID value in the MO_STATUS table has reached its limit.

Solution:

To resolve this issue, run the following query on your Policy Manager database:

```
select MAX(ROLLUPDATAID) from MO_ROLLUPDATA
update MO_STATUS set max_id = <result from the above query>
update SOA_QRTZ_TRIGGERS set TRIGGER_STATE = 'WAITING' where
job_name='ms.generate.rollups.job.Trigger'
```

Historical Charts Displayed for Some Increments but Not Others

Note: This issue might occur in the Policy Manager 6.x environment for systems upgraded from an earlier version of Policy Manager. For new 6.x installations it will not occur.

Issues with historical chart information display are frequently due to the time zone configuration settings in Policy Manager. For example, if you can see daily data by the hour and weekly data by the day, but cannot see monthly data by day or week, this is caused by a configuration issue.

Historical chart data is stored in the ROLLUP data tables in the database. By default, this data is stored in GMT time. However, when you go to the Policy Manager Workbench, on the monitoring tab of the service, you will see that the time is shown in the timezone you configured in your Policy Manager profile.

To see accurate historical information for your implementation, this data should be set to display in the same time zone as your Policy Manager profile.

Solution:

To configure the time zone setting for the rollup data tables, follow the steps below.

To configure the time zone setting for the rollup data tables

1 Log in to the Policy Manager Admin Console.

2 Click the **Configuration** tab.

3 In the Configuration Categories section on the left, choose **com.soa.rollup.configuration**.

4 In the right pane, set the monitoring.rollup.configuration.dailyRollupTimeZones property.

This property should list the time zones for which you want to collect the historical data. For example, to collect usage data for the GMT and MST time zones, you would enter: **GMT, MST**.

5 In the right pane, set the **statistic.dao.timeZoneMappings** property.

This property value should list the time zones that you want the data to display in when it is viewed in the console. For example, to display the historical charts for both GMT and MST, you would enter: **UTC:GMT, America/Phoenix:MST**.

Note: If you are not sure what value to use for time zone, you can check the setting in Policy Manager. In the Policy Manager Console, at the top right, click MyProfile and check the value specified in the Time Zone field. The user profile and the rollup tables should both be set to the same time zone.

Historical Data Shows but Real-Time Data Does Not Show

Note: This issue might occur in the Policy Manager 6.x environment for systems upgraded from an earlier version of Policy Manager. In new 6.x installations it will not occur.

If data shows in historical charts but not in real-time charts, this might be because of inconsistent time zone settings on different machines.

For example, if the Network Director time is set to one hour earlier than the Service Manager machine, you will never see any data in the real-time charts, since there is only a one-hour window in which to view the data.

Solution:

Verify that the time zones are the same on the Service Manager machine and the Network Director or embedded Agent machines.

Console Login Issues

- Cannot Log In to Policy Manager Console When Using Load Balancer
- Lost the Only Admin Password
- Access to the Admin Console Needs to Be Restricted to Localhost Only

Cannot Log In to Policy Manager Console When Using Load Balancer

The user is redirected to the login page when trying to log in to the Policy Manager Console if the Policy Manager Workbench can't access the session, so the user is treated as a new user.

If this occurs, there are two things to check:

- **Application Layer Persistence setting on load balancer** (JSESSION Cookie). If the persistence setting is not enabled, the JSESSION cookie is not passed on to the user, and the user is redirected back to the login page.
- **Redirect Rewrite Setting on load balancer** (SSL Offloading)

Application Layer Persistence setting (JSESSION Cookie)

Each login session is tracked by a JSESSION cookie. The load balancer must be able to access the session cookie and pass it back to the user.

Make sure the Application Layer Persistence setting is enabled on the load balancer. If the persistence on the load balancer is not turned on, the JSESSION cookie is not passed on to the user. Because the session information is not passed on, the user is redirected back to the login page.

The Application Layer Persistence setting is generally enabled by default, but if you are experiencing difficulty logging in it's best to make sure it hasn't been disabled.

The proper response to the login page request from the host is shown below. Note the JSESSION cookie on the last line.

```
GET /ms/index.do HTTP/1.1
Host: pm_host:9900
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.17 (KHTML, like Gecko) Chrome/24.0.1312.56
Safari/537.17
Referer: http://pm_host:9900/
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: JSESSIONID_pm_container=6jl7s7i4lm8qg
```

Solution:

Check/modify the Application Layer Persistence setting in the load balancer configuration page.

Redirect Rewrite Setting on Load Balancer (SSL Offloading)

If your implementation includes SSL Offloading (HTTPS to HTTP) for the load balancer, some Policy Manager console requests are redirected.

SSL Offloading is sometimes used in environments with multiple instances of Policy Manager and a single load balancer receiving traffic on HTTPS when Policy Manager has an HTTP endpoint.

Solution:

In this scenario, you must enable the Redirect Rewrite setting, to follow the redirects. You can modify this setting in the load balancer configuration page.

Lost the Only Admin Password

There is only one administrator password for Policy Manager and it isn't available.

Solution:

You can reset the Policy Manager Console Admin password via the Policy Manager Admin Console. Follow the steps below.

To reset the Admin password

1 Log in to the Policy Manager Admin Console.
2 Click the **Configuration** tab.
3 In the Configuration Categories section on the left, choose **com.soa.admin.console.task.status**.
4 In the right panel, set the value of the **com.soa.create.admin.user** property to **false**.
5 Click Apply Changes.
6 Log out, and then log back in again.
7 Click the **Installed Features** tab. Create Policy Manager Admin User is listed at the bottom as a pending task.
8 Click Complete Configuration and set up the admin user.

Note: You will need to restart Policy Manager for the new settings to take effect.

1 Run the following database query, which resets the password for the administrator account (and nothing else):
2 Log in using the following credentials:
   - Username: **administrator**
   - password: **password**
3 Once you're logged in, change the password to a unique and secure password.

Access to the Admin Console Needs to Be Restricted to Localhost Only

For security reasons, it's best to make sure that access to the Admin Console is restricted so that it's only accessible from the local machine (localhost).

To make sure the Admin Console is accessible only from localhost, follow the procedure below.

To restrict access to the Admin Console so that it is accessible only from localhost

1 Create a file in the ./sm60 directory named: **com.soa.admin.console.cfg**. Enter the following lines in the file:

```
admin.console.localhost.only=true
admin.console.access.restricted=true
```

2 Copy the **com.soa.admin.console.cfg** file into the ./sm60/instances/<instance_name>/deploy directory.
3 From the Admin Console, go to the Configuration tab. Verify that there is a configuration category named com.soa.admin.console and that it includes these two properties:
   - admin.console.localhost.only property set to true

- admin.console.access.restricted property set to true

4 Restart the container.

Once this setting is in place, when the container is up and running, the Admin Console should only be accessible on the local machine. If an attempt is made to access it from another machine, a 404 error is returned.

Issues with Alerts

This section provides information about possible issues related to alerts and alert emails, including email configuration and notifications. It includes:

- Alert Notifications Not Configured
- Incorrect "From" Address On Alert Notifications
- CA Revocation Emails Not Being Sent
- Too Many Alerts/Backlogged Alerts
- Alert SMTP Server Not Set Up

Alert Notifications Not Configured

If you want emails to be sent out for alerts generated, you must configure email alert forwarding and set up email alert properties.

If the necessary configuration is not done, no alert messages are sent out.

Solution:

Configure the email alert forwarding settings.

To configure email alerts

Note: Before configuring email alerts you must set up the SMTP server if it isn't set up yet.

1 Log in to the Policy Manager.
2 Click the **Alerts** tab.
3 Click Email Groups.
4 Add or modify email groups as needed.

As part of adding or modifying an email group, you must specify the SMTP server used to send the emails. You can verify that the setup is correct by clicking **Verify Connection**. This sends a test message to all email addresses in the group.

Incorrect "From" Address On Alert Notifications

Email alert notifications are being sent using the default "From" email address (alert_notification@soa.com) if the default has not been modified.

Solution:

Configure the “from” address.

To configure the “From” address for alert emails

1 Log in to the Policy Manager Admin Console.
2 Click the **Configuration** tab.
3 In the Configuration Categories section on the left, choose **com.soa.console**.
4 Add the following property: **email.sender**.
5 For the property value, type the email address that should display in the “From” field for alert messages sent out by Policy Manager. Click **Apply**.
6 Click Apply Changes.

Note: The new setting takes effect after a short delay. You do not need to restart the container.

If you remove this property, the “From” address reverts to the default after the next restart of the Policy Manager container.

CA Revocation Emails not Being Sent

If CA revocation emails are not being sent, one possible cause is that the SMTP server isn’t configured for the Certificate Authority.

Solution:

In Policy Manager, configure the SMTP server for the CA.

To configure the SMTP server for the certificate expiration email

1 Log in to the Policy Manager.
2 Click the **Configure** tab.
3 Click **Email**.
4 Click Modify SMTP Email Host.
5 Set the applicable values and save changes.

Alerts Not Showing Up on the Workbench

If expected alerts are not showing up on the Workbench, it might be because alerts are backlogged.

By default, Policy Manager is set to process up to 20 alerts per minute.

If the number of alerts being generated exceeds Policy Manager’s capability to process them, the alerts will backlog in Policy Manager. This can result in important information not reaching the right individual quickly enough; it can also result in alerts being irrelevant or even misleading due to being out of date.

Solution:

If the alerts are backlogged because the normal volume is higher than 20 per minute, you'll need to contact the Policy Manager Admin Console Administrator, who can implement one or both of the following:

- Increase the number of alerts Policy Manager can process per minute.
- Delete backlogged alerts from the database.

For instructions and additional information, refer to *Alert Emails Not Being Sent* later in this chapter.

Alert SMTP Server Not Set Up

In Policy Manager 6.x, you can set up SMTP messaging to email the following notifications to users:

- Alert notifications
- Certificate expiration notifications
- Out of memory errors on the error log

When adding or modifying an email group, you must specify the SMTP server used to send the emails for that group. You can verify the email setup by sending a test email to all addresses within the group. Follow the steps below.

To send a test email for an email group

Pressing verify connection under the Authenticated box will immediately send a test email to all addresses within the group.

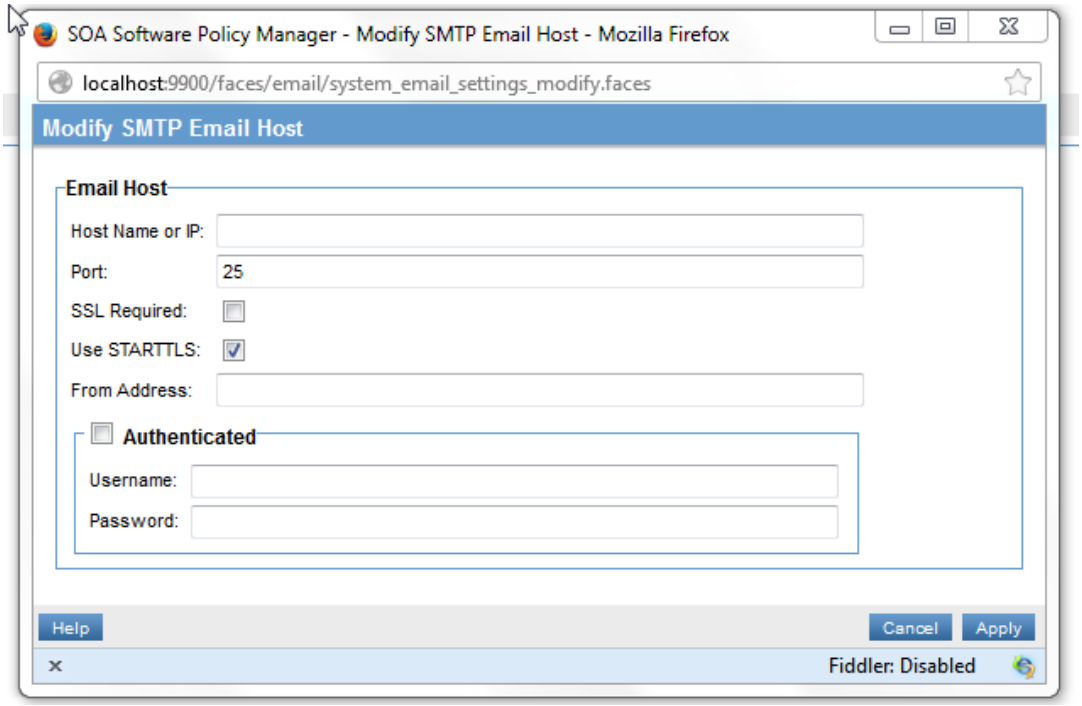
To configure Policy Manager to send certificate expiration notifications

1 Log in to the Policy Manager console.

2 Click the **Configure** tab and then click **Email**.

3 Click Modify SMTP Email Host.

Certificate expiration notifications can be configured in the Policy Manager management console under Configure-> Email -> Modify SMTP Email Host, as shown below.



To configure Policy Manager to send email alert notifications to group members

1 Log in to the Policy Manager console.

2 Click the **Alerts** tab and then click **Email Groups**.

3 Add a new email group, or modify an existing email group.

4 In the Email Group overlay, add, update, or verify the email group details, including host information.

5 Click Verify Connection. The Alert Manager sends a test email to the addresses defined for the email group.

6 Conditional: If there is an issue, the emails are not sent out, and you will see an error message. Resolve as needed, and then try again.

To send alerts with a specific FROM: address

You can configure your alert emails to display a specific address in the “From” field on the email. Follow the steps below.

To set up a specific “From” address for alert emails

1 Log in to the Policy Manager Admin Console.

2 Click the **Configuration** tab.

3 In the Configuration Categories section on the left, choose **com.soa.console**.

4 Add the following property: **email.sender**.

5 For the property value, type the email address that should display in the “From” field. Click **Apply**.

6 Click Apply Changes.

Note: The new setting takes effect after a short delay. You do not need to restart the container.

If you remove this property, the "From" address reverts to the default, alert_notification@soa.com, after the next restart of the Policy Manager container.

Unable to Start a Container

If the container will not start, it could be because of one of the following reasons:

- Incompatible JRE version
- Cannot Bind to an Interface
- Cannot Start a Container After an Update

Incompatible JRE Version

If the JRE version is incompatible with the Policy Manager version, the container will not start.

Note: SOA Software Container Instances created prior to Policy Manager Update 6.0.4.3 cannot run with Java 6.

Solution:

Verify that the JRE and update you are using are supported by the installed version of Policy Manager. Compatibility information is available in the installation documentation and on the support site.

Cannot Bind to an Interface

It might be that there is an issue with binding to a virtual machine interface, and the container is not listening on the expected host/IP and port.

If the container is being run on a machine with multiple interfaces, it might be necessary to bind a particular host/IP and port to a specific interface.

Solution:

To ensure the container listens on the specified interface, ensure that the "bind to all interfaces" option for the container listener in the Policy Manager console is **not** checked.

To resolve this issue, follow the steps below.

To clear the "Bind to All Interfaces" setting

1 Log in to the Policy Manager console.

2 For all affected containers, do the following:

- From the organization tree, select the container.
- In the center pane, under Inbound Listeners, in the Actions drop-down list, select Modify Container Listener. The Configure HTTP Container Listener overlay opens.
- Clear the **Bind to all interfaces** checkbox and then click **Finish**.

3 Unregister the service using /sm60/bin/unregisterservice.bat.

4 Re-register the service using /sm60/bin/registerservice.bat.

Cannot Start a Container After an Update

If there is an error when starting Policy Manager/Network Director containers installed as a Windows service, it could be because of installation or configuration issues.

Solution:

To troubleshoot this problem, follow the steps below.

- **Run at command line**—First, try starting the containers from the command line with this command:

  (**start.bat <container>**). Based on the results, determine the next step:

  - If it runs from the command line: the problem is an issue with the Windows service. Go on to the next step to reinstall the service.
  - If it does not run from the command line: the issue is with the container itself. The container might be trying to bind to a network interface that it cannot bind to. If so, because you can't start the Policy Manager, you must edit the **system.properties** file. Go to ***To clear the Bind to all interfaces setting in the system.properties file*** below. Use netstat to verify this.
- **Reinstall Windows service**—If the container doesn't start from the command line, you'll need to reinstall the Windows service. To do this, first unregister the service and then register it again. Using the script in the /sm60/bin folder, run the following commands:

```
UnregisterContainerService.bat <container_name>

RegisterContainerService.bat <container_name>
```

To clear the Bind to all interfaces setting in the system.properties file

1 Open up the **system.properties** file: /sm60/instances/<PMcontainerName>/system.properties.

2 Find the following default property:

```
com.soa.http.bind.all=true
```

If the property doesn't exist, add it.

3 Set the value for this property to **false**.

4 Save and exit.

Note: This property is typically modified if you have trouble connecting to the container listener. Another scenario where this might occur is if the machine has been assigned two different IP addresses. In this case, you must set the property to **false**. If you don't, the container Java process will bind to both IP addresses and be accessible on both addresses.

Troubleshooting Issues: Policy Manager Administrator

This section provides information about issues a Policy Manager Administrator might encounter. It includes:

- Cannot Connect to Service
- Can't Create Service
- Virtual Service Can't Connect to Physical Service
- Authentication/Authorization Alerts
- Alert Emails Not Being Sent

Alert Emails Not Being Sent

If alert emails are not being sent out, it might be because of one of the following:

- Too many alerts pending. By default, Policy Manager is configured to process 20 alerts per minute.
- SMTP settings are not configured properly.

Solution:

To clear the backlog of pending alert emails, run the following database query:

```
update AM_ALERTDISPSTAT set lastalertsid = (select max(alertsid) from am_alerts)
```

In addition, if the issue was not caused by an abnormal spike in alerts, you'll need to increase the number of alerts Policy Manager can process per minute.

To increase the number of alerts Policy Manager can process per minute

1 Log in to the Policy Manager Admin Console.
2 Click the **Configuration** tab.
3 In the Configuration Categories section on the left, choose **com.soa.framework**.
4 Add the following property:

```
number.of.alerts.to.dispatch.in.one.run
```

5 Set the value to 1000.
6 Save changes.

Miscellaneous Items

This section includes:

- HTTPS Listener Not Listening
- Out of memory errors on the error log
- Containers Not Starting After Update

- Cannot Log In to Policy Manager Console using LDAP

HTTPS Listener Not Listening

If the HTTPS listener is not listening on the Policy Manager container, it might be because the HTTP listener is not configured with applicable security.

All HTTPS listeners must be configured with PKI keys and X.509 certificate. If they are not, they will not work.

Solution:

Verify that the HTTPS listener is correctly configured, using the instructions below. If needed, take further troubleshooting steps as explained in the second procedure below.

To verify that an HTTPS listener is configured with PKI keys and X.509 certificate

1 Log in to the Policy Manager console.
2 Under the organization tree on the left, select the container for the HTTPS listener.
3 In the right pane, click the Details tab.
4 Under Inbound Listeners, on the Actions drop-down list, choose Modify Container Listener.
5 Under PKI Key Details and Certificate Details you should see the base64 encoded public key and the details of the X.509 certificate. If they are not present, generate PKI keys and X.509 certificate and add them.

To troubleshoot issues with the listener not working

1 On the machine on which the container is hosted, verify that the container is listening on the configured port and there are no other processes configured to listen on the container port. Shut down the container and verify that there is no process running that is listening on the same port as the configured container. For example, you could use a tool such as netstat.
2 Verify that the listener's container is started.
3 Check the logs of the container.

Out of memory errors on the error log

Out of memory errors in the log file for the container indicate that the container does not have enough memory reserved.

Solution:

If you find that you need more memory than the default of 1GB, you will need to convert to 64-bit JRE before increasing the memory. For instructions, see below.

Note: Before you convert, check with Support to see which JRE update is supported with Policy Manager. As of September 2013, JRE 6.0 Update 36 is supported. The latest update is update 43, which

isn't yet supported. We are constantly certifying new versions. For Policy Manager 6.1.15 we added support for JRE 7.0. Again, check which update is supported.

To convert to 64-bit JRE

This information is also in the SOA Support Knowledge Base: https://support.soa.com/support/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=343.

If Policy Manager and Network Director are installed as a Windows service, uninstall them before following the procedure below. Use the uninstall batch file: \sm60\bin\UnRegisterContainerService.bat.

1 Download the JRE 1.6 64-bit version from the Oracle website. Use one of the following:
   - For Linux: Linux-64bit-jre-1.6.0_37
   - For Windows: Windows-64bit-1.6.0_32
2 Install the JRE into a separate directory on the Policy Manager or Network Director machine. It can be in any location.
3 Copy the **bcprov-jdk15-141.jar** file from the original PM ./sm60/jre/lib/ext directory to the Java 6 ./jre/lib/ext directory.
4 Edit the <Java6_install_location>/jre/lib/security/**java.security** file to add the following security provider:

```
security.provider.9=org.bouncycastle.jce.provider.BouncyCastleProvider
```

5 Rename the current ./sm60/jre directory to ./sm60/jre_15.
6 Copy the <Java6_install_location>/jre directory into the Policy Manager or Network Director ./sm60 directory tree (./sm60/jre).
7 Edit the /sm60/bin/startup.sh or startup.bat file to make the change shown below:
   - From: JAVA_OPTS="-Xmx1024M -XX:MaxPermSize=128M"
   - To: JAVA_OPTS="-Xmx2048M -XX:MaxPermSize=256M"
8 On Windows, edit the /sm60/bin/RegisterContainerService.bat file to make the change shown below:
   - From: JAVA_OPTS=-Xmx1024M -XX:MaxPermSize=128M
   - To: JAVA_OPTS=-Xmx2048M -XX:MaxPermSize=256M
9 In the \sm60\bin folder, rename **JavaService.exe** to **JavaService32.exe**.
10 Copy **JavaService64.exe** (you can request it from SOA Support) to \sm60\bin and rename it to **JavaService.exe**.
11 Edit the \sm60\bin\RegisterContainerService.bat file to make the change shown below:
   - From: SET JAVA_DLL="%JAVA_HOME%\bin\client\jvm.dll"
   - To: SET JAVA_DLL="%JAVA_HOME%\bin\server\jvm.dll"

Note: We recommend that you use 2GB of memory when using 64-bit JRE. If you have a large deployment with many concurrent requests and many hosted services in the Network Director, you might need a larger heap size.

Containers Not Starting After Update

A likely cause for this issue is that the configurator cache was not cleared before the update.

Solution:

It's important that the configurator's cache folder is cleared before updating Policy Manager. If the container doesn't start after an update, and you determine that the update was started without first clearing the configurator cache, contact SOA Software Technical Support for assistance.

Cannot Log In to Policy Manager Console using LDAP

If you're experiencing trouble logging in, you will first need to determine whether you have connectivity with the LDAP server. If you do, there might be such a high volume of calls that it isn't readily available. If this is the case they you will need to define a failover server.

Solution:

To check connectivity, first try logging in on the local domain. To do this, switch your domain to localdomain and then log in using the localdomain Admin ID.

If needed, define one or more failover LDAP servers. Follow the steps below.

To define a failover LDAP server

1 Log in to the Policy Manager console.
2 Click the **Configure** tab and then click **Security**.
3 Click Identity Systems, and then click Modify Identity System.
4 Add failover URLs and save changes.

Chapter 3 | Troubleshooting: Network Director

This chapter includes information to help you troubleshoot issues that might come up with Network Director, including:

Connection Errors Returned for Configured Context Paths

A number of different issues might cause a connection error to be returned from the Network Director. For example:

- There might be a 404 error on loading the WSDL for a SOAP service. If you use the browser to access the WSDL using **<endpoint>?wsdl**, and get a 404 error rather than the WSDL file, the first step in troubleshooting is to check that the virtual service is providing a WSDL. For instructions, see ***To check that the Network Director can retrieve the virtual service WSDL*** later in this section.
- For a SOAP or REST service, you might send a request to the virtual service and receive a 404 in response.

If you are getting a 404 when invoking a virtual service, here are some things you can check:

- Check to see if the service is being hosted. To do this, enable the jetty URL to verify that all services/context paths are available. For instructions, see *Check Context Paths Hosted on Network Director* below).
- Make sure that the context path being sent by the consumer matches the context path for the virtual service being invoked.
- For a REST service:
  - Verify that the context path being sent by the consumer matches the virtual service context path.
  - Make sure the correct content type is being set in the HTTP header.
  - If there is a payload, make sure the payload is consistent with the content-type.
- Check the usage logs to see if the physical service is responding with the 404. If it is the physical service responding with a 404, verify the physical service access point.
- Check if there is an issue with the firewall or load balancer that the consumer is sending the request through.

Check Context Paths Hosted on Network Director

If a 404 is returned to the consumer when trying to invoke a virtual service, check the context paths hosted on the Network Director.

Solution:

Possible reasons for this issue are:

- The service is not deployed on the Network Director. See *To check whether the service is deployed to the Network Director* below.
- A 404 was returned from the physical service (physical service is down). See *Virtual Service Cannot Connect to Physical Services* below.

To check whether the service is deployed to the Network Director

Check the contexts hosted on the Network Director.

There is a URL you can use to list all the context paths hosted on the Network Director. To view the context paths, you must first enable a configuration setting as described below.

To check context paths from the Network Director

1 Log in to the Admin Console at http://<nd_host>:<nd_port>/admin/console.html.
2 Click the **Configuration** tab.
3 In the Configuration Categories section on the left, choose **com.soa.transport.jetty.defaultservlet**.
4 Set the value of the jetty.information.servlet.listContexts property to **true**.
5 Click **Apply Changes**.
6 Check the URL to get the list of context paths on the Network Director and see if your service is listed:

```
http://<nd_host>:<nd_port>/com.soa.transport.jetty/information
```

Virtual Service Cannot Connect to Physical Service

If the virtual service cannot connect to the next-hop service or physical service, two possible causes are:

- The physical service is down.
- The wrong access point has been configured for the physical service.

Solution:

To help determine where the issue lies, first send a request to the endpoint you listed under the physical service access point. Verify that the response was received. Depending on the results:

- If the physical service is down, contact the physical service provider.
- If the direct request was successful, and there is a firewall between the virtual service and the physical service, check in case there's an issue with either of the following:
  - Firewall
  - Proxy server

Unable to Access Policy Manager Container

In some cases it has happened that consumers were unable to connect to the Policy Manager 6.1 services, with no error when loading bundles, and with the log showing the following entry:

```
ERROR - Attempting to invoke method refresh on
com.soa.container.configuration.service.ContainerConfigPollingService.
```

One possible cause of this issue is that the maximum number of threads for the HTTP listener is set to 0 and must be increased.

Solution:

As a workaround, you can edit the system.properties file to create a temporary HTTPS listener entry. This will allow you to log in and increase the number of threads on the HTTP listener. You must then restore the original system.properties file.

To increase the maximum number of threads for the HTTP listener

1 Go to the ./sm60/instances/<pm_instance> folder on your machine and find the **system.properties** file. Save a backup copy of the original file.

2 In the file, find the following property:

org.osgi.service.http.port: set it to **9900** (or your original port)

3 Modify the property name and value as shown below:

org.osgi.service.http.port.secure: set it to 9943 (or some other port)

Note: This change creates a temporary HTTPS listener so that you can log in and update the thread count for the HTTP listener.

4 Restart the container.

5 Go to https://host:9943/ (or applicable port number) and log in to the Policy Manager console.

6 Change the default listener pool parameters to valid values. For example:

- min thread=5
- max thread=200

7 Restore the original **system.properties** file.

8 Restart the container.

Virtual Service Client Cannot Connect to Physical Service

If the client application cannot connect to the physical service, check the following:

1 If it isn't a SOAP service, go to ***Hosted Service Issues*** below to check if the service is running.

2 If it is a SOAP service, check that the virtual service is providing a WSDL. See ***To check that the Network Director can retrieve the virtual service WSDL*** below.

3 Depending on the results, do one of the following:

- If there is an error retrieving the WSDL, there is an issue with hosting the virtual service. Go to the **Hosted Service Issues** section below.
- If there was no error with the WSDL, the issue is at the policy/contract level. For additional troubleshooting steps, go to ***To check policy configuration*** below. If it is an issue with the policy or contract there should be an error in the alerts or the monitoring data for the service.

To check that the Network Director can retrieve the virtual service WSDL

1 Open a browser.

2 Enter the URL of the virtual service:

```
<nd_host>:<nd_port>/<service_context_path>
```

3 Append **?wsdl** to the end of the URL.

The WSDL file for the virtual service should be displayed in the browser. Proceed depending on what you see:

- If the WSDL file is not displayed, there is an issue with the hosted service. For additional troubleshooting steps, go to the next section, *Hosted Service Issues*, below.
- If the WDSL file is displayed, this means that the service is hosted correctly; therefore, the physical service address must be wrong, or there must be an issue with the physical service. Check the access point in the Policy Manager user interface to make sure it is correct. One possible scenario is that the physical endpoint changed after setup. You can make sure you can successfully call the physical service in the same way you did for the virtual service in Step 2, using the URL of the physical service as set up in Policy Manager container.

Hosted Service Issues

If you cannot connect to the service, and you were not able to retrieve the WSDL file, follow the steps below.

To resolve issues with hosting the virtual service

1 Verify the access point being used. To do this:
- In Policy Manager, from the organization tree, select the virtual service.
- In the right pane, click the Access Points tab.
- Verify that the access point is still listed for that service. If it isn't listed, go to the Network Director container, Hosted Services tab, and click Host Virtual Service. Select the virtual service to host on the Network Director container or cluster.

2 Next, verify the status of the container. To do this:
- In Policy Manager, from the organization tree, select the container that hosts the virtual service.
- In the right pane, click the Details tab.
- Check the status of the container. The status should display as **Started**, with a green icon.

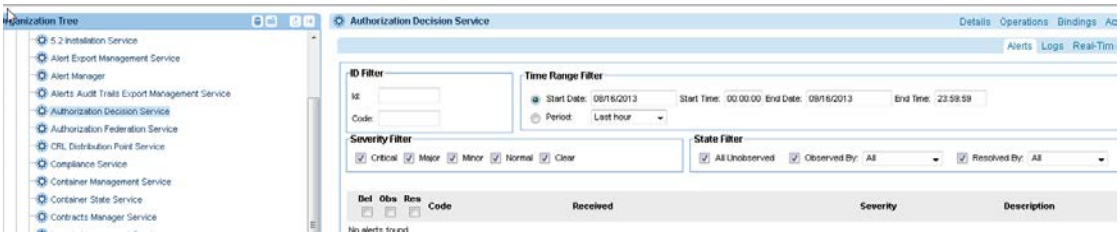
3 Take additional steps depending on the container status and settings:
- If the container has not started, check that the bundles have loaded.

- Stopped or Unresponsive: In Network Director, go to the Network Director Container Detail Page for the container and view the status indicator for the container. There are three statuses: Started, Stopped, and Unresponsive. The status is communicated from Network Director to Policy Manager every 15 seconds using the Policy Manager service called Container State Service. If Policy Manager doesn't receive a response from Network Director in a certain amount of time, the status is reported as **Unresponsive**. If there is no response for an extended period of time the status is reported as **Stopped**. This indicates a communication problem between Policy Manager and Network Director.
- Check the Network Director log file and see if there are any issues connecting to the Policy Manager.
- Check the Policy Manager log to see if there are any errors when the Network Director is connecting to Policy Manager to update its state.
- HTTPS address listed as service access point: Verify that the HTTPS listener has PKI keys and an X.509 certificate attached.

To check policy configuration

1 Log in to the Policy Manager console.

2 Select the virtual service and then check for errors under Workbench > Monitoring > Alerts.



3 Make sure:

- The consumer is included in the contract of the service.
- The contract is activated.
- There is only one contract active for the service.

- Authorization Failed Error Message When Consuming a Service

Contract Not Configured

If an "Authorization Failed" message is returned when consuming a service, one possible cause is that the contract is not configured.

Solution:

To check whether the contract is configured correctly, and correct as needed, follow the steps below.

To configure a contract

1 Log in to the Policy Manager console.

2 From the organization tree, select the virtual service.

3 Verify that the intended consumer is listed under the consumers portlet for the virtual service.

Note: If the intended consumer is not listed, you'll need to create another version of the contract. On the action panel to the right, click Start New Version. Under consumer identities, add the new consumer and then activate the new version of the contract. This will create a new version that includes the appropriate consumer.

4 Verify that the approval status of the provided contract is Activated.

5 If the contract is listed as Deactivated, activate it:

a) From the Consumers portlet, select the contract.

b) From the actions portlet, select Activate Contract.

c) Wait for approximately one minute for the contract to go into effect.

Cannot Connect to Physical Service that Requires WS-Security Headers

If requests to a physical service that requires WS-Security headers fail, it might be because the WS-Security headers are being stripped out.

By default, the Network Director strips out the WS-Security headers before sending the request to the physical endpoint.

Solution:

If the WS-Security headers are required by the physical endpoint, you can set a property in the Network Director Admin console so that the headers are not stripped out.

To modify configuration to keep the WS-Security headers

1 Log in to the Network Director Admin Console (http://<nd_host>:<nd_port>/admin).

2 Click the **Configuration** tab.

3 In the Categories portlet, select the **com.soa.wssecurity** category.

4 Set the value of the **keepsecurityHeader** property to **true**.

5 Click Apply Changes.

Chapter 4 | Reference: Database Queries

This section provides information about some database queries that you can use for gathering additional information that cannot be obtained by Workbench.

You can use your preferred database client, such as TOAD, to run these queries.

It includes:

- Query: Find Consumed Named Contracts Attached at all Levels
- Query: List All Users and the Organizations They Are Assigned to
- Query: Get Service Usage Data and Contract by Organization
- Query: Find All Virtual Services (Keys and IDs)
- Query: List All Services and Organizations They Are Attached to
- Query: Find Services with Basic Auditing Policy Attached
- Query: Find Services with No Policies Attached
- Query: Find All Virtual Services and Their Details
- Query: Find Services with SOAP 1.1 and 1.2 Bindings
- Query: Find Active Contracts Attached at the Organization Level by Service
- Query: Find Active Contracts Attached at the Service Level of a Service
- Query: Find Active Contracts Attached at the Operation Level by Service
- Query: Find Contracts by Provider Organization
- Query: Find Service by Access Point Keyword
- Query: Find Primary Contacts for Organizations
- Query: Find Contracts Attached to Service
- Query: Find Contacts for Organizations
- Query: Find Services with Attached Contracts

Note: These database queries are all available in the SOA Software Knowledge Base: https://support.soa.com/support/index.php?_m=knowledgebase&_a=view&parentcategoryid=91&pcid=21. Refer to the knowledge base for the latest version of all information.

Query: Find Consumed Named Contracts Attached at all Levels

Summary:

An organization can have a parent organization and can also have a grandparent organization that serves as an attachment point for a contract to their service. Because of this, when looking for a named contract it is necessary to make sure all parent /grandparent organizations are checked. A query for the named contract for a service will search for four different contracts:

- Contract attached at org level
- Contract attached at parent-grandparent org level
- Contract attached at service level
- Contract attached at operation level

Only when all four contracts are accounted for will this query return a correct result. This query will not take into account anonymous contracts or deactivated contracts.

The query must be run as a script. Temporary tables are created only for the duration of the query.

Query Syntax for Database:

Oracle

Query:

```
CREATE TABLE PARENT_ORGS(CHILD_ORG number(38),PARENT_ORG number(38));
CREATE TABLE QUERY_RESULTS( CONTRACTNAME varchar2(512), CONTRACTVERSIONKEY varchar2(64));
DECLARE
var_child_org number;
service_uddi varchar2(255);
BEGIN
DELETE PARENT_ORGS;
DELETE QUERY_RESULTS;
service_uddi := 'uddi:83e6a3a6-9caa-11e2-8723-c48ae6547392';
SELECT UB.BUSINESS_ENTITY_ID INTO var_child_org FROM uddi_business ub, uddi_service us
WHERE UB.BUSINESS_ENTITY_ID = US.BUSINESS_ENTITY_ID
and US.SERVICE_KEY = service_uddi;
INSERT INTO parent_orgs
WITH parent_org_recursion (TO_BUSINESS_ID, FROM_BUSINESS_ID) AS
(
SELECT TO_BUSINESS_ID, FROM_BUSINESS_ID
FROM UDDI_PUB_ASSERTION
WHERE TO_BUSINESS_ID = var_child_org
UNION ALL
SELECT upa.TO_BUSINESS_ID, upa.FROM_BUSINESS_ID
FROM UDDI_PUB_ASSERTION upa
INNER JOIN parent_org_recursion p ON p.FROM_BUSINESS_ID = upa.TO_BUSINESS_ID
)
SELECT * FROM parent_org_recursion;
WHILE var_child_org != '1003'
LOOP
```

```
INSERT INTO QUERY_RESULTS (contractname, contractversionkey)
SELECT cv.contractname as "CONTRACTNAME", CV.CONTRACTVERSIONKEY as "CONTRACTKEY"
from uddi_service us,
uddi_business ub join uddi_pub_assertion upa on UB.BUSINESS_ENTITY_ID = upa.TO_BUSINESS_ID
join resourceset_orgs rsv on UPA.FROM_BUSINESS_ID = RSV.ORGANIZATIONID
join auz_rules ar on RSV.RESOURCESETID = AR.RESOURCESETID
join auz_rulesets ars on ARS.RULESETID = AR.RULESETID
join contracts_rulesets cr on CR.RULESETID = ARS.RULESETID
join contracts_versions cv on CV.CONTRACTVERSIONID = CR.CONTRACTVERSIONID
where UB.BUSINESS_ENTITY_ID = var_child_org
and US.SERVICE_KEY = service_uddi
and CV.ACTIVE = 'Y';
SELECT P.PARENT_ORG INTO var_child_org
FROM PARENT_ORGS p
WHERE P.CHILD_ORG = var_child_org;
END LOOP;
INSERT INTO QUERY_RESULTS
(select cv.contractname as "CONTRACTNAME", CV.CONTRACTVERSIONKEY as "CONTRACTKEY"
from uddi_business ub, uddi_service us join svc_operations so on US.BUSINES_SERVICE_ID = SO.SERVICEID
join resourceset_svcops rsv on SO.OPERATIONID = RSV.OPERATIONID
join auz_rules ar on RSV.RESOURCESETID = AR.RESOURCESETID
join auz_rulesets ars on ARS.RULESETID = AR.RULESETID
join contracts_rulesets cr on CR.RULESETID = ARS.RULESETID
join contracts_versions cv on CV.CONTRACTVERSIONID = CR.CONTRACTVERSIONID
where us.service_key = service_uddi
and CV.ACTIVE = 'Y'
)
union
(select cv.contractname as "CONTRACTNAME", CV.CONTRACTVERSIONKEY as "CONTRACTKEY"
from uddi_business ub, uddi_service us join resourceset_svcs rsv on US.BUSINES_SERVICE_ID =
RSV.SERVICEID
join auz_rules ar on RSV.RESOURCESETID = AR.RESOURCESETID
join auz_rulesets ars on ARS.RULESETID = AR.RULESETID
join contracts_rulesets cr on CR.RULESETID = ARS.RULESETID
join contracts_versions cv on CV.CONTRACTVERSIONID = CR.CONTRACTVERSIONID
where us.service_key = service_uddi
and CV.ACTIVE = 'Y'
)
union
(select cv.contractname as "CONTRACTNAME", CV.CONTRACTVERSIONKEY as "CONTRACTKEY"
from uddi_service us, uddi_business ub join resourceset_orgs rsv on UB.BUSINESS_ENTITY_ID =
RSV.ORGANIZATIONID
join auz_rules ar on RSV.RESOURCESETID = AR.RESOURCESETID
join auz_rulesets ars on ARS.RULESETID = AR.RULESETID
join contracts_rulesets cr on CR.RULESETID = ARS.RULESETID
join contracts_versions cv on CV.CONTRACTVERSIONID = CR.CONTRACTVERSIONID
where UB.BUSINESS_ENTITY_ID = US.BUSINESS_ENTITY_ID
and US.SERVICE_KEY = service_uddi
and CV.ACTIVE = 'Y'
);
End;
/
SELECT substr(CONTRACTNAME, 1, 64) as CONTRACTNAME, CONTRACTVERSIONKEY FROM
QUERY_RESULTS;
DROP TABLE PARENT_ORGS;
DROP TABLE QUERY_RESULTS;
```

Query Sample Results:

CONTRACTNAME	CONTRACTVERSIONKEY
TEST_CONTRACT	cbc429bf-9caa-11e2-8723-c48ae6547392:2871
AnonymousForPing	829a5dc6-7d22-11e1-8e42-c6230bd8bd38:2641
TEST_CONTRACT_AMEX	df5e3526-9cab-11e2-8723-c48ae6547392:2911

Query: List All Users and the Organizations They Are Assigned to

Summary:

Returns a list of users and the organizations they are assigned to.

Query Syntax for Database:

Oracle, MySql

Query:

```
SELECT pu.organizationid, un.name, pu.username, pki.purpose,
 OI.organizationid AS assignedorganizationid, una.name AS assignedorganizationname
FROM pm_pkikeys pki, pm_users pu, uddi_business ub, uddi_name un, uddi_name una,
ORGANIZATION_IDENTITIES OI
WHERE pu.username like '%'
AND pu.usersid = pki.usersid
AND pu.usersid = oi.usersid
AND pu.organizationid = ub.business_entity_id
AND ub.business_entity_id = un.ref_id
AND un.ref_type = 'B'
AND una.ref_id = OI.organizationid
```

Query Sample Results:

ORGANIZATIONID	NAME	USERNAME	PURPOSE	ASSIGNEDORGANIZATIONID	ASSIGNEDORGANIZATIONNAME
1003	Registry	TMS_SSL	Identity	3553	Total Merchant Services - TMS
1003	Registry	TSYS_SSL	Identity	3554	TSYS Acquiring Solutions
1003	Registry	TSYS_Message	Identity	3554	TSYS Acquiring Solutions

Query: Get Service Usage Data and Contract by Organization

Summary:

Provides usage data for all services under a certain organization as well as the contract they are defined in.

Query Syntax for Database:

Oracle

Query:

```
select
r.INTVLSTARTDTS,
org.BUSINESS_KEY, orgn.NAME ORGNAME, s.SERVICE_KEY, sn.NAME SVCNAME,
sum(USAGECOUNT) as TOTALUSAGECOUNT, sum(TOTALRESPTIME)/greatest(sum(USAGECOUNT),1) as
AVGRESPTIME,
sum(r.SUCCESSCOUNT), sum(r.TOTALSUCCESSRESPTIME)/greatest(sum(r.SUCCESSCOUNT),1) as
AVGSUCCESSRESPTIME,
sum(r.ERRORCOUNT),sum(r.TOTALERRORRESPTIME)/greatest(sum(r.ERRORCOUNT),1) as
AVGERRORRESPTIME, V.CONTRACTNAME
from
contracts_versions v, UDDI_BUSINESS org, UDDI_NAME orgn, UDDI_NAME sn, UDDI_SERVICE s
left outer join
mo_rollupdata r on s.BUSINES_SERVICE_ID=r.SERVICEID
and r.INTVLSTARTDTS >= to_date ('2013-03-01', 'YYYY-MM-DD')
and r.INTVLSTARTDTS < to_date ('2013-03-15', 'YYYY-MM-DD')
and s.BUSINES_SERVICE_ID=r.SERVICEID
where
r.contractid != '0'
and V.CONTRACTVERSIONID = r.contractid
and org.BUSINESS_ENTITY_ID=orgn.REF_ID and orgn.REF_TYPE='B'
and s.BUSINES_SERVICE_ID=sn.REF_ID and sn.REF_TYPE = 'S'
and s.BUSINESS_ENTITY_ID=org.BUSINESS_ENTITY_ID
and (org.business_key = '<ORGANIZATION KEY>'
or
org.business_key in (
select business_key from uddi_business where business_entity_id in
 (select to_business_id from
 uddi_pub_assertion where from_business_id in
 (select business_entity_id from uddi_business
 where business_key ='<ORGANIZATION KEY>')))
or
org.business_key in (select business_key from uddi_business where business_entity_id in
 (select to_business_id from uddi_pub_assertion where from_business_id in
 (select business_entity_id from uddi_business where business_key in
 (select business_key from uddi_business where business_entity_id in
 (select to_business_id from uddi_pub_assertion where from_business_id in
 (select business_entity_id from uddi_business
 where business_key ='<ORGANIZATION KEY>'))))))
)

group by (
org.BUSINESS_KEY, s.SERVICE_KEY, orgn.NAME, sn.NAME, r.INTVLSTARTDTS, v.contractname)
order by
```

```
r.INTVLSTARTDTS desc, s.SERVICE_KEY;
```

Query Sample Results:

```
INTVLSTARTDTS           BUSINESS_KEY ORGNAME        SERVICE_KEY   SVCNAME
        TOTALUSAGECOUNT     AVGRESPONSETIME     SUM(R.SUCCESSCOUNT)
        AVGSUCCESSRESPTIME          SUM(R.ERRORCOUNT)   AVGERRORRESPTIME
        CONTRACTNAME
3/12/2013  2:11:45 A.M.    uddi:4aec3117-7f8f-11e2-bcd9-da0bd5f63124        A-ACherryl-2013  uddi:ccc2141d-
8ab9-11e2-9ffb-b0c496eb5bb2     CustomerProfileService_vs0        2        266      2        266      0
        0          CustomerProfile
3/12/2013  2:11:40 A.M.    uddi:4aec3117-7f8f-11e2-bcd9-da0bd5f63124        A-ACherryl-2013  uddi:ccc2141d-
8ab9-11e2-9ffb-b0c496eb5bb2     CustomerProfileService_vs0        1        230      1        230      0
        0          CustomerProfile
3/12/2013  2:11:35 A.M.
```

Query: Find All Virtual Services (Keys and IDs)

Summary:

Returns all Virtual Services (keys and IDs) not made internally by Policy Manager.

Query Syntax for Database:

MySql

Query:

```
SELECT US.BUSINES_SERVICE_ID, US.SERVICE_KEY
FROM UDDI_SERVICE US
   JOIN UDDI_CATEGORY_BAG UCB on US.BUSINES_SERVICE_ID = UCB.REF_ID
   JOIN UDDI_KEYED_REF UKR on UCB.CATEGORY_BAG_ID = UKR.REF_ID
WHERE BUSINESS_ENTITY_ID <> 1003 AND 1000 AND 1001
   AND UKR.KEY_NAME = 'Virtual Service'
```

Query Sample Results:

```
BUSINES_SERVICE_ID    SERVICE_KEY
20051    uddi:ef2f9784-cc8b-11e2-97db-b7b05e140af3
20052    uddi:cf7e1e09-c86f-11e2-9770-e11cbec9bf72
20053    uddi:3e7eb489-a938-11e2-8756-f454b8fcae25
```

Query: List All Services and Organizations They Are Attached to

Summary:

Returns a list of service names and keys, along with the name and key of the organization that they belong to.

Query Syntax for Database:

Oracle, MySql

Query:

```
select a.business_key, c.name as business_name, b.service_key, d.name as service_name
from uddi_business a, uddi_service b, uddi_name c, uddi_name d
where  a.business_entity_id = b.business_entity_id
 and a.business_entity_id = c.ref_id and c.ref_type = 'B'
 and b.busines_service_id = d.ref_id and d.ref_type = 'S'
order by a.business_key
```

Query Sample Results:

```
BUSINESS_KEY BUSINESS_NAME          SERVICE_KEY    SERVICE_NAME
uddi:0270a056-0d00-11de-bbc6-a429f2cfd8d9          Points.com          uddi:041516da-19ff-11df-88e8-
eacc60ee139f      PIE
uddi:02d3c77f-f05a-11de-8495-86276bdad2b4          Communications Utility      uddi:a23e51a8-f577-11de-b142-
dcd7878b3ecc      ContextEngineAPIWebServiceWrapped_vs0
uddi:02d3c77f-f05a-11de-8495-86276bdad2b4          Communications Utility      uddi:2a26423a-f576-11de-b142-
dcd7878b3ecc      CMSAPIWebServiceWrapped_vs0
```

Query: Find Services with Basic Auditing Policy Attached

Summary:

Returns name and key of services with basic auditing policy attached.

Query Syntax for Database:

Oracle, MySql

Query:

```
SELECT n.Name, s.Service_Key
FROM policies p JOIN policy_attachments pa on p.policyid=pa.policyid
   JOIN uddi_service s on pa.attachpointid=s.busines_service_id
   JOIN uddi_name n on s.busines_service_id = n.ref_id
WHERE p.policykey='BasicAuditing';
```

Query Sample Results:

```
NAME    SERVICE_KEY
Fee&RatesScheduleProcessService_vs0      uddi:b4ecab31-f2e3-11dd-b97e-f7ac69e24a6c
EBSOutboundXML           uddi:a6f29370-f3ad-11dd-bbc6-a429f2cfd8d9
EBSOutboundXML_vs0     uddi:d886af83-f3ad-11dd-bbc6-a429f2cfd8d9
```

Query: Find Services with No Policies Attached

Summary:

Returns name and key of all services with no policies attached.

Query Syntax for Database:

Oracle, MySql

Query:

```
SELECT n.Name, s.Service_Key
FROM uddi_service s JOIN uddi_name n on s.busines_service_id = n.ref_id
WHERE s.busines_service_id
   NOT IN(
      SELECT s.Busines_service_id
      FROM policies p JOIN policy_attachments pa on p.policyid=pa.policyid
         JOIN uddi_service s on pa.attachpointid = s.busines_service_id
         JOIN uddi_name n on s.busines_service_id = n.ref_id
      WHERE s.business_entity_id != 1000
         and p.policytype != 'Denial of Service'
   )
and s.business_entity_id != 1000;
```

Query Sample Results:

```
NAME    SERVICE_KEY
Fee&RatesScheduleProcessService_vs0      uddi:b4ecab31-f2e3-11dd-b97e-f7ac69e24a6c
EBSOutboundXML           uddi:a6f29370-f3ad-11dd-bbc6-a429f2cfd8d9
EBSOutboundXML_vs0     uddi:d886af83-f3ad-11dd-bbc6-a429f2cfd8d9
```

Query: Find All Virtual Services and Their Details

Summary:

Finds all virtual services and associated details.

Query Syntax for Database:

Oracle, MySql

Query:

```
select
        s.SERVICE_KEY, sn.NAME SVCNAME, orgn.NAME ORGNAME,
        btkrl.KEY_VALUE LISTENERNAME, c.NAME CONATAINERNAME, c.CONTAINERKEY,
ap.ACCESS_URL,
        wb.BINDINGTYPE BINDINGTYPE, wb.NAMESPACEURI BINDINGNAMESPACE, wb.LOCALNAME
BINDINGLOCALPART from
        UDDI_SERVICE s, UDDI_NAME sn, WSDL_PORT wp, UDDI_BINDING b, UDDI_ACCESS_POINT ap,
UDDI_KEYED_REF btkrc,
        UDDI_KEYED_REF btkrl, UDDI_KEYED_REF_GRP btkrg, UDDI_CATEGORY_BAG btcb,
MS_SVCCONTAINER c, WSDL_BINDING wb,
        UDDI_NAME orgn
where
           s.BUSINES_SERVICE_ID in (select SERVICEID from SVC_OPERATIONS where
OPERATIONTYPE='V')
        and sn.REF_ID = s.BUSINES_SERVICE_ID and sn.REF_TYPE='S'
        and orgn.REF_ID = s.BUSINESS_ENTITY_ID and orgn.REF_TYPE='B'
        and s.BUSINES_SERVICE_ID=wp.SERVICEID
        and ap.BINDING_TEMPLAT_ID=b.BINDING_TEMPLAT_ID
        and wb.BINDINGID = wp.BINDINGID
        and btkrc.REF_TYPE='K'
        and btkrc.REF_ID=btkrg.KEYED_REF_GROUP_ID
        and btkrl.REF_TYPE='K'
        and btkrl.REF_ID=btkrg.KEYED_REF_GROUP_ID
        and btkrl.KEY_NAME='listenerName'
        and btkrg.CATEGORY_BAG_ID=btcb.CATEGORY_BAG_ID
        and btcb.REF_TYPE='BT'
        and btkrc.KEY_NAME='containerKey'
        and btcb.REF_ID=b.BINDING_TEMPLAT_ID
        and wp.PORTID = b.BINDING_TEMPLAT_ID
        and btkrc.KEY_VALUE=c.CONTAINERKEY ;
```

Query Sample Results:

```
SERVICE_KEY    SCVNAME         ORGNAME         LISTENERNAME            CONTAINERNAME
        CONTAINERKEY            ACCESS_URL    BINDINGTYPE    BINDINGNAMESPACE
        BINDINDLOCALPART
uddi:b4ecab31-f2e3-11dd-b97e-f7ac69e24a6c          Fee&RatesScheduleProcessService_vs0     FX International
Payments        HTTP Outbound   AXPCluster1     AXPCluster1
        http://dwebservices.trcw.us.aexp.com:80/Fee&RatesScheduleProcessService_Dev         binding.soap11
        http://soap.sforce.com/schemas/class/feeandrateschedulProcess
        feeandrateschedulesProcessBinding
uddi:b4ecab31-f2e3-11dd-b97e-f7ac69e24a6c          Fee&RatesScheduleProcessService_vs0     FX International
Payments        HTTP Outbound   NewCluster2-old container-11
```

	http://devoutboundhttp.americanexpress.com:80/Fee&RatesScheduleProcessService http://soap.sforce.com/schemas/class/feeandrateschedulProcess feeandrateschedulesProcessBinding		binding.soap11	
uddi:b4ecab31-f2e3-11dd-b97e-f7ac69e24a6c		Fee&RatesScheduleProcessService_vs0	FX International Payments	HTTP Outbound

Query: Find Services with SOAP 1.1 and 1.2 Bindings

Summary:

Returns service key and access point of service with SOAP 1.1 and 1.2 bindings, and keeps track of duplicate URLs.

Query Syntax for Database:

Oracle, MySql

Query:

```
SELECT US.SERVICE_KEY, UAP.ACCESS_URL, COUNT(UAP.ACCESS_URL) AS NUMOCC
FROM UDDI_SERVICE US LEFT OUTER JOIN WSDL_PORT WP ON WP.SERVICEID =
US.BUSINES_SERVICE_ID
LEFT OUTER JOIN WSDL_BINDING WB ON WB.BINDINGID = WP.BINDINGID
LEFT OUTER JOIN UDDI_ACCESS_POINT UAP ON UAP.BINDING_TEMPLAT_ID = WP.PORTID
WHERE (WB.BINDINGTYPE = 'binding.soap11'
OR WB.BINDINGTYPE = 'binding.soap12')
AND UAP.BINDING_TEMPLAT_ID = WP.PORTID
AND US.SERVICE_KEY NOT LIKE 'uddi:soa.com%'
GROUP BY US.SERVICE_KEY, UAP.ACCESS_URL
HAVING (COUNT(UAP.ACCESS_URL)>1);
```

Query Sample Results:

```
SERVICE_KEY    ACESS_URL       NUMOCC
uddi:dbde605b-de99-11de-842b-a55ca974b1ff          http://192.216.212.94:88/Services/2.3/ClientServices/.asmx
          2
uddi:5c90ce40-a9ed-11dd-93e6-8a8ce9206e16          https://xmltest.teletrack.com/inquiry.asmx      2
uddi:db92077d-e09a-11df-b2af-b32e0ed3c2b7          https://utc.b2b.ihg.com/amex/b2b/xml/2005A/hotels.xml
          3
```

Query: Find Active Contracts Attached at the Organization Level by Service

Summary:

Returns contracts attached at the organization level when given service key.

Query Syntax for Database:

Oracle, MySql

Query:

```
select cv.contractname as "CONTRACTNAME", CV.CONTRACTVERSIONKEY as "CONTRACTKEY"
from uddi_service us, uddi_business ub join resourceset_orgs rsv on UB.BUSINESS_ENTITY_ID =
RSV.ORGANIZATIONID
join auz_rules ar on RSV.RESOURCESETID = AR.RESOURCESETID
join auz_rulesets ars on ARS.RULESETID = AR.RULESETID
join contracts_rulesets cr on CR.RULESETID = ARS.RULESETID
join contracts_versions cv on CV.CONTRACTVERSIONID = CR.CONTRACTVERSIONID
where UB.BUSINESS_ENTITY_ID = US.BUSINESS_ENTITY_ID
and US.SERVICE_KEY = '<SERVICE KEY>'
and CV.active= 'Y'
```

Query Sample Results:

```
CONTRACTNAME          CONTRACTKEY
named_contract_MSU    9750914b-7b91-11e2-bcd9-da0bd5f63124:2792
TEST_CONTRACT_AME     df5e3526-9cab-11e2-8723-c48ae6547392:2911
```

Query: Find Active Contracts Attached at the Service Level of a Service

Summary:

Returns all contracts attached at the service level of a particular service.

Query Syntax for Database:

Oracle, MySql

Query:

```
select UNIQUE cv.contractname as "CONTRACTNAME", CV.CONTRACTVERSIONKEY as "CONTRACTKEY"
from uddi_business ub, uddi_service us join resourceset_svcs rsv on US.BUSINES_SERVICE_ID =
RSV.SERVICEID
join auz_rules ar on RSV.RESOURCESETID = AR.RESOURCESETID
join auz_rulesets ars on ARS.RULESETID = AR.RULESETID
join contracts_rulesets cr on CR.RULESETID = ARS.RULESETID
join contracts_versions cv on CV.CONTRACTVERSIONID = CR.CONTRACTVERSIONID
where us.service_key = '<SERVICE_KEY>'
and CV.active='Y'
```

Query Sample Results:

```
CONTRACTNAME          CONTRACTKEY
ZootService4Gaj  bee0b952-afc9-11df-baa6-abc70f628665:2139
ZootService4Gaj  bee0b952-afc9-11df-baa6-abc70f628665:2795
```

Query: Find Active Contracts Attached at the Operation Level by Service

Summary:

Returns all contracts that are attached at the operation level of a service.

Query Syntax for Database:

Oracle, MySql

Query:

```
select UNIQUE cv.contractname as "CONTRACTNAME", CV.CONTRACTVERSIONKEY as "CONTRACTKEY" from
uddi_business ub, uddi_service us join svc_operations so on US.BUSINES_SERVICE_ID = SO.SERVICEID
join resourceset_svcops rsv on SO.OPERATIONID = RSV.OPERATIONID
join auz_rules ar on RSV.RESOURCESETID = AR.RESOURCESETID
join auz_rulesets ars on ARS.RULESETID = AR.RULESETID
join contracts_rulesets cr on CR.RULESETID = ARS.RULESETID
join contracts_versions cv on CV.CONTRACTVERSIONID = CR.CONTRACTVERSIONID
where us.service_key = '<Service Key>'
and CV.ACTIVE='Y'
```

Query Sample Results:

```
OPERATIONKEY            OPERATIONNAME          CONTRACTVERSIONID   CONTRACTNAME
7d0b8bd0-afc9-11df-baa6-abc70f628665    getDecision        2766
ZootDecision2ServiceSFDC_MSU_Salesforce
```

Query: Find Contracts by Provider Organization

Summary:

Returns the contract name and key of contracts provided by organization key input into the query.

Query Syntax for Database:

Oracle, MySql

Query:

```
select cv.contractname as "CONTRACTNAME", CV.CONTRACTVERSIONKEY as "CONTRACTKEY"
from uddi_business b join contracts_versions cv on ((cv.providerorgkey = b.business_key) or (cv.consumerorgkey =
b.business_key))
where cv.providerorgkey = '<PROVIDER_ORG_KEY>'
```

Query Sample Results:

```
Using Provider key 'uddi:132614f0-3bbb-11df-88e8-eacc60ee139f':
CONTRACTNAME            CONTRACTKEY
ZootService4Gaj  bee0b952-afc9-11df-baa6-abc70f628665:2139
ZootService4Gaj  bee0b952-afc9-11df-baa6-abc70f628665:2139
ZootDecision2ServiceSFDC_MSU_Sales      4ec557bc-6e57-11df-a6b5-a41ff225560f:2766
```

Query: Find Service by Access Point Keyword

Summary:

Returns the name of all services with a specific keyword in their access point URL.

Query Syntax for Database:

Oracle, MySql

Query:

```
SELECT UN.name, UAP.access_url
FROM UDDI_ACCESS_POINT UAP, UDDI_BINDING UB, UDDI_NAME UN
WHERE UAP.binding_templat_id = UB.binding_templat_id
AND UB.busines_service_id = UN.ref_id
AND UN.ref_type = 'S'
AND UAP.access_url like ('%<KEYWORD>%')
```

Query Sample Results:

```
Using keyword "asmx"
NAME    ACCESS_URL
SetupAcctEnrollment         http://sdpfessql01.aescf.us.aexp.com/zyncSecure/SetupAcctEnrollment.asmx
GetPaymentEligibility       http://sdpfessql01.aescf.us.aexp.com/bobcatAOT/GetPaymentEligibility.asmx
GetPaymentEligibility       http://sdpfessql01.aescf.us.aexp.com/bobcatAOT/GetPaymentEligibility.asmx
```

Query: Find Primary Contacts for Organizations

Summary:

Returns the primary contacts for organizations and sub-organizations.

Query Syntax for Database:

Oracle, MySql

Query:

```
select distinct n.name as Organization, a.USE_TYPE as Class, a.DESCRIPTION,  b.ADDRESS_ID,
b.ADDRESS_LINE1, b.ADDRESS_LINE2, b.ADDRESS_LINE3, b.ADDRESS_LINE4, b.ADDRESS_LINE5,
b.USE_TYPE as ADDRESS_USE_TYPE
from uddi_business be inner join uddi_name n
on be.business_entity_id = n.ref_id and n.ref_type='B',
UDDI_CONTACT a left outer join UDDI_ADDRESS b on a.CONTACT_ID = b.CONTACT_ID
where a.USE_TYPE = 'Primary'
and be.business_entity_id = a.business_entity_id
```

Query Sample Results:

```
ORGANIZATION CLASS  DESCRIPTION    ADDRESS_ID    ADDRESS_LINE1          ADDRESS_LINE2
          ADDRESS_LINE3          ADDRESS_LINE4          ADDRESS_LINE5          ADDRESS_USE_TYPE
Digitas   Primary             2458      355 Park Avenue South     New York, 10291 USA      www.digitas.com
          Primary
Sample Loyalty Vendor     Primary  Lead Programmer Analyst 2513      American Express Technologies      TRCN,
Phoenix,            Arizona, USA, 85032                              Primary
AXESS INTERNATIONAL NETWORK INC    Primary  Tatsuya Takahashi          2655      SEA FORT SQUARE
Center   Bldg.      2-3-12 Higashishinagawa,Shinagawa-ku       Tokyo     140-8619                    Primary
```

Query: Find Contracts Attached to Service

Summary:

Returns all contracts attached to a service in the form of contract key and respective service key.

Query Syntax for Database:

Oracle, MySql

Query:

```
select cv.CONTRACTVERSIONKEY AS CONTRACTKEY,s.SERVICE_KEY AS SERVICEKEY from
uddi_business b,uddi_service s,contracts_versions cv
where (s.BUSINESS_ENTITY_ID = b.BUSINESS_ENTITY_ID)
and
(cv.PROVIDERORGKEY = b.BUSINESS_KEY)
```

Query Sample Results:

CONTRACTKEY	SERVICEKEY
ee892c86-a63c-11df-baa6-abc70f628665:2114	uddi:cb818675-bb1a-11dd-b4ed-eb7d71949a33
ca23a7eb-2dd2-11de-bbc6-a429f2cfd8d9:1357	uddi:cb818675-bb1a-11dd-b4ed-eb7d71949a33
29345b92-038e-11de-bbc6-a429f2cfd8d9:1316	uddi:cb818675-bb1a-11dd-b4ed-eb7d71949a33

Query: Find Contacts for Organizations

Summary:

Finds the contacts for organizations.

Query Syntax for Database:

Oracle

Query:

```
SELECT msc.NAME, msc.ENTITYKEY, a.CONTACT_ID as CONTACT_ID, a.USE_TYPE as
CONTACT_USE_TYPE, a.DESCRIPTION,  b.ADDRESS_ID, b.ADDRESS_LINE1, b.ADDRESS_LINE2,
b.ADDRESS_LINE3, b.ADDRESS_LINE4, b.ADDRESS_LINE5, b.USE_TYPE as ADDRESS_USE_TYPE
from UDDI_CONTACT a left outer join UDDI_ADDRESS b on a.CONTACT_ID = b.CONTACT_ID, uddi_business
ubiz, entity_names msc
where (ubiz.BUSINESS_ENTITY_ID = a.BUSINESS_ENTITY_ID)
and (ubiz.BUSINESS_KEY = msc.ENTITYKEY)
```

Query Sample Results:

```
NAME    ENTITYKEY       CONTACT_ID      CONTACT_USE_TYPE    DESCRIPTION    ADDRESS_ID
        ADDRESS_LINE1           ADDRESS_LINE2           ADDRESS_LINE3           ADDRESS_LINE4
        ADRESS_LINE5  ADDRESS_USE_TYPE
American Express        uddi:f8cda618-67f8-11dd-8de8-e93862cacbf4        4200       testJan1320125PM 1
        testJan1320125PM 1      3800      testJan1320125PM 1      testJan1320125PM 1
        testJan1320125PM 1      testJan1320125PM 1      testJan1320125PM 1      testJan1320125PM 1
MYCA    uddi:9a99530d-67f9-11dd-8de8-e93862cacbf4        4300       temp16Jan20112PM
        temp16Jan20112PM        3900      temp16Jan20112PM        temp16Jan20112PM
        temp16Jan20112PM        temp16Jan20112PM        temp16Jan20112PM        temp16Jan20112PM
```

Query: Find Services with Attached Contracts

Summary:

Returns service and contract information of all services with an active contract attached.

Query Syntax for Database:

Oracle

Query:

```
select d.name as service_name, c.name as Organization, a.business_key, b.service_key,
CONTRACTS_VERSIONS.CONTRACTNAME, CONTRACTS_VERSIONS.ACTIVE,
CONTRACTS_VERSIONS.STARTDTS,
CONTRACTS_VERSIONS.EXPIRE, CONTRACTS_VERSIONS.ENDDTS,
CONTRACTS_VERSIONS.DESCRIPTION,
CONTRACTS_VERSIONS.ANONYMOUS, CONTRACTS_VERSIONS.PROVIDERORGKEY,
CONTRACTS_VERSIONS.CONSUMERORGKEY
from uddi_service b, uddi_name c, uddi_name d, CONTRACTS, CONTRACTS_VERSIONS_ARCHIVE,
uddi_business a
left outer join CONTRACTS_VERSIONS on CONTRACTS_VERSIONS.PROVIDERORGKEY = a.business_key
where  a.business_entity_id = b.business_entity_id
and a.business_entity_id = c.ref_id and c.ref_type = 'B'
and b.busines_service_id = d.ref_id and d.ref_type = 'S'
and CONTRACTS.ACTIVEVERSIONID = CONTRACTS_VERSIONS.CONTRACTVERSIONID
and CONTRACTS_VERSIONS.ACTIVE = 'Y'
and CONTRACTS.ACTIVEVERSIONID = CONTRACTS_VERSIONS_ARCHIVE.CONTRACTVERSIONID
ORDER BY service_name ASC
```

Query Sample Results:

```
Service_Name    Organization    BUSINESS_KEY SERVICE_KEY    CONTRACTNAME        ACTIVE
        STARTDTS        EXPIRE          ENDDTS          DESCRIPTION
        ANONYMOUSPROVIDERORGKEY         CONSUMERORGKEY
5.2 Container Service       SOA Software Policy Manager     uddi:soa.com:managementconfigurationbusinesskey
        uddi:soa.com:container-servicekey  Default Contract for Policy Manager Services        Y       57:36.0
        N               Default Contract for Policy Manager Services that allows anonymous access and defers
authorization to the service implementations.           Y       uddi:soa.com:managementconfigurationbusinesskey
5.2 Installation Service    SOA Software Policy Manager     uddi:soa.com:managementconfigurationbusinesskey
        uddi:soa.com:installationsvcs-mgr  Default Contract for Policy Manager Services        Y       57:36.0
        N               Default Contract for Policy Manager Services that allows anonymous access and defers
authorization to the service implementations.           Y       uddi:soa.com:managementconfigurationbusinesskey
ACHTransactionService   TCPS    uddi:72fa44db-a486-11dd-93e6-8a8ce9206e16       uddi:670cfd45-481d-11df-
8d89-bd31f6116dd5       Acxiom AddressStandardizationService to TCPS    Y       00:00.0  N
        Y       uddi:72fa44db-a486-11dd-93e6-8a8ce9206e16
```