CA Spectrum®

Report Manager Installation and Administration Guide

Release 9.3

CA Technologies Product References

This document references the following CA Technologies products:

- CA Spectrum® (CA Spectrum)
- CA Spectrum® Report Manager (Report Manager)
- CA Spectrum® IP Routing Manager
- CA Spectrum® Service Performance Manager (SPM)
- CA Spectrum® Network Configuration Manager (NCM)
- CA Business Intelligence (CABI)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Introduction

This section contains the following topics:

CA Spectrum Report Manager

CA Spectrum Report Manager generates reports in graphical and text-based formats. Reports related to CA Spectrum features are service management, performance management, response time statistics, VPLS reports, and others. The on-demand reporting feature provides a custom report development tool that reports on multiple CA Spectrum data attributes.

You access the InfoView application server from any compatible Web browser. InfoView is a web-based interface that lets you manage reports. You can generate custom reports and also one-time or periodic scheduled reports.

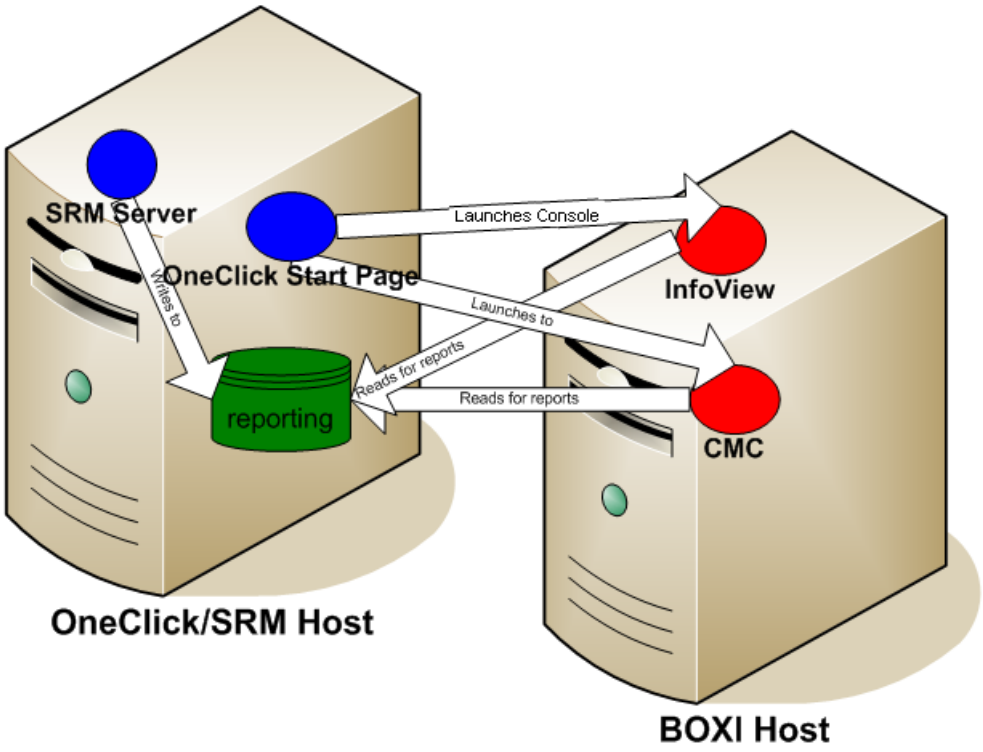
As an administrator, your responsibilities include installing, configuring, and maintaining the Report Manager application. In addition, you can schedule and manage reports for members of your organization.

CA Spectrum Report Manager uses CA Business Intelligence (CABI) to display and generate reports. CABI is a reporting and analytic software package that CA Spectrum and other CA products use to present information and support business decisions. CA Spectrum uses CABI to integrate, analyze, and present vital information that is required for effective enterprise IT management.

Report Manager Architecture

Report Manager can integrate with a BOXI instance that is running on the same server or on a remote server.

The following graphic illustrates the interactions between a OneClick/CA Spectrum Report Manager server and BOXI in a distributed environment:



Event/Alarm Data

At startup, Report Manager retrieves event and alarm data from Archive Manager for each SpectroSERVER through OneClick. After the recorded events and alarms have been processed and stored in the reporting database, Report Manager establishes an event poller. The poller processes new alarm event information from each SpectroSERVER every hour.

Note: If Report Manager is stopped, it gathers and processes all event and alarm data. The OneClick/Tomcat web server receives the last alarm before Report Manager shuts down.

Initial Data - Asset Availability

After processing the network asset information, the Report Manager processes the information from the event stream and measures the availability. Report Manager processes any event that indicates the start or the end of an outage for that asset or any of its interfaces. This includes Up/Down events, but it can also include Maintenance Mode events and certain VNM events.

Report Manager uses the collected availability event data to compile a list of outages, and stores this information in the reporting database. CA Spectrum Reporting presents this data in the availability reports.

To keep the device information current, the Report Manager continuously collects data by polling for events every hour. Because certain asset information, such as firmware revision or system contact changes less frequently, Report Manager polls devices for this data every 24 hours and updates the reporting database accordingly. Device polling is distributed randomly across all devices in the reporting environment to minimize spikes in network traffic.

The 24-hour device polling interval means that a change in asset status (for example, a system contact change) is not recorded in the reporting database for up to 24 hours. Thus, reports do not provide detailed device information changes immediately, but are recorded in the reporting database within the next 24 hours.

Initial Data - Asset Inventory

At startup, the Report Manager obtains an asset inventory list from the SpectroSERVERs and list of common attributes such as IP address, MAC address, and location for each asset. After obtaining the common attributes, the Report Manager obtains processes and stores them in the reporting database, a list of physical interfaces with appropriate interface attributes for each device.

Chapter 2: About CA Business Intelligence

This section contains the following topics:

Introducing CA Business Intelligence (CABI)

CA Spectrum Reporting uses CA Business Intelligence (CABI) to display reports.

CABI is a reporting and analytic software package that CA Spectrum and other CA products use to present information and support business decisions. CA Spectrum uses CABI to integrate, analyze, and present information that is required for effective enterprise IT management, through reports.

CABI is composed of SAP BusinessObjects Enterprise XI, with a set of tools for information management, reporting, querying, and analysis.

CABI installs SAP BusinessObjects Enterprise XI (BOXI) as a standalone component. The installation runs independently and enables other CA products to share Business Intelligence services. CABI installation is a distinct activity within the overall CA product installation process.

For more information, see the *CA Business Intelligence Implementation Guide* and the *CA Business Intelligence Release Notes.*

Introducing BusinessObjects Enterprise XI (BOXI)

CA Business Intelligence packages and delivers BusinessObjects Enterprise XI (BOXI). BOXI is a flexible, scalable, and reliable business intelligence reporting system that can be integrated into an information technology infrastructure.

CA Spectrum uses an extensive set of business intelligence capabilities that include reporting, querying, and analyzing using BusinessObjects Enterprise technology. CA Spectrum uses the following reporting technologies that BusinessObjects Enterprise offers:

-  Crystal Reports®, a common reporting framework enables CA products to deliver reports through BusinessObjects Enterprise Crystal Reports Viewer. Reports from the Crystal Reports framework have the Crystal Reports icon.
-  BusinessObjects Web Intelligence® (WEBI) is an improvised query and analysis tool for easy data access, exploration, and interaction. The WEBI drag-and-drop interface lets you construct your own reports. Reports from the WEBI interface have the WEBI icon.

Rights in BusinessObjects Enterprise

Rights are the base units for controlling user access to the objects, users, applications, servers, and other features in BusinessObjects Enterprise. They play an important role in securing the system by specifying the individual actions that users can perform on objects.

Rights enable you to perform the following functions:

- Control access to your BusinessObjects Enterprise content.
- Delegate user and group management to different departments.
- Provide your IT people with administrative access to servers and server groups.

Note: Rights are set on objects such as reports and folders rather than on the principals (the users and groups) who access them.

For example, to give a manager access to a particular folder, in the Folders area, add the manager to the access control list for the folder. This list includes all users who have access to an object. You cannot give the manager access by configuring rights settings in the Users and Groups area. The rights settings for the manager in the Users and Groups area are used to grant other principals (such as delegated administrators) access to the manager as an object in the system. Principals are themselves objects for others with greater rights to manage.

Each right on an object can be granted, denied, or unspecified. By default, an unspecified right is denied. In addition, if settings result in a right being both granted and denied to a user or group, the right is denied. The denial-based design ensures that users and groups do not automatically acquire rights that are not explicitly granted.

Important! Child object rights override the rights inherited from a parent object. This exception also applies to users who are members of groups. If a user is explicitly granted a right that the user group denies, the user receives the right.

Introducing InfoView

BusinessObjects Enterprise InfoView (InfoView) is a web-based interface that lets you manage reports with the following features:

- Browsing and searching capabilities.
- Content access (creating, editing, and viewing).
- Content scheduling and publishing.

InfoView functions like a Windows application rather than a simple web application. The InfoView toolbar dynamically changes to provide actions through context menus that are consistent with the function you want to perform. Report structures are consistent and provide security and authorizations.

InfoView also provides access to the Web Intelligence (WEBI) designer. The WEBI designer lets you create customized reports with a simple drag-and-drop interface. Custom data object selection with effective filtering options enables reporting capabilities for your environment. You can use Preferences to personalize your InfoView start page, specify viewing options, and perform other tasks.

You can use Preferences to personalize your InfoView start page, specify viewing options, and perform other tasks. For more information, see the *CA Business Intelligence Implementation Guide*.

What Does InfoView Replace?

Before CA Spectrum r9.2, CA Spectrum Reporting used a proprietary, custom user interface, and folder organization.

CA Spectrum Reporting functions are now available through CA BusinessObjects Enterprise XI InfoView. The primary benefit of InfoView is that most CA products with reporting capabilities are presented in a consistent way. With InfoView, CA products use the report content that is stored in a common repository. The common InfoView interface ensures that the CA Reports are run and scheduled in the same manner.

Introducing the Central Management Console (CMC)

Central Management Console (CMC) is a web-based tool that offers a single interface through which you can perform a wide range of administrative tasks such as user, content, and server management. CMC enables you to publish, organize, and set security levels for all the BusinessObjects Enterprise content.

Any user with valid credentials to BusinessObjects Enterprise can log in to CMC and can set personal preferences. However, if you are not a member of the Administrators group, then you cannot perform any of the available management tasks without the granted rights.

Report Security Roles

CA Spectrum Reporting security is managed by Central Management Console (CMC). For more information, see the *CA Business Intelligence Implementation Guide*.

To support effective security maintenance, CA Business Intelligence provides the following default user groups with a default set of permissions:

Note: If a user is part of more than one group, then the group having the lower permission level gets preference.

CA Reports Admin

(Highest level of access) Users in this group are the administrators for the CA Reports and CA Universes folders, explicitly granted all the rights on these folders.

CA Reports Author

(Medium level of access) Users in this group are granted rights to access, create, edit, copy, move, or schedule any of the objects in the CA Reports folder. This group does not have rights to delete any of the existing objects and instances except those objects that the user created and owns in the CA Reports folder.

Note: To create customized CA Spectrum on-demand reports, users can be classified at the CA Reports Author level.

CA Reports Viewer

(Lowest level of access) Users in this group are granted rights to view and schedule any of the objects in the CA Reports folder. This group does not have access to create, edit, or delete any of the existing objects or instances in the CA Reports folder.

This 'CA Reports Viewer' level is the default assignment for a user created in OneClick. If you have to add the user to another role, it can be done manually using the Central Management Console (CMC).

Note: To access CA Spectrum reports, users must be classified at the CA Reports Viewer level.

CA Universe Developer

(Specialized access) This group is specifically for Universe development. Users in this group have full control to the CA Universes folder.

Users who develop both reports and Universes can be part of both CA Universe Developer and CA Reports Author groups.

Chapter 3: Installation

This section contains the following topics:

Installation Components

The OneClick with Report Manager installation package includes the following components:

- The most recent supported version of CA Business Intelligence

  Note: CABI installation includes the most recent version of BOXI that is supported.

- CA Spectrum OneClick with Report Manager

  The Report Manager component that installs with OneClick provides collection and non-Business Objects administrative capabilities, such as Outage Editor and Archive Expert.

New and Upgrade Installations

A new installation is a first-time installation or an installation that you perform after you have uninstalled all components of the previous version of BusinessObjects XI. The components include the Central Management server database (report data), all registry entries (Windows), program directories, and files.

An upgrade installation is an installation that you perform on a server that has a previous version of BOXI installed. Perform an upgrade to migrate the following report data:

- Scheduled Reports
- User Accounts
- User Folder content

Upgrade Considerations with Legacy Folders:

If you are upgrading from a previous version of Report Manager, your scheduled reports are automatically placed in the Legacy Reports folder.

Note: These reports still run as scheduled with the parameter values that existed before the upgrade. These reports lack the official CA branding. If you have any problems during an upgrade maintaining your previous CA Spectrum reports, contact CA Support.

Operating System and Client Requirements

This section describes operating system requirements for BOXI R3.1 SP5, browser requirements for accessing InfoView, and software requirements for printing reports.

A full list of system prerequisites is available. For more information, see the *CA Spectrum Installation Guide*.

Windows Operating Systems

BusinessObjects Enterprise XI (BOXI) 3.1 SP5 supports the following Windows Products and Server Products:

- Windows XP SP2 Professional
- Windows XP SP3 Professional
- Windows Vista SP1 (1)
- Windows Vista SP2 (1)
- Windows 7 (1)
- Windows Server 2003 SP2 (1) (2)
- Windows Server 2003 R2 SP2 (1) (2)
- Windows Server 2008 (1) (2)
- Windows Server 2008 SP2 (1) (2)
- Windows Server 2008 R2 (2) (3)

(1) 32-bit and 64-bit O/S editions supported

(2) Data Center Edition, Enterprise Edition, Standard Edition, Web Edition

(3) 64-bit O/S editions supported

For more information, see http://www.sdn.sap.com.

Solaris Operating Systems

BusinessObjects Enterprise XI (BOXI) 3.1 SP5 supports the following Solaris Operating Systems:

- Solaris 9 for SPARC
- Solaris 10 for SPARC (1)

(1) BusinessObjects Enterprise has been tested and certified to function properly within Sun Solaris 10 Containers for this release.

Note: The following Solaris packages are prerequisites for BOXI on Solaris:

- SUNWgzip
- SUNWscpu
- SUNWbash
- SUNWbcp
- SUNWxcu4
- SUNWxwfnt

- SUNWxwplt
- SUNWlibC
- SUNWeu8os
- SUNWeuluf
- SUNWuiu8
- SUNWulcf
- SUNWmfrun
- SUNWxwice

For more information, see http://www.sdn.sap.com.

Linux Operating Systems

BusinessObjects Enterprise XI (BOXI) 3.1 SP5 supports the following Linux operating systems:

- Red Hat Enterprise Linux 4 (Enterprise Server)
- Red Hat Enterprise Linux 5 (Advanced Server)
- Red Hat Enterprise Linux Server 5
- Red Hat Enterprise Linux Advanced Platform 5

  Note: For Red Hat Linux version 4 or 5, the compat-libstdc++-33-3.2.3-47.3.i386.RPM or higher packages are required before installing BOXI. Otherwise, BOXI does not install successfully.
- Red Hat Enterprise Linux Server 6
- Red Hat Enterprise Linux Advanced Platform 6

  Note: For Red Hat Linux 6, the following packages are required before installing BOXI:

  - compat-libstdc++-33-3.2.3-69.el6.i686 (compatibility standard C++ library from GCC 3.3.4)
  - glibc-2.12-1 (Red Hat advisory RHBA-2007:0619-3)
  - libXext.i386
  - libncurses.so.5
- SuSE Linux Enterprise Server 9 SP3
- SuSE Linux Enterprise Server 10
- SuSE Linux Enterprise Server 10 SP2

For more information, see http://www.sdn.sap.com.

Web Browser Requirements for Clients

You can access CA Spectrum Reporting with any compatible Web browser. You must enable cookies on browsers that are used to access CA Spectrum Reporting. The following table lists the browser requirements:

Operating System	Browser
Windows	Microsoft Internet Explorer 6.0 SP2 or greater, Mozilla Firefox 2.0 or greater
Solaris/Linux	Microsoft Internet Explorer 6.0 SP2 or greater, Mozilla Firefox 2.0 or greater

Prerequisites for Non-English Locales

Review the following prerequisites for locales other than English:

1. Install the MS Arial Unicode font to run reports for non-English locales.
2. For Japanese, Traditional Chinese, and Simplified Chinese, use the 24-hour time format in InfoView pages. The AM, PM option is not available for the Date parameter.

Disk Space Requirements

CA Business Intelligence (CABI) has different disk space requirements for each supported platform. Platform-specific system requirements information is on the CABI Installation media, in the 'Docs' subdirectory and the '*Minimum Hardware Requirements*' section. Specifically, this information can be found in a document titled <*platform*>-Supported Platforms-SP5.pdf where <*platform*> is Windows, Linux, or Solaris.

Important! The disk space requirements outlined in the '*Minimum Hardware Requirements*' section represent absolute minimum requirements. Therefore, we recommend having at least twice the minimum disk space that is specified.

Virus Protection Exceptions for MySQL

Report Manager does not include antivirus software. We recommend installing your preferred antivirus software to protect the networking environment.

Important! To avoid potential database corruption, exclude the MySQL data directory and its subdirectories from scans by the local instance of your antivirus client. Also exclude these directories from and any remote scans that a remote antivirus instance performs.

The current default MySQL data directory location is *$SPECROOT*/mysql/data; however, this directory could be located at either <CA Spectrum Install>/SS/DDM/mysq/data or <*OneClick Install*>/mysql/data if upgrading from a previous release.

Install OneClick with Report Manager

This section describes how to install OneClick with Report Manager. For more information, see the *CA Spectrum Installation Guide*.

Important! We recommend that you back up the reporting data on the installation server before you upgrade from an earlier version of OneClick with Report Manager.

Migrate Report Data from a Previous Report Manager Installation

During the installation of OneClick with Report Manager, you are prompted to migrate report data from a remote (source) reporting database to the new CA Spectrum reporting database. The prompt applies to upgrade situations where data from a previous installation is preserved. This migration is optional. Therefore, you can either accept or decline the migration.

If you prefer to migrate data, enable access to the source report database from the remote server as described in this section.

Follow these steps:

1. Launch a MySQL client session on the source server with root account credentials. For example:
   `oscmdline> ./mysql -uroot -p<localrootpassword>;`
2. Let data be extracted from the source database by a remote account. You can provide temporary access to a remote root account.

   For example, if the CA Spectrum r9.2 target OneClick Linux server is named target-linux.ca.com, issue the following command at the MySQL command line:
   `mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'target-linux.ca.com' IDENTIFIED BY '<remoterootpassword>';`

   Note: Provide the fully qualified host name.

3. Verify that this new permission is available to all existing sessions by issuing the following command:
   `mysql> FLUSH PRIVILEGES;`
4. (Windows Only) Verify that Windows Firewall settings on the source server allow remote connections to MySQL.
   a. Click Start, Control Panel, and then Windows Firewall.
   b. Under the Exceptions tab, click Add Port and configure values as follows:
      - Enter **MySQL** for the name.
      - Enter **3306** for the Port Number.
      - Select **TCP**.
   c. (Optional) Click Change to restrict the scope of access to MySQL.
   d. Specify the location of your CA Spectrum server.
   e. Configure the option to allow remote connections to MySQL only from the migration destination server. For more information, see Windows Help and Support.

   Access to the report database on the Windows server is enabled.

Prepare for the Migration

Before you start migrating the data, verify the connection between the source and destination server databases. Verify that the data you plan to migrate is updated.

Follow these steps:

1. Verify the database connection to the remote host containing data that you plan to migrate. Issue the following command on the CA Spectrum server:
   `telnet <remote-srm-host> 3306`

   The following message indicates that the permissions have been set properly:
   ```
   Escape character is '^]'. 7
   4.1.11-nt î&#9786;  t#J0Mu'] ,&#9787;   #2p^giYa]0t{
   &#9644;  &#9786;&#9830;#08S01Bad handshakeConnection closed by foreign host.
   ```

   The following message indicates that the permissions have not been set correctly:
   ```
   Q  &#9830;#HY000Host 'user.com' is not allowed to connect to this MySQL server
   Connection closed by foreign host.
   ```

   If you are unable to connect to the MySQL server, verify that your MySQL permissions are configured correctly on your previous SRM MySQL database. Verify that the privileges are flushed before you reattempt to connect.
2. Stop all reporting processes on the remote, source server by removing all entries from the Report Manager Admin Tools, CA Spectrum Status option.

3. Wait for 5 minutes to verify that any outstanding data changes are committed to the report database.

   The root database account on the remote destination server can extract report data on the source server.

   The connection is verified.

Post Migration

Perform the following tasks after migration:

- Enable the integration of CA Spectrum with CABI. For more information, see Business Objects Integration (see page 52).

  Note: If you have integrated CA Spectrum with CABI before migration, we recommend you to disable the previous integrations.

- To ensure that the most recent reporting content (such as Crystal Reports) is available, update the existing content that is installed by CA Spectrum in Business Objects. For more information, see Manage Business Objects Content (see page 53).

Initialization Considerations for InnoDB Storage

With CA Spectrum Release 9.3, reporting data is now stored using only the InnoDB storage-engine based tables.

For new installations, Report Manager automatically ensures that InnoDB is used for all of the reporting tables.

For upgrade installations, Report Manager migrates all the reporting tables from MyISAM to InnoDB.

Important! Before you upgrade, verify that the amount of free disk space on the system is at least twice the size of the largest MYD file under *$SPECROOT*/mysql/data/reporting.

Calculating Disk Requirements for Event Storage

Use the following formula to estimate the amount of disk space that is required to support the reporting database for a specific amount of time.

```
Total Gigabytes Required = ((Number of Devices) * (Average Number of Events per Device per Day) * (Number of Days Storage Required) * (Average Size of Event in Kilobytes)) / 1048576
```

The following variables are used:

- Number of Devices – The number of devices at your site. Consider the future growth of your site when determining this value.
- Average Number of Events per Device per Day – The total number of events that are generated on a daily basis that are associated with a single device model. This number includes all events that would result from related application, port, and interface models. The easiest way to get an approximation is to look at the total number of events that were generated on a single SpectroSERVER in a single day and divide it by the number of devices that are modeled on that SpectroSERVER.
- Number of Days Storage Required – The number of days that your site requires storage.
- Average Size of Event in Kilobytes – An estimation of the amount of disk space a single event ends up consuming in the Reporting database.
- 1048576 – A conversion factor for gigabytes.

In addition to the number of devices and the number of days of storage, two variables are required to estimate the database size:

Average Number of Events per Device per Day

Query the DDMDB to see the average number of events that are generated on a given day.

If you are a new CA Spectrum user and do not know the average number of events, use a default value. Three hundred events per day, per device for 500 devices would equate to 150,000 events a day. Therefore, 300 would be a reasonable default value.

Average Size of Each Event in Reporting DB

An appropriate amount of space to store your average event and corresponding records is 1 KB. This number can increase if most of the events that are being handled are large events that contain much data. Also the types of events affect data size. Alarm events turn into multiple reporting table records. Network Configuration Manager (NCM) events only affect a single table (event).

Here are some examples:

Example A – User has 600 devices and wants to keep data for 4 years (1460 days).

The user does not know how many events per device, therefore consider 300 as the default value.

```
Total GBs required = (600 * 300 * 1460 * 1) / 1048576
Total GBs required = 262,800,000 / 1,048,576
Total GBs required = 250 GBs
```

Example B – User has 1900 devices across three servers and wants to keep data for 2 years (730 days).

The user seems to be averaging 400 events per device, per day. In this example, the three servers are not considered.

```
Total GBs required = (1900 * 400 * 730 * 1) / 1048576
Total GBs required = 554,800,000 / 1,048,576
Total GBs required = 530 GBs
```

How to Calculate Average Daily Event Rate per Device

To estimate the average daily number of events that generated per device, you first need to know how many events get generated each day. Use the following queries on the DDMDB database.

The following query returns the total event count for the last ten days:

```
SELECT date(from_unixtime(utime)) as x, count(*) as cnt
  FROM event GROUP BY x
  ORDER BY x DESC LIMIT 10;
```

The following query returns the days and event volume for the busiest ten days:

```
SELECT date(from_unixtime(utime)) as x, count(*) as cnt
  FROM event GROUP BY x
  ORDER BY cnt DESC LIMIT 10;
```

Use the result of these queries to come up with a reasonable event count. Once you know the event count, divide the number of events by the total number of modeled devices on the server to derive the average event count per device, per day.

Report Manager Installation

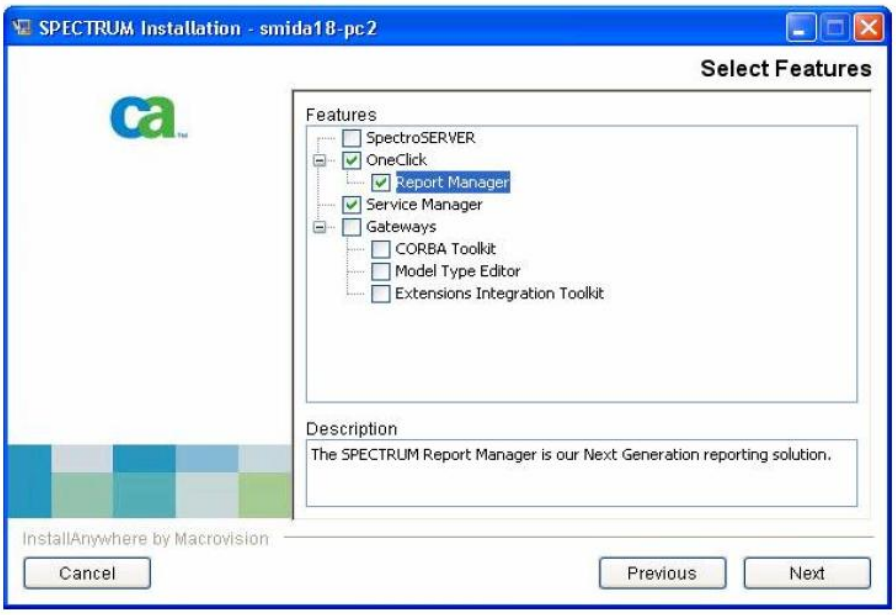
You can install OneClick with Report Manager by specifying Report Manager as a feature selection during the OneClick installation process. To install Report Manager, you need OneClick, however, Report Manager is not required to run OneClick. During installation, you can migrate the report data from a previous Report Manager installation.

Important! The disk space that is required for a Report Manager upgrade installation is two times the table size for each table that is converted to InnoDB. If enough space is not available, the installer displays a warning.

Note: Multiple Report Manager installations using a common set of SpectroSERVERs can result in inconsistencies between the primary and secondary Report Manager installations. For more information, see Report Manager and Fault Tolerance (see page 28).

Follow these steps:

1. Select the Report Manager option from the Select Features window during the installation:



2. When prompted during the installation, specify the names of the CA Spectrum servers from which you want Report Manager to collect data.

   The Report Manager Servers dialog lets you specify the names of more CA Spectrum servers, in addition to the primary server specified for OneClick. You can also modify the servers list after you have completed the installation using Report Manager Admin Tools.

   Note: Use CA Spectrum landscape names to specify servers.

3. Select to migrate historical report data associated with a previous release of OneClick with Report Manager to the new reporting database. For more information, see Migrate Report Data from a Previous Report Manager Installation (see page 22).
   - If you select to migrate reporting data, specify the following options:
     a. Specify the host from which you want to migrate the data in the Source host name field.
     b. Enter the password to access the MySQL installation on the remote server in the Source Host 'root' Database Password and Verify Password fields. The default password is ‘root’.
     c. Click Next.
   - If you do not want to migrate reporting data, do not type any values in the window and click Next.
4. Follow the onscreen instructions, to continue the OneClick installation.

   OneClick with Report Manager is installed successfully.

Report Manager and Fault Tolerance

Support for fault tolerance exists for the CA Spectrum application, but does not extend to the Report Manager component. Architectural limitations within the Report Manager do not enable a Fault Tolerant configuration beyond standard database/file replications.

Multiple Report Manager installations using a common set of SpectroSERVERs can result in inconsistencies between the primary and secondary Report Manager installations. The inconsistencies occur due to the lack of an integrated fault tolerance architecture within the Report Manager components.

Verify Installation by Testing Access Methods

Verify the Report Manager environment after installing OneClick with Report Manager. Verify that all of the SpectroSERVERs have started.

Follow these steps:

- Open InfoView from the OneClick web console and run several CA Spectrum reports.

  For more information, see the *CA Spectrum Report Manager User Guide*.

  Note: If you do not install OneClick with Report Manager correctly, then you cannot generate reports or notice any other application irregularities. For more information, see Troubleshooting (see page 87).

Upgrade the Report Parameter Pages

If you update Report Manager, run the spectrum-wkp-update.bat tool on the BOXI server that is integrated with Report Manager. The spectrum-wkp-update.bat tool downloads updated files from the CA Spectrum web server and deploys them on the BOXI server.

Procedure for Windows

Follow these steps:

1. Open Command Prompt.
2. Run the following command (words in italics indicate installation-specific values):
   ```
   % cd "C:/Program Files/CA/SC/CommonReporting3/spectrum"
   % spectrum-wkp-update.bat -host http://spectrum-hostname:port -username
   admin_name -password admin_password
   ```
   The -host flag can also specify an https URL, if SSL is configured on CA Spectrum.
3. Follow the onscreen instructions to upgrade the Report Parameter pages.

   Report Parameter pages are upgraded.

Procedure for Linux or Solaris

Follow these steps:

1. Open Command Prompt.
2. Run the following command (words in italics indicate installation-specific values):
   ```
   % cd /opt/CA/SharedComponents/CommonReporting3/spectrum
   % spectrum-wkp-update.sh -host http://spectrum-hostname:port -username
   admin_name -password admin_password
   ```
   The -host flag can also specify an https URL, if SSL is configured on CA Spectrum.
3. Restart the Tomcat server.

   The process to upgrade the Report Parameter pages is completed.

How to Install CA Business Intelligence (CABI)

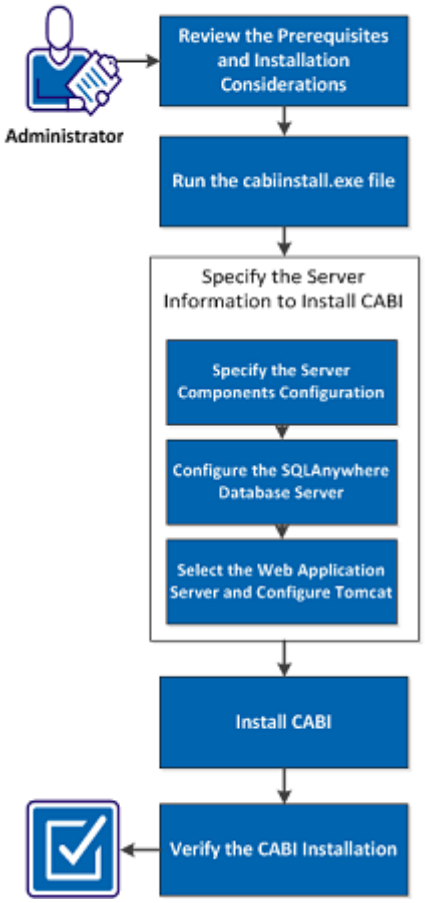
CA Business Intelligence (CABI) is a set of reporting and analytic software that various CA products use to present information and support business decisions. CA products use CABI to integrate, analyze, and present the vital information through various reporting options that is required for an effective enterprise IT management.

CABI installs SAP BusinessObjects Enterprise XI (BOXI) as a standalone component. The installation runs independently and enables other CA products to share Business Intelligence services. CABI installation is a distinct activity within the overall CA product installation process. You can activate the integration between CABI and Report Manager after installing CABI on your system. For more information, see Business Objects Integration (see page 52).

Important! We recommend that you disable the antivirus software in your system while installing CABI.

The following diagram illustrates the process to install CABI:

How to Install CA Business Intelligence (CABI)



Perform the following tasks to install CA Business Intelligence (CABI):

1. Review the Prerequisites and Installation Considerations (see page 31)
2. Run the cabiinstall.exe file (see page 37)
3. Specify the Server Information to Install CABI (see page 38)
    a. Specify the Server Components Configuration (see page 39)
    b. Configure the SQLAnywhere Database Server (see page 40)
    c. Select the Web Application Server and Configure Tomcat (see page 41)
4. Install CABI (see page 42)
5. Verify the CABI Installation (see page 42)

Important! Do not uninstall BOXI software unless CA Support recommends it. Uninstalling BOXI or OneClick uninstalls Report Manager and removes all reports.

For more information, see the *CA Business Intelligence Implementation Guide* and *CA Spectrum Installation Guide.*

Review the Prerequisites and Installation Considerations

Review the following prerequisites and installation considerations before installing CABI:

1. Verify the network connectivity between all computers that are part of your deployment.
2. If you have integrated CABI with LDAP, verify that the following information is available after updating the cabi_default_groups.xml file of CABI 3.3 installer:

    ```
    <?xml version="1.0"?>

    <biconfig version="1.0">

    </biconfig>
    ```

    For more information, see LDAP User Scheduled Reports Failed to Work (see page 88).
3. If you are using your own database server:
    - Create a database for the CMS.
    - Create an auditing database, if required.
    - Create a user ID and password with access to your existing database (if you are integrating your existing database server software), so that the installation can access your database to configure the CMS database.

- Verify your login credentials.
- Test the database connection between the computer hosting the database servers and the CMS.
- If you are using DB2 or Sybase, verify that your database is created with the correct settings (Some settings cannot be modified after the database is created).
- Verify that the database client software is configured correctly.

4. Verify that you have installed the most recent versions of the required Service Packs, Hotfix Bundles, Critical Updates, and Software Release Notes (SRN) for the supported version of BOXI. These components are available on the CA Support website.

For Unix:

- If you plan to connect remotely to install, verify that the terminal setting is set to VT100 before starting the installation.
- If you are not using Tomcat, verify that your existing web application server has the JDK installed.
- UNIX user account under which the install is run must have read, write, and execute permissions to the directory where BOXI is installed.

For Windows:

- If you are installing on Windows Server 2003 Service Pack 1 or Windows Server 2003 Service Pack 2, ensure that the Update for Windows Server 2003 (KB925336) is installed on your computer.
- If you are installing on Windows XP, prepare the computer with the Workaround provided by Microsoft (under the Workaround section).

Note: CABI installation takes about an hour. A Windows installation takes more time than a Linux/Solaris installation. Do not invoke CABI installation using 'sudo' on Linux or Solaris. A root user account is required. For more information, see the *CA Business Intelligence Implementation Guide*.

Supported Operating Systems

For Windows:

Desktop

- Windows XP SP3 Professional, Windows Vista SP2 , Windows 7, and Windows 7 with SP1 32-bit and 64-bit O/S editions are supported.
- Windows Server 2003 SP2, Windows Server 2003 R2 SP2, and Windows Server 2008 with SP2 32-bit and 64-bit O/S editions, Data Center, Enterprise, Standard, web editions are supported.
- Windows Server 2008 R2, and Windows Server 2008 R2 SP1 with Data Center, Enterprise, Standard, Web, and 64-bit O/S editions are supported.

Note: The 32-bit compiled binaries of SAP BusinessObjects Enterprise software are supported on 32-bit and 64-bit versions of the Windows operating system (running on either x86 or x64 CPUs made by AMD and Intel).

For Linux:

- Red Hat Enterprise Linux 4 (Enterprise Server)
- Red Hat Enterprise Linux 4 (Advanced Server)
- Red Hat Enterprise Linux Server 5
- Red Hat Enterprise Linux Advanced Platform 5
- Red Hat Enterprise Linux Server 6
- Red Hat Enterprise Linux Advanced Platform 6
- SUSE Linux Enterprise Server 9 SP3
- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 10 SP2
- SUSE Linux Enterprise Server 11

Note: Red Hat Enterprise Linux 6 is a new platform support addition in Service Pack 5 which is only available for support on the SP5 full release install of SAP Business Objects Enterprise. The SP5 patch only release of SAP Business Objects Enterprise does not provide support for this new platform.

For Solaris:

- Solaris 9 for SPARC
- Solaris 10 for SPARC (SAP BusinessObjects Enterprise has been tested and is certified to function properly within Sun Solaris 10 Containers for this release).

Minimum Hardware Requirements

For Windows:

- 2.0 GHz Pentium 4-class processor
- 2 GB RAM
- Hard disk space availability (with English language only) for full release install:
  - 6.0 GB for SAP BusinessObjects Enterprise install
  - 1.0 GB for SAP BusinessObjects Enterprise client install
  - 0.2 GB for SAP BusinessObjects Live Office install
- Additional hard disk space availability (each individual language pack) for full release install:
  - 0.6 GB for SAP BusinessObjects Enterprise install
  - 0.1 GB for SAP BusinessObjects Enterprise client install
  - 0.2 GB for SAP BusinessObjects Live Office install
- Hard disk space availability (with English language only) for patch release install:
  - 4.0 GB for SAP BusinessObjects Enterprise install
  - 1.3 GB for SAP BusinessObjects Enterprise client install
  - 0.2 GB for SAP BusinessObjects Live Office install
- Additional hard disk space availability (each individual language pack) for patch release install:
  - 0.5 GB for SAP BusinessObjects Enterprise install
  - 0.2 GB for SAP BusinessObjects Enterprise client install
  - 0.1 GB for SAP BusinessObjects Live Office install

For Linux:

- 2.0 GHz Pentium 4-class processor
- 2 GB RAM
- Hard disk space availability (with English language only) for full release install:
  - 5.5 GB for SAP BusinessObjects Enterprise install

- Additional hard disk space availability (each individual language pack) for full release install:
  - 0.4 GB for SAP BusinessObjects Enterprise install
- Hard disk space availability (with English language only) for patch release install:
  - 2.1 GB for SAP BusinessObjects Enterprise install
- Additional hard disk space availability (each individual language pack) for patch release install:
  - 0.2 GB for SAP BusinessObjects Enterprise install

Minimum Patch Level for Red Hat

A minimum operating system installation is required, with the following patches:

- Red Hat 4: compat-libstdc++-33-3.2.3-47.3.i386.rpm
- Red Hat 5: RHBA-2007:0619-3
- Red Hat 6: compat-libstdc++-33-3.2.3-69.el6.i686 (compatibility standard C++ library from GCC 3.3.4), glibc-2.12-1 (RedHat advisory RHBA-2007:0619-3), libXext.i386, libncurses.so.5
- SLES 9: XFree86-4.3.99.902-43.22 (XFree86) and XFree86-libs-4.3.99.902-43.22 (XFree86 Libs)

  Note: For SLES 9, 10, 10 SP2 and 11, no additional components are required.

Later patches beyond the specified minimum patch requirement can be used, but they may not be officially tested against SAP BusinessObjects products.

For Solaris:

- SPARC v8plus
- 2 GB RAM
- Hard disk space availability (with English language only) for full release install:
  - 5.3 GB for SAP BusinessObjects Enterprise install
- Additional hard disk space availability (each individual language pack) for full release install:
  - 0.3 GB for SAP BusinessObjects Enterprise install

Hard disk space availability (with English language only) for patch release install:

- 2.1 GB for SAP BusinessObjects Enterprise install

- Additional hard disk space availability (each individual language pack) for patch release install:
  - 0.2 GB for SAP BusinessObjects Enterprise install

Note: The 32-bit compiled binaries of SAP BusinessObjects Enterprise software are supported on 32-bit and 64-bit versions of the Solaris operating system.

Minimum Patch Level for Solaris 9

Install Solaris 9 with the following packages:

- kernel patch 112233-11 or higher
- libc 112874-16 or higher
- C++ run-time 111711-11 or higher
- linker patch 112963-17 or higher
- zlib patch 115754-02 or higher
- libm.so.1 SUNW_1.1.1

Note: Later patches beyond the specified minimum patch requirement can be used, but they may not be officially tested against SAP BusinessObjects products. For more information, see the *CA Business Intelligence Implementation Guide*.

Minimum Patch Level for Solaris 10

Install Solaris 10 with the following packages:

- SUNWgzip
- SUNWzlib
- SUNWscpu
- SUNWbash
- SUNWbcp
- SUNWxcu4 XCU4 Utilities
- SUNWxwfnt
- SUNWxwplt
- SUNWlibC
- SUNWeu8os - American English/UTF-8 L10N For OS Environment User Files

- SUNWeuluf - UTF-8 L10N For Language Environment User Files
- SUNWuiu8 - Iconv modules for UTF-8 Locale
- SUNWulcf - UTF-8 Locale Environment Common Files
- SUNWmfrun
- SUNWxwice

Note: Later patches beyond the specified minimum patch requirement can be used, but they may not be officially tested against SAP BusinessObjects products.

Run the cabiinstall.exe file

You can run the cabiinstall.exe file from the root directory of the CABI DVD as an initial step of setting up your BOXI installation on Windows.

After running the CABI Installer, select the language for the installation setup, language packs, installation type, and installation directory.

Follow these steps:

1. If you are installing from a DVD and the Windows Autoplay setting is enabled, the installer starts automatically. If Autoplay is not enabled, or you are installing from a hard drive, run the cabiinstall.exe file from the root directory of the CABI DVD.

   The Please Choose Setup Language dialog opens.

2. Select the language as English, then click OK.

   The Introduction dialog opens.

3. Click Next.

   The CA Technologies License Agreement dialog opens

4. Accept the CA Technologies License Agreement, then click Next.
5. Click Yes to install the CA Technologies report templates, then click Next.
6. If you want to save the CABI response file, click Yes.
7. Enter the response filename and the directory to create the response file, then click Next.

   The following default locations are available:

   - For windows 32-bit computers: C:\Program Files\CA\SC\CommonReporting3
   - For x64 computers: C:\Program Files X(86)\CA\SC\CommonReporting3

   The Review Settings dialog opens.

8. Click Install.

   The CABI installation wizard appears.

9. Click Next.

   The BusinessObjects Enterprise License Agreement dialog opens.

10. Accept the BusinessObjects Enterprise License Agreement, then click OK.

    The Choose Language Packs dialog opens.

11. Select the language packs that you want to install.

12. Click Next.

    The Install Type window appears. For more information, see the *CA Business Intelligence Implementation Guide*.

13. Select New.

14. Select one of the following options:

    - Install SQL Anywhere Database Server if you do not have a system database server and you want to install MySQL Anywhere on the current computer.
    - Use an existing database server if you want to use an existing database server.

15. Select the Enable servers upon installation check box if you want to launch BusinessObjects Enterprise when the installation process is completed. If you do not select this option, manually enable and run the BusinessObjects Enterprise application server from the CMS after installation.

16. Specify the destination to install the BusinessObjects Enterprise components (verify that enough disk space is available).

    The following default locations are available:

    - C:\Program Files\CA\SC\CommonReporting3 (for 32-bit computers)
    - C:\Program Files X(86)\CA\SC\CommonReporting3 (for x64 computers)

17. Click Next.

    The Server Components Configuration window appears.

Specify the Server Information to Install CABI

You can specify the server information to install CABI (such as the information about your CMS, Server Intelligence Agent Information). Performing a new installation deploys all of the required and optional components to the computer. You can perform the following tasks to install CABI:

a. Specify the Server Components Configuration (see page 39)

b. Configure the SQLAnywhere Database Server (see page 40)

c. Select the Web Application Server and Configure Tomcat (see page 41)

Specify the Server Components Configuration

Use the Server Components Configuration screen to enter the port number and an administrator password for the new Central Management System (CMS). CMS is the only server that accesses the CMS system database. The CMS system database stores configuration, authentication, user, auditing, and other BOXI-related information. The CMS system database allows CMS to maintain security, manage objects, and manage servers. The CMS uses a database to store system information. For more information, see the *CA Business Intelligence Implementation Guide*.

Follow these steps:

1. From the Server Components Configuration screen, specify a port number in the CMS port field.

   The default CMS port number is 6400.

   CMS communicates with other BOXI servers through the specified port.

2. Specify a password for the CMS administrator account in the Password and Confirm password fields.

   Note: Select the Configure the BOXI Administrator password later check box if you want to configure the Administrator password, after the installation is complete. If you select this option, log in to the CMC with a blank password for the first time to be able to change the Administrator password.

3. Click Next.

   The Server Intelligence Agent screen appears.

   Note: A Server Intelligence Agent (SIA) node is automatically created during installation of BOXI. For more information, see the *CA Business Intelligence Implementation Guide*.

4. In the Server Intelligence Agent screen, provide a unique name to identify the SIA node in the Node Name field.

   Note: Do not use spaces or non-alpha-numeric characters in a SIA node name. By default, the node name is same as the system host name.

5. Specify a port number for the SIA in the Port field (default is 6410). The SIA uses this port to communicate with the CMS.

6. Click Next.

   Once the SIA information is entered, the port number is validated before you can proceed to configure the CMS database for your installation. A warning displays if the port you specified (6410) is not available. To continue, specify unused and valid port numbers.

Configure the SQLAnywhere Database Server

In BOXI, a database can be defined as a data repository that organizes information into structures (tables) for rapid search and information retrieval.

The CMS uses a database to store system information. If you install SQL Anywhere as part of the BOXI installation, SQL Anywhere CMS database is created.

The SQL Anywhere Database Server Configuration screen displays if you select the option to install SQL Anywhere as part of the BOXI installation. For more information, see the *CA Business Intelligence Implementation Guide*. If you do not have a database system ready, the BOXI installer can create and configure a SQL Anywhere database system as part of the installation process. The SQL Anywhere database server lets you group the tables together into collections of logically related tables (tablespaces). Tables are grouped into tablespaces within a database system in the same way that files are grouped into a directory within a file system.

Follow these steps:

1. From the CMS System Database Configuration screen, specify the Data Source Name for the SQL Anywhere database server.

   The default name is BOE120.

2. Specify the port number for the SQL Anywhere database server in the SQL Anywhere Port Number field.

   The default port number is 2638.

3. Specify and confirm a password for the SQL Anywhere DBA user account in the SQL Anywhere DBA User Account area.

4. Confirm the user name and specify a password for the SQL Anywhere BusinessObjects database user account in the SQL Anywhere BusinessObjects User Account area.

   Note: The user name must be unique on the network.

5. Click Next.

   The Select Web Application Server screen displays.

   SQL Anywhere Database Server is configured.

Note: You can use any database system with BOXI as long as the CA Technologies product implementing BOXI supports the database system. If you use your own database system, first configure the system and confirm that the system is operational. For more information, see the *CA Business Intelligence Implementation Guide*.

Select the Web Application Server and Configure Tomcat

The Web application server runs BOXI web applications such as InfoView, the CMC, and custom web applications. Use the Select Web Application Server screen to select the web application.

To configure a Java web application server for BOXI, the web application server administrator account name, password, and the listener port number are required.

Follow these steps:

1. From the Select Web Application Server screen, select Java Web Application Server.
2. Select one of the following options:
   - Install Tomcat application server and deploy to it. This option automatically installs and configures Tomcat.
   - Automatically deploy to a pre-installed Web Application Server.
3. Specify the configuration and authentication information.
4. Click Next.

   The Configure Tomcat screen displays.
5. Accept the default values or specify new port numbers for the Connection port, Shutdown port, and Redirect port.
6. Click Next.

   Note: If the port numbers that you specified are in use, a warning message displays. To continue, specify unused and valid port numbers.

   The Start Installation screen displays.

   Web Application Server is selected and Tomcat is configured.

Note: If you select an existing server in the Select Web Application Server screen, provide specific configuration information about your existing web application server. For more information, see the *CA Business Intelligence Implementation Guide.*

Install CABI

After selecting the Web Application Server and configuring Tomcat, start the Installation Process.

Follow these steps:

1. From the Configure Tomcat screen, click Next to start the installation process.

   Once the installation is complete, the Installation Complete screen displays.

2. Click Finish to complete the BOXI installation.

   The CA Business Intelligence Completion screen displays with a summary of the installation.

3. After the installation is complete, the Restart Machine option is selected by default. If you do not want to restart the system immediately, select Restart later, and click Done.

   CABI installation is completed.

Note: A GUI-based CABI installation is not supported on UNIX. Console based and silent installation of CABI is supported on UNIX. For more information, see the *CA Business Intelligence Implementation Guide*.

Verify the CABI Installation

After installing CABI, you can verify the status of the installation. Verification of CABI installation depends on the deployment type and the components that are selected in the installation process. You can use the following methods to verify the CABI installation:

- Verify that CMS (6400), SIA (6410), and Tomcat (8080) are running.
- In the Central Configuration Manager (CMC), verify if all the 28 servers are running and enabled. However, in Unix, you can see 29 servers running in CMC. For more information, see the *CA Business Intelligence Implementation Guide.*

Follow these steps:

1. On Windows, select Start, All Programs, BusinessObjects XI, BusinessObjects Enterprise, and Central Configuration Manager.

   The Central Configuration Manager window opens.

2. Verify the status of Tomcat and Server Intelligence Agent (SIA).

3. Click the Manage Servers icon.

   The Log On window opens.

4. Enter the name of your system, provide your credentials, and click Connect.

   A list of servers that are related to CABI is displayed.

5. Verify that all the servers related to CABI are running and enabled.

   CABI installation is verified.

Uninstall CABI

Use Add/Remove Programs in Windows to uninstall CABI. After uninstalling CABI from Add/Remove programs, uninstall a fix pack/service pack from CABI using the biekpatch utility. To locate the patches that are installed on your system, open the biek.properties file that is located in *INSTALLDIR*\CommonReporting3. Find the [Patches] section. It contains the list of patches that are installed.

Example

```
[Patches]
Level=1
Patches=1
Patch1=FP1_5
```

For Windows

Follow these steps:

1. Click Start, Settings, Control Panel, Add/Remove Programs.

   A list of installed programs is displayed.

2. Select CA Business Intelligence and click Change/Remove.

   The CABI uninstaller is displayed.

   Note: If CABI is installed through a silent installation, then skip step 3 and 5.

3. Click Uninstall.

   The uninstallation process begins.

4. Click Done.

5. Verify the following information to confirm the CABI uninstallation:

   - All of the shortcut menu items that are related to CABI or BusinessObjects Enterprise are removed from the Programs menu.
   - You cannot log in to the CMC or InfoView.

   Note: After a successful uninstallation, the Commonreporting3 folder remains in the installation directory.

6. To uninstall a fix pack/service pack, navigate to the following biekpatch utility:

   INSTALLDIR/Uninstall CA Business Intelligence

7. From a DOS prompt, run the following command:

   `biekpatch –u patch_name`

   The specific fix pack/service pack is uninstalled.

   Note: If you are using Windows 2008, delete the registry entry, HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/ComputerAssociates/Shared/CommonReporting3 from Registry. For more information, see the *CA Business Intelligence Implementation Guide*.

8. To uninstall all the fix packs/service packs for the installation, navigate to the following biekpatch utility:

   INSTALLDIR/Uninstall CA Business Intelligence

9. From a DOS prompt, run the following command:

   `biekpatch –u ALL`

   All the fix packs/service packs are uninstalled.

For UNIX/Linux/Solaris

Follow these steps:

1. Navigate to the installation location of CABI (for example, /opt/CA/SharedComponents/CommonReporting3/Uninstall) and run the following script:

   `./Uninstall_CA_Business_Intelligence 3.3`

2. Select to uninstall the full installation.
3. Select Remove and press Enter.

   The uninstallation proceeds.

4. If you are using an upgraded version of CABI 3.3 (upgraded from 3.2 and equal to SP5), navigate to the biekpatch utility, and run the following command to uninstall SP5:

   ```
   biekpatch –u SP5
   ```

5. After uninstalling SP5, uninstall CABI 3.2.

   For more information, see the *CA Business Intelligence Guide.*

6. To confirm the CABI uninstallation, verify the following information:

   - All folders inside the parent directory are deleted.
   - You cannot log in to the CMC or InfoView.

   CABI uninstallation is successful.

Important! Attempting to uninstall BusinessObjects Enterprise manually is not recommended. Manual uninstallation can lead to instability for other CA products that use CABI. You can manually uninstall CABI from UNIX if you have terminated the installation process and you want to clean the computer for the next successful installation. For more information, see the *CA Business Intelligence Guide*.

Testing LDAP with BOXI and Report Manager

The Lightweight Directory Access Protocol (LDAP) is an application protocol for accessing and maintaining distributed user directory information services. A cluster of hosts uses the LDAP method to enable centralized security authentication and access to user and group information. Both CA Spectrum and BOXI support LDAP to manage user security. If LDAP is configured, you can access CA Spectrum and BOXI applications with your LDAP user name and password. This eliminates the need to recreate individual user and group accounts within each application.

To test LDAP with BOXI and Report Manager, perform the following tasks:

1. Specify the CA Spectrum LDAP Settings (see page 46)
2. Specify the BOXI LDAP Settings (see page 46)
3. Configure the Report Manager for LDAP Single Sign-On (see page 47)

Specify CA Spectrum LDAP Settings

You can specify the CA Spectrum LDAP settings on the OneClick home page. As a CA Spectrum administrator, you can specify the appropriate values in the LDAP server settings section.

Follow these steps:

1. Log in to the OneClick start page as a CA Spectrum administrator
2. Select Administration, LDAP Configuration.
3. Fill in the appropriate values in the 'LDAP Server Settings' section.
4. Configure the 'Save LDAP passwords to CA Spectrum database' section as needed.
5. Configure the 'User Name Lookup' section as appropriate to your LDAP configuration.
6. Enter a username and password and select Test.
7. If you were able to authenticate with the LDAP server, select Save.

Specify BOXI LDAP Settings

You can specify the BOXI LDAP settings on the Central Management Console (CMC) home page.

Follow these steps:

1. Log in to the CMC as the Administrator user and select Authentication from the home page.
2. Double-click the LDAP option and select 'Start LDAP Configuration Wizard'.
3. Add the LDAP server in the form: <hostname>:CA Portal.
4. Select the LDAP server type.
5. Enter the 'Base LDAP Distinguished Name'.
6. For the LDAP referral credentials, enter the distinguished name of an administrator user.

   For example, 'uid=ASmith,ou=Users,dc=ca,dc=com' as the user and enter that user password. The LDAP server administration credentials are not required.
7. Select the 'Type of SSL Authentication'.
8. Select the 'Single Sign-On Authentication type'.

9. For the LDAP and alias users, select the following options:
   - New Alias Options - Create an account for every LDAP alias
   - Alias Update Options - Create new aliases when the Alias Update occurs
   - New User Options - New users are created as concurrent users
10. Click Finish. The LDAP settings screen displays, if the information was entered correctly.
11. In the 'Mapped LDAP Member Groups' section of the page, add the group cn=BOXI and ou=Users.

    For example, 'cn=BOXI,ou=Users,dc=ca,dc=com'.
12. Click Update to save your changes.
13. Close the LDAP settings window.
14. Under groups, specify the group specified in step 11 a member of the 'CA Report Viewers' group.

    Note: By default LDAP server users are in the 'CA Report Viewers' group.

    Within a few minutes, the users in your LDAP server are created in your BOXI environment automatically. You can add any of LDAP server users to the Administrators group to grant more privileges.

    Important! Users on an LDAP server must put the LDAP group within the 'CA Report Viewers' folder, so that they can log in to InfoView/BOXI and CA Spectrum with the same credentials.

Configure Report Manager Integration for LDAP Single Sign-On

With LDAP enabled on both ends, you can enable Single Sign-On between CA Spectrum and BOXI for InfoView. To enable Single Sign-On, you can configure the Report Manager integration from the OneClick home page.

Follow these steps:

1. As a CA Spectrum Administrator, navigate to the Administration tab and the Report Manager administration area, and select Business Objects Integration.
2. Navigate to the Single Sign-On with Business Objects InfoView section, and select 'Enable Single Sign-On with Business Objects InfoView'.
3. Verify that the “SSO Authentication Type” is set to ‘secLDAP’ and select Save.
4. Close your OneClick browser window.
5. Log in as any of the LDAP users for which you created an Administrator CA Spectrum role.

6. Select Administration, Report Manager.
7. Select Business Objects InfoView and log in to InfoView without username/password.

   Note: It can take a few minutes for all of the above changes to take effect. If the login attempt fails, wait a few minutes and try again.

Enable Trusted Authentication between Report Manager and BOXI InfoView

Trusted Authentication is a single sign-on solution from Business Objects that establishes trust between Central Management Server (CMS) and Report Manager. As a result, you can launch InfoView from the OneClick web console without providing InfoView login credentials. First enable trusted authentication for BOXI. Then enable trusted authentication in Report Manager.

Follow these steps:

1. Log in to the Central Management Console with administrative rights.
2. Navigate to the Authentication management area of CMC, and click the Enterprise tab.
3. Click Enable Trusted Authentication.
4. Create a shared secret for your users.

   Note: The shared secret lets the client and CMS to create a trusted authentication password. This password is used to establish trust.

When trusted authentication has been enabled for BOXI, complete the configuration on the Report Manager server.

Follow these steps:

1. Click the Administration tab, navigate to the CA Spectrum Administration area, and select Business Objects Integration.
2. Navigate to the 'Single Sign-On with Business Objects InfoView' section.
3. Select 'Enable Single Sign-On with Business Objects InfoView'.
4. Verify that the SSO Authentication Type is set to Trusted Authentication.
5. Specify the BOXI shared secret that you created previously.

   CA Spectrum uses this shared secret to establish trust between the client and CMS.
6. Save the changes.
7. To test the settings, launch InfoView from the CA Spectrum web console.

Chapter 4: Application Administration

This section contains the following topics:

About Administration Tools and User Account Privileges

This chapter describes how to use the Report Manager Administration Tools and the Central Management Console (CMC) to configure and manage Report Manager. The Report Manager Administration Tools are accessed with the OneClick web console.

Important! Only users with OneClick Administration rights have access to the Report Manager Administration tools. For more information, see the *CA Spectrum Administrator Guide*.

Notes:

- CMC handles many of the processes that are done with Administration Tools for Report Manager versions earlier than r9.2. Functions such as changing the BOXI Administrator password and checking BOXI server status are now done with CMC.
- Users on an LDAP server must put the LDAP group within the 'CA Report Viewers' folder, so that they can log in to InfoView/BOXI and CA Spectrum with the same credentials.
- When OneClick users are added to CA Spectrum, they are automatically added to BOXI. However, Report Manager has to poll for events and the process can take up to an hour before users appear in BOXI.
- BOXI handles User IDs with case-insensitivity, regardless of the authentication mechanism. For example, if 'Dave', 'dave', and 'DAVE' are created in OneClick, the first username created (for example, 'Dave') is added to BOXI, the other usernames are disregarded. Adjust User IDs accordingly.

Once you create CA Spectrum Reporting users, you can specify the actions that they can perform with reports.

Note: You can add users to Business Objects, but not to CA Spectrum OneClick. For more information, see the *CA Business Objects Implementation Guide.*

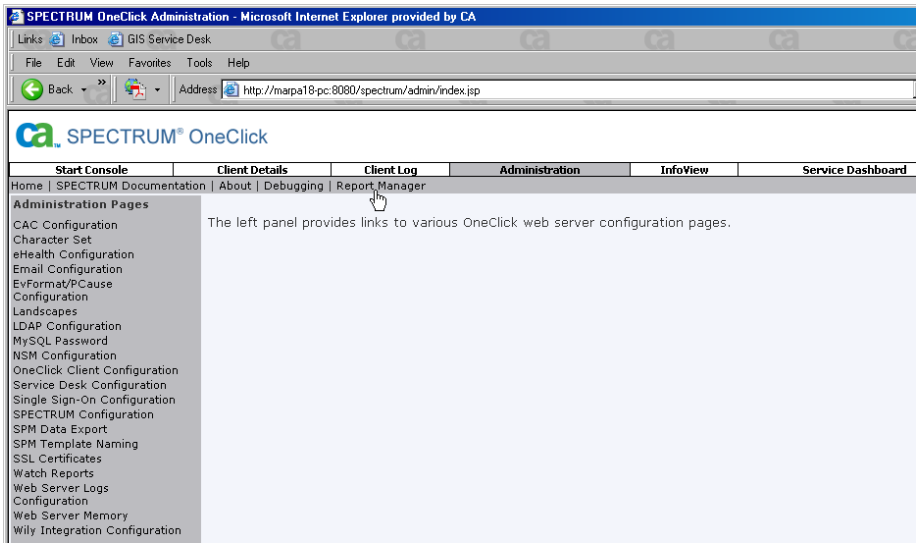
Access Administration Tools

The Report Manager Administration Tools are accessed from the OneClick web console. Users with OneClick administration rights have access to the Report Manager Administration tools.

Follow these steps:

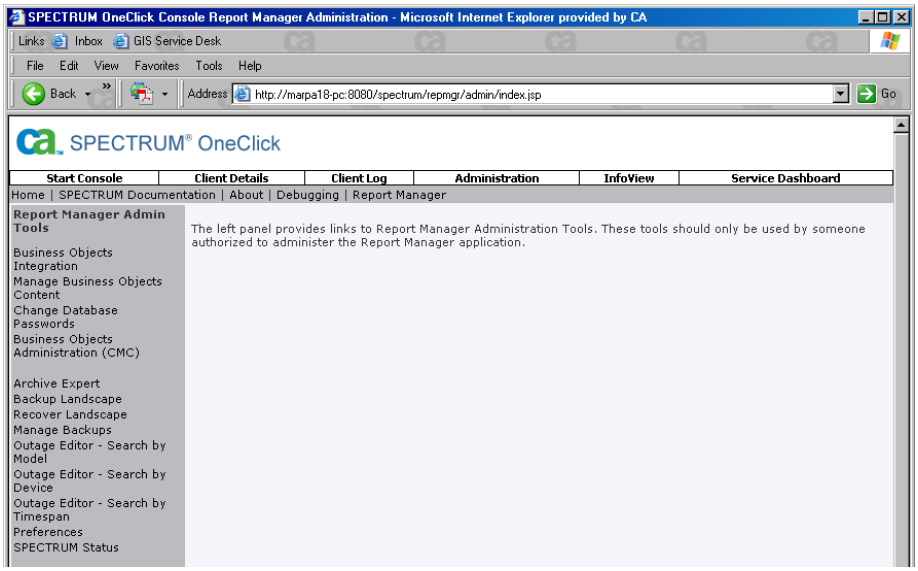
1. Access the OneClick home page.
2. From the OneClick menu bar, select the Administration tab.

   The Administration Pages panel appears on the left side.



3. From the Administration Pages menu bar, select Report Manager.

   The Report Manager Admin Tools panel appears on the left side.



Options on the Report Manager Admin Tools page are discussed in the order they appear on the panel.

Business Objects Integration

To activate or disable the integration between BOXI and Report Manager, provide connection information for CMC and InfoView.

If you disable an integration, reporting and report administration capabilities are disabled. However, disabling the integration does not cause Report Manager to stop collecting and managing data from the monitored SpectroSERVERs.

Follow these steps:

1. Access the Report Manager Admin Tools
2. Select the Business Objects Integration option.
3. Specify the following information:

   Same Server as CA Spectrum Report Manager

   Verify only if your BOXI instance is on the same server as CA Spectrum Tomcat.

   BO Server host name

   Specify the host name of your BOXI instance if it is not the same server as CA Spectrum Tomcat.

   BO Server CMS Port

   Specify the port upon which the BOXI Central Management Console server is running. Default is 6400.

   BO Admin User

   Specify the BOXI Admin User ID ('Administrator').

   BO Admin Password

   Fill in the password for the Admin User ID in BOXI.

   BO Authentication Type

   Specify the authentication type. The default of 'secEnterprise' is recommended.

   BO Tomcat Port

   Specify the port where BOXI Tomcat is running. The BO Tomcat port cannot be the same port that CA Spectrum Tomcat uses, if BOXI and OneClick are on the same server.

BO Integration

Verify Enabled or Disabled.

If Disabled is selected and saved, CA Spectrum Tomcat no longer connects or launches into the BOXI instance.

Single Sign-On with Business Objects InfoView - SSO Credentials

Specify the way that the OneClick home page attempt to use Single Sign-On to log in to Business Objects InfoView.

4. Click Test to ensure the parameters that you entered previously are valid.
5. If the Test option proves that the parameters are valid, click Save to enable the integration.

Important: This process can take a minute. Therefore, do not cancel or navigate from this page until you get a success message. During this process all the Report Manager report content is imported from the OneClick server into Business Objects.

Once the integration is configured, Report Manager report content is installed and can connect to the MySQL reporting database. The link for the 'Business Objects Administration (CMC)' and the menu-bar 'InfoView' link now launches the BOXI web applications on the BOXI instance that you specified.

Manage Business Objects Content

The Manage Business Objects Content option lets you update or remove the content that CA Spectrum installs on Business Objects. For example, you can perform the following management tasks:

- Update the CA Spectrum content on Business Objects to a newer version.
- Restore CA Spectrum content on Business Objects that was accidentally removed.
- Update the Business Objects host with which CA Spectrum integrates, if it has changed in the initial activation.

Important! Wait for the process to complete. Do not navigate away from the page or cancel the process.

You can update the content that Report Manager installs.The Business Objects integration must already be activated to update Report Manager content.

Follow these steps:

1. Access the Report Manager Admin Tools.
2. Select the Manage Business Objects Content option.

   The Manage Business Objects Content panel appears.

3. Click Update Content to update the existing content installed by CA Spectrum in Business Objects.

   Once complete, all Report Manager content is re-imported.

   Note: After *any upgrade* of OneClick with Report Manager, click the 'Update Content' button to ensure that the most recent reporting content is made available for use.

After deactivating the integration, Report Manager report content still exists on Business Objects. If you want to remove all content that is installed by Report Manager, do not remove the values that are specified previously for the Business Objects Integration (such as BO host name, BO Port), otherwise, CA Spectrum Tomcat cannot reconnect to this BOXI instance to remove the content.

You can remove Report Manager from Business Objects. Removing report content lets you continue to use Business Objects without integrating with CA Spectrum.

Follow these steps:

1. Access the Report Manager Admin Tools.
2. Select the Manage Business Objects Content option.

   The Manage Business Objects Content panel appears.
3. Click Remove Content.

   The existing content installed by CA Spectrum in Business Objects is removed.

Change Passwords

You can change the passwords of the database users who are accessing the CA Spectrum Reporting data from the Business Objects applications.

Follow these steps:

1. Navigate to the Report Manager Admin Tools.
2. Select the Change Database Passwords option.

   The Change Database Passwords panel appears.
3. Specify the following options:

   Select database password to change

   Crystal Reports User (CR_user) - for on demand reports

   WEBI Reports User (WEBI_user) - for ad hoc reports

   Default BOXI User Password (All Report Manager users)

   Current Password

   Specify the current password.

   Note: When you set the default BOXI user password for the first time, the Current Password is blank.

   New Password

   Specify the new password.

   Retype New Password

   Retype the new password for verification.
4. Click Change Password.

   All present and future Business Objects content installed by CA Spectrum is modified to use the new password.

Change the BOXI Administrator Password

The Central Management Console (CMC) offers a single interface. You can use CMC to perform a wide range of business objects administrative tasks such as user, content , and server management. CMC lets you publish, organize, and set security levels for all the BusinessObjects Enterprise content. For more information, see the *CA Business Objects Implementation Guide*.

Use CMC to change the BOXI Administrator password.

Note: By default, the BOXI Administrator password is blank unless it has been changed previously or explicitly set during the BOXI installation.

Important! The BOXI Administrator password enables any user who does not have a Report Manager user account to access all CA Spectrum Reporting features. We recommend that you save the password and limit its availability to authorized users.

Follow these steps:

1. Access the Report Manager Admin Tools
2. Select the Business Objects Administration (CMC) option.

   You are taken to CMC.

   For more information, see the *CA Business Objects Implementation Guide.*
3. Test the password by logging off and then logging on using the new password.

   Contact CA Support for assistance if you cannot log in using the new password.

Note: If a hostname is changed for a BOXI installed system, then you can update BOXI with the new hostname. Contact CA Support for assistance.

Configure Data Retention

The Report Data Retention functionality enables you to archive or purge the following high-growth types of report data: alarm, event, asset, availability, and SPM test result data.

You can specify a retention period in days for the data you want to keep available in the reporting database. Archive Expert provides table capacity and disk space consumption statistics for key, rapidly accumulating report data tables and suggests a retention period applicable to all database tables based on consumption trends.

It is critical to understand the difference between the archiving and purging options. Archiving moves the data out of the operational reporting database into a separate archival database. Purging removes the data altogether from the installation; therefore, ensure that any data you specify to purge is no longer needed.

The data you archive is not available for reports. If your organization users are not required to generate historical reports from a period before a particular point in time, you can safely use archiving to remove this data from the reporting database. For example, if you only want to generate reports from the last 90 days, you would specify a 90-day retention period. All data that is accumulated in the reporting database outside this 90-day window is automatically archived on a daily basis, unless you specified a data retention policy of purge.

By archiving or purging older data, you provide more room in the reporting database for current and more recent historical data. You can generate reports more quickly and can prevent problems that occur if the report database capacity is reached.

Enable archiving or purging if your organization requires historical report data only for the retention period you specify. Ensure that you understand your organization reporting requirements before you set a retention period. If you set it longer than required, you retain unnecessary data. Conversely, if you do not set it long enough, data that you want to view is unavailable. To save disk space, you can purge rather than archive reporting data.

Note: The *Deployment Capacity and Optimization Best Practices Guide* provides detailed sizing guidance for the Report Manager database.

Follow these steps:

1. Access the Report Manager Admin Tools.
2. Select the Archive Expert option.

   The Archive Expert panel is displayed.
3. Review the following field values.

   You can change the field values. For more information, see Preferences (see page 66).

   Data Retention Period (days) - Transformed Tables

   (Default = 90 days) Displays the retention period (in days) for transformed tables. 'Transformed tables' refers to all rapidly accumulating tables that contain information that is derived from events (for example, alarms, outages).

   The event table retention period is set independently. Data older than the retention period is archived at 12:30 AM daily.

   Note: Uncleared alarms and ongoing outages that fall within the retention period are not archived or purged. The alarm or outage data is archived or purged, if the alarm is cleared or the outage ends outside of the retention period (before the beginning of the retention period).

   Data Retention Policy

   - All Data — (Default) Retains all data in the SRM reporting database for reporting purposes. No archival or purging of SRM data occurs.
   - Archive — Moves data from the reporting database to the archival database.
   - Purge — Purges data older than the specified ‘retention period’. Data is permanently removed from the Report Manager database.

Data Retention Period (days) - Event Table

Displays the retention period for the event table specifically. This event table is one of the fastest growing tables, you can set the retention period individually.

For example, you can keep 60 days of event data, but 365 days (1 year) for the transformed tables data. The event retention period is much smaller than the transformed retention period because the event table grows much faster than the other tables.

Data Table Utilization Statistics

Archive Expert lists report data table utilization statistics for the high-growth types of report data that you select to archive. The statistics that are associated with the tables determine the recommended retention period. The tables provide you with at-a-glance indication of current utilization and capacity and trends for both. This information helps you make informed decisions about archiving. The following image is an example data capacity table:

EVENT Table	
Available Capacity (GB)	92.85
Current Size (GB)	< 10 MB
Average Daily Growth (MB)	0.03
History (Days)	1
Earliest Record Time	May 23, 2008 1:12:59 PM
Latest Record Time	May 23, 2008 1:18:38 PM
Days until Full	> 365

The following statistical definitions are presented within the EVENT Table:

Availability Capacity (GB)

The remaining capacity available for additional record storage. The capacity value is constrained by the MySQL table capacity or physical disk space available (whichever is smaller).

Current Size (GB)

Defines the current table size as reported by MySQL.

Average Daily Growth (MB)

Defines the 'Current Size (GB)' divided by 'History (Days)' converted to Megabytes.

History (Days)

Displays the number of days between the 'Earliest Record Time' and 'Latest Record Time' values.

Earliest Record Time

Displays the timestamp that is associated with the earliest record in table.

Latest Record Time

Displays the timestamp that is associated with the latest record in table.

Days until Full

Calculates the estimated number of days it takes to consume ‘Available Capacity (GB)’ given a straight-line growth estimate that is based on the ‘Current Size (GB)’ and ‘Average Daily Growth (MB)’.

Back Up Landscape

The Database Maintenance option lets you back up and restore landscape-specific data from the reporting database. Available backup lets you revert to an earlier version of the reporting database when a landscape server database backup is restored and you want to align reporting data with SpectroSERVER data. The Database Maintenance option enables you to manage the number of backups you want to retain by allowing you to remove the backup that you no longer require.

Important! The amount of data in the reporting database for all landscapes is dependent on the retention period (default = 90 days) specified by the Archive Expert option. Coordinate your database, and archive management settings to institute a data-storage and data-backup strategy that meets your data management requirements.

Follow these steps:

1. Access the Report Manager Admin Tools
2. Select the Backup Landscape option.

   The Backup Reporting Landscape panel appears.
3. Select a landscape from the 'Select a Landscape to Backup' drop-down list.
4. (Optional) Enter a description of the backup.
5. Click Start to begin the backup.

   Report Manager displays the backup progress and notifies you when it is complete. Date and time are used to identify each backup version.

Recover Landscape

When you recover landscape data, it replaces the current data for the landscape in the reporting database.

Note: If you attempt to recover an older version of the reporting database than the version currently in use, a warning message appears. The message recommends you to contact CA Support for more information.

Follow these steps:

1. Access the Report Manager Admin Tools.
2. Select the Recover Landscape option.

   The Recover Reporting Landscape panel appears.
3. Select the landscape to recover from the 'Select the Landscape to Recover' drop-down list.
4. Select the backup version to recover from the 'Select a Backup Database to Use' drop-down list.
5. Click Start to begin the restoration.

   CA Spectrum Reporting displays the recovery progress and notifies you when it is complete.

Manage Backups

You can update the descriptions for backups or remove backups you no longer require. Manage your backup files in the Admin Tools section.

Follow these steps:

1. Access the Report Manager Admin Tools.
2. Select the Manage Backups option.

   The Manage Landscape Backups panel appears.
3. Select the landscape for which you want to update or remove backups from the 'Select a Landscape' drop-down list.
4. Select the backups that you want to update or remove from the Existing Landscapes list.
5. (Optional) Modify the description text for backups if you want to update backups.
6. Click Update to save modifications, or click Remove to delete selected backups.

   The Backup files are managed.

Outage Editor

The Outage Editor lets you edit the outage records for all managed assets. You can retrieve outage records for particular models or for particular devices and interfaces, change the status of an outage in a record, annotate an outage record, and suspend an ongoing outage status for an asset that is available. Also, if you modify an asset outage that has caused an outage for a service model (because the asset is a service resource), you can modify the outage status for that service model.

Note: If Report Manager model-based security is enabled, the user who is logged on to OneClick can only review and edit outages that are associated with the models that this user can access. For more information, see the *CA Spectrum Report Manager User Guide*.

About Outages and Availability Reports

CA Spectrum Reporting calculates availability for managed assets by comparing their actual availability to their expected availability. Actual availability is derived from CA Spectrum event data. This comparison provides the basis for the availability percentage that is used in Reporting Availability Reports.

For any given time period, you specify an availability percentage objective when you configure an Availability Report, and CA Spectrum Reporting calculates the actual availability percentage. The difference between the two is the interval during which an asset is presumed to be unexpectedly unavailable. CA Spectrum Reporting does not include planned outages (downtime) from assets in *maintenance mode* when it calculates availability. For example, if a device is in maintenance mode, all the outages from that device are planned outages which are not considered in availability reports.

An unplanned outage can result from asset malfunction or from other events that are unrelated to asset performance. For example, availability is affected by a power outage, inadvertent shutdowns, or instances where an off-line asset model was not put in maintenance mode. Outages that are caused by the latter events misrepresent the actual availability of an asset. These are the types of outages you would typically want to redefine as exempt or planned outages.

Note: Report Manager does not support cluster-specific availability reports. Therefore, you cannot generate the Availability Reports for Clusters.

Outage Editing Status Report

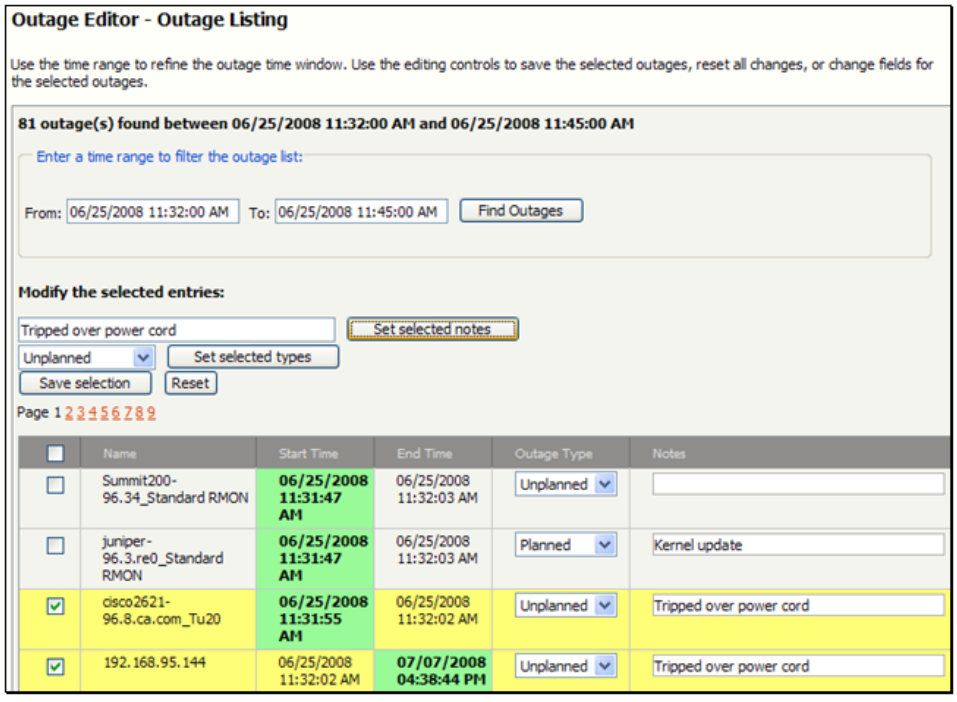
You receive an Outage Editing Status Report after editing the outage records. The results of an Outage Editor search list all outages that match your selection criteria. Each entry in the table contains the name of the model that experienced the outage, and notes, the outage start time, end time, and type. You can edit the outage type and notes. If no end time is available for an outage, it is listed as 'Ongoing' with an option to manually end the outage. Each entry in the table is preceded by a check box that lets you select the corresponding outage for mass editing.

In addition, the page contains *master controls* that annotate multiple outages simultaneously. Any outages that have been selected are modified by these controls. When changes have been made to any entry, 'Save selection' is enabled. Click it to save all selected entries. The 'Reset' button restores the listing to the state it was in after the most recent save.

If no outages are available in the selected period, only '0 Outage(s) Found' is displayed – the master controls and table do not appear.

If more than 500 outages are detected, the results are split up into 'pages'. Each page displays up to 500 outages and the master controls affect only the displayed outages.

The following image highlights the result of an 'Outage Editor - Search by Timespan' search. With multiple rows selected, it shows an example of mass editing. Selected entries are highlighted yellow, and times outside of the chosen range are highlighted green.



Modify Outage Records

The Outage Editor lets you modify Outage Records. When you edit an outage record, you can change its outage status and enter comments to it that describe why the record was edited or any other pertinent information. You can also end an ongoing outage status for a record that does not accurately indicate the actual availability of the asset referenced by the record.

Follow these steps:

1. Select Admin Tools, Outage Editor.

   Two options appear: Model Outages and Device/Interface Outages.

2. Select one of the options.

3. Enter a filter term to display the models or devices/interfaces that have had outages you want to view, and then click Find (Models or Devices). For example, to display a list of Cisco devices or interfaces or Cisco models that have had outages, simply enter Cisco.

   The editor displays a list of assets that match your filter term.

4. Select the asset whose outage records you want to retrieve.

   - If you are working with a model list and you want to edit outage records for a model, select the model.
   - If you are working with a device/interface list and you want to edit device outage records, select the device.
   - If you are working with a device/interface list and you want to edit outage records for a particular device interface, click Show Interfaces for the device. An interface list appears. It includes a filtering field that you can use to locate the interfaces you want to work with.

   At the bottom of the asset list, the Outage Editor indicates the number of outage records that it found for the selected asset. A date range filter lets you narrow the outage record list.

5. Accept the default date range, which extends to the current date from the date of the earliest outage known by Report Manager, or restrict the range as required, and then click Find Outages.

   The Outage Editor displays a list of outage records for the asset. An outage record indicates when an outage began and ended, the outage type, and any notes that have been entered to the record. Instead of indicating an end time, a record may indicate that an outage is ongoing (because Report Manager has not yet received an end outage event).

6. Update the records you want to change. You can change the outage status for particular records in their Outage Type fields or you can change the status for all listed outages in the Set all outage types to field. The following outage status types are available:

   Unplanned

   An unplanned outage is an unexpected outage. Availability reports designate time that an asset was in an unplanned outage state as time the asset was unavailable. Unplanned outages are typically the result of a hardware failure (broken cable) or software failure (bad configuration, incompatible protocols) or any situation where an asset is off-line while not in maintenance mode in CA Spectrum.

   Planned

   A planned outage is an outage that was intended, when an asset model in CA Spectrum was put into maintenance mode. CA Spectrum does not generate alarms on assets in maintain mode. Planned outages do not count against availability in Availability reports.

   For more information about maintenance mode, see the *Operator Guide*.

   Exempt

   An outage that evidence indicates was not unplanned, typically a situation where an asset that was taken off-line for maintenance but its model in CA Spectrum was not put into maintenance mode. You can designate any outage as exempt. Exempt outages do not count against availability.

   Note: If you change the status of an outage for an asset that is a resource of a service model and is also the cause of a service outage, the Affected Services Editor window appears. It lists the service outages that are caused by the asset outage enables you to change the status of the service outages. For more information, see the *CA Spectrum Service Manager User Guide*.

7. (Optional) You can (annotate outage records) add new notes or can overwrite existing ones for particular records in their Notes fields. You can also use the 'Set Selected Notes' field if you want to enter a note, edit a note, or clear notes from all records. When users generate Availability reports, they can specify Notes text as a filtering criterion.

8. (Optional) Click End Outage in the End Time field. You can end an ongoing outage immediately. For example, end an ongoing outage for an asset when you know that it is available and you do not require an availability report to misrepresent the asset availability.

9. Click Update to save your edits.

   The outage status is updated and saved.

Outage Editor - Search by Model

Outage Editor-Search by Model helps you to locate models for outage editing. Model name or model class is used to locate a model.

Follow these steps:

1. Access the Report Manager Admin Tools.
2. Select the 'Outage Editor - Search by Model' option.

   The Outage Editor - Model Listing panel appears.
3. Enter the Filter for a model name or model class.
4. Click Find Models.

   The model names with their outages are displayed for editing.

Outage Editor - Search by Device

Outage Editor-Search by Device is used to locate devices for outage editing with the device names.

Follow these steps:

1. Access the Report Manager Admin Tools.
2. Select the 'Outage Editor - Search by Device' option.

   The Outage Editor - Device Listing panel appears.
3. Enter the Filter to match the device names.
4. Click Find Devices.

   The device name with their outages is displayed for editing.

Outage Editor - Search by Timespan

Outage Editor - Search by Timespan displays any outage that begins before the selected end time and finishes after the selected start time.

Follow these steps:

1. Access the Report Manager Admin Tools.
2. Select the 'Outage Editor - Search by Timespan' option.

   The Outage Editor - Time Span Search panel appears.

3. Enter the time and date range filters in the From and To fields.

   Note: Leave the end time blank to search up to the current time.

4. Click Find Outages.

   The outages during the selected timespan are displayed for editing.

Set Report Manager Preferences

The Preferences option enables you to configure multiple Report Manager options.

Follow these steps:

1. Access the Report Manager Admin Tools.
2. Select the Preferences option.

   The Preferences panel appears.

3. Specify the following information:

   Data Retention Period (days) - Transformed Tables

   (Default = 90 days) Specifies the retention period by entering the number of days in the Retention Period (days) field. Archive Expert provides a suggested retention period estimate that is based on disk space consumption trends for the alarm, asset, availability, event, and SPM test result data tables.

   Data older than the retention period is archived at 12:30 AM daily.

   Note: Uncleared alarms and ongoing outages that fall within the retention period are neither archived nor purged. The alarm or outage data is archived or purged if the alarm is cleared or the outage ends outside of the retention period (for example, before the beginning of the retention period).

   Data Retention Policy

   - All Data — (Default) Retains all data in the Report Manager reporting database for reporting purposes. No archival or purging of Report Manager data occurs.
   - Archive — Moves data from the reporting database to the archival database.
   - Purge — Purges data older than the specified ‘retention period’. Data is permanently removed from the Report Manager database.

Monitor SRM using a Spectrum model

CA Spectrum creates a Report Manager Application model that is associated with the local VNM on the installation server when Report Manager is first started after installation. By default, the model serves as a destination for events and alarms that are generated by Report Manager. This means you can monitor the status of Report Manager from the OneClick Console. You can, however, select the destination for event and alarm information. If you disable monitoring, event information is written to the Tomcat log files.

Report Manager monitors its own status. It sends events to the Report Manager application model when the following indications occur:

- Report Manager loses and regains contact with a landscape, is not monitoring any landscapes, landscapes are added and removed from the list of monitored landscapes.
- Report Manager loses and regains contact with the CA Spectrum Archive Manager.
- Report Manager has an event processing failure and the event processing is resumed.

CA Spectrum generates (non-persistent) alarms for some of these events and clears them when they are rectified.

If the Report Manager Tomcat server is not connected to the model domain that contains the SRM Application model, events are sent to a log file.

OneClick server

This field represents the OneClick server URL used for model-based contextual report launches. For example, asset links within reports are launched to that model in OneClick. By default, the OneClick Console opens from the OneClick server installed with CA Spectrum Reporting. You can specify another server in the OneClick Server field.

CA Spectrum opens a default OneClick Console view when you click Start OneClick in the option menu. It also opens a OneClick Console topology view of an asset when you click an asset link in a report. By default, the OneClick Console opens from the OneClick server installed with CA Spectrum Reporting. You can specify another server in the OneClick Server field.

If you plan to access OneClick from a domain that is different from the domain in which the OneClick is located, enter the fully qualified server name. Enter the port number of the OneClick server you want to access *only* if the OneClick server was installed using a port number other than 80.

- If the port number HTTP default 80, enter:

  http://<*servername or fully qualified servername*>

- If the port number is not default 80, enter:

  http://<*servername or fully qualified servername*>:<*portnumber*>

Data Retention Period (days) - Event Table

Enter the retention period for the event table specifically. As this is one of the fastest growing tables, you can set this retention period individually. The data retention amounts are saved via Archive Expert.

Enable Security

Enables model-based security in the CA Spectrum Reporting environment. By default, security is not enabled. For more information, see the *Report Manager User Guide*.

4. Click Update Preferences to save preference settings.

   The Report Manager preference settings are saved.

Configure CA Spectrum Monitoring Status

The CA Spectrum Status option lists all SpectroSERVERs known by the OneClick Server to which Report Manager is connected. It indicates whether the servers are up (green) and Archive Managers are running (green). This option lets you select the SpectroSERVERs that Report Manager monitors according to your Report Manager license agreement and configures Report Manager polling options.

Important! Event processing is required for most reports. Turning off event processing results in reporting data not being updated, such as model creation/deletion, global collection membership updates, alarm information, outage information, and SPM test information. Reports that are generated for time periods after event processing has been turned off may not be accurate.

Follow these steps:

1. Access the Report Manager Admin Tools.
2. Select the CA Spectrum Status option.

   The CA Spectrum Status panel appears with the following fields displayed Landscape, SpectroSERVER Status, Archive Manager Status, and Last Event Field.

3. Select the following boxes:

   Monitor?

   Specifies that Report Manager actively collect data from the selected SpectroSERVER. If monitoring is disabled, reports are generated from historical data in the Report Manager database.

   Asset Polling?

   Specifies that Report Manager maintain daily polling of models on the SpectroSERVER for asset change data. This means that asset data in the Report Manager database is kept up to date. If asset polling is disabled, reports are generated from historical data in the Report Manager database.

Event Processing?

Specifies that Report Manager maintain hourly polling of the SpectroSERVER for event data. This means that event data in the Report Manager database is kept up to date. If event processing is disabled, event, availability, and alarm reports are generated from historical data in the Report Manager database.

4. Click Update Monitored Servers to assert your selections.

Note: If you select not to monitor a server, you can remove landscape data from the server that remains in the reporting database by running the RpmgrInitializeLandscape.bat utility. For more information, see Initialize the Database for Specific Landscapes (see page 101).

Chapter 5: Maintenance and Troubleshooting

This chapter describes the Report Manager maintenance procedures and troubleshooting issues and solutions.

This section contains the following topics:

General Application Maintenance Issues

This section describes typical issues with application maintenance for CA Spectrum Report Manager. The topics in this section provide the procedures to follow for customizing the application and resolving issues.

End Ongoing Outages

In some cases, Report Manager does not receive the event indicating that a given outage has ended, and thus the outage is incorrectly reported as ongoing. You can use the Outage Editor to end the ongoing outage.

Synchronize Report Data

If you reinitialize the SpectroSERVER database for a landscape that is reported by Report Manager, then you must reinitialize that landscape in the reporting database. Otherwise the data cannot be synchronized with the data in the SpectroSERVER.

No Tests Available in a Response Time Report

You can discover that no tests are available for the time period that you specify when configuring a Response Time report. At the same time, OneClick indicates that tests do exist for the time period from which you want to generate a report. This contradiction is caused by the circumstances under which the tests were discovered in CA Spectrum Service Performance Manager. For more information, see the *CA Spectrum Service Performance Manager User Guide*.

More Information

Initialize the Database for Specific Landscapes (see page 101)

Change the Report Logo

You can replace the default CA Spectrum logo on reports with another. The replacement logo must be a bitmap (.bmp) file with 200 pixels in width and 75 pixels in height.

Follow these steps:

1. Save the logo that you want to use to a location on the BOXI server file system. You can save the file to a location outside of the BOXI installation folders. Note the file path.
2. Navigate to the Report Manager Administration Tools page and select Preferences.
3. For the 'Custom report logo image file path' entry, set the file path from the BOXI server filesystem.
4. Click Update Preferences.
5. (Solaris/Linux only) Verify that the logo file has at least read permissions for owner, group, and other.

   The default logo.bmp file is replaced.

Change Vendor Names in Reports

You can change a vendor name in reports that is associated with a specific enterprise number in the Report Manager database. You can verify the following reasons to change a vendor name in Report Manager:

- Abbreviating a lengthy name.
- Renaming a vendor when the vendor name is changed.

Important! Verify that this change is performed on the OneClick Tomcat server, but not on the BOXI Tomcat server.

Follow these steps:

1. Shut down the Tomcat server.
2. Copy the vendor.xml file to the custom Report Manager configuration directory.

   ```
   cp
   <$SPECROOT>/tomcat/webapps/spectrum/WEB-INF/repmgr/config/vendor.xml
   <$SPECROOT>/custom/repmgr/config/vendor.xml
   ```

3. Edit the <*$SPECROOT*>/custom/repmgr/config/vendor.xml file.

   For each vendor name you want to change, create a <vendor></vendor> entry. In the <vendor_ID></vendor_ID> field, specify the vendor number in hexadecimal or decimal format, and the vendor name within the <vendor_name></vendor_name> field.

   For example, the following file format shows two vendor name changes:

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <root>
   <vendor>
   <!-- Changes the first vendor name -->
   <vendor_ID>Enterprise #</vendor_ID>
   <vendor_name>Some new name</vendor_name>
   </vendor>
   <vendor>
   <!-- Changes the second vendor name -->
   <vendor_ID>Enterprise #</vendor_ID>
   <vendor_name>Some new name</vendor_name>
   </vendor>
   </root>
   ```

   Definitions:

   - *Enterprise #* - The enterprise number for a vendor product that is referenced in the report.
   - *Some new name* - The new name that is associated with the enterprise number.

4. Save your changes.
5. Restart the Tomcat server.

   The vendor names are changed.

Change Event Names in Reports

You can supply custom names for events that appear in event reports. Overriding default event names lets you clarify specific items for event report recipients.

Follow these steps:

1. Shut down the Tomcat server.
2. Copy the eventtitle.xml file to the custom Report Manager configuration directory.
   ```
   cp
   <$SPECROOT>/tomcat/webapps/spectrum/WEB-INF/repmgr/config/eventtitle.xml
   <$SPECROOT>/custom/repmgr/config/eventtitle.xml
   ```
3. Edit the <*$SPECROOT*>/custom/repmgr/config/eventtitle.xml file.

   For each event name you want to change, create an <event></event> entry. Specify the event type code in hexadecimal or decimal format in the <event_type></event_type> field and the event name in the <event_title></event_title> field.
   ```
   <?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
   <root>
   <event>
   <!-- Identifies the event type code-->
   <event_type>An event type code</event_type>
   <!-- Specifies the custom event name-->
   <event_title>A custom event name</event_title>
   </event>
   </root>
   ```
4. Save your changes.
5. Restart the Tomcat server.

   The event name is changed.

Change Probable Cause Names in Reports

You can supply custom names for probable causes that appear in alarm reports. Overriding default probable cause names lets you clarify specific items for alarm report recipients.

Follow these steps:

1. Shut down the Tomcat server.
2. Copy the pcausetitle.xml file to the custom Report Manager configuration directory.
   ```
   cp
   <$SPECROOT>\tomcat\webapps\spectrum\WEB-INF\repmgr\config\pcausetitle.xml
   <$SPECROOT>\custom\repmgr\config\pcausetitle.xml
   ```
3. Edit the <*$SPECROOT*>\custom\repmgr\config\pcausetitle.xml file.

For each pcause name you want to change, create an <pcause></pcause> entry. Specify the pcause ID in the <pcause_type></pcause_type> field and the pcause name in the <pcause_title></pcause_title> field.

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<root>
<pcause>
<!-- Identifies the probable cause ID-->
<pcause_type>A pcause ID</pcause_type>
<!-- Specifies the custom probable cause name-->
<pcause_title>A custom pcause title</pcause_title>
</pcause>
</root>
```

4. Save your changes.
5. Restart the Tomcat server.

   The probable cause name is changed.

Change the OC_user MySQL Password

When CA Spectrum Reporting connects to the database, you can use a user ID and a password to authenticate against the database. In previous CA Spectrum releases, one password was used for authentication. However OneClick usernames are now used for background processing (OC_user and OC_admin) to add events and data in the database.

In addition, Crystal Report users need a CR_user password for on-demand reports. WEBI Report users need a WEBI_user for adhoc reports.

For more information, see Change Passwords (see page 54).

Analyze Table

Analyze Table is a command that can be executed on the MySQL command-line tool to update database statistics and improve the overall query performance. MySQL uses the table statistics to determine the order in which tables can be joined. In addition, table statistics can be used to select indexes to use for a specific table within a query.

If multiple modifications (such as INSERT or DELETE) are performed on a database table over time, the table statistics can become out of order. The MySQL Query optimizer which uses the table statistics can produce inefficient query execution plans and can cause MySQL performance degradation. Therefore, we recommend using Analyze Table to update table statistics.

The Analyze Table operation reads the entire database table and rebuilds the table statistics with the information about the distribution of key values. You can run this command on MyISAM and InnoDB tables. During the analysis, the table is locked with a read lock. When locked, the table cannot be accessed for other operations.

How to Run Analyze Table

To improve the performance of the database, run the Analyze Table command. You can run the Analyze Table on any of the following tables:

- event
- modeloutage
- model
- devicemodel
- alarminfo
- alarmactivity

Follow these steps:

1. From the OneClick menu bar, select the Administration tab.

   The Administration Pages panel appears on the left side.

2. From the Administration Pages menu bar, select Report Manager.

   The Report Manager Admin Tools panel appears on the left side.

3. Select Spectrum Status.

   The Spectrum Status page opens.

4. Clear all Monitor check boxes to stop all landscape monitoring.

5. Close all other reports (scheduled or on-demand) that are running.

6. Invoke a MySQL command prompt, and run the following command:

   ```
   ANALYZE TABLE table_name
   ```

   The task to run Analyze Table is complete.

Note: Before running Analyze Table stop event and asset polling. Set the data retention policy to 'all data' to disable the reporting database archiving. Restart event and asset polling after running the analyze table and set the data retention policy to its default value. For more information, see Configure CA Spectrum Monitoring Status (see page 68) and Set Report Manager Preferences (see page 66).

Define Events Types for Availability Processing

You can manage the volume and scope of outages to include in availability reports. You can specify the Report Manager availability handler determined events that indicate the beginning and end of planned and unplanned outages. You can designate events as UP, DOWN, IN MAINT MODE, and OUT OF MAINT MODE event types in the availability.xml file. You can override default event type designations and can assign types to new events. You can also specify that the availability handler ignores and does not process particular event types. A copy of the file is located in the following directory:

`<$SPECROOT>/tomcat/webapps/spectrum/WEB-INF/repmgr/config`

The availability.xml file is formatted as follows:

```
<root>
  <up_event></up_event>
  <down_event></down_event>
  <in_mm_event></in_mm_event>
  <out_mm_event></out_mm_event>
  <ignore></ignore>
</root>
```

You can designate an event as a particular type by entering the event code in decimal or hexadecimal format.

Follow these steps:

1. Make a copy of the availability.xml file.
2. Configure event designations using the tags included in the availability.xml file. All event type tags must be nested within the root tags.

   The following example shows that event 1111 and 5555 are designated as DOWN events, event 3333 is designated as an UP event, and 0xabcd is designated as an ignored event type.

   ```
   <root>
     <down_event>1111</down_event>
     <up_event>3333<up_event>
     <down_event>5555<down_event>
     <ignore>0xabcd</ignore>
   </root>
   ```
3. Save and copy the customized availability.xml file to the following directory:
   `<$SPECROOT>/custom/repmgr/config`

   The content of the file is written to the AvailabilityEvent database table and read by the availability handler when it compiles availability statistics for the availability reports.
4. Restart the OneClick Tomcat server to enable specified event designations.

More Information:

CA Spectrum Events Used by Report Manager (see page 107)

Filtering Event Processing

Event processing filters are defined by an XML file that can exclude certain events from being loaded into the Report Manager database. Specifically, events that are associated with the event types or model handles that are listed in the event-processing-filter.xml filter file are not loaded into the Report Manager database.

Before you modify the supplied event-processing-filter.xml file, you can determine the event types and model handles for which event activity can be excluded. Excluded events are not available in Report Manager for historical reporting purposes.

Follow these steps:

1. Copy the event-processing-filter.xml and event-processing-filter-schema.xsd files to the 'custom' directory. For example, see the following syntax:

```
cp
<$SPECROOT>/tomcat/webapps/spectrum/WEB-INF/repmgr/config/event-processing-filter-schema.xsd
<$SPECROOT>/custom/repmgr/config/
cp
<$SPECROOT>/tomcat/webapps/spectrum/WEB-INF/repmgr/config/events/event-processing-filter.xml
<$SPECROOT>/custom/repmgr/config/
```

2. Edit the event-processing-filter.xml to reflect your selected filtering strategy.

   For example, see the following syntax:

```
<ignore>
    <event-type>0x1245</event-type>
    <event-type>0xffa0004</event-type>
    <model>0x00d40010</model>
    <model>0xff0100d1</model>
</ignore>
```

   Note: You can only ignore events that are associated with specific models or event types.

3. Restart Tomcat.

   The specified event processing filters are now in effect.

Define Event Filters for Event Reports

Event filters are uniquely named sets of predefined event codes. When you configure an event report, you can select event types to include or exclude data in the report from events in a particular event filter.

An event filter is defined by an XML file that specifies the event codes. You can create new event filter files and can copy or modify the event filter files that are included with Report Manager. Before you create or modify event filters, determine the types of events that are important in your deployment.

Set Up Event Filtering

To set up event filtering, copy the XML schema and predefined configuration events file that are provided by Report Manager to the custom directory (*$SPECROOT/*custom/repmgr/config/events).

Follow these steps:

1. Copy the following schema file:

   ```
   cp
   $SPECROOT/tomcat/webapps/spectrum/WEB-INF/repmgr/config/events/event-filter.x
   sd
   $SPECROOT/custom/repmgr/config/events
   ```

2. Copy the following predefined configuration events file:

   ```
   cp
   $SPECROOT/tomcat/webapps/spectrum/WEB-INF/repmgr/config/events/event_filter_f
   ile.xml $SPECROOT/custom/repmgr/config/events
   ```

The possible values for the *event_filter_file* variable are as follows:

ADES-events-filter.xml

Contains the most significant Active Directory and Exchange Server (ADES) event codes to create a basic report.

ncm.xml

Specifies event codes for Network Configuration manager (NCM) activities in CA Spectrum.

vhm.xml

Contains the most significant Virtual Host Manager (VHM) event codes to create a basic report.

vhmtrap.xml

Contains a large list of all the potential Virtual Host Manager (VHM) traps to create a comprehensive report.

Cluster.xml

Contains all cluster events, including IBM and Microsoft.

IBM-Cluster-all.xml

Contains all of the IBM cluster events.

IBM-run-status.xml

Contains all of the IBM cluster events that are related to Status (such as up, down, offline).

MS-Cluster-all.xml

Contains all of the Microsoft cluster events.

MS-run-status.xml

Contains the Microsoft cluster events that are related to Status (such as up, down, offline).

ClusterTrap.xml

Contains only the trap events from IBM and Microsoft clusters.

Cluster-spectrum-managing.xml

Contains the CA Spectrum management events, such as cluster proxy events, management events, and polling events.

The files are copied to the custom directory and event filtering setup is complete.

Create an Event Filter File

You can create event filter files and can copy or modify the event filter files that are included with Report Manager.

Follow these steps:

1. Define an XML file that includes any number of event type codes in either hexadecimal or decimal format. For example, see the following filter format:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<filter xmlns="http://www.aprisma.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.aprisma.com ./event-filter.xsd">
<event_type>event type code</event_type>
<event_type>event type code</event_type>
</filter>
```

2. Save the file under a name that suggests the types of events to the custom directory. For example, see the following format:

   <$SPECROOT>/custom/repmgr/config/events

   An event filter file is created.

Exempt All Unplanned Outages for a Particular Day

You can use the exemptOutagesForDay command-line utility to exclude data from the Availability reports for all unplanned outages that have occurred on a non-working, or non-SLA day (for example, a holiday or a planned shutdown day). The utility also includes a parameter that lets you exempt any service outages that are caused by the device/interface outages. You can unexempt planned outages.

Note: You can exempt only those device/interface outages that have occurred for a single day and not a range of days. If you want to exempt outages for multiple days, you can run the utility for each day.

For more information, see How the Exempt Outage Utility Handles Particular Outage Scenarios (see page 83).

The utility is located in the /spectrum/bin directory.

Syntax:

```
exemptOutagesForDay <mysql username> <mysql password>
<exempt service outages> [-undo <YYYY-MM-DD>] YYYY-MM-DD day
```

Examples:

The following example exempts device/interface outages from January 1, 2006 and all service outages resulting from the device/interface outages:

```
exemptOutagesForDay root root yes 2006-01-01 New Year's Day
```

The following example exempts device/interface outages from January 1, 2006 but not service outages resulting from the device/interface outages:

```
exemptOutagesForDay root root no 2006-01-01 New Year's Day
```

The following example unexempts device/interface outages from January 1, 2006 and all service outages resulting from the device/interface outages:

```
exemptOutagesForDay root root yes -undo 2006-01-01 New Year's Day
```

The following example unexempts device/interface outages from January 1, 2006 but not service outages resulting from the device/interface outages:

```
exemptOutagesForDay root root no -undo 2006-01-01 New Year's Day
```

How the Exempt Outage Utility Handles Particular Outage Scenarios

Not all outages begin and end during the exempt period. The exemptOutagesForDay utility responds to outages that begin or end outside the exempt day period in various ways. You can verify the following outage scenarios that are handled by the exemptOutagesForDay utility:

- The outage begins before the exempt day and ends during it.

  The utility ends the existing outage at the start of the exempt day. A new exempt outage from the start of it to the end of the original outage is created.

- The outage begins before the exempt day and ends after it.

  The utility ends the existing outage at the start of the exempt day. A new exempt outage during the exempt day, and a new unplanned outage from the end of the exempt day to the end of the original outage is created.

- The outage begins during the exempt day and ends after it.

  The utility ends the existing outage at the end of the exempt day. The utility converts the outage to an exempt outage, and then creates a new unplanned outage from the end of the exempt day to the end of the original outage.

- The service outage begins before or during the exempt day and ends during or after it.

  The entire service outage is exempted.

Configure User-Defined Device Attribute Polling

The Report Manager historical device management feature polls devices for well-known attributes, such as device name and network address. However, you can pull more data from devices, such as vendor-specific data, or settings that are applicable to a business environment. Therefore, Report Manager enables you to tailor the device polling behavior.

Custom device polling is organized by model type, and then by attributes within the model type. The polling supports a maximum of ten additional attributes, in three attribute type areas. You can verify the following list for the attribute type and the associated CA Spectrum type mappings.

Type	Supported CA Spectrum Type Mapping	Maximum Number of Attributes (per type)
Varchar-based	All character-based and numeric types	4
Integer-based	Numeric, scalar types	4
Date/Time	Timestamp, time period types	2

Mapping Polled Attributes to Storage

If you are interested in storing the additional device attributes, you can determine the attributes to store. You can accomplish this task in the OneClick Attribute Editor view of a given device. Locate the desired attributes, and note the hexa-based attribute IDs (for example, 0x1006e) and the corresponding Type (for example, Integer, Text String).

You can select the attributes and can assign them to one of the open storage locations. The mapping occurs in an XML file, which is at:

```
<SPECROOT>/tomcat/webapps/
    spectrum/WEB-INF/repmgr/config/devicemodel-polling.xml
```

For a model type, each attribute id is mapped to a storage location. Consider the following example, for the model type 'Rtr_Cisco', that maps the attribute ID '0x118b8' to string storage location '1':

```
<devicemodel-polling …>
    <user-defined-poll modelType="Rtr_Cisco">
        <!-- Company name attribute -->
        <poll-attribute attrId="0x118b8">
            <varchar-storage id="1"/>
        </poll-attribute>
    </user-defined-poll>
</devicemodel-polling>
```

Next, consider the following example that maps several attributes, across several model types:

```
<devicemodel-polling …>
    <user-defined-poll modelType="Rtr_Cisco">
        <!-- Company name attribute -->
        <poll-attribute attrId="0x118b8">
            <varchar-storage id="1"/>
        </poll-attribute>
        <!-- Disposable precedence attribute -->
        <poll-attribute attrId="0x114e2">
            <int-storage id="4"/>
        </poll-attribute>
    </user-defined-poll>
    <user-defined-poll modelType="JuniperJUNOSRtr">
        <!-- Company name attribute -->
        <poll-attribute attrId="0x118b8">
            <varchar-storage id="2"/>
        </poll-attribute>
        <!-- Create time now attribute -->
        <poll-attribute attrId="0x11b41">
            <datetime-storage id="1"/>
        </poll-attribute>
    </user-defined-poll>
</devicemodel-polling>
```

In the previous example, two model types are configured for custom attribute polling. For 'Rtr_Cisco' devices, the company name attribute is stored at string storage '1' and the disposable precedence attribute is stored at long storage '4'. For 'JuniperJUNOSRtr' devices, the company name attribute is storage at string storage '2' (note the difference from the 'Rtr_Cisco' configuration) and the create time attribute is stored at date/time storage '1'.

A full example XML file can be found at:

```
<SPECROOT>/tomcat/webapps/
    spectrum/WEB-INF/repmgr/config/devicemodel-polling-example.xml
```

Reporting Labels

You can retrieve the attributes that are stored in the database, and can identify the attributes that are stored in 'varchar storage 1' for the 'Rtr_Cisco' model type. The reporting label lets you describe the purpose of an attribute and user-oriented interfaces.

The reporting label is configured in the following example:

```
<devicemodel-polling …>
    <user-defined-poll modelType="Rtr_Cisco">
        <!-- Company name attribute -->
        <poll-attribute attrId="0x118b8">
            <varchar-storage id="1"/>
            <reports label="Company Name" />
        </poll-attribute>
    </user-defined-poll>
</devicemodel-polling>
```

If you require to display the user-defined device attribute, the label text can be used to identify the attributes purpose.

Displaying Attributes in Reports

You can display the user-defined attributes as part of a Business Objects WEBI document using the CA Spectrum Universe. You can browse for subfolders that are prefixed with 'User Specified Device Attributes', while selecting result objects for the WEBI Document query.

For example, consider the following location:

Asset/Additional Device Information/User Specified Device Attributes – Asset.

For each polled attribute, the following objects and their source location are available in the folder:

- Attribute ID - configured in .xml file
- Label - configured in .xml file
- Value - polled from device

You can drag the desired result objects to the relevant WEBI panel to incorporate the objects into the query.

Polling Behavior:

When a device is polled, only the current user-defined polling configuration is applied. Therefore, if a configuration change is made, a device is polled again. The attributes and storage locations reflect the current configuration. Attributes of the devices that are polled before the configuration change and the old storage locations are cleared before storing the current attribute values.

Troubleshooting

This section describes problems that can occur with BOXI and Report Manager. You can follow the solutions provided to resolve the BOXI Installation and Operation errors.

BOXI Installation and Operation Errors

This section describes typical BOXI installation and operation errors. You can access the log files that are generated during BOXI installation and in many cases, you can troubleshoot the errors that you find there. For more information, see the *CA Business Intelligence Implementation Guide.*

Failed to Open the Connection Error

Symptom:

The following error message appears when you try to run a report after integrating the newly installed CABI with CA Spectrum:

```
Failed to open the connection
```

Solution:

You can encounter this issue if MySQL drivers are not set correctly in your system. To resolve the issue, take the following steps:

1. From the CABI installer, navigate to the patch folder, and copy the CA_NVM_EXE folder to any drive.

   For example, copy the patch folder from C:\cabi\Windows\Disk1\cabi\patch\CA_NVM_EXE to E:\ drive.

2. From the CLI window, run the following batch file:

   ```
   E:\CA_NVM_EXE\nvm_boxi_post_install_windows.exe
   ```

   nvm_post_install log files are created.

Note: Rewritable permissions are required before making any changes to the NVM_EXE folder and the mysql.jar file, which is at C:\Program Files (x86)\CA\SC\CommonReporting3\common/4.0/java/lib/external.

LDAP User Scheduled Reports Failed to Work

Symptom:

When I am logged in as an LDAP user, I am unable to view the Reports folder hierarchy in InfoView. In addition, reports that are scheduled by LDAP users are not working.

Solution:

This issue occurs if the cabi_default_groups.xml file of the CABI 3.3 installer does not contain the updated scripts.

Before upgrading CABI 3.2 to 3.3, update the cabi_default_groups.xml file and verify the updated information is available in the cabi_default_groups.xml file. Take the following steps to verify the updated content:

1. From the CABI 3.3 installer, navigate to the following path:

   `Disk1/cabi/content/`

2. Search for the following file:

   `cabi_default_groups.xml`

3. Verify for the following information in the .xml file:

   ```
   <?xml version="1.0"?>
   <biconfig version="1.0">
   </biconfig>
   ```

Segmentation Fault Installing BOXI R3.1 on Linux Running on AMD Chipset

Symptom:

During the BOXI R3.1 installation on Linux servers with AMD MultiCore Opteron processors, a segmentation fault occurs. The problem is due to the third-party library libWrapCryptoC, which creates the segmentation violation in this specific combination of AMD Opteron multicore CPU and SAP Business Objects.

Solution:

Take the following steps:

a. Download and extract wra00000.tar.gz file from ftp.ca.com under `/CAproducts/CABI/3.0/SAP_Note_1384092`.

b. In the installation media, replace pkg/wra00000.tar.gz with the file downloaded.

c. Verify that ownership and permissions match the other tar.gz files in this directory (for example, 755).

d. Launch the CABI install script to reinstall the product.

Windows Script Error

Symptom:

During the BOXI installation on Windows, the following error message appears several times:

```
Windows Script Host: There is no script engine for file extension ".js".
```

The BOXI installation requires access to a JavaScript engine. This problem is caused due to the following reasons:

- Windows does not have a program that is associated with the .js file extension.
- Microsoft Windows Script is not installed.

Solution:

Install the latest version of Microsoft Windows Script, which can be downloaded from Microsoft. Once the download is installed, you can reinstall BOXI.

Maximum Records Error (Windows)

Symptom:

The following message appears when you try to run a report:

```
Maximum processing time or maximum records limit reached.
```

Solution:

The BOXI record limit is set too low. After a first-time installation of BOXI, this value is defaults to 20,000.

To set the record limit to unlimited, perform the following steps:

1. Open CMC, and click Servers.
2. Find the server labeled 'Crystal Reports Processing Server' (formerly known as the Page Server).
3. Right click 'Crystal Reports Processing Server', and select Properties.
4. Find the field labeled 'Database Records Read When Previewing or Refreshing'.
5. Enter 0, and click Save and Close.
6. Right click the server and select Restart Server.

Note: This procedure temporarily prevents users from generating reports. Once the Processing Server restarts, report generation can resume.

SQL Server Memory Usage (Windows)

Symptom:

If you are still using Microsoft SQL Server as the CMS database server, you can observe that when the BOXI SQL server activity is low, its memory usage continues to increase on the host server. This behavior is considered normal and expected. Microsoft attributes this behavior to the SQL Server buffer pool, which is designed to release memory as it is required by other processes. For more information, see the *Microsoft Knowledge Base Article 321363*.

Solution:

Not applicable.

Reporting Troubleshooting Topics

This section describes the following reporting errors and the suggested solutions to fix these errors.

View the Modification of Custom Configuration Files (see page 90)

Missing Outage Data Error (see page 91)

Invalid Security Credentials Error (see page 91)

Reset Report Manager Application Model (see page 92)

Resolving Java Error in Report Manager Sample (WEBI) Reports (see page 92)

View the Modification History of Custom Configuration Files

Symptom:

You are interested in monitoring Report Manager customization changes that are made through the configuration files. These files are located under *$SPECROOT*/custom/repmgr/config.

Solution:

Log in to the MySQL client as 'root' and run the following command to see the chronology of changes for all of the custom configuration files:

```
SELECT filename, FROM_UNIXTIME(last_modified/1000) as time
FROM reporting.configchangelog
ORDER BY filename, time;
```

Missing Outage Data Error

Symptom:

CA Spectrum Reporting is missing outage data. The Tomcat log includes a message similar to the following message:
<$*SPECROOT*>\tomcat\logs\stdout.log:

```
Jul 29, 2009 10:00:34 AM - SRMAvailabilityHandler:

WARNING: Historical update has failed for domain = 0x400000 due to error =
Connection to event domain timed out.
```

Solution:

The outage data indicates one of the following situations:

- The CA Spectrum Archive Manager for the domain that is specified in the message is not running.
- A network connectivity issue between the OneClick web server and the Archive Manager on the domain that is specified in the message.

To resolve this issue, start the Archive Manager or resolve any network connectivity issues.

When Report Manager determines that the Archive Manager is running again, it automatically retrieves all of the historical availability event data that it requires to update the reporting database.

When Archive Manager is not running, the SpectroSERVER caches the event data. When the Archive Manager is running again, the SpectroSERVER sends it to the cached event data. However, the SpectroSERVER event cache is limited in size. If the Archive Manager is down for a prolonged period, event data can be lost. For more information, see the CA Spectrum *Database Management Guide*.

Invalid Security Credentials Error

Symptom:

The following message appears when you try to run a report:

```
An error occurred at the server: The Page Server cannot logon to the
CMS. This is due to invalid security credentials. Please verify your
user ID and password.
```

Solution:

The session has timed out. To resolve the issue, perform the following steps:

1. Exit Report Manager.
2. Re-establish the CA Spectrum Reporting session, and try running the report again.

Reset Report Manager Application Model

Symptom:

If the Main Location Server (MLS) is removed from a Distributed SpectroSERVER environment, Report Manager can no longer assert events on the SRMApplication model. As a result, monitoring of Report Manager status through the SRMApplication model cannot occur.

Solution:

Remove the model handle entry for the SRMApplication model from the registry table using the following MySQL command (logged on as 'root'):

```
mysql>USE reporting;
mysql>UPDATE registry SET SRM_Model = 0;
```

Resolving Java Error in Report Manager Sample (WEBI) Reports

Symptom:

A Java error is observed in the Report Manager Sample (WEBI) Reports. When a sample report is opened, following error message is displayed:
`Java has discovered application components that could indicate a security concern -- Block potentially unsafe components (recommended).`

If yes is selected, java blocks the result of the report from being displayed.

Solution:

This issue occurs when running the browser on Windows with versions higher than Java 6 Update 17. To resolve this issue, perform the following steps:

1. Open Java from Control Panel.
2. Select the Advanced Tab
3. Expand the Security option.
4. Expand the Mixed Code option.
5. Select 'Enable - hide warning and run with protections'.

This setting recovers the original format and allows you to use the most recent version of the JRE instead of rolling back to a previous version.

Commands for BOXI Management on Solaris/Linux

This section describes basic commands for managing BOXI servers and the BOXI-related MySQL daemon. You can issue commands from the *BOXI Install Directory/bobje directory*.

View BOXI-Related Processes

You can view the BOXI-related processes to verify the status of all processes. To view BOXI-related processes, use the following commands:

To view all processes:

```
ps -ef | grep bobje
```

To view all processes except MySQL processes:

```
ps -ef | grep bobje | grep -v mysql
```

Start and Stop BOXI Servers

In certain instances, you can start and stop the BOXI servers to fix the BOXI-related issues. The following commands can be used to start and stop all the BOXI-related servers.

To start all servers:

```
./startservers
```

To start a specific server, use CMC.

To stop all servers:

```
./stopservers
```

To stop a specific server, use CMC.

Start and Stop the BOXI-Related MySQL Daemon

You can start and stop mysql services related to BOXI. Use the following commands:

To start the MySQL daemon:

```
./mysqlstartup.sh
```

To stop the MySQL daemon:

```
./mysqlshutdown.sh
```

Start and Stop the BOXI-Related SQL Anywhere Daemon

You can start and stop the BOXI-related SQL Anywhere daemon while working on CA Spectrum reporting. Use the following commands:

To start the SQL Anywhere daemon:

```
./sawstartup.sh
```

To stop the SQL Anywhere daemon:

```
./sawstop.sh
```

Start and Stop BOXI Tomcat

When working on processes related to CA Spectrum reporting (for example, backup or restore reporting data), we recommend you to stop and start the BOXI Tomcat process. Use the following commands:

To start the Tomcat process:

```
./tomcatstartup.sh
```

To stop the Tomcat process:

```
./tomcatshutdown.sh
```

How to Manually Purge Reporting Data from the Reporting Database

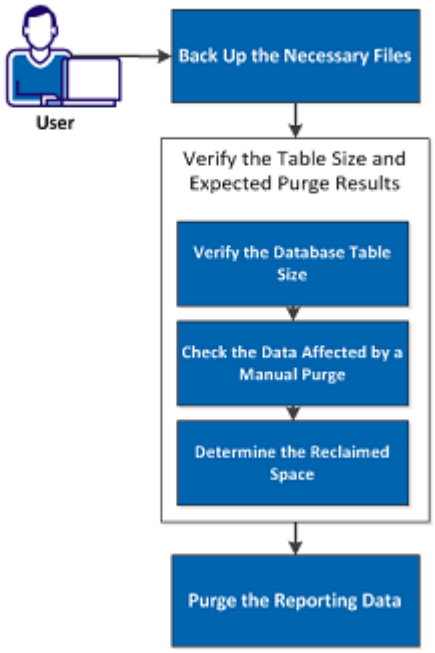
The performance of the database is affected when the tables in the reporting database grow too large. To improve database performance, you can purge the data manually from the reporting database. The following tables affect the database performance in the reporting database:

- modeloutage
- alarminfo
- alarmactivity
- spmbasictestresults
- spmhttpfulltestresults
- spmjittertestresults

Event Tables are also considered as major volume drivers in the reporting database. You can configure the data retention period that is available for Event Tables and can improve the database performance.

The following diagram illustrates the process to manually purge reporting data from the reporting database:

How to Manually Purge Reporting Data from the Reporting Database



Perform the following tasks to manually purge reporting data:

1. Back Up the Necessary Files (see page 95)
2. Verify the Table Size and Expected Purge Results (see page 96)
   - Verify the Database Table Size (see page 97)
   - Check the Data Affected by a Manual Purge (see page 98)
   - Determine the Reclaimed Space (see page 98)
3. Purge the Reporting Data (see page 99)

Back Up the Necessary Files

Back up the database or at least the tables that are affected before purging data from the existing database. MySQL database tables are stored as a set of files. You can back up the database using the following methods:

- Use the mysqldump utility, as described in Back Up CA Spectrum Reporting and Archive Data (see page 102).
- Create backup copies of selected files, as described in the following procedure.

Follow these steps:

1. Stop the Spectrum Tomcat service.
2. Stop the Spectrum MYSQL Database Server.
3. Stop the Archive Manager if it is running on this server.
4. Perform one of the following steps to copy the necessary files:
   - To back up the entire reporting database, copy the <*$SPECROOT*>/mysql/data/reporting directory to a newly named directory (for example, reporting_backup) within the <*$SPECROOT*>/mysql/data directory.

     Note: By creating the backup directory in this location you can easily switch between the reporting database and the reporting_backup database within the MySQL console window.
   - To back up only those tables that are purged, copy the following files from the <*$SPECROOT*>/mysql/data/reporting directory to a newly named directory (for example, reporting_backup) within the <*$SPECROOT*>/mysql/data directory:

     `alarmactivity.*`

     `alarminfo.*`

     `modeloutage.*`

     If you use SPM, copy the following files too:

     `spmbasictestresults.*`

     `spmhttpfulltestresults.*`

     `spmjittertestresults.*`

     Note: Typically, MySQL creates three different file types for each database table: .frm, .MYD, and .MYI. Copy all the three files. If these files are copied, renamed and stored within the reporting directory, then MySQL treats them as additional database tables.
5. Restart the CA Spectrum MySQL Database Server service.

   The file backup is complete.

Verify the Table Size and Expected Purge Results

You can evaluate the amount of data that is affected before you start purging the data. You can use a few SQL commands to examine the current volume and capacity of the tables.

Important! In the SQL sample syntax that we have provided, a value of "2007-04-01" (April 1st, 2007) is used as an example cutoff date. This sample syntax indicates that records that are created before this date are deleted. Substitute an appropriate date. However, once you have selected a date, use the same date across all tables to maintain the data integrity.

Take the following steps to verify the table size and expected purge results:

1. Verify the Database Table Size (see page 97)
2. Check the Data Affected by a Manual Purge (see page 98)
3. Determine the Reclaimed Space (see page 98)

Verify the Database Table Size

You can use the SHOW TABLE STATUS command to verify the size of a database table.

Follow these steps:

1. Open a command prompt, and execute the following command in <*$SPECROOT*>/mysql/bin:

   ```
   mysql -uroot -proot reporting
   ```

2. At the mysql> prompt, execute the following SQL commands:

   ```
   SHOW TABLE STATUS LIKE "modeloutage";
   ```

   ```
   SHOW TABLE STATUS LIKE "alarminfo";
   ```

   ```
   SHOW TABLE STATUS LIKE "alarmactivity";
   ```

   Table statistics appear.

3. Verify the following fields:
   - rows – the total number of rows
   - avg_row_length – average length (in bytes) of each row
   - data_length – current size (in bytes) of the table
   - max_data_length – maximum size (in bytes) that the table can grow to

4. If you are using SPM, execute the following commands:

   ```
   SHOW TABLE STATUS LIKE "spmbasictestresults";
   ```

   ```
   SHOW TABLE STATUS LIKE "spmjittertestresults";
   ```

   ```
   SHOW TABLE STATUS LIKE "spmhttpfulltestresults";
   ```

   Table size verification is complete.

Check the Data Affected by a Manual Purge

You can use the SELECT COUNT(*) command to find the number of rows that are affected by the data purge.

Follow these steps:

1. At the mysql> prompt, execute the following SQL commands:

```
SELECT COUNT(*) FROM modeloutage
WHERE end_time < "2007-04-01" AND outage_type > 0;
```

```
SELECT COUNT(*) FROM alarminfo
WHERE clear_time < "2007-04-01";
```

```
SELECT COUNT(*) FROM alarminfo, alarmactivity
WHERE alarminfo.alarm_key = alarmactivity.alarm_key
AND alarminfo.clear_time < "2007-04-01";
```

2. If you are using SPM, run the following commands:

```
SELECT COUNT(*) FROM spmbasictestresults
WHERE timestamp < "2007-04-01";
```

```
SELECT COUNT(*) FROM spmjittertestresults
WHERE timestamp < "2007-04-01";
```

```
SELECT COUNT(*) FROM spmhttpfulltestresults
WHERE timestamp < "2007-04-01";
```

The affected data identification is complete.

Determine the Reclaimed Space

You can use results from the SHOW TABLE STATUS and SELECT COUNT(*) statements in the previous procedures to find the amount of space that is freed after the purge.

Follow these steps:

1. Execute the following command to get the table size:

```
SHOW TABLE STATUS LIKE "modeloutage";
```

From the results, it is determined that the average row length (avg_row_length) is 121 bytes.

2. Execute the following command to find the number of rows that are affected:

```
SELECT COUNT(*) FROM modeloutage
WHERE end_time < "2007-04-01" AND outage_type > 0;
```

From the results, the count value is 4851.

3. Perform the following calculation to determine the amount of space that would be freed for this table:

   ```
   Avg_row_length * (number of rows Affected) = freed space
   121 bytes * 4851 = 586,971 bytes.
   ```

   The amount of space reclaimed is determined.

Note: After you delete the data, you can optimize the table to reclaim unused space.

Purge the Reporting Data

A series of DELETE commands are used to delete data. After data is deleted, it is important to optimize the tables to reclaim unused space.

Important! In the SQL sample syntax that we have provided, a value of "2007-04-01" (April 1st, 2007) is used as an example cutoff date. This sample syntax indicates that records that are created before this date are deleted. Substitute an appropriate date. However, once you have selected a date, use the same date across all tables to maintain the data integrity.

Follow these steps:

Important! The order in which the data is deleted must be strictly followed to avoid database corruption.

1. At the mysql> prompt, enter the following SQL commands:

   ```
   DELETE FROM modeloutage
     WHERE end_time < "2007-04-01" AND outage_type > 0;
   ```

   ```
   DELETE alarmactivity FROM alarmactivity, alarminfo
     WHERE alarminfo.alarm_key = alarmactivity.alarm_key
     AND alarminfo.clear_time < "2007-04-01";
   ```

   ```
   DELETE FROM alarminfo
     WHERE alarminfo.clear_time < "2007-04-01";
   ```

   Note: Execution time of these commands depends on the number of records that are effected.

2. If you are using SPM, run the following commands:

   ```
   DELETE FROM spmbasictestresults
     WHERE timestamp < "2007-04-01";
   ```

   ```
   DELETE FROM spmjittertestresults
     WHERE timestamp < "2007-04-01";
   ```

   ```
   DELETE FROM FROM spmhttpfulltestresults
     WHERE timestamp < "2007-04-01";
   ```

3. After the data is deleted, enter the following command to reclaim unused space:

   ```
   OPTIMIZE TABLE modeloutage, alarmactivity, alarminfo;
   ```

   Note: Execution time of this command depends on the size of the tables.

4. If you are using SPM, run the following command:

   ```
   OPTIMIZE TABLE spmbasictestresults, spmjittertestresults,
     spmhttpfulltestresults;
   ```

5. (optional) Run the following commands to verify space savings:

   ```
   SHOW TABLE STATUS LIKE "modeloutage";
   ```

   ```
   SHOW TABLE STATUS LIKE "alarminfo";
   ```

   ```
   SHOW TABLE STATUS LIKE "alarmactivity";
   ```

6. (optional) If you are using SPM, run the following commands:

   ```
   SHOW TABLE STATUS LIKE "spmbasictestresults";
   ```

   ```
   SHOW TABLE STATUS LIKE "spmjittertestresults";
   ```

   ```
   SHOW TABLE STATUS LIKE "spmhttpfulltestresults";
   ```

7. Restart Spectrum Tomcat service and Archive Manager (if previously stopped on this server).

   Data purging is complete.

Reporting Database Management

Report Manager uses a MySQL database named reporting to store data. As with any database, you can maintain this database to help it function efficiently. This section describes utilities and procedures that you can use to manage the reporting database.

This section includes the following topics:

Initialize the Database for Specific Landscapes

This section describes a utility that you can use to optimize and initialize the database for a specific landscape. Perform several actions before initializing the database.

Follow these steps:

1. Navigate to the /spectrum/bin directory.
2. Use the following default MySQL administrator login credentials:

   username:root

   password:root

   Note: Use a bash shell or command prompt to run the utility. Do not run it from a MySQL prompt.
3. Run the following command-line utility to remove all data for one or more or all landscapes from the reporting database:
   `RpmgrInitializeLandscape`

   Usage:
   `RpmgrInitializeLandscape` *`username password`*
   `-skipInitialHistory -initHist` *`# of days`* `-all`
   `landscape1 landscape2 ...`

   Definitions:

   - skipInitialHistory

   Report Manager does not retrieve or store events during event processing that have occurred before the utility is run. This flag overrides -initHist *# of days* if it is also included in the command line.

   - initHist *# of days*

   Report Manager processes initial historical events from the past number of days that are specified before the utility is run.

   - all

   Report Manager removes data for all landscapes in the reporting database.

   landscape1 landscapeN

   Report Manager removes data for each specified landscape.

Back Up CA Spectrum Reporting and Archive Data

Backing up reporting and archive data lets you maintain the reporting continuity. If you lose data (for example, during an upgrade installation), you can recover the data by restoring the backups.

Procedure for Windows

Follow these steps:

1. Select Control Panel, Administrative Tools, Services, and then Spectrum Tomcat.

   The Spectrum Tomcat Properties dialog opens.

2. Click Stop to stop Tomcat.
3. Navigate to the *$SPECROOT*/mysql/bin directory.
4. Using the mysqldump utility, back up the reporting and archive databases using this command:
   `mysqldump --routines --databases -uroot -proot reporting archive > backup_filename.sql`
5. Restart Tomcat and the CA Spectrum MySQL Database Server.

Procedure for Linux/Solaris

Follow these steps:

1. Stop processd to stop the Tomcat and MySQL processes.
   `$SPECROOT/lib/SDPM/processd.pl stop`
2. Navigate to the *$SPECROOT*/mysql/bin directory.
3. Using the mysqldump utility, back up the reporting and archive databases using this command:
   `mysqldump --defaults-file=../my-spectrum.cnf -uroot -proot --routines --database reporting archive > backup_filename.sql`
4. Restart processd to restart the Tomcat and MySQL processes:
   `$SPECROOT/lib/SDPM/processd.pl start`

   The reporting and archive data backup is complete.

Restore CA Spectrum Reporting and Archive Data

You can restore the reporting and archive data from a backup copy. Stop the Tomcat and MYSQL server before restoring the data from a backup copy.

Procedure for Windows

Follow these steps:

1. To stop Tomcat, select Control Panel, Administrative Tools, Services, Spectrum Tomcat, and click Stop in the Spectrum Tomcat Properties box.
2. To stop the Spectrum MYSQL database server, select Control Panel, Administrative Tools, Services, Spectrum MYSQL Database Server, and then click Stop in the Spectrum MYSQL Database Server Properties box.
3. Navigate to the *$SPECROOT*/mysql/bin directory.
4. Load the reporting and archive data from a backup copy using this command:

   `mysql -uroot –p root_pw reporting < backup_filename.sql`
5. Restart Tomcat and Spectrum MYSQL Database Server.

Procedure for Linux/Solaris

Follow these steps:

1. Stop processd to stop the Tomcat and MySQL processes.
   `$SPECROOT/lib/SDPM/processd.pl stop`
2. Navigate to the *$SPECROOT*/mysql/bin directory.
3. Load the reporting and archive data from a backup copy using this command:

   `mysql --defaults-file=../my-spectrum.cnf -uroot –p root_pw reporting < backup_filename.sql`
4. Restart processd to restart the Tomcat and MySQL processes:
   `$SPECROOT/lib/SDPM/processd.pl start`

   The reporting and archive data is restored from a backup copy.

Report Manager Utility Scripts

The Report Manager utility scripts are used to perform a specific task in the reporting database. For example, the backup utility gathers information that is specific to a landscape and dumps it into another database schema. Each database backup has an entry that is stored in its MySQL table for later reference.

The recovery utility initializes the landscape (using RpmgrInitializeLandscape) and copies all the table entries from the backup database into the current database.

Note: We recommend performing these operations when Tomcat is offline to avoid populating tables in the reporting database.

The following Report Manager utility scripts are commonly used in the reporting database:

BackupReportingDBLandscape

The BackupReportingDBLandscape utility script captures a landscape data to a backup database. Use the following format to execute this command:

`BackupReportingDBLandscape` *`user password domain name`* `[description]`

user

Indicates MySQL username.

password

Indicates MySQL password.

domain name

Indicates the SpectroSERVER domain name.

description

Describes the backup comments.

DisplayReportingDBBackups

The DisplayReportingDBBackups script displays the backups that exist on the system. You can use this script, if you are removing backups by database name from CLI.

Use the following format to execute this command:

`DisplayReportingDBBackups` *`mysql user password domain name`*

mysql user

Indicates MySQL username.

password

Indicates MySQL password.

domain name

Indicates the SpectroSERVER domain name.

exemptOutagesForDay

The ExemptOutagesForDay script converts unplanned outages to exempt outages when the outages coincide with an exemption period (for example, a bank Holiday).

Use the following format to execute this command:

exemptOutagesForDay *mysql username mysql password exempt service outages* [-undo *YYYY-MM-DD*] YYYY-MM-DD day

mysql username

Indicates MySQL username.

mysql password

Indicates MySQL password.

exempt service outages

Exempts the service outages.

Example:

exemptOutagesForDay user pass yes 2010-01-01 New Year\'s Day

RecoverReportingDBLandscape

The RecoverReportingDBLandscape script recovers a single landscape in the reporting database from a backup database.

Use the following format to execute this command:

RecoverReportingDBLandscape *user password backup database name*

user

Indicates MySQL username.

password

Indicates MySQL password.

backup database name

Indicates the name of the backup database.

RemoveReportingDBBackups

The RemoveReportingDBBackups script removes a backup database that is created for a landscape in Report Manager. Use the following format to execute this command:

`RemoveReportingDBBackups` *`user password backup database name`*

user

Indicates MySQL username.

password

Indicates MySQL password.

backup database name

Indicates the name of the backup database.

Appendix A: CA Spectrum Events Used by Report Manager

This appendix lists CA Spectrum events that Report Manager uses to start and stop calculating outage time for devices and interfaces. It also lists Service Performance Manager events.

This section contains the following topics:

Outage Events

This section lists events that mark the beginning and end of either a planned or unplanned model outage.

DOWN events indicate that an unplanned outage has begun.

- CONTACT LOST (0x10302)
- PORT BAD (0x10d11)
- PORT DISABLED (0x10d12)
- PORT UNREACHABLE (0x10d14)
- PORT LOWER LAYER DOWN (0x10d16)
- PORT CONNECTED TO DOWN PORT OR DEVICE (0x10d18)
- PORT BAD BUT CONNECTED TO WALINK EVENT (0x10d2d)
- PORT LOST (0x10d66)
- APPLICATION LOST (0x10d09)
- DEVICE UNRESPONSIVE (0x10d35)

UP events indicate that an unplanned outage has ended.

- CONTACT ESTABLISHED (0x10301)
- PORT GOOD (0x10d10)
- PORT REACTIVATED (0x10d66)
- PORT UP BUT LINKED WITH DOWN PORT (0x10d17)
- APPLICATION REACTIVATED (0x10d0b)
- DEVICE RESPONSIVE EVENT (0x10d30)

IN MAINT MODE events indicate that a planned outage has begun. If a model is in an unplanned outage state when the model is put into maintenance mode, the unplanned outage ends immediately.

- DEVICE INTO HIBERNATE (0x10226)
- DEVICE INTO MAINTENANCE (0x10222)
- PORT INTO MAINTENANCE (0x10224)

OUT OF MAINT MODE events indicate that a planned outage has ended.

- DEVICE OUT OF HIBERNATE (0x10227)
- DEVICE OUT OF MAINTENANCE (0x10223)
- PORT OUT OF MAINTENANCE (0x10225)

Additional events that are of interest to Availability reporting:

- VNM STARTED (0x10101)
- VNM STOPPED (0x10102)
- MODEL DESTROYED (0x10202)

Alarm Events

ALARM events are events that affect alarms.

- ALARM SET(0x10701)
- ALARM CLEARED (0x10702)
- USER CLEARED ALARM (0x10706)
- ALARM UPDATED (0x10707)
- SECONDARY ALARM SET EVENT (0x10714)
- SECONDARY ALARM CLEAR EVENT (0x10715)

Additional events that are of interest to Alarm reporting:

- VNM STARTED (0x10101)
- VNM STOPPED (0x10102)
- MODEL DESTROYED (0x10202)

Model Name Changes

Model name change events are used to update and track name changes for CA Spectrum models:

- MODEL NAME CHANGE (0x1a100)

Appendix B: CA Spectrum Reporting Application Model Events and Alarms

This appendix describes the events and alarms that you can monitor from the CA Spectrum Reporting Application model.

This section contains the following topics:

Application Events

CA Spectrum Reporting generates the following events on the CA Spectrum Reporting Application model:

- Report Manager is not monitoring any landscapes.

  Asserts alarm - Report Manager: NO LANDSCAPES MONITORED

- Landscape X has been added to Report Manager list of monitored landscapes.

  Clears alarm- Report Manager: NO LANDSCAPES MONITORED

- Landscape X has been removed from the Report Manager list of monitored landscapes.

  Clears alarms- Report Manager: LANDSCAPE CONTACT LOST and Report Manager: ARCHIVE MANAGER CONTACT LOST

- Report Manager has lost contact with the X landscape.

  Asserts alarm - Report Manager: LANDSCAPE CONTACT LOST

- Report Manager has regained contact with the X landscape.

  Clears alarm - Report Manager: LANDSCAPE CONTACT LOST

- Report Manager has lost contact with the X Archive Manager.

  Asserts alarm - Report Manager: ARCHIVE MANAGER CONTACT LOST

- Report Manager has regained contact with the X archive manager.

  Clears alarm - Report Manager: ARCHIVE MANAGER CONTACT LOST

- Report Manager has encountered an error while processing events. (for more information, see the *OneClick log file*)

  Asserts alarm - Report Manager: EVENT PROCESSING FAILURE

- The Report Manager server is stopping. Alarms that are based on landscape {S 1} are cleared and reasserted at startup, if needed.

  Clears alarms - Report Manager: LANDSCAPE CONTACT LOST and Report Manager: ARCHIVE MANAGER CONTACT LOST for each landscape that SRM is monitoring.

- The Report Manager server is stopping. Event processing failure alarms are cleared and reasserted at startup, if needed.

  Clears alarm - Report Manager: EVENT PROCESSING FAILURE

Application Alarms

CA Spectrum Reporting generates the following alarms from CA Spectrum Reporting Application model events:

- Report Manager: NO LANDSCAPES MONITORED, Alarm Severity - Yellow
- Report Manager: LANDSCAPE CONTACT LOST, Alarm Severity - Orange
- Report Manager: ARCHIVE MANAGER CONTACT LOST, Alarm Severity - Orange
- Report Manager: EVENT PROCESSING FAILURE, Alarm Severity - Red

Appendix C: CA Spectrum Attributes Used by CA Spectrum Reporting

This appendix lists CA Spectrum attributed that CA Spectrum Reporting uses in Asset, Availability, and Change Management reports. CA Spectrum Reporting polls CA Spectrum for these attribute values every 24 hours.

This section contains the following topics:

Device Attributes

0x1006e: MODEL_NAME_ATTR_ID

0x11ee8: MODEL_CLASS_ATTR_ID

0x11b41: CREATE_TIME_ATTR_ID

0x11026: MODEL_CREATOR_ATTR_ID

0x10001: MODEL_TYPE_ATTR_ID

0x10009: SECURITY_STRING_ATTR_ID

0x1027f: IP_ATTR_ID

0x110df: MAC_ATTR_ID

0x10030: SERIAL_NUMBER_ATTR_ID

0x10052: SYS_DESC_ATTR_ID

0x10053: SYS_OID_ATTR_ID

0x1102e: LOCATION_ATTR_ID

0x10b5a: CONTACT_PERSON_ATTR_ID

0x10245: SYS_UPTIME_ATTR_ID

0x23000e: DEVICE_TYPE

0x110ed:CONTACT_STATUS_ID

0x12a6d:NRM_LINE_CARD_DATA_ATTR_ID

Interface Attributes

0x1006e: MODEL_NAME_ATTR_ID

0x11ee8: MODEL_CLASS_ATTR_ID

0x11b41: CREATE_TIME_ATTR_ID

0x10001: MODEL_TYPE_ATTR_ID

0x10009: SECURITY_STRING_ATTR_ID

0x129ed: PORT_TYPE_ATTR_ID

0x129e0: PORT_DESC_ATTR_ID

0x11ee3: IF_SPEED_ATTR_ID

0x1027f: IP_ATTR_ID

0x10e43: PORT_IP_ATTR_ID

0x110df: MAC_ATTR_ID

0x10f1b: PORT_LINK_STATUS

0x12980: IF_LAST_CHANGE_ATTR_ID

0x10e41: IF_IN_OCTETS_ATTR_ID

0x11f82: IF_ALIAS

0x1006a: COMPONENT_OID

0x10000: MODEL_TYPE_NAME_ATTR_ID

User Defined Attributes

0x12bfb: USER_AssetTag

0x12bfc: USER_AssetID

0x12bfd: USER_AssetOwner

0x12bfe: USER_AssetOrganization

0x12bff: USER_AssetOffice

0x12c00: USER_AssetContractNumber

0x12c01: USER_AssetContractStartDate

0x12c02: USER_AssetContractEndDate

0x12c03: USER_AssetDescription

Appendix D: CA Spectrum Report Manager Database API (SRMDBAPI)

This section contains the following topics:

SRMDBAPI Overview

The CA Spectrum Report Manager Database API (SRMDBAPI) provides a fully documented set of read-only database objects to support your custom data analysis requirements. Specifically, the SRMDBAPI consists of a set of database views that are contained within a dedicated multidimensional schema in the MySQL instance that is used by Report Manager.

The SRMDBAPI contains the following basic content areas:

- Asset
- Alarm
- Outage/Availability
- Event

The following add-ons are part of the SRMDBAPI but require additional license purchase for usage:

- SPM
- NCM

Note: The SRMDBAPI is a read-only API. Data modification is not supported.

Design Methodology

The SRMDBAPI has been implemented using a multidimensional modeling approach. The multidimensional model is selected due to its inherently flexible design. This model is not driven by the requirements of a specific report or set of reports. Rather, the multidimensional schema is optimized for the analysis of facts (for example, event, outage) across any number of related dimensions (for example, model, time). The multidimensional model is ideally suited for reports. However, this particular schema design does not preclude you in extracting data from the supplied views into other repositories.

How to Establish Remote Access

At installation, the SRMDBAPI database objects are available to a pre-established 'srmapi' MySQL database user. If more user(s) require access to the dedicated API schema, you can establish them manually.

For more information, see How to Create Additional SRMDBAPI Users (see page 137)

Note: If you are connecting from a remote server using the 'srmapi' database user, additional grants need to be performed.

Follow these steps:

1. On the Report Manager server, log in to mysql as 'root'.
2. To provide remote access to the ‘srmapi’ database user, issue the following grants:

   ```
   mysql>GRANT SELECT, EXECUTE ON srmdbapi.* TO 'srmapi'@'%';

   mysql>GRANT SELECT ON reporting.* TO 'srmapi'@'%';

   mysql>FLUSH PRIVILEGES;
   ```

3. Logout of mysql.

   Remote Access is established.

Example Use Cases

The SRMDBAPI feature is enabled to provide access to mission critical Report Manager data. We published our SRMDBAPI to point your Business Intelligence (BI) tools to valuable CA Spectrum data. Some of the possible use cases are as follows:

- Query this critical data using the BI tool in which your company has already invested.
- Extract the Report Manager data and place it within another data repository.
- Incorporate Report Manager data into a separate CMDB or financial database.

Inventory of SRMDBAPI Views

Each view that is contained in the SRMDBAPI includes the data type and description.

Note: For the Key column, the following legend applies:

- UNQ - unique
- PK - primary key
- FK - foreign key

The following views are presented:

v_dim_alarm_condition

This view enumerates the various alarm conditions (for example, Minor, Major) and associated criticality values.

Field	Key	Type	Length	Description
condition_id	PK	int(unsigned)	10	Internal ID/Key that uniquely identifies a record in this view
condition_name		varchar	11	Condition Name
criticality	UNQ	tinyint	2	Criticality (1=Maintenance, 2=Minor, 3=Major, 4=Critical)

v_dim_alarm_title

This view enumerates the various alarm titles and associated probable causes that have occurred in the reporting database.

Field	Key	Type	Length	Description
alarm_title_id	PK	int(unsigned)	10	Internal ID/Key that uniquely identifies a record in this view
alarm_title		varchar	255	Alarm Title
pcause_id_hex		varchar	24	Probable Cause Code (hexadecimal form)
pcause_id_dec		int(unsigned)	10	Probable Cause Code (decimal form)
pcause_title		varchar	100	Probable Cause Title

v_dim_alarm_user

This view enumerates the various usernames that are associated with alarm activity captured in the reporting database.

Field	Key	Type	Length	Description
alarm_user_key	PK	int(unsigned)	10	Internal ID/Key that uniquely identifies a record in this view
alarm_user_name	UNQ	char	255	Username

v_dim_device_model

This view enumerates all devices (active and destroyed) that are captured historically in the reporting database.

Field	Key	Type	Length	Description
model_key	PK	int(unsigned)	10	Internal ID/Key that uniquely identifies a record in this view
model_h_dec		int(unsigned)	10	Model handle (decimal form)
model_h_hex		varchar	24	Model handle (hexadecimal form)
landscape_h_dec	FK	int(unsigned)	10	Landscape handle (decimal form); join to v_dim_landscape for additional landscape information.
landscape_h_hex		varchar	24	Landscape handle (hexadecimal form)
model_name		varchar	4000	Device Name
create_time		datetime		Creation Time
model_creator		varchar	255	Model Creator
security_string		varchar	255	Security String
destroy_time		datetime		Destroy Time
device_type		varchar	255	Device Type
ip		varchar	255	Network Address
mac		varchar	32	MAC Address
serial_nbr		varchar	255	Serial Number
sys_desc		varchar	255	System Descriptor
fw_rev		varchar	255	Firmware Version
sys_oid		varchar	255	System Object ID
location		varchar	255	Location
contact_person		varchar	255	Contact Person
last_reboot		datetime		Last reboot time
last_reboot_text		varchar	19	Last reboot time (text form)
last_successful_poll		datetime		Last successful poll time
model_destroyer		varchar	255	Model Destroyer
cust_asset_tag		varchar	255	Asset Tag

Field	Key	Type	Length	Description
cust_asset_id		varchar	255	Asset ID
cust_asset_owner		varchar	255	Asset Owner
cust_asset_organization		varchar	255	Asset Organization
cust_asset_office		varchar	255	Asset Office
cust_asset_contract number		varchar	255	Asset Contract Number
cust_asset_contract startdate		varchar	255	Asset Contract Start Date
cust_asset_contract enddate		varchar	255	Asset Contract End Date
cust_asset_description		varchar	255	Asset Description
sdm_host_address		varchar	255	SDM Host Address
mclass_name		varchar	32	Model Class Name
mtype_h_dec		int(unsigned)	10	Model Type Handle (decimal form)
mtype_h_hex		varchar	24	Model Type Handle (hexadecimal form)
mtype_name		varchar	128	Model Type
vendor_name		varchar	32	Vendor Name
topology_model_name_string		varchar	4000	Topology Model Name String; this field can be used to support container-based reporting capabilities.
varchar_1_attrid_hex		varchar	24	Custom Attribute ID (Varchar1)
varchar_2_attrid_hex		varchar	24	Custom Attribute ID (Varchar2)
varchar_3_attrid_hex		varchar	24	Custom Attribute ID (Varchar3)
varchar_4_attrid_hex		varchar	24	Custom Attribute ID (Varchar4)
integer_1_attrid_hex		varchar	24	Custom Attribute ID (Integer1)
integer_2_attrid_hex		varchar	24	Custom Attribute ID (Integer2)
integer_3_attrid_hex		varchar	24	Custom Attribute ID (Integer3)
integer_4_attrid_hex		varchar	24	Custom Attribute ID (Integer4)
datetime_1_attrid_hex		varchar	24	Custom Attribute ID (Datetime1)
datetime_2_attrid_hex		varchar	24	Custom Attribute ID (Datetime2)
varchar_1_label		varchar	255	Custom Attribute Label (Varchar1)

Field	Key	Type	Length	Description
varchar_2_label		varchar	255	Custom Attribute Label (Varchar2)
varchar_3_label		varchar	255	Custom Attribute Label (Varchar3)
varchar_4_label		varchar	255	Custom Attribute Label (Varchar4)
integer_1_label		varchar	255	Custom Attribute Label (Integer1)
integer_2_label		varchar	255	Custom Attribute Label (Integer2)
integer_3_label		varchar	255	Custom Attribute Label (Integer3)
integer_4_label		varchar	255	Custom Attribute Label (Integer4)
datetime_1_label		varchar	255	Custom Attribute Label (Datetime1)
datetime_2_label		varchar	255	Custom Attribute Label (Datetime2)
varchar_1_value		varchar	4000	Custom Attribute Value (Varchar1)
varchar_2_value		varchar	4000	Custom Attribute Value (Varchar2)
varchar_3_value		varchar	4000	Custom Attribute Value (Varchar3)
varchar_4_value		varchar	4000	Custom Attribute Value (Varchar4)
integer_1_value		bigint	20	Custom Attribute Value (Integer1)
integer_2_value		bigint	20	Custom Attribute Value (Integer2)
integer_3_value		bigint	20	Custom Attribute Value (Integer3)
integer_4_value		bigint	20	Custom Attribute Value (Integer4)
datetime_1_value		datetime		Custom Attribute Value (Datetime1)
datetime_2_value		datetime		Custom Attribute Value (Datetime2)

v_dim_device_module

This view enumerates more information at the slot level for chassis-based devices.

Field	Key	Type	Length	Description
module_id	PK	int(unsigned)	10	Internal ID/Key that uniquely identifies a record in this view
model_key	FK	int(unsigned)	10	Model Key associated with the parent device recorded in v_dim_device_model view; use this field to join to v_dim_device_model for additional device information.
module_index		int	10	Module Index (Slot)

Field	Key	Type	Length	Description
module_name		varchar	255	Module Name (Description)
serial_nbr		varchar	255	Serial Number
software_rev		varchar	255	Software Version

v_dim_event

This view enumerates all of the Event Types encountered while processing events for reporting purposes.

Field	Key	Type	Length	Description
type_dec	PK	int(unsigned)	10	Event Type (decimal form); this field also uniquely identifies a record in this view.
type_hex		varchar	24	Event Type (hexadecimal form)
title		varchar	255	Event Title

v_dim_event_creator

This view enumerates all the event creators that are encountered while processing events for reporting purposes.

Field	Key	Type	Length	Description
creator_id	PK	int(unsigned)	10	Internal ID/Key that uniquely identifies a record in this view
creator_name		varchar	255	Creator Name

v_dim_global_collection_member

This view enumerates all global collection members in the reporting database. You have a separate record for every global collection/model pairing.

Field	Key	Type	Length	Description
gc_rec_ID	PK	int(unsigned)	10	Internal ID/Key that uniquely identifies a record in this view
gc_name		varchar	255	Global Collection Name

Field	Key	Type	Length	Description
model_key	FK	int(unsigned)	10	Foreign key that uniquely identifies a member model. This field can be used to join to v_dim_model, v_dim_device_model, or v_dim_interface_model for additional member model information.

v_dim_interface_model

This view enumerates all interfaces captured in the reporting database.

Field	Key	Type	Length	Description
model_key	PK	int(unsigned)	10	Internal ID/Key that uniquely identifies a record in this view
model_h_dec		int(unsigned)	10	Model handle (decimal form)
model_h_hex		varchar	24	Model handle (hexadecimal form)
landscape_h_dec	FK	int(unsigned)	10	Landscape handle (decimal form) associated with this model; this field can be used to join to v_dim_landscape for additional landscape information.
landscape_h_hex		varchar	24	Landscape handle (hexadecimal form)
model_name		varchar	4000	Interface Name
create_time		datetime		Creation Time
security_string		varchar	255	Security String
destroy_time		datetime		Destroy Time
port_type		varchar	255	Port Type
port_desc		varchar	255	Port Description (raw value)
port_desc_text		longtext		Port Description (transformed value)
if_speed		Bigint (unsigned)	20	If Speed (Bytes/Sec)
ip		varchar	255	Network Address
mac		varchar	32	MAC Address
port_link_status		int(unsigned)	10	Port Link Status (raw value)

Field	Key	Type	Length	Description
port_link_status_text		varchar	32	Port Link Status (transformed value)
iflastchange		bigint (unsigned)	20	Last Change
ifinoctets		bigint (unsigned)	20	If In Octets
Datelastsignificant traffic		datetime		Date Last Significant Traffic
hours_idle		bigint	21	Hours Idle
days_idle		bigint	21	Days Idle
ifalias		varchar	4000	If Alias
component_oid		varchar	255	Component OID
device_model_key	FK	int(unsigned)	10	Foreign Key that uniquely identifies the parent device for this interface. Use this field to join to v_dim_device_model.model_key for additional, parent device information.
device_model_name		varchar	4000	Parent Device Name
port_status		varchar	32	Port Status
mclass_name		varchar	32	Model Class
mtype_h_dec		int(unsigned)	10	Model Type Handle (decimal form)
mtype_h_hex		varchar	24	Model Type Handle (hexadecimal form)
mtype_name		varchar	128	Model Type
connected_model_h_dec	FK	int(unsigned)	10	Model Handle of Connected Device (decimal form); this will be NULL if no device is connected. Use this field to join to v_dim_device_model.model_h for additional connected device information.
connected_model_h_hex		varchar	24	Model Handle of Connected Device (hexadecimal form); this will be NULL if no device is connected.
is_connected		int	1	1 indicates that there is a connected device, 0 indicates no connected device

Field	Key	Type	Length	Description
duplex_status		varchar	255	Duplex Status

v_dim_landscape

This view enumerates all of the landscapes that have been encountered during processing reporting data.

Field	Key	Type	Length	Description
landscape_h_dec	PK	int(unsigned)	10	Landscape handle (decimal form)
landscape_h_hex		varchar	24	Landscape handle (hexadecimal form)
landscape_name		varchar	255	Landscape(Domain) Name

v_dim_model

This view enumerates all of the models that are encountered in the course of processing reporting data.

Field	Key	Type	Length	Description
model_key	PK	int(unsigned)	10	Internal ID/Key that uniquely identifies a record in this view
model_h_dec		int(unsigned)	10	Model handle (decimal form)
model_h_hex		varchar	24	Model handle (hexadecimal form)
model_name		varchar	4000	Model Name
network_address		varchar	255	Network Address
landscape_h_dec	FK	int(unsigned)	10	Landscape Handle (decimal form); join to v_dim_landscape for additional landscape information.
landscape_h_hex		varchar	24	Landscape Handle (hexadecimal form)
mclass_name		varchar	32	Model Class
mtype_h_dec		int(unsigned)	10	Model Type Handle (decimal form)
mtype_h_hex		varchar	24	Model Type Handle (hexadecimal form)
mtype_name		varchar	128	Model Type Name

Field	Key	Type	Length	Description
security_string		varchar	255	Security String
destroy_time		datetime		Destroy Time (if applicable)

v_dim_ncm_event

This view enumerates all event codes that are associated with Network Configuration Management (NCM).

Field	Key	Type	Length	Description
type_dec	PK	int(unsigned)	10	Event Type (decimal form); this field also uniquely identifies a record in this view.
type_hex		varchar	22	Event Type (hexadecimal form)
title		varchar	255	Event Title

v_dim_spm_test

This view enumerates all the SPM Tests that are created in the course of processing.

Field	Key	Type	Length	Description
test_id	PK	int(unsigned)	11	Internal ID/Key that uniquely identifies a record in this view
test_name		varchar	64	SPM Test Name
model_key	FK	int(unsigned)	10	Internal Key that uniquely identifies the SPM Test Model in v_dim_model.
model_h_dec		int(unsigned)	10	Model Handle of the SPM Test Model (decimal form)
model_h_hex		varchar	24	Model Handle of the SPM Test Model (hexadecimal form)
model_name		varchar	255	Model Name of the SPM Test Model
source_address		varchar	64	Source Address
dest_address		varchar	255	Destination Address
port		mediumint (unsigned)	8	Port

Field	Key	Type	Length	Description
lookup_string		varchar	255	Lookup String
filename		varchar	255	Filename
packet_size		int	10	Packet Size
test_host_position		tinyint (unsigned)	3	Test Host Position
username		varchar	64	Username
proxy		varchar	255	Proxy
tos		int(unsigned)	10	Type of Service
alt_packet_addr		varchar	64	Alternate Packet Address
alt_packet_port		mediumint (unsigned)	8	Alternate Packet Port
landscape_h_dec	FK	int(unsigned)	10	Landscape Handle (decimal form); join to v_dim_landscape for additional landscape information.
landscape_h_hex		varchar	24	Landscape Handle (hexadecimal form)
effective_start		datetime		Effective start time of the test
effective_end		datetime		Effective end time of the test (if applicable)

v_dim_time

This view enumerates a separate record for every day in the calendar.

Field	Key	Type	Length	Description
time_id	PK	int(unsigned)	10	Internal ID/Key that uniquely identifies a record in this view
calendar_date	UNQ	date		Calendar Date
day_name		varchar	9	Day Name (e.g. Wednesday)
day_number_in_week		tinyint (unsigned)	3	Day Number in Week (Sunday=1, Saturday=7)
day_number_in_month		tinyint (unsigned)	3	Day Number in Month
day_number_in_year		smallint (unsigned)	5	Day Number in Year

Field	Key	Type	Length	Description
week_number_in_year		tinyint (unsigned)	3	Week Number in Year
month_name		varchar	9	Month Name (e.g. January)
month_number_in_year		tinyint (unsigned)	3	Month Number in Year (January = 1, December = 12)
year_number		smallint (unsigned)	5	Year Number
weekend_flag		char	1	Weekend Flag (Y, if Saturday or Sunday)
last_day_in_month_flag		char	1	Last Day in Month Flag (Y, if last day of month)

v_fact_alarm_activity

This view enumerates alarm activities (for example, sets, clears, acknowledgements) that are processed in reporting database.

Field	Key	Type	Length	Description
alarm_key		int(unsigned)	10	Internal ID/Key that uniquely identifies a record in this view
activity		int(unsigned)	10	Internal Code used to identify various activities (1=Set, 2=Ack, 3=Assigned By, 33=Assigned To, 4 or 5=Clear, 6=Ticketed)
activity_title		varchar	17	Activity Title (for example, Set, Acknowledged, and so on)
time		datetime		Time at which activity occurred
username_text		varchar	50	Username associated with activity
set_count		int	1	Set Count
ack_count		int	1	Acknowledgment Count
assign_by_count		int	1	Assign By Count
assign_to_count		int	1	Assign To Count
clear_count		int	1	Clear Count
ticketed_count		int	1	Ticketed Count
data		char	255	Additional details

v_fact_alarm_info

This view enumerates a separate record for every alarm that is processed in reporting database.

Field	Key	Type	Length	Description
alarm_key	PK	int(unsigned)	11	Internal ID/Key that uniquely identifies a record in this view
landscape_h_dec	FK	int(unsigned)	10	Landscape Handle (Decimal Form); join to v_dim_landscape for additional landscape information.
landscape_h_hex		varchar	24	Landscape Handle (Hexadecimal Form)
orig_event_key	FK	bigint (unsigned)	20	Originating Event Key; join to v_fact_event.event_key to capture additional event details.
condition_id	FK	int	11	Condition ID; join to v_dim_alarm_condition for additional condition information.
cause_id		int(unsigned)	10	Cause ID
set_time		datetime		Set Time
clear_time		datetime		Clear Time (if applicable)
duration_seconds		bigint	21	Duration in Seconds
duration_label		varchar	24	Duration Label (HH:MM:SS)
clear_user_key	FK	int(unsigned)	10	Uniquely identifies user who cleared this alarm; join to v_dim_alarm_user.alarm_user_key for more information.
alarm_title_id	FK	int(unsigned)	10	Uniquely identifies an alarm title; join to v_dim_alarm_title for more information.
model_key	FK	int(unsigned)	10	Uniquely identifies the model associated with this alarm; join to v_dim_model for more information.
ack_time		datetime		Acknowledgment Time
time_to_ack_seconds		bigint	21	Time to Acknowledge (Seconds)
time_to_ack_duration_ label		varchar	23	Time to Acknowledge (HH:MM:SS)

Field	Key	Type	Length	Description
ack_user_key	FK	int(unsigned)	10	Uniquely identifies the acknowledging user in v_dim_alarm_user; join to v_dim_alarm_user.alarm_user_key for more information.
first_assigned_time		datetime		Time at which alarm was first assigned
time_to_first_assign_ seconds		bigint	21	Difference in time between set time and time to first assignment (Seconds)
time_to_first_assign_ duration_label		varchar	23	Difference in time between set time and time to first assignment (HH:MM:SS)
first_assigned_user_key	FK	int(unsigned)	10	Uniquely identifies the first assigned user in v_dim_alarm_user; join to v_dim_alarm_user.alarm_user_key for more information.
first_assigning_user_ key	FK	int(unsigned)	10	Uniquely identifies the first assigning user in v_dim_alarm_user; join to v_dim_alarm_user.alarm_user_key for more information.
last_assigned_time		datetime		Time at which alarm was last assigned.
time_to_last_assign_ seconds		bigint	21	Difference in time between set time and time to last assignment (Seconds)
time_to_last_assign_ duration_label		varchar	23	Difference in time between set time and time to last assignment (HH:MM:SS)
last_assigned_user_key	FK	int(unsigned)	10	Uniquely identifies the last assigned user in v_dim_alarm_user; join to v_dim_alarm_user.alarm_user_key for more information.
last_assigning_user_key	FK	int(unsigned)	10	Uniquely identifies the last assigning user in v_dim_alarm_user; join to v_dim_alarm_user.alarm_user_key for more information.
set_troubleticket_time		datetime		Troubleticket Time

Field	Key	Type	Length	Description
time_to_trouble_ticket_ seconds		bigint	21	Difference in time between set time and trouble ticket time (Seconds)
time_to_trouble_ticket_ duration_label		varchar	23	Difference in time between set time and trouble ticket time (HH:MM:SS)
set_troubleticket_user_ key	FK	int(unsigned)	10	Uniquely identifies the trouble ticket user in v_dim_alarm_user; join to v_dim_alarm_user.alarm_user_key for more information.
set_troubleticket_id		char	255	Trouble Ticket ID
assignment_duration_ seconds		bigint	21	Difference in time between last assigned time and clear time (Seconds)
assignment_duration_ label		varchar	24	Difference in time between last assigned time and clear time (HH:MM:SS)

v_fact_event

This view enumerates every event record that is processed in the reporting database.

Field	Key	Type	Length	Description
event_key	PK	bigint (unsigned)	20	Internal ID/Key that uniquely identifies a record in this view
landscape_h_dec	FK	int(unsigned)	10	Uniquely identifies a landscape associated with the model on which this event occurred (decimal form); join to v_dim_landscape for additional landscape information.
landscape_h_hex		varchar	24	Uniquely identifies a landscape associated with the model on which this event occurred (hexadecimal form)
model_key	FK	int(unsigned)	10	Uniquely identifies the model associated with this event; join to v_dim_model for more information.
time		datetime		Time at which event occurred.

Field	Key	Type	Length	Description
type_dec	FK	int(unsigned)	10	Event Type (decimal form); join to v_dim_event for more information.
type_hex		varchar	24	Event Type (hexadecimal form)
creator_id	FK	int(unsigned)	10	Uniquely identifies the creator for this event; join to v_dim_creator for more information.
event_msg		text		Fully constituted event message associated with this event.

v_fact_model_outage

This view enumerates all outages that are processed in reporting database.

Field	Key	Type	Length	Description
model_outage_id	PK	bigint (unsigned)	20	Internal ID/Key that uniquely identifies a record in this view
model_key	FK	int(unsigned)	10	Uniquely identifies the model associated with this outage; join to v_dim_model for more information.
landscape_h_dec	FK	int(unsigned)	10	Uniquely identifies a landscape associated with the model on which this event occurred (decimal form)
landscape_h_hex		varchar	24	Uniquely identifies a landscape associated with the model on which this event occurred (hexadecimal form)
start_time		datetime		Start Time of Outage
end_time		datetime		End Time of Outage (if applicable)
duration_seconds		bigint	21	Outage Duration (seconds)
duration_label		varchar	24	Outage Duration (HH:MM:SS)
start_event_key	FK	bigint (unsigned)	20	Uniquely identifies the event that started this outage; join to v_fact_event on event_key for more information.

Field	Key	Type	Length	Description
end_event_key	FK	bigint (unsigned)	20	Uniquely identifies the event that ended this outage; join to v_fact_event on event_key for more information.
notes		char	250	Outage Notes
outage_type		int(unsigned)	10	Outage Type (0=Initial, 1=Unplanned, 2=Planned, 3=Exempt)
outage_desc		varchar	NO	Outage Description

v_fact_spm_basic_test_results

This view enumerates test results for the following Service Performance Manager (SPM) test types: ICMP Ping, UDP, Path Echo, TCP, DNS Lookup, POP3, DHCP, FTP, SMTP, and HTTP (total time only).

Field	Key	Type	Length	Description
test_id	PK	int(unsigned)	11	Combination of Test ID and Timestamp uniquely identifies a record in this view. Timestamp corresponds with time at which result occurred.
timestamp		datetime		
time_id	FK	int(unsigned)	11	Uniquely identifies a day in v_dim_time; join to v_dim_time for more information.
hh		tinyint (unsigned)	3	Hours field of "timestamp" field.
mm		tinyint (unsigned)	3	Minutes field of "timestamp" field.
ss		tinyint (unsigned)	3	Seconds field of "timestamp" field.
latency		int(unsigned)	10	Latency in milliseconds
packet_loss		double	53,29	Packet Loss
timeout		tinyint	2	1=timeout occurred, 0=no timeout occurred

v_fact_spm_http_full_test_results

This view enumerates historical results that are associated with Service Performance Manager (SPM) HTTP tests.

Field	Key	Type	Length	Description
test_id	PK	int(unsigned)	11	Combination of Test ID and Timestamp uniquely identifies a record in this view. Timestamp corresponds with time at which result occurred.
timestamp		datetime		
time_id	FK	int(unsigned)	11	Uniquely identifies a day in v_dim_time; join to v_dim_time for more information.
hh		tinyint (unsigned)	3	Hours field of "timestamp" field.
mm		tinyint (unsigned)	3	Minutes field of "timestamp" field.
ss		tinyint (unsigned)	3	Seconds field of "timestamp" field.
http_response_time		int(unsigned)	10	Overall HTTP response time
dns_resolution_time		int(unsigned)	10	Portion of HTTP response time for DNS resolution
tcp_connect_time		int(unsigned)	10	Portion of HTTP response time for TCP connection
http_download_time		int(unsigned)	10	Portion of HTTP response time for HTTP Download
timeout		tinyint(2)	2	1=timeout occurred, 0=no timeout occurred

v_fact_spm_jitter_test_results

This view enumerates historical results that are associated with Service Performance Manager (SPM) Jitter tests.

Field	Key	Type	Length	Description
test_id	PK	int(unsigned)	11	Combination of Test ID and

Field	Key	Type	Length	Description
timestamp		datetime		Timestamp uniquely identifies a record in this view. Timestamp corresponds with time at which result occurred.
time_id	FK	int(unsigned)	11	Uniquely identifies a day in v_dim_time; join to v_dim_time for more information.
hh		tinyint (unsigned)	4	Hours field of "timestamp" field.
mm		tinyint (unsigned)	4	Minutes field of "timestamp" field.
ss		tinyint (unsigned)	4	Seconds field of "timestamp" field.
response_time		int(unsigned)	10	Latency
src_to_dest_pl		double	53,29	Source to Destination Packet Loss
dest_to_src_pl		double	53,29	Destination to Source Packet Loss
mia		double	53,29	Missing in Action – Packet Loss with Unknown Direction
late_arrival		double	53,29	Late Arrival
busies		double	53,29	Busies
pos_src_to_dest_jitter		int(unsigned)	10	Positive Source to Destination Jitter
neg_src_to_dest_jitter		int(unsigned)	10	Negative Source to Destination Jitter
pos_dest_to_src_jitter		int(unsigned)	10	Positive Destination to Source Jitter
neg_dest_to_src_jitter		int(unsigned)	10	Negative Destination to Source Jitter
timeout		tinyint	2	1=timeout occurred, 0=no timeout occurred

How to Create Additional SRMDBAPI Users

Administration is not required if the 'srmapi' MySQL user is used to interact with the SRMDBAPI. However, if more accounts are required, you can establish them using the MySQL client application.

For example, you can create a user, srmdbapi_user, with a capability to read all view data from the SRMDBAPI.

Follow these steps:

1. On the SRM server, log in to mysql as 'root'.

2. Establish the new username and password combination in the MySQL database instance and access to both the srmdbapi and reporting schemas:
   ```
   mysql>GRANT SELECT, EXECUTE ON srmdbapi.* TO 'srmdbapi_user'@'%' IDENTIFIED BY 'somepassword';
   mysql>GRANT SELECT ON reporting.* TO 'srmdbapi_user'@'%';
   mysql>FLUSH PRIVILEGES;
   ```
3. Logout of mysql.

   srmdbapi_user is created.

Note: The previous 'GRANT' statements lets 'srmdbapi_user' connect to the SRM server from the local or any remote server. The 'srmdbapi_user' only have read-only access to the 'srmdbapi' schema which represents the database implementation of the SRMDBAPI.

How to Access Views

The primary way to access the reporting data in the MySQL database is using the MySQL client. For more information, see http://dev.mysql.com.

For important login information, the user ID is 'srmdbapi' and the password is 'srmdbapi'.

Procedure for Windows

Follow these steps:

1. Log in with a password.
2. Access the following directory:
   ```
   C:\win32app\spectrum\mysql\bin
   ```
3. Enter the following command:
   ```
   mysql -usrmapi -psrmapi srmdbapi
   ```
   You are now connected to the MySQL for Windows.

Procedure for Linux/Solaris MySQL

Follow these steps:

1. Log in with the password, root.
2. Enter 'bash'.
3. Access the following directory:
   ```
   cd/usr/spectrum/mysql/bin
   ```

4. Enter the following command:
   `./mysql --defaults-file=../my-spectrum.cnf -usrmapi -psrmapi srmdbapi`

   You are now connected to the MySQL for Solaris.

5. To show SRMDBAPI view names on both Windows and Linux/Solaris MySQL client, type the following command at the MySQL prompt:
   `show tables;`

   The SRMDBAPI table/view names are displayed.

6. To display column names for a given SRMDBAPI view on both Windows and Linux/Solaris MySQL client, type the following command at the MySQL prompt:
   `desc 'xxx';`

   Where 'xxx' is the table name.

   The columns in each table/view are displayed.

Example

Here is an example with the 'v_dim_alarm_condition' table.

You would type the following command at the mysql prompt:

```
mysql> desc v_dim_alarm_condition;
```

MySQL displays the following table:

```
+----------------+------------------+------+-----+---------+-------+
| Field          | Type             | Null | Key | Default | Extra |
+----------------+------------------+------+-----+---------+-------+
| condition_id   | int(10) unsigned | NO   |     | NULL    |       |
| condition_name | varchar(11)      | NO   |     | NULL    |       |
| criticality    | tinyint(2)       | NO   |     | NULL    |       |
+----------------+------------------+------+-----+---------+-------+
Three rows in a set (0.00 seconds)
```

Sample SRMDBAPI Queries

The following sample SQL queries are presented to both demonstrate the potential of the SRMDBAPI and serve as a training aid. These queries merely represent a subset of what is possible from a functional perspective.

Note: Each query contains a 'LIMIT X' records clause to ensure that too much data is not initially returned to the MySQL client.

Log in to MySQL Server

You can log in to the MySQL server using the 'srmapi' user before executing the following sample queries:

On Linux/Solaris:

```
$SPECROOT/mysql/bin/mysql --defaults-file=../my-spectrum.cnf -usrmapi -psrmapi
srmdbapi
```

On Windows:

```
$SPECROOT/mysql/bin -usrmapi -psrmapi srmdbapi
```

Get All 'model created' and 'model destroyed' Events on a Specified Day

You can perform a query to obtain all 'model created' and 'model destroyed' events that occurred on a specified day (2009-12-29). The result set contains event time, model name, event title, and the event message.

```
mysql>SELECT e.time,
           m.model_name,
           de.title,
           e.event_msg
FROM v_fact_event e,
           v_dim_model m,
           v_dim_event de
WHERE e.model_key = m.model_key
AND e.type_dec = de.type_dec
AND e.type_dec IN ( 66049,66050 )
AND e.time BETWEEN '2009-12-29 00:00:00' AND '2009-12-29 23:59:59'
LIMIT 10;
```

Note: '66049' and '66050' are the decimal values that correspond with 'model created' and 'model destroyed' events.

Get All 'device create' and 'device destroy' Events on a Specified Day

You can perform a query to obtain all 'device create' and 'device destroy' events that occurred on a specified day (in this example, we use 2009-12-29). This query is similar to the previous one; however, v_dim_model are replaced with v_dim_device_model to ensure that only device-related events are returned.

```
mysql>SELECT e.time,
            d.model_name,
            de.title,
            e.event_msg
FROM v_fact_event e,
            v_dim_device_model d,
            v_dim_event de
WHERE e.model_key = d.model_key
AND e.type_dec = de.type_dec
AND e.type_dec IN ( 66049,66050 )
AND e.time BETWEEN '2009-12-29 00:00:00' AND '2009-12-29 23:59:59'
LIMIT 10;
```

Get All 'device create' and 'device destroy' Events on a Specified Day in a Global Collection

You can perform a query to obtain all device create and destroy events that occurred on a specified day (2009-12-29) for devices that are contained in a particular global collection. This query is similar to the previous one; however, the v_dim_global_collection_member view has been added and joined to the v_dim_device_model view. In addition, the query constrains results to the collection name of your choosing.

```
mysql>SELECT e.time,
           d.model_name,
           de.title,
           e.event_msg
FROM v_fact_event e,
           v_dim_device_model d,
           v_dim_event de,
           v_dim_global_collection_member gcm
WHERE e.model_key = d.model_key
AND e.type_dec = de.type_dec
AND d.model_key = gcm.model_key
AND gcm.gc_name = 'Your Collection Name'
AND e.type_dec IN ( 66049,66050 )
AND e.time BETWEEN '2009-12-29 00:00:00' AND '2009-12-29 23:59:59'
LIMIT 10;
```

Get the List of Top 20 Events on a Specific Day

You can perform a query to obtain the list of top 20 (most frequent) events that occurred on a specified day (2009-12-29). This query considers all models (not simply devices).

```
mysql>SELECT de.title,
              COUNT(1) as event_count
FROM v_fact_event e,
          v_dim_event de
WHERE e.type_dec = de.type_dec
AND e.time BETWEEN '2009-12-29 00:00:00' AND '2009-12-29 23:59:59'
GROUP BY de.title
ORDER BY event_count DESC
LIMIT 20;
```

Sample SRMDBAPI Data Extraction to Flatfile

This process illustrates how to execute a query and extract the associated result set to a flatfile. Once data has been extracted to a flat file, it can be reviewed in any text viewing client (for example, vi, notepad). The following sequence generates a text file named 'top_20_events_20091229.out' containing the results from the query that is outlined in the previous section. The .out file is placed in $SPECROOT/mysql/bin by default.

```
mysql>\T top_20_events_20091229.out

mysql>SELECT de.title,
            COUNT(1) as event_count
FROM v_fact_event e,
            v_dim_event de
WHERE e.type_dec = de.type_dec
AND e.time BETWEEN '2009-12-29 00:00:00' AND '2009-12-29 23:59:59'
GROUP BY de.title
ORDER BY event_count DESC
LIMIT 20;

mysql>\t
```

Create an ODBC Datasource for the SRMDBAPI

This section illustrates the process to set up an SRMDBAPI ODBC datasource through the ODBC Datasource Administrator. Once the SRMDBAPI ODBC datasource is created, the applications such as Microsoft Excel can use ODBC datasource to query the database directly without using the MySQL client.

Follow these steps:

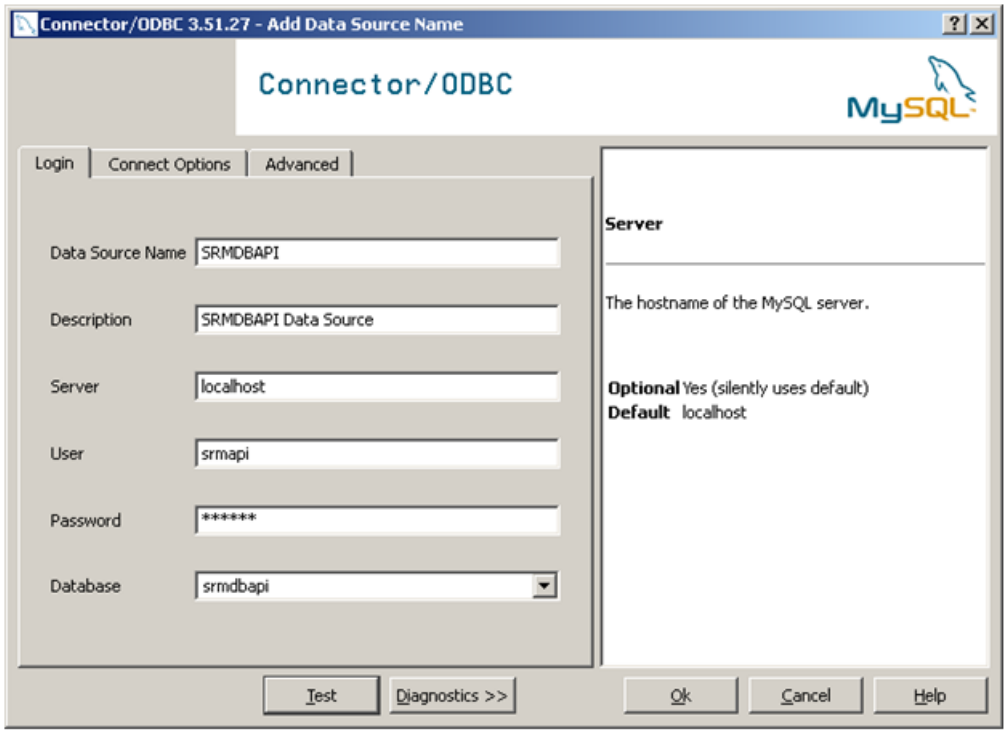
1. Navigate to the Windows Control Panel.

   Note: This path varies depending on the version of Windows that is installed.

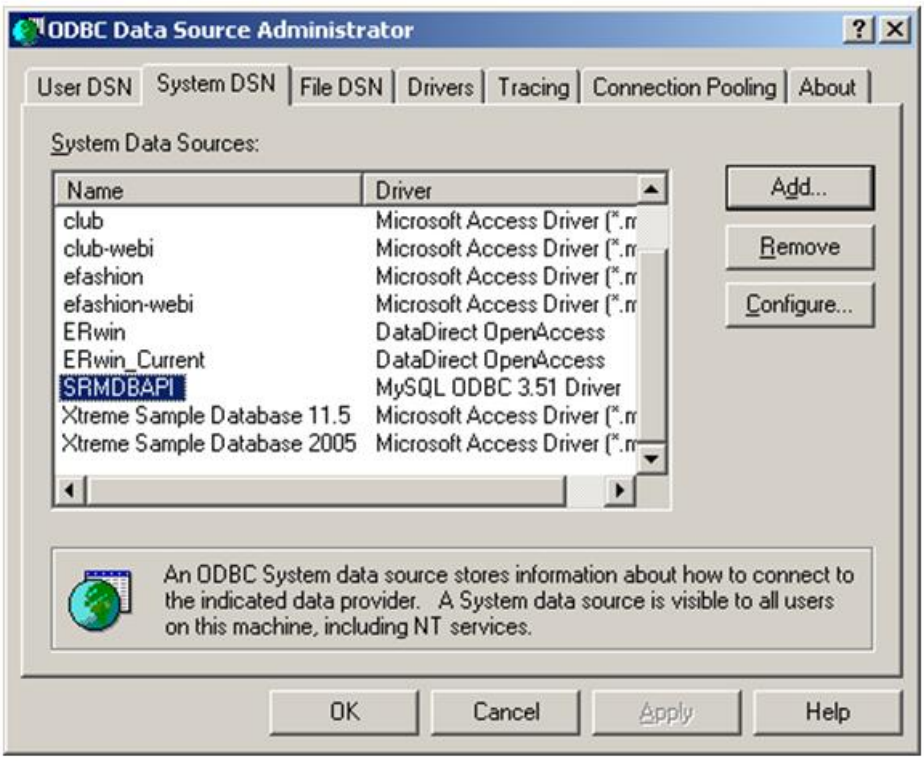
2. Double-click 'Administrative Tools'.
3. Double-click 'Datasource (ODBC)'.
4. Click 'System DSN' tab.
5. To add a System Data Source, click the Add button.
6. Select the 'MySQL ODBC 3.51 Driver'.

Important! If MySQL ODBC 3.51 driver is not available in the picklist, download and install the 'MySQL ODBC 3.51 Driver' directly from MySQL. The driver can be acquired at: http://dev.mysql.com.

7. Configure the new SRMDBAPI Data Source by specifying the following information in the Login tab.



8. To verify the connectivity, click Test.
9. After verifying the connectivity, click OK to create the data source.
10. Verify that the SRMDBAPI Data Source appears on the System DSN tab.



Setup is completed and the Data Source is now available to client applications such as Microsoft Excel.

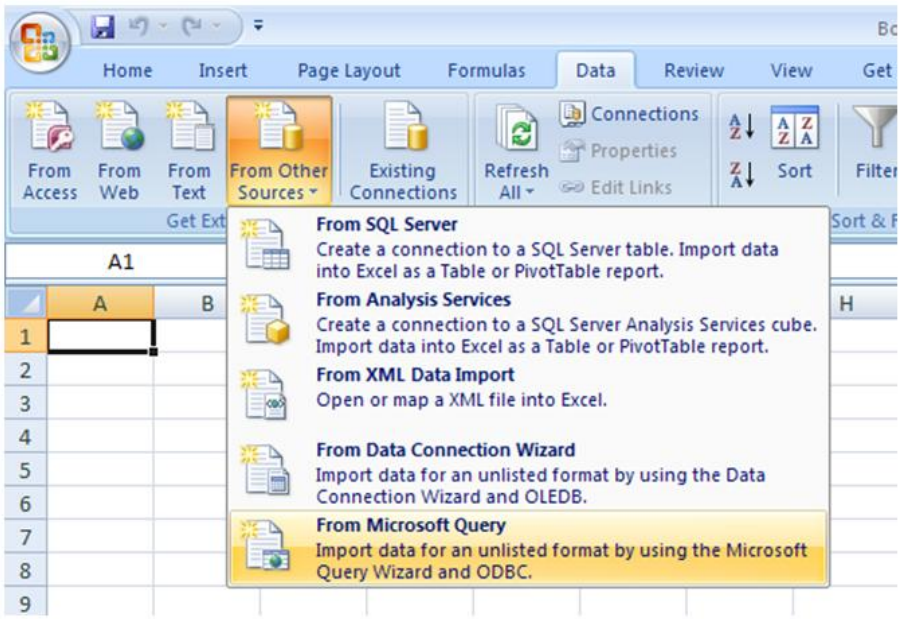
Create a Sample Query that Uses the ODBC Data Source

You can use Excel 2007 and the embedded Microsoft Query application to create a sample query. You can generate a sample query against the SRMDBAPI database and then return the associated result set into an Excel spreadsheet. Excel 2007 uses ODBC data source to query the database directly without using the MySQL client.

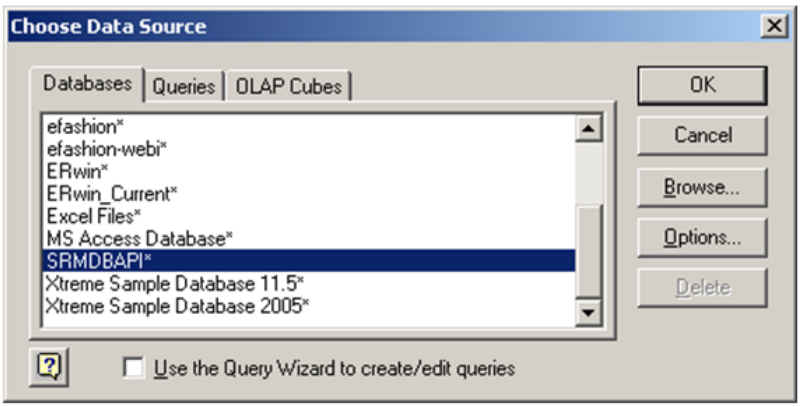
Follow these steps:

1. Launch Excel 2007.
2. Click the Data tab in the menu structure.

3. Click the From Other Sources icon, and select the From Microsoft Query option from the resulting drop-down list.



4. From the Databases tab, select the SRMDBAPI* database, clear the 'Use the Query Wizard to create/edit queries' check box, and click OK.



Microsoft Query launches immediately and prompts you for the tables to report on.

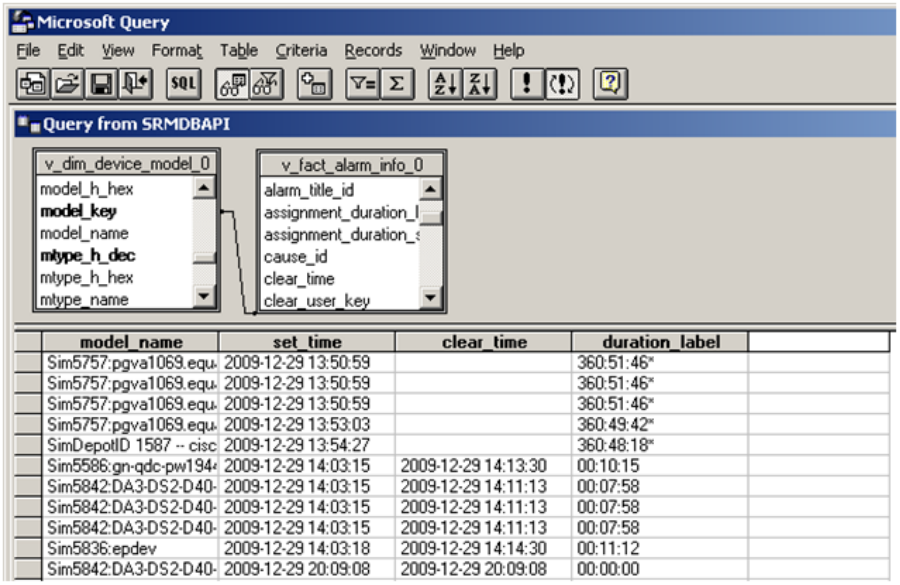
For this example, select and add both the v_dim_device_model and v_fact_alarm_info views to make them available for querying.

Note: Microsoft automatically joins the two views on the model_key column ,which is correct.

5. Double-click the 'model_name' column from the 'v_dim_device_model' view to add this field to the query.

6. Double-click the 'set_time', 'clear_time', and 'duration_label' columns from the 'v_fact_alarm_info' view to add these fields to the query.

   The following image illustrates the Microsoft Query environment:



7. Select Add Criteria from the Criteria option in the menu structure.

   The Add Criteria dialog opens.

8. Select 'v_fact_alarm_info_0.clear_time' for the Field and 'is Null' for the Operator value.

9. Click Add to ensure that the query only displays ongoing alarms.

10. Execute the query by clicking  in the menu bar.

11. Return the result set to Excel by selecting the file 'Return Data to Microsoft Office Excel' in the menu bar.

    The Import Data dialog provides options for incorporating the results into the Excel spreadsheet.

    For this example, select Table; however, other options are available, such as Pivot Table Report and Pivot Chart.

12. Select Existing worksheet to include data in the current worksheet.

    The results of your query are captured in an Excel table.

Because results are formatted for Excel, you can take advantage of other capabilities in the application such as charting, pivot tables, and conditional formatting to analyze the data.

SRMDBAPI Potential Issues and Best Practices

The following guidelines helps you to use SRMDBAPI successfully:

- Run an explain plan first before executing your actual query. Determine the approximate number of rows returned.
- When developing queries, you can provide a 'LIMIT X' records clause in your SQL code to ensure that only few records are returned.
- Qualify your queries as much as possible. Most often, you can supply a time frame to restrict result set sizes.
- When qualifying queries, try to restrict to fields that are indexed.
- Join as few tables as possible to satisfy your data requirements; join operations are typically expensive operations.
- Limit sorting unless indexes are available to support such an operation.
- Limit data grouping unless indexes are available to support such an operation.

Appendix E: Report Manager Debugging

This appendix provides information that is used when debugging Report Manager.

This section contains the following topics:

Debug Options

The following options are available on the Debug Controller page, which you can access from the OneClick home page by clicking the following options: Administration, Debugging, Web Server Debug Page (Runtime).

Important! Only use debugging tools with assistance from CA Support.

For more information, see the CA Spectrum *Administrator Guide*.

To enable an option, select ON. See the following CA Spectrum tomcat logs for detailed information:

- For Windows: <*$SPECROOT*>/tomcat/logs/stdout.log
- For Linux or Solaris: <*$SPECROOT*>/tomcat/logs/catalina.out

The following debug options are available for Report Manager:

SRM - BOXI - Content Installer

Logs in BIAR file import operations to the BOXI server. If you encounter any issues while updating the Report Manager content, then enable this option on the BOXI server.

SRM - Core - Asset Manager

Helps in troubleshooting Report Manager device information event processing. Enable this option when new devices are not found in the reporting database or if the deleted device information is not reflected in the reporting database.

SRM - Core - Control

Helps in debugging the current state of BOXI Integration. This option is useful when troubleshooting BOXI user creation and BOXI user association with OneClick users.

SRM - Core - Entity Group

Helps in troubleshooting Report Manager entity group event processing. Enable this option to debug the device grouping into predefined groups (such as vendor, model class, or landscape) or user-defined groups (such as global collections).

SRM - Core - Entity Manager

Logs the internal processing events for the model management within Report Manager. This option is useful in understanding how Report Manager is interpreting new models.

SRM - Core - Model Manager

Helps in troubleshooting Report Manager model creation in the reporting database. Enable this option if a problem arises with model key generation in the reporting database.

SRM - Core - Report Manager

Controls the Report Manager core logger, which can be used to debug Report Manager initialization, landscape monitoring for a device, and configuration of events and event filters.

SRM - Core - Scheduling

Logs scheduling information for archiving tasks, such as events archiving and CA Spectrum Service Performance Manager test data archiving.

SRM - Core - User Security

Assists in troubleshooting problems when logging in to InfoView from the CA Spectrum web console.

SRM - DB - Data Access

Logs Report Manager custom user data like Event titles (eventtitle.xml), PCauseTitles (pcausetitle.xml), and Custom vendors (vendor.xml); and tracks new device model insertion into the reporting database.

SRM - DB - Queries

Assists in troubleshooting BOXI general integrations, such as granting a report access and changing reporting database password and universe password. Logs most of the interaction between the BOXI CMS database (for the user and group information) and the Report Manager registry table.

SRM - DB - SPM Test Query

Assists in troubleshooting Service Performance Manager test data activities. Use this option with the 'SRM - Handler - SPM Event' option for a complete Service Performance Manager test data processing log.

SRM - Handler - Alarm

Assists in troubleshooting alarms processing within Report Manager. For example, logs the presence of unprocessed alarm table files in the reporting database.

SRM - Handler - Availability

Assists in troubleshooting problems with the Report Manager availability handler, which processes the availability or outage events for models. Enable this option if there are any issues with model outages.

SRM - Handler - Device Availability

Assists in troubleshooting device availability events that are processed within Report Manager. This legacy option is useful in debugging availability data migration issues (from CA Spectrum 9.1 to 9.2).

SRM - Handler - Generic Event

Debugs the event processing issues that do not fall under any other handlers.

SRM - Handler - Interface Availability

Assists in troubleshooting interface availability events processing within Report Manager. This legacy option is useful in debugging availability data migration issues (from CA Spectrum 9.1 to 9.2).

SRM - Handler - Model Create Destroy

Assists in troubleshooting model and global collection management events, such as create, destroy, or rename global collection.

SRM - Handler - Model State

Assists in troubleshooting the event processing for VPLS reports.

SRM - Handler - NCM Config

Assists in troubleshooting Network Configuration Manager event processing issues.

SRM - Handler - SPM Event

Assists in troubleshooting Service Performance Manager test event processing issues. Use this option with the 'SRM - DB - SPM Test Query' for a complete Service Performance Manager test data processing log.

SRM - Handler - Security

Assists in troubleshooting issues that are related to model access in reports and BOXI CA Spectrum users. Use this option with the 'SRM - Core - Control' option for better debugging.

SRM - Spectrum Poller - Device

Assists in troubleshooting Report Manager device polling issues.

SRM - Spectrum Poller - Event

Assists in troubleshooting Report Manager event polling. Enable this option when the reporting database is not in sync with the archive manager.

SRM - Tools - Archiver

Assists in troubleshooting reporting data archiving issues.

SRM - Tools - Monitor

Logs events that are related to the SRMApplication model. If 'Monitor SRM using a Spectrum model' is disabled, this option routes SRMApplication model events to the debug log.

Note: The 'Monitor SRM using a Spectrum model' option is on the Report Manager Preferences page. You can access the page from the OneClick home page by navigating to Administration, Report Manager, and Preferences. For more information, see Preferences (see page 66).

Debugging Report Parameter Pages

Enable the debug log in the CABI server for the issues that are related to report parameter pages.

Follow these steps:

1. On the CABI server, open the following file for editing:

   `<CABI_tomcat>/webapps/SpectrumCustomParams/WEB-INF/classes/log4j.properties`

   CABI_tomcat

   Indicates the location of the tomcat root folder on the CABI server.

2. Change the log4j.logger.com.ca.spectrum.repmgr parameter from WARN to DEBUG.
3. Save and close the file.
4. Restart the CABI tomcat server.

   Logs for Report Manager report parameter pages are now written to the following file on the CABI server:

   `/tomcat/logs/SpectrumCustomParams.log`

Index