Service Level Agreement Guide

Operations Center 5.5

November 6, 2013

Legal Notices

Contents

About This Guide

The *Service Level Agreement Guide* provides information for managing Service Level Agreements (SLAs).

Audience

This guide is intended for Operations Center system administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the *User Comments* feature at the bottom of each page of the online documentation.

Additional Documentation & Documentation Updates

This guide is part of the Operations Center documentation set. For the most recent version of the *Service Level Agreement Guide* and a complete list of publications supporting Operations Center, visit our Online Documentation Web Site at Operations Center 5.5 online documentation.

The Operations Center documentation set is also available as PDF files on the installation CD or ISO; and is delivered as part of the online help accessible from multiple locations in Operations Center depending on the product component.

Additional Resources

We encourage you to use the following additional resources on the Web:

- NetIQ User Community: A Web-based community with a variety of discussion topics.
- NetIQ Support Knowledgebase: A collection of in-depth technical articles.
- NetIQ Support Forums: A Web location where product users can discuss NetIQ product functionality and advice with other product users.

Technical Support

You can learn more about the policies and procedures of NetIQ Technical Support by accessing its Technical Support Guide.

Use these resources for support specific to Operations Center:

- Telephone in Canada and the United States: 1-800-858-4000
- Telephone outside the United States: 1-801-861-4000
- E-mail: support@netiq.com
- Submit a Service Request

Documentation Conventions

A greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path. The > symbol is also used to connect consecutive links in an element tree structure where you can either click a plus symbol (+) or double-click the elements to expand them.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a forward slash to preserve case considerations in the UNIX* or Linux* operating systems.

A trademark symbol (®, ™, etc.) denotes a NetIQ trademark. An asterisk (*) denotes a third-party trademark.

1 About Service Level Agreements

A Service Level Agreement (SLA) is a contract between a service provider and a customer that specifies in measurable terms the service to be provided. Operations Center tools, particularly the Business Service Level Manager (SLM), allow you to define SLAs, and monitor and manage those agreements.

1.1 What are SLAs?

Businesses set up agreements with customers to provide a specific standard of service. The service provider and the customer together define an acceptable level of service by establishing key objectives. Each objective must be measurable so that both sides can determine if it is complies with the agreement. There is usually a defined time interval associated with measuring the success of each objective.

Typically the types of measurable data are:

- **Incidents:** Events that occur when the service reaches or exceeds a specified condition.
- **Outages:** Incidents that result in key services, such as data or call centers, becoming unavailable (going offline).
- **Downtime:** The total elapsed time of an incident.
- **Availability:** The amount of time that a service is operational. Also defined as the amount of time that an element has not reached a specified condition. Availability is expressed as a percentage of total time.

Objectives are written based on this data as follows:

- **Incidents:** The service can have a specific number of incidents during a defined time period.
- **Outages:** The service can have a specific number of outages during a defined time period.
- **Downtime:** The service can be down or unavailable for a specific amount of time during a defined time period.
- **Availability:** The service must be up or available for a specific amount of time during a defined time period.
- **Calculation:** The service must meet a custom objective that is defined by either:
  - A mathematical calculation performed on element properties
  - A key metric formed from querying data in an external data source

The objectives are combined into one agreement called a Service Level Agreement (SLA). The agreement can specify the number of objectives that must be met during a specified time period. Health measurements determine whether the objectives are met.

Health and other measurements require the collection of data. The data collected depends on the type of service. For services involving technology, data can be collected about the status of the physical machines as well as the network connection.

Operations Center represents data as objects or elements. Each element has properties associated with it, and each element has a condition. This condition is based on either its own properties or other elements based on the relationships between elements. Use elements and the relationships between them to build service models that logically represent the critical services in an organization.

Objectives for SLAs are defined on elements. The relationship among elements is a factor for calculating the data for objectives. For example, an objective can apply to only one element, or that element and other elements associated with it.

1.2 Getting Started

The ongoing task of determining whether a service provider is in compliance with its SLAs involves the following processes:

- Collecting data
- Storing data
- Defining objectives
- Defining SLAs
- Monitoring
- Reporting

Operations Center has various tools to aid in each of these steps, which are described in more detail in the sections of this guide. The last section of the guide is a demo to set up and walk through to gain some hands-on experience with the tools described. Operations Center components all have licensing requirements. For more information, see the documentation for these components, or contact Technical Support (https://www.netiq.com/support/).

- Section 1.2.1, “Data Collection and Storage,” on page 10
- Section 1.2.2, “SLA Implementation,” on page 11
- Section 1.2.3, “Monitoring and Reporting,” on page 11

1.2.1 Data Collection and Storage

Determining if service quality meets the levels contractually required by SLAs requires measurable data, such as availability. To calculate such data, Operations Center requires data input regarding the components of the service, such as hardware and network connections. It is necessary to specify the following:

- **Sources for collecting data:** Operations Center has adapters and other tools to aid in the collection of relevant data. This data is integrated into Operations Center. In addition, it is possible to use data already collected in a central database.
- **Where to store data:** You must establish databases and database connections to store the data. Operations Center has databases to store the data or you can connect Operations Center to an external data source.

- **Data to collect:** For data integrated into Operations Center, select the elements that represent your service and the relevant properties that define the elements. Also establish relationships between elements. These relationships, as well as the properties of an element, determine the element condition. For data in an external data source, decide which properties are relevant and how those properties relate to each other.
- **When to collect data:** Operations Center provides time management functionality for specifying when to collect data that is stored in the Operations Center server.

The two main approaches for collecting SLA data are:

- **Integrate Data into Operations Center:** This approach can take advantage of all the Operations Center capabilities for defining SLAs and monitoring them, and for reporting on SLA-related data. Operations Center has adapters for integrating data from other business management systems, and tools for collecting data.
- **Use Data from an External Data Source:** This approach allows you to determine a key metric based on data stored in an external database and define an SLA based on that key metric. It is not necessary to integrate any existing data into Operations Center, which avoids creating a duplicate data store. However, you must be very familiar with the data in the external data source and how it is stored and structured.

Use either or both of these approaches for different elements.

1.2.2 SLA Implementation

The Service Level Manager (SLM) is Operations Center's tool for defining and implementing SLAs. SLM has the following components:

- **SLM Engine:** Measures and monitors service level metrics and handles all warning and violation activity.
- **Business Service Warehouse:** Stores service level metrics, alarm history, and historical performance data.
- **Console:** Client used to access SLM data and functionality.

To use SLM, you must purchase a SLM license key for each Operations Center server. This includes all Operations Center servers that are used for capturing and monitoring data including data captured using an InterCommunication adapter. For more information about licensing, contact Technical Support (https://www.netiq.com/support/).

The SLM tool is explained more fully throughout this guide.

1.2.3 Monitoring and Reporting

Operations Center dashboard has various options for monitoring and reporting on SLA data. For more information, see the *Operations Center 5.5 Dashboard Guide*

SQL Views provides functionality in Operations Center that allows for third-party applications to have read access to Operations Center data in the warehouse. For more information, see the *Operations Center 5.5 SQL Views Guide*.

The Operations Center Web Services Application Programmer Interface (WSAPI) (also known as Web Services) is an integration point for customer or third-party applications to interact with the Operations Center server including SLA data. For more information, see the *Operations Center 5.5 Web Services Guide*.

2 Integrating SLA Data into Operations Center

Integrating data into Operations Center for use in SLAs involves using an adapter to integrate the data and possibly another Operations Center tool to collect the data and establishing a database to store the data. After data is stored, specify when and what data to collect for elements in Operations Center and the factors for determining the condition of those elements. Also specify other time management rules for determining when Operations Center calculates SLA metrics.

2.1 Understanding the Integration Tools

Operations Center integrates data from other management systems that collect data relevant to SLAs. The types of data vary and include trouble ticket systems and technology monitoring.

Operations Center also has three other tools for collecting data:

- **Data Integrator:** Integrates business metrics from databases, such as sales totals and help desk tickets, as well as analytics from business intelligence tools.

  For more information, see the *Operations Center 5.5 Data Integrator Guide*.
- **Experience Manager:** Monitors Web sites and application availability from a user perspective.

  For more information, see the *Operations Center 5.5 Experience Manager Guide*.

Operations Center uses adapters to connect to connect to and communicate with third-party management systems. Different Operations Center adapters exist for different management systems; create an adapter for each specific management system that integrates with Operations Center. In some cases, the adapter communicates directly with the management system. In other cases, communication occurs through an Object Request Broker (ORB) supplied by Operations Center. For more information, see the *Operations Center 5.5 Adapter and Integration Guide*.

IMPORTANT: Notes about data from adapters:

- When using an Event Manager adapter to collect historical data for SLAs, set the *Use Alarm Times for Condition Changes* adapter property to `True`. For historical alarm data, the properties are recorded based on the alarm record time instead of the alarm receipt time. This is important for the calculation of objectives based on alarm properties.
- Be sure that element properties created by an adapter meet the supported schema.

  To store alarm history, SLA data, or performance data, the element properties created by an adapter must meet the supported schema as specified in the Data Dictionary. Otherwise a "value too large" error occurs, displaying the maximum allowed length for a property value and the actual length. For example, dnames cannot exceed 3,000 characters.

2.2 Using Data Storage

The service level metrics necessary to analyze whether service level compliance is being met and service level health is acceptable are stored in a database called the Business Service Warehouse (BSW).

This database is external to Operations Center and can be one of the following types of databases:

- IBM DB 2
- Microsoft SQL
- Oracle
- PostgreSQLs
- Sybase

The database must be set up and configured. After it is ready for use, define the database in the Operations Center console.

By default, the BSW has a backup repository. There is also a default job to purge data at 3 AM daily; this can be changed.

To manually start and stop the engine that collects data for storage in the BSW:

1. In the Operations Center console, expand *Enterprise* > *Administration*, then locate *Data Warehouse* in the hierarchy.
2. Right-click *Data Warehouse*, then select *Stop Data Warehouse* or *Start Data Warehouse*.

For more information about the Service Warehouse and how it is configured, see the *Operations Center 5.5 Server Configuration Guide*.

2.3 Configuring the Properties Stored

Operations Center uses profiles to select elements for which alarm and performance data are collected. Profiles can be seen in the hierarchy in the Operations Center console under *Enterprise* > *Administration* > *Data Warehouse*. The profile sets when the data is captured and how long it is

retained (requires Data Warehouse restart). Every profile also contains expressions that specify the properties of an element that are stored. Properties collected in expressions can also be used to analyze performance.

By default, all elements that have an objective defined on them are automatically assigned to a profile called Service Levels. The Service Levels profile contains one predefined expression called Element Condition Change, which captures real-time condition changes including service level breach and warning alarms, outages, and so on. By default, the expression also captures root cause data with the threshold set to the severity level of Critical. There is an option to not collect root cause data or change the severity level to another condition for the threshold.

You can create additional expressions to capture other properties in the Service Level profile.

- Section 2.3.1, "Setting Service Levels Profile Properties," on page 15
- Section 2.3.2, "Creating Expressions," on page 17

2.3.1 Setting Service Levels Profile Properties

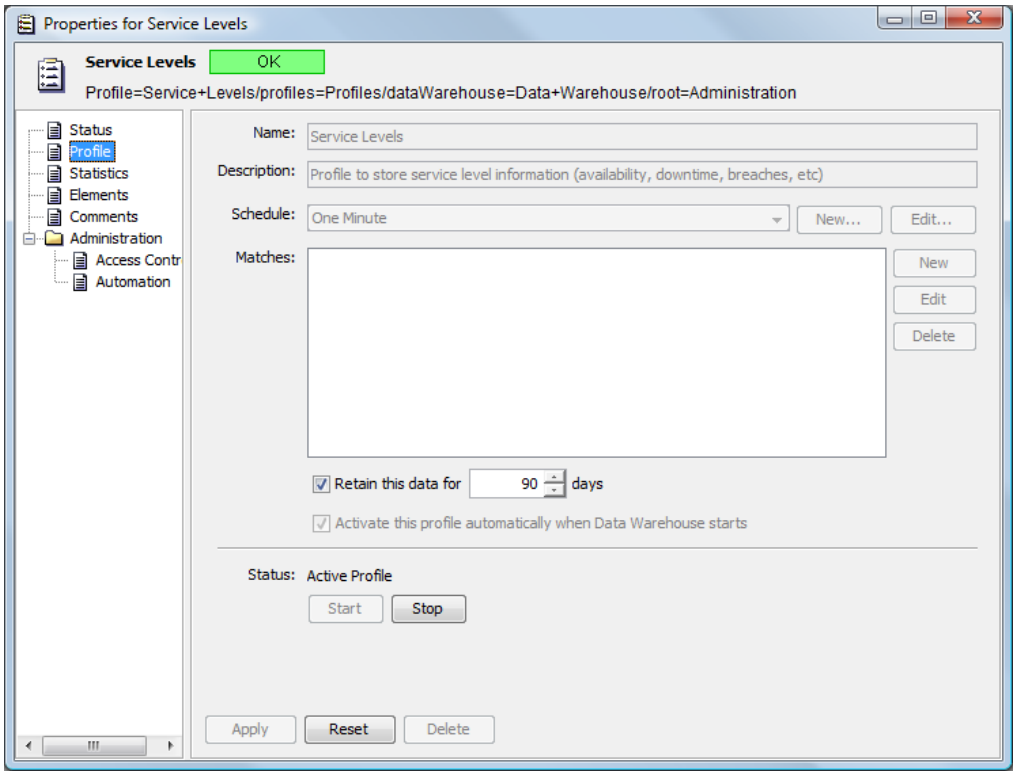
Operations Center automatically applies the Service Levels profile to all elements that have an objective defined. You cannot add or remove elements from this profile.

The schedule is permanently set to one minute. This schedule merely represents the frequency with which data is updated in the BSW. Service level data is constantly captured.

Data is retained for 90 days by default. You can change this setting. However, when the data retention setting is changed for a profile, the new retention time applies only to data collected from that point forward.

To access the Service Level Profile properties:

1. In the *Operations Center* Explorer pane, expand *Enterprise* > *Administration* > *Data Warehouse* > *Profiles*, then locate *Service Levels*.
2. Right-click *Service Levels*, then select *Properties* to display the properties dialog box:



3. In the left pane of the properties page, click *Profile*.

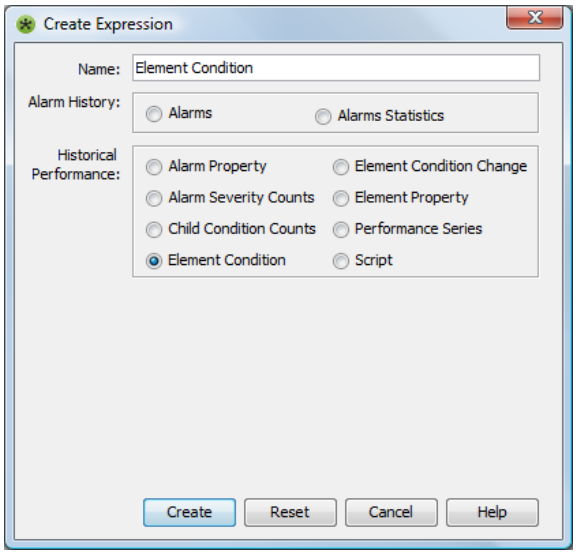
   For more information about the Service Level Profile, see "Understanding Default Service Level Management Profiles"in the *Operations Center 5.5 Server Configuration Guide*.

2.3.2 Creating Expressions

There is no need to create additional expressions to support Service Level Agreements. However, to capture additional properties for analyzing performance for SLAs, add expressions to the Service Levels profile. Carefully consider the number of expressions that are added, as the amount of data stored can increase significantly.

To create an expression:

1 In the *Explorer* pane, expand *Enterprise* > *Administration* > *Data Warehouse* > *Profiles*, right-click *Service Levels*, then select *Create Expression* to display:



2 In the Create Expression dialog box, provide a name, then select the options.

The following types of properties can be stored for historical performance:

Expression	Data Saved
Alarm Property	A property in the *Alarms* view, such as date/time, priority, class. The list of valid property names varies among adapters. Use the same spelling (including underscores) that is used in the alarm column headings displayed in the *Alarms* view or in the alarm property pages. Some commonly used alarm columns: ◆ *severity* to obtain the alarm's severity ◆ *id* to obtain the alarm's ID ◆ *last_update* to obtain the most recent update time for an alarm ◆ *persistent_id* to obtain the persistent identifier for the alarm To specify that the incoming string values are treated as numerals, select the *Force Numeric* check box.
Alarm Severity Counts	The total number of alarms by severity for a selected elements.
Child Condition Counts	The condition codes (Critical, Major, Minor, and so on) of all child elements for a selected element.
Element Condition	The condition code (Critical, Major, Minor, and so on) for a selected element.

Expression	Data Saved
Element Condition Change	Any change in condition for a selected elements. Select the *Store Root Cause* check box to capture information regarding the root cause for the condition change. If capturing the root cause, specify a severity level to act as a trigger.
Element Property	The values of a selected element property. Specify the name of an element property to monitor, such as memory usage or response time. The *Property* list is populated only if the profile's elements have custom properties, meaning properties other than Element Condition, Last Reported, and Element Name.
Performance Series	Data derived from measurements made by an external management system. Select a name for the series from, then specify the property to monitor. The values vary among different management systems. By default, the expression Name value is created using the Series value and the Property value, separated by a period (such as Series.Property). The default Name value is editable. Wildcards can be used. For example, enter the asterisk (*) as the Series and Property values. If an object has multiple series, they are all stored.
Script	The values resulting from running a script. Enter the entire contents of a script (written using NOC Script that determines the type of data to include.

For more information on expressions, see "Creating Expressions" in the *Operations Center 5.5 Server Configuration Guide*.

3 Click *Create*.

The Alarms property provides data for historical alarms that can be viewed in the *Alarms* view of the Operations Center console. For more information on alarms, see "Filtering and Managing Alarms" in the *Operations Center 5.5 User Guide*.

2.4 Understanding the Element Condition

The condition of elements is determined by an algorithm and is based on either the element's properties or the condition of other elements if the element is related to other elements. Using elements and their relationships to each other, build service models that logically represent business services.

For more information on the condition of elements and service models, see the *Operations Center 5.5 Service Modeling Guide*.

2.5 Managing Time

When gathering service level data, specify when information is captured and used in service level calculations using the following:

- **Time categories:** Identify blocks of time for a specific use
- **Calendars:** Associate time periods to time categories
- **Schedules:** Identify the time intervals for capturing data for specific calendars

Time Management options are set in the Operations Center console in the hierarchy under *Enterprise > Administration > Time Management*.

Review the following sections to configure and understand time management:

- Section 2.5.1, "Customizing Time Categories," on page 19
- Section 2.5.2, "Configuring Calendars," on page 20
- Section 2.5.3, "Understanding Schedules," on page 24

2.5.1 Customizing Time Categories

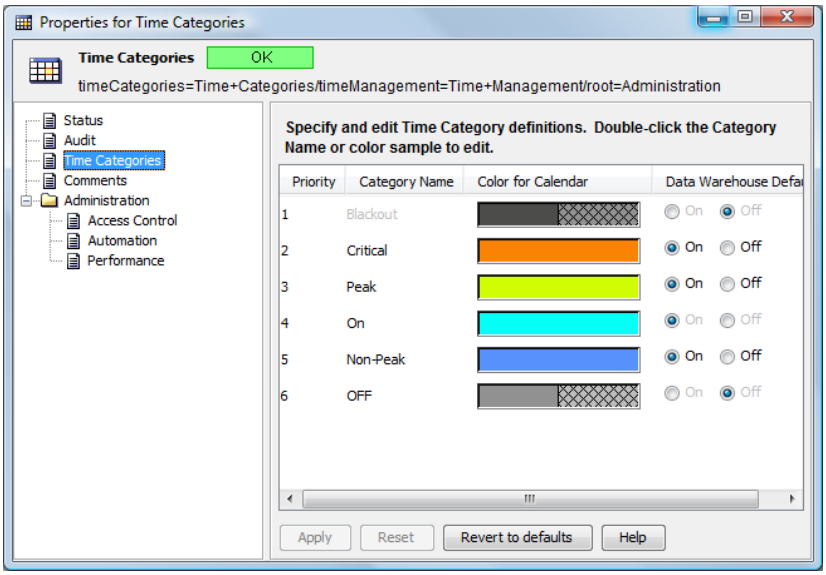
Time categories classify the operational windows associated with business services so that you can support services at various levels at various times. Time categories are used to identify blocks of time. They are essentially labels that are used by calendars to band sections of time.

Operations Center provides six default time categories:

- Off
- Nonpeak
- On
- Peak
- Critical
- Blackout

Except for blackout, these categories can be customized. Note that these time categories are also used for condition and severity for alarms.

Figure 2-1 *Time Categories*



Time categories are fundamental to objectives that require a time category during which the objective applies. For example, establish a 100% availability objective during peak hours when a service is Critical and a 95% availability objective during off peak hours.

To customize a time category:

1. Expand *Enterprise* > *Administration* > *Time Management*, right-click *Time Categories*, then select *Properties*.
2. Click *Time Categories*.
3. To change the *Category Name*, double-click the name and specify a new name.

   The *Blackout* category cannot be edited.
4. To change the color, double-click the color in the *Color for Calendar* column, then select a new color in the Select a Color dialog box.
5. To change the default in the Business Service Warehouse, click *On* (next to the category in the *Data Warehouse Default* column).
6. Click *Apply*.

2.5.2 Configuring Calendars

A calendar defines a specific range of time and days for monitoring the changes in the state of objects.

- "Understanding Calendars" on page 21
- "Creating Calendars" on page 22
- "Creating a Time Definition for a Calendar" on page 23
- "Copying a Time Definition" on page 23
- "Modifying a Time Interval" on page 24

- "Linking to an Existing Calendar" on page 24
- "Creating a Blackout Calendar" on page 24

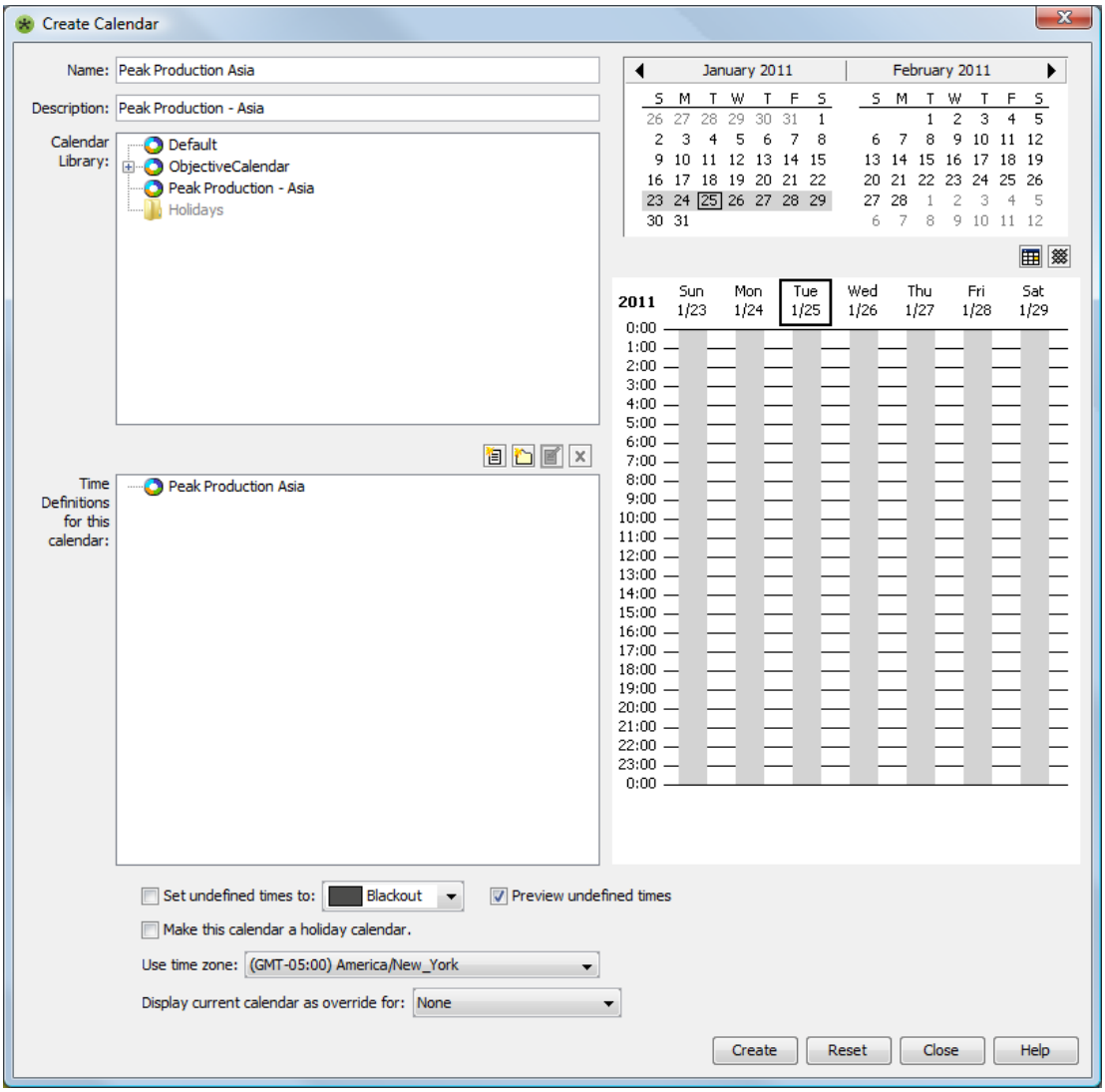
Understanding Calendars

Calendars can associate bands of time with a time category to add meaning to data and metrics. For example, the hours between 8 AM and 5 PM on Monday through Friday might be defined as peak times, while the hours between 1 AM and 3 AM on Sundays might be defined as maintenance times.

Operations Center ships with a default calendar that is set to 24x7 operational (ON) hours. The default calendar cannot be edited. It is necessary to define new calendars to handle additional needs.

A calendar can consists of one or more calendars that can be used repeatedly to capture performance data. New calendars can be defined from previously defined calendars.

Figure 2-2 *Calendar*



The *Calendar Library* section shows all existing calendars. Any calendars for which the *Make This Calendar a Holiday Calendar* option is selected appear in the *Holidays* folder. The *Calendar Visualization* section on the right side shows a two-month period with a weekly calendar underneath. The weekly

calendar displays shaded boxes of time to represent each time definition (which are shown in the *Time Definition* section). The (Go to Today) icon changes the display to the current date. When enabled, the (Show/Hide BSA Off Times) icon displays a black grid displays in the calendar to identify when SLA data collection is turned off.

Create new calendars by copying an existing calendar and changing the time definition. The time definition is made up of time intervals that you can modify individually.

Concerning defining overnight time definitions, if a time definition is set up to start on one day and finish sometime the next day (such as it runs overnight), on the first day the calendar is used, it starts running at the Start Time specified by the time definition. For example, assume the time definition specifies a peak time from 8PM until 5AM. On the first affected day, the calendar starts running at 8 PM. The calendar does not run from midnight until 5AM on that first day. To capture that time, a separate time definition must be defined.

It is possible to link a calendar to another calendar. Linked calendars are only editable in the original calendar definition and changes affect all calendars that are link to them.

When creating an SLA, select a calendar to use.

In calendars applied to SLAs, define blackout periods that are maintenance periods or downtime. This calendar is applied to eliminate data used in SLA calculations. However, the data continues to be stored in the Business Service Warehouse to ensure that data is available in the event that the calendar is revised at a later time.

In addition to blackout periods, define a blackout calendar and apply that to elements to specify when the element is down for scheduled or routine maintenance. Like blackout periods in a calendar, Operations Center observes the blackout for calculating SLA health and metrics but continues to collect data. A blackout calendar overrides all other calendar settings for service level metrics.

Creating Calendars

To create a calendar

1. Expand *Enterprise* > *Administration* > *Time Management*, right-click *Calendars*, then select *Create Calendar*.
2. Enter a name and description.
3. Set the time definition or select a calendar from which to copy the time definition.

   For steps to create a new time definition, see "Creating a Time Definition for a Calendar" on page 23.

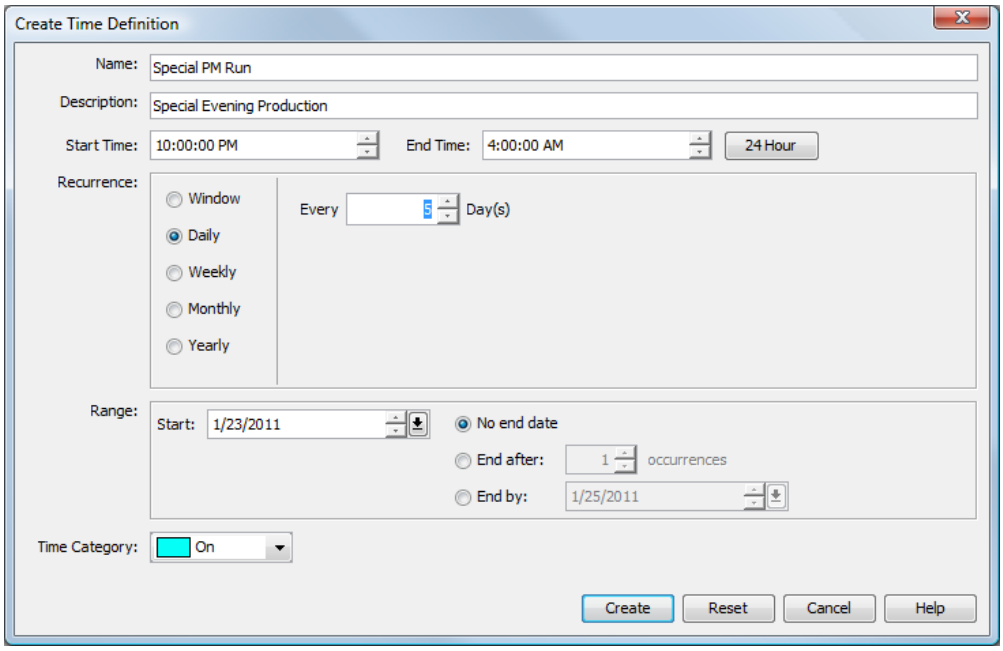
   For steps to copy a time definition from a calendar, see "Copying a Time Definition" on page 23.
4. To make the calendar a holiday calendar, select the *Make This Calendar a Holiday Calendar* option.
5. To use a different time zone, select it from the drop-down list for the *Use Time Zone* option.
6. To display a view of the current calendar with another calendar, select it for the *Display Current Calendar As Override For* option.

   The time definitions of the selected calendar display in a merged view with the current calendar. This is just for viewing purposes; the merged view cannot be saved.
7. Click *Create*.
8. If blackout times apply, continue to "Creating a Blackout Calendar" on page 24.

Creating a Time Definition for a Calendar

To create a new time definition for a calendar:

1 In the *Time Definitions* section of the Create Calendar dialog box, click (*New Time Definition*).



2 Enter the name and description.

3 Specify a start time and end time or click *24 Hour* to set the time definition to run a full 24 hours from the start time.

You can enter seconds for the start and end times, but seconds are not utilized as Time Definitions resolve to the minute.

4 Select an option for Recurrence to set when the time definition is applied.

5 (Optional) Select an end date for *Range*.

6 Select a time category to apply to the time definition.

7 Click *Create*.

8 To set the time category for all times not included in a time definition, click the *Set Undefined Times* option, then select a time category from the Calendar dialog box.

Copying a Time Definition

To copy a time definition from one calendar to another:

1 In the *Calendar* section of the Create Calendar dialog box, navigate to a calendar to use as the basis of the new calendar.

2 Right-click the calendar, then select *Copy*.

3 In the *Time Definitions for This Calendar* section, right-click the folder in which to save the new calendar, then click *Paste* to duplicate the calendar.

Modifying a Time Interval

To modify a time interval:

1. Right-click in the *Calendar Visualization* section of the Calendar dialog box.
2. Click *Create Override* to change the start and/or end time or time category for the time interval.

   To remove the override later and use the default interval defined by the time definition, you can right-click the interval, then select *Remove Override*.
3. Click *Cancel this Interval* to remove the time interval from the time definition.

   To restore the interval later, you can right-click the interval, then select *Restore Cancelled Interval*.
4. Click *Select on Definitions Tree* to select the time definition associated with the interval.

Linking to an Existing Calendar

To link to an existing calendar:

1. In the *Calendar* section of the Create Calendar dialog box, navigate to a calendar to use as the basis of the new calendar.
2. Right-click the calendar, then select *Copy*.
3. In the *Time Definitions for This Calendar* section, right-click the folder in which to save the new calendar, then click *Paste Link*.

Creating a Blackout Calendar

To create a blackout calendar for a specific element:

1. In the Operations Center hierarchy, expand *Enterprise*, then navigate to the element for which the blackout calendar is needed.
2. Right-click the element, then select *Edit Blackout Calendar*.
3. Create time definitions as necessary to specify blackout times when data is not collected for this element.

   SLA data continues to be collected by the BSW by not applied in the SLA objective.
4. Click *Apply*.

2.5.3 Understanding Schedules

A schedule defines the time intervals for capturing performance data. Schedules can be linked to a selected calendar to further refine when data is captured.

The default schedules (*One Minute*, *Five Minutes*, *Audit Schedule*) are not editable. Define additional schedules as necessary.

For example, assume a calendar defines a time category (such as `ON`) for data capture every Monday and Friday, every month, from 3:00 PM – 6:00 PM. A master schedule can be defined that captures data continuously at fifteen-minute intervals. Then, a second schedule can be defined that uses the same calendar, but captures data at one-minute intervals for a specified period of time.

2.6 Custom Configurations

There are a couple of parameter settings that can be configured for the Operations Center server to customize the calculation and evaluation of SLA data. These include:

- Defining health grade ranges that are used to evaluate if an agreement or objective is in compliance.

  For more information about configuring health grades, see Section 4.2.6, "Configuring Health Grades," on page 56.

- Customizing the weekly time interval to start on Monday instead of Sunday. Time intervals are set on objectives to declare the span of time in which the objective measures and calculates values.

  For more information about configuring the start of the weekly time window, see Section 5.4.3, "Customizing the Weekly Time Interval," on page 67.

2.7 SLA Use Case

A company named *Acme IT Services* manages the IT infrastructure of banking services for a financial service company named ABC Bank. These services include online banking for ABC Bank customers and all of ABC Bank's communication infrastructure, particularly e-mail. Acme has a Service Level Agreement (SLA) with ABC Bank, which states that all services will have 99 percent availability each month.

In addition, Acme operates an internal customer support center (help desk), which receives calls from ABC Banking employees who need help with their IT infrastructure. Acme maintains a trouble ticket system to track how well it responds to those calls. Acme executives want to see measurable data so they can evaluate the performance of the customer support center and possibly market these services to other customers. Acme management has set up an internal SLA with the customer support center regarding response levels to trouble tickets.

(This use case does not provide details about using the different features described in the solution. Refer to other sections in this guide and in other guides as indicated.)

To set up and report on the results of these two SLAs, Acme must do the following:

- Collect data (see Section 2.7.1, "Data Collection," on page 26)
- Store data (see Section 2.7.2, "Data Storage," on page 27)
- Represent data in Operations Center (see Section 2.7.3, "Data Relationships," on page 30)
- Define an SLA in Operations Center (see Section 2.7.4, "Objective and Service Level Agreement Definitions," on page 30)
- Report on data using a Operations Center reporting tool (see Section 2.7.5, "Reporting," on page 34)

2.7.1 Data Collection

Acme needs to collect data for ABC Bank's online banking system and its e-mail communication as well as Acme's own trouble ticket system.

Acme needs to collect the following data regarding ABC Bank's IT infrastructure:

- Hardware availability
- Database availability
- Software availability

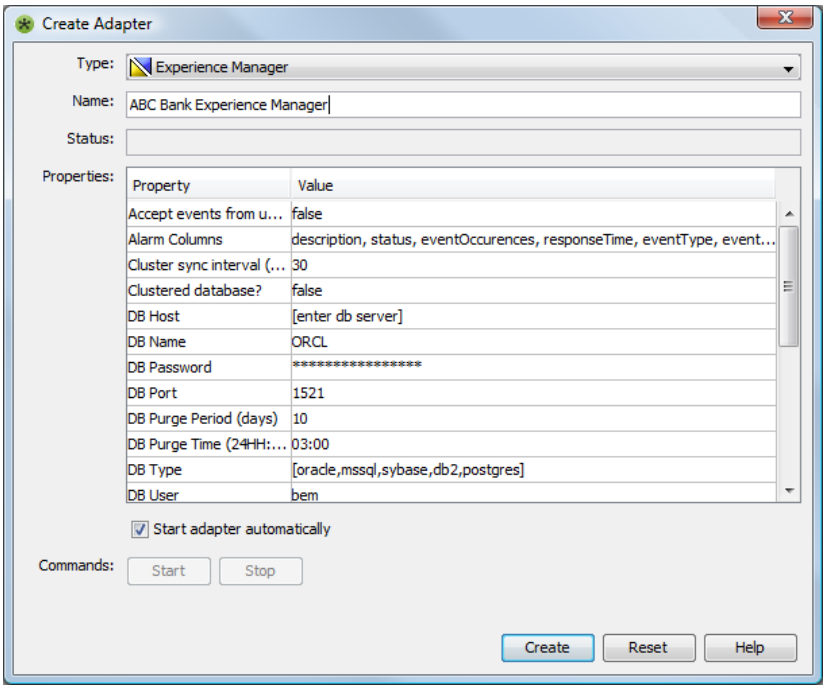
The following sections illustrate adapters in the Operations Center console:

- "BEM Adapter in the Operations Center Console" on page 26

BEM Adapter in the Operations Center Console

Acme also needs information about Web site and application availability from an end user perspective for the online banking services. Acme installs the Experience Manager to collect this data and creates an Experience Manager adapter in the Operations Center console to integrate this data into Operations Center.

Figure 2-3 *Creating an Experience Manager Adapter*



For more information about installing and configuring the Experience Manager, see the *Operations Center 5.5 Experience Manager Guide*.

Acme already stores its trouble ticket data in an Oracle database and is comfortable managing the data using that system and just wants to maintain it. Acme considers integrating the trouble ticket data into Operations Center, but does not want duplicate data. Therefore, Acme decides to connect Operations Center to the Oracle database to collect the data required for an SLA on the trouble ticket system.

2.7.2 Data Storage

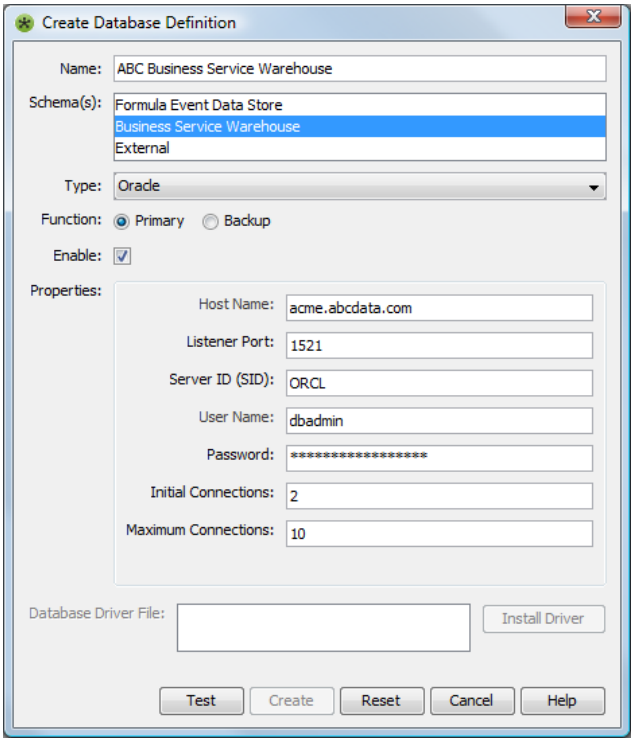
SLA data that is integrated into Operations Center is stored in the Service Warehouse. Acme creates a database and a database definition in Operations Center for the Service Warehouse:

- "Database Definition" on page 27
- "New Calendar" on page 28
- "New Time Definition" on page 29
- "Database Definition for an External Data Source" on page 30

For more information, see Section 2.7.2, "Data Storage," on page 27. Also, for how to create database definitions, see the *Operations Center 5.5 Server Configuration Guide*.

Database Definition

Figure 2-4 *Database Definition for the Business Service Warehouse in Operations Center console*

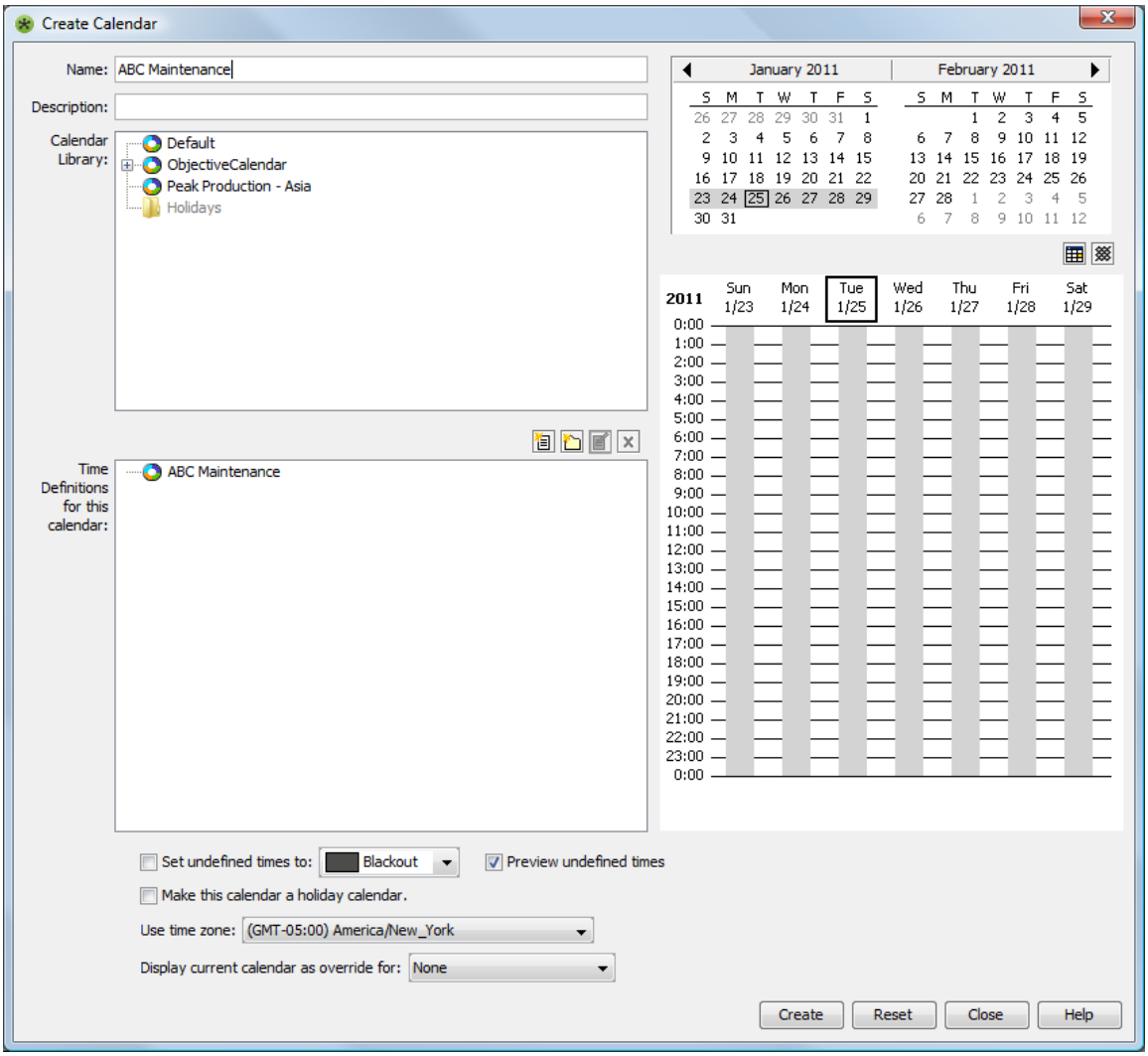


By default, Operations Center calculates SLA data 24 hours a day for 365 days per year based on the default calendar. ABC Bank requires that its services be available 99 percent of the time except for maintenance periods, which occur every Saturday and Sunday night from 1 Am to 5 Am.

New Calendar

To identify maintenance periods, Acme creates a new calendar:

Figure 2-5 *New Calendar for ABC Maintenance Periods in Operations Center console*

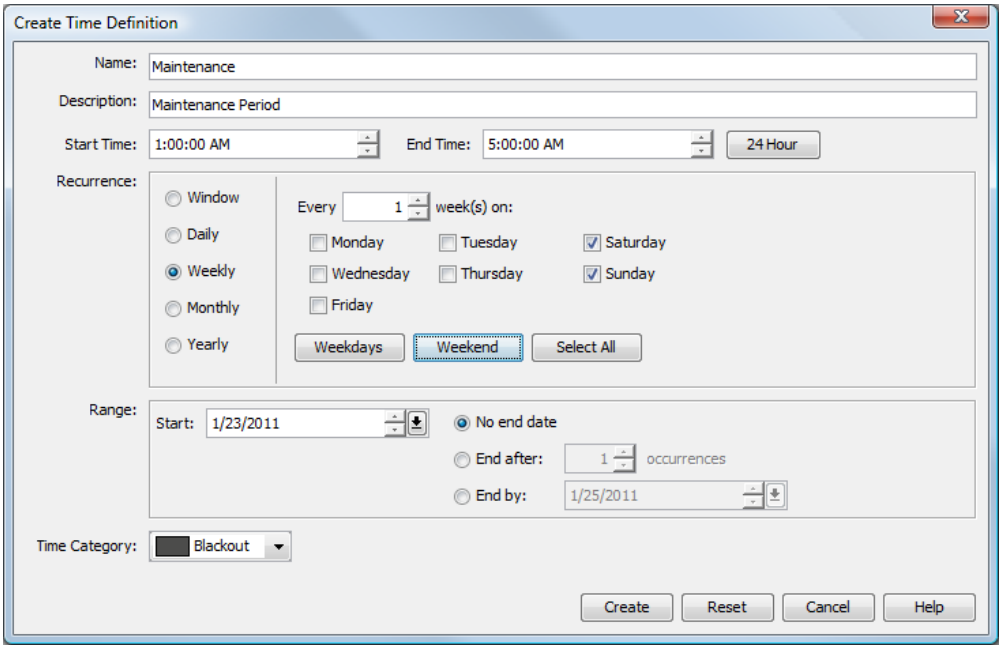


For more information, see Section 2.5, “Managing Time,” on page 19. Also, for more information on how to create calendars, see “Time Categories, Calendars, and Schedules” in the *Operations Center 5.5 Server Configuration Guide*.)

New Time Definition

For this new calendar, Acme defines a time definition to indicate that Saturday and Sunday, from 1 AM to 5 Am, are maintenance periods.

Figure 2-6 *New Time Definition for New Calendar in Operations Center console*

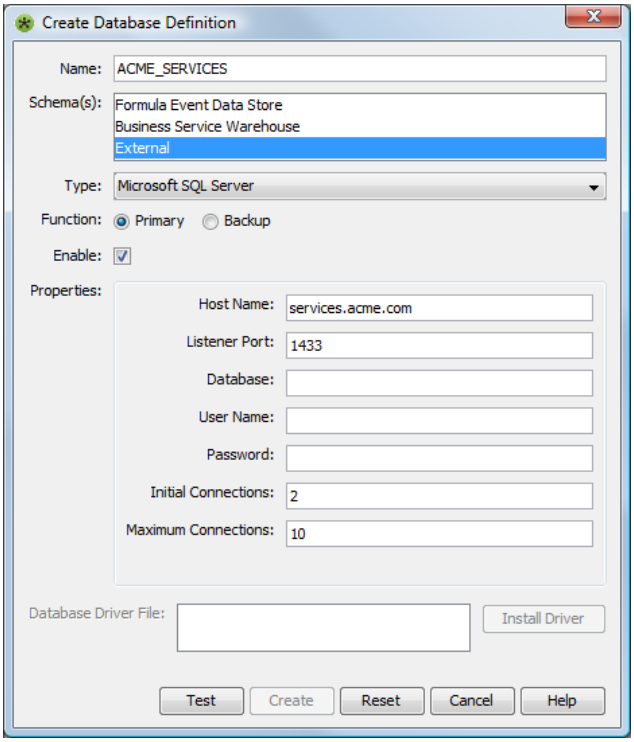


This calendar will be applied to the SLAs defined for ABC's services.

Database Definition for an External Data Source

To connect Operations Center to the data source, which stores trouble ticket data, Acme creates a database definition to an external data source:

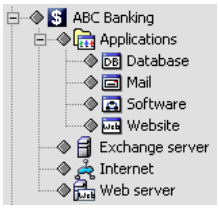
Figure 2-7 *Database Definition for External Data Source in Operations Center console*



2.7.3 Data Relationships

To represent the services for ABC Banking, Acme creates a service model in Operations Center:

Figure 2-8 *ABC Banking Service Model*



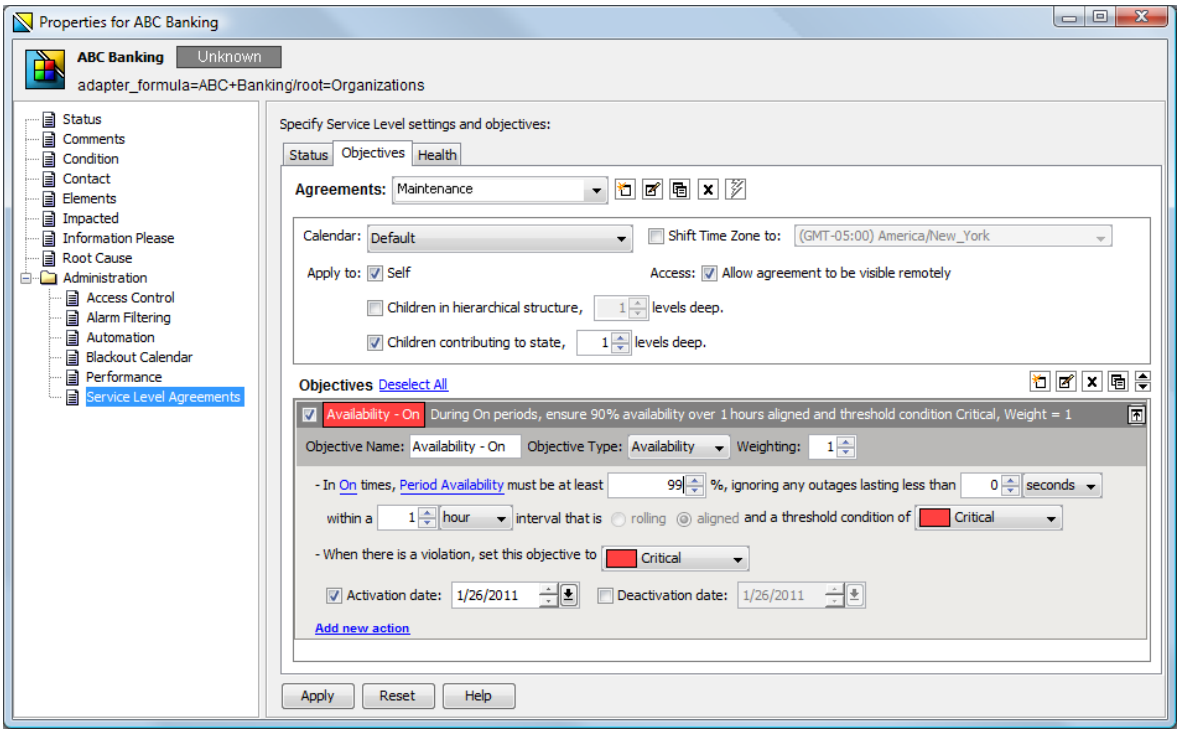
2.7.4 Objective and Service Level Agreement Definitions

- "Availability Objective" on page 31
- "Outages Objective" on page 32
- "SLA Metric Catalog" on page 33

Availability Objective

Acme has a Service Level Agreement (SLA) with ABC Bank, which states that all services will have 99 percent availability each month. The SLA is named Standard Availability and applies to the *ABC Banking* element, and propagates three levels down. It contains an Availability objective, which requires at least 99 percent availability. Note the Maintenance calendar is specified, so that maintenance times (stated earlier) are exempt from the objective requirement.

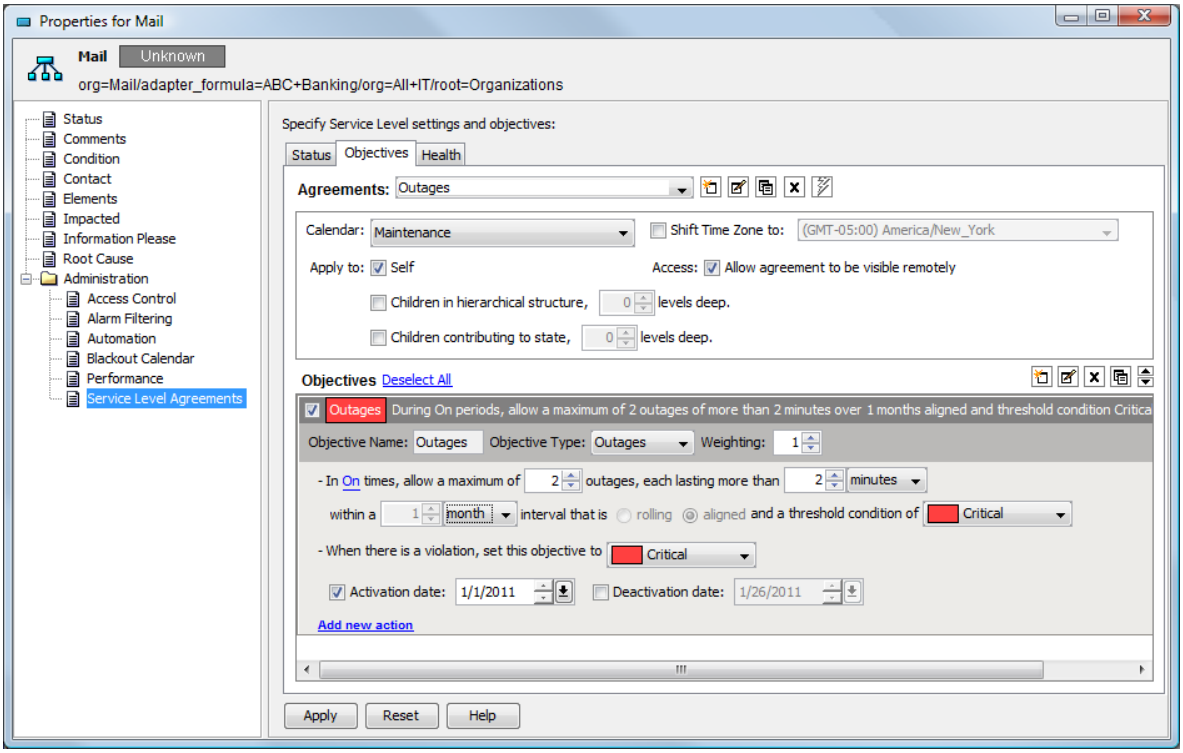
Figure 2-9 *Availability objective tracks the percentage of time that banking services are available.*



Outages Objective

The *Mail* element contains an additional Outages objective for e-mail communications, which allows one outage lasting no more than one hour per month except unlimited outages during maintenance periods.

Figure 2-10 *Outages objective for tracking the e-mail application*

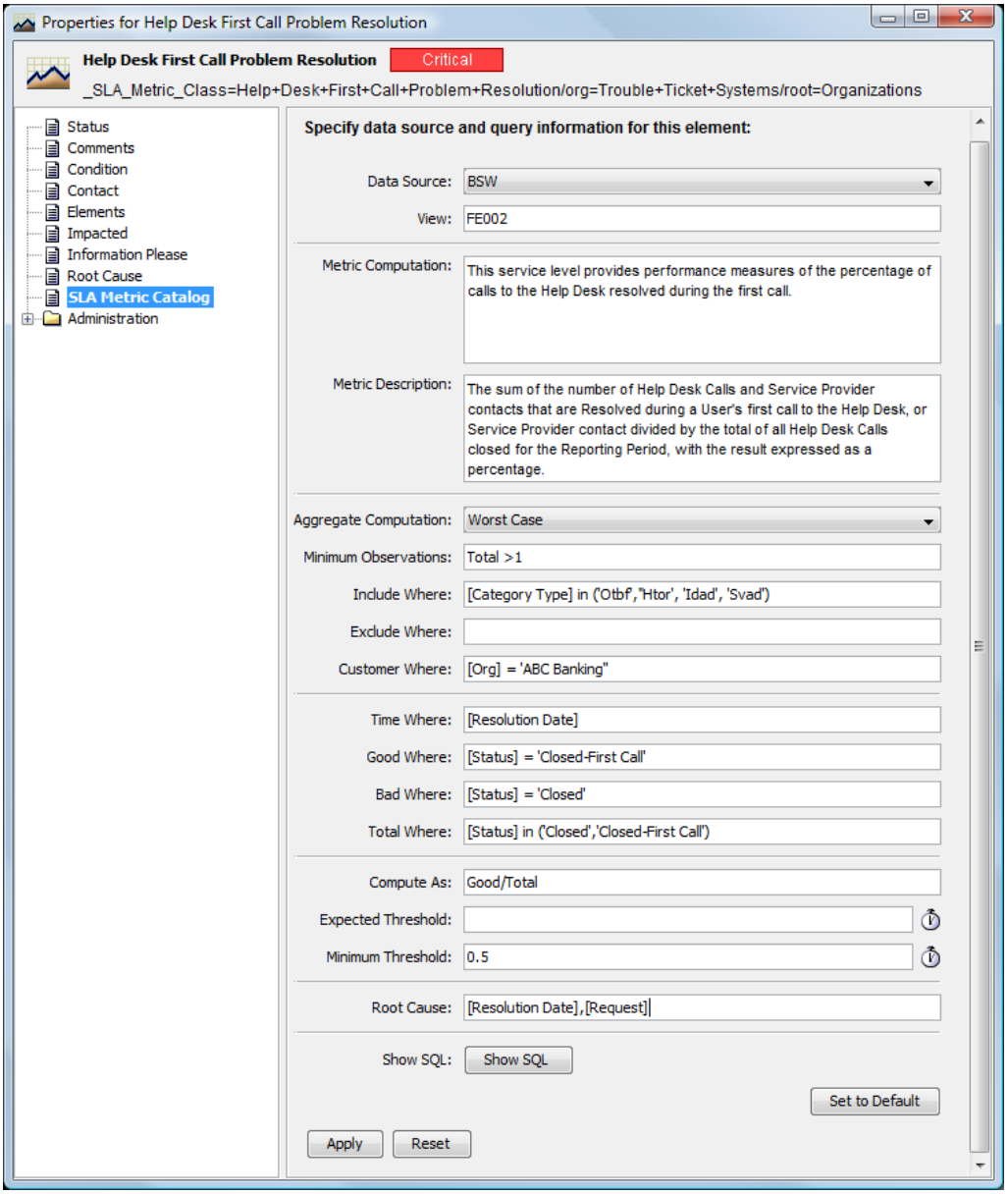


SLA Metric Catalog

Acme management has set up an internal SLA with the customer support center regarding response to trouble tickets. The SLA has a calculation objective (with the SLA metric catalog) for the trouble ticket system.

Acme sets up an element under *Service Models* called *Trouble Ticket System* and applies the SLA Metric Catalog to it. The SLA Metric Catalog captures the number of calls received and logged, the initial response time, the number of resolved calls, and the time to resolve a call. For more information, see Section 3.2.3, "Managing the SLA Metric Catalog Properties," on page 43.

Figure 2-11 *SLA Metric Catalog*



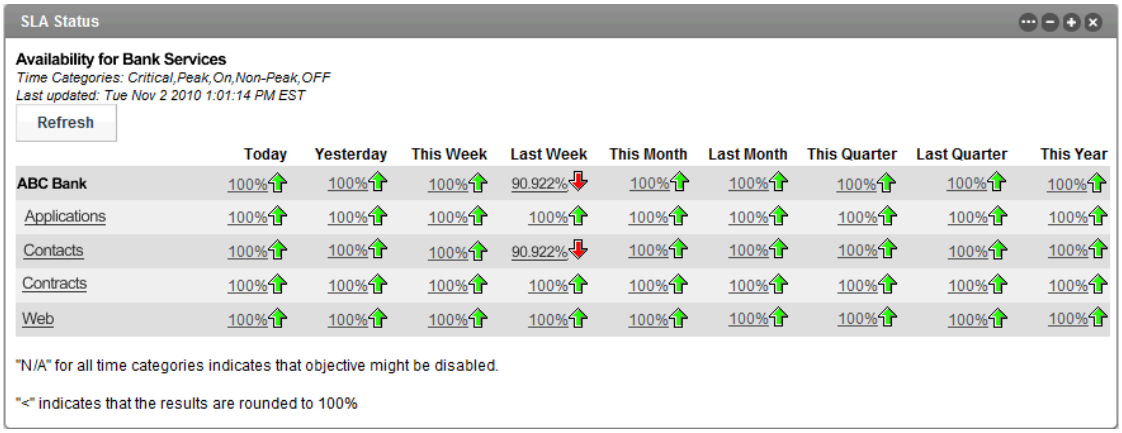
The SLA Metric Catalog properties create an SQL statement that Operations Center uses to acquire custom properties for the element from an external data source and evaluate the properties to determine a key metric.

2.7.5 Reporting

Acme uses the Operations Center dashboard to create a Portal page that is accessible to the line of business owners.

In the Operations Center dashboard, add an SLA Status report to the portal page that reports on the availability of the services. Figure 2-12 shows the SLA Status Report pointed at the *Bank Services* element:

Figure 2-12 *SLA Status Report*



According to the SLA objectives, all services should have at least 99% availability.

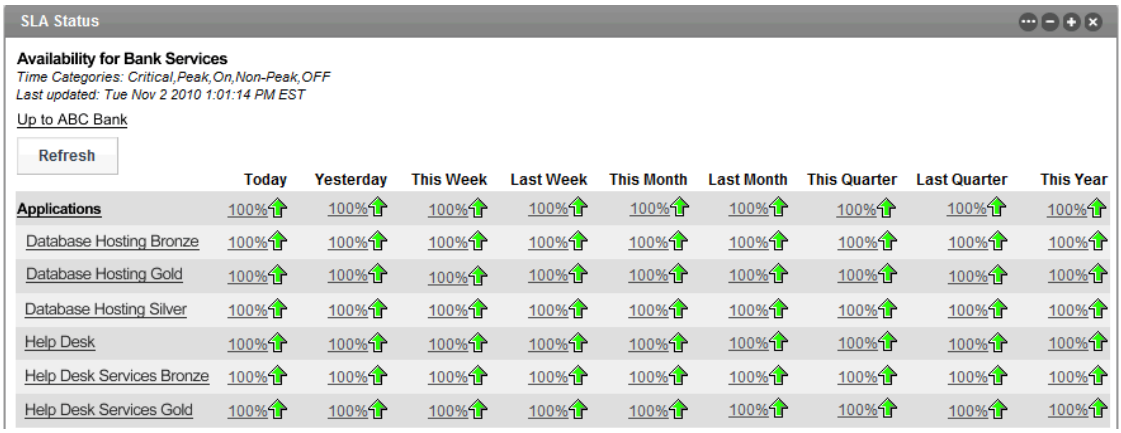
The time periods are:

Today
Yesterday
This Week
Last Week
This Month
Last Month

At a glance, owners can see the SLA objectives are being met. Problem areas are highlighted in red.

In this report, drill down to subelements by simply clicking one of the links in the far left column. Figure 2-13 shows the detailed report for the *Applications* element:

Figure 2-13 *SLA Status Report*



Review the details for subelements of the *Applications* branch. When you are ready to return to a higher level, click the *Up to ABC Bank* link.

For details on creating portal pages and portlets, see the *Operations Center 5.5 Dashboard Guide*.

The final step is to send the URL to the portal reports to the line of business owner for review.

3 Using External Data Source for SLA Data

SLAs can be based on business metric data stored in an external data source instead of data integrated into Operations Center. Configure Operations Center to read data from a SQL Server 2005 database or Oracle 10g database, create elements based on this data, define custom properties for these elements and their relationship by creating an SLA metric catalog, and define an objective that measures SLA compliance. Operations Center translates the custom properties into SQL in order to access the data from the external data source and generate SLA metrics as well as root cause failures. Use Operations Center reporting features to monitor and report on the SLA metrics.

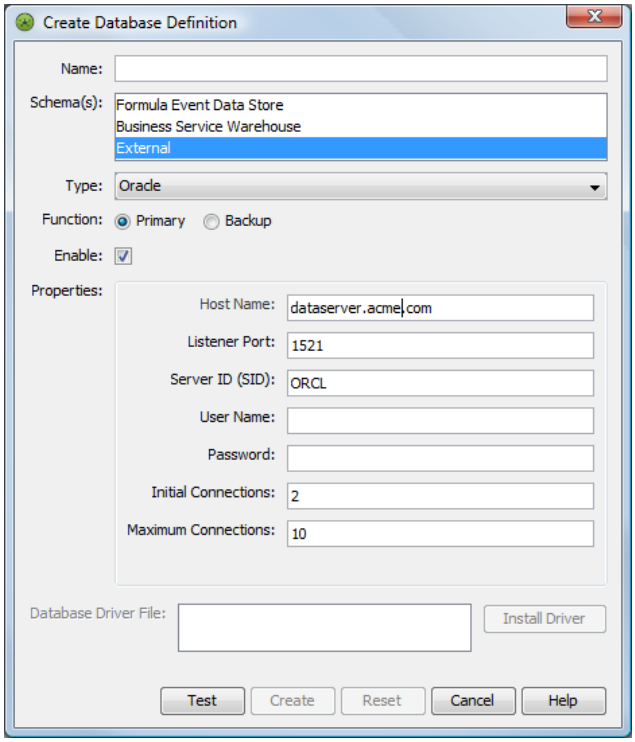
3.1 Configuring a Data Source

In the Operations Center, create a connection to an external data source by defining the connection credentials. Connect to either an SQL Server 2005 database or Oracle 10g database.

Using data stored in an external data source can save the time and effort required to integrate it into Operations Center and the need to store it in two locations. However, as the data is not integrated into MOperations Center, not all Operations Center functionality is available. Operations Center only uses historic data from the external data source, not real time data. Also, you must be thoroughly familiar with the data and its structure in the external data source in order to configure it with Operations Center.

To configure an external data source for use in Operations Center, establish a database connection using connection credentials:

1 In the Operations Center console, expand *Enterprise* > *Administration*, right-click *Database Definitions*, then select *Create Database Definition*:



2 Select *External* for the schema, then enter all other credentials to connect to the external database.

3 Specify values for *Listener Port* and *Initial Connections*.

For more information about database definitions, see the *Operations Center 5.5 Server Configuration Guide*.

4 Click *Create*.

3.2 Customizing Properties

The SLA metric catalog defines the custom properties of an element captured for the purpose of computing metrics to determine compliance with Service Level Agreements (SLAs). A SLA metric catalog is typically established for elements based on data from an external data source. This data source can be any data schema in any database that stores SLA metric data. It is common practice to establish a connection to an SQL Server 2005 database or Oracle 10g database that is already used to store business data.

In Operations Center, behavior models, classes, and property pages define attributes for elements and relationships between elements. Property pages are associated with elements through behavior models via class.

To capture properties for the SLA metric catalog involves the following new components:

- SLA Metric Model
- SLA Metric Class
- SLA Metric Computed property page
- SLA Metric Catalog properties for an element

You cannot create custom behavior models, classes, or property pages to define properties of elements based on data from an external data source.

Behavior models, classes, and property pages are defined in the Operations Center console under *Enterprise* > *Administration* > *Metamodel*. It is possible to view and use the new behavior model, class, and property page only if you have a license for Business Service Level Manager (SLM). For more information about licensing, contact Technical Support (https://www.netiq.com/support/).

- Section 3.2.1, "Viewing SLA Metric Model and Class," on page 39
- Section 3.2.2, "Using the SLA Metric Computed Property Page," on page 41
- Section 3.2.3, "Managing the SLA Metric Catalog Properties," on page 43

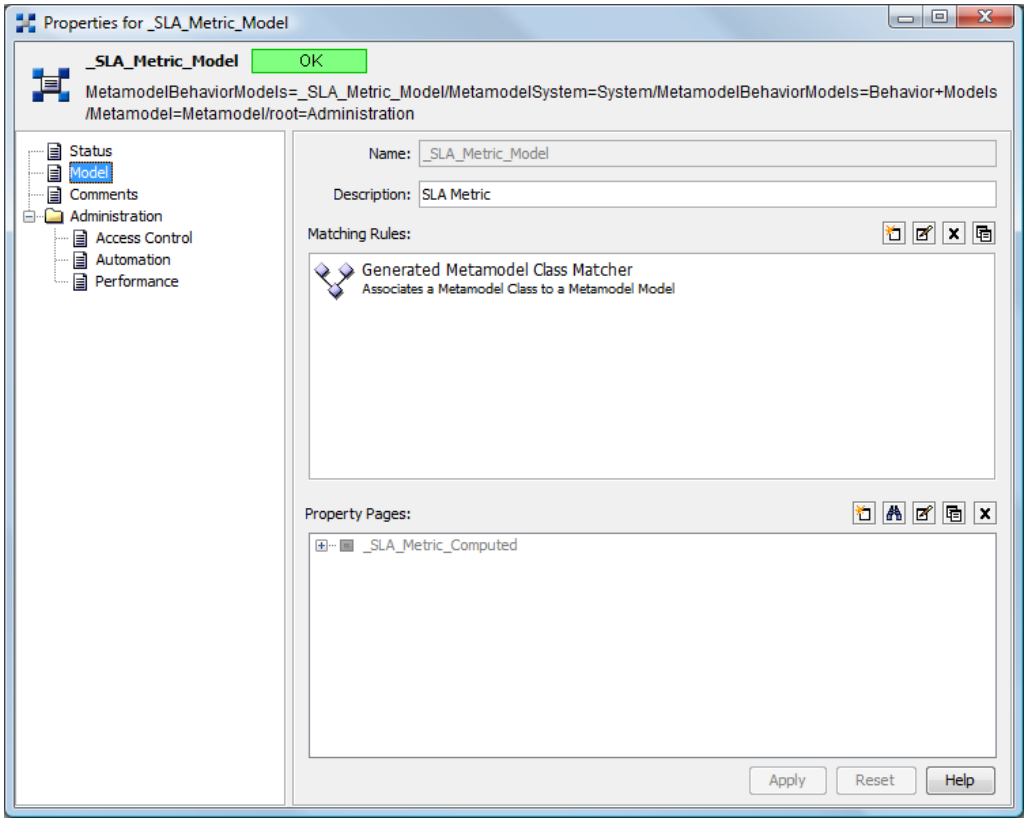
3.2.1 Viewing SLA Metric Model and Class

The SLA Metric Model is a new system type behavior model that associates all elements of the SLA Metric Class to the SLA Metric Computed property page. This model cannot be edited.

- "Viewing the Properties of the SLA Metric Model" on page 40
- "Viewing the Properties of the SLA Metric Class" on page 41

Viewing the Properties of the SLA Metric Model

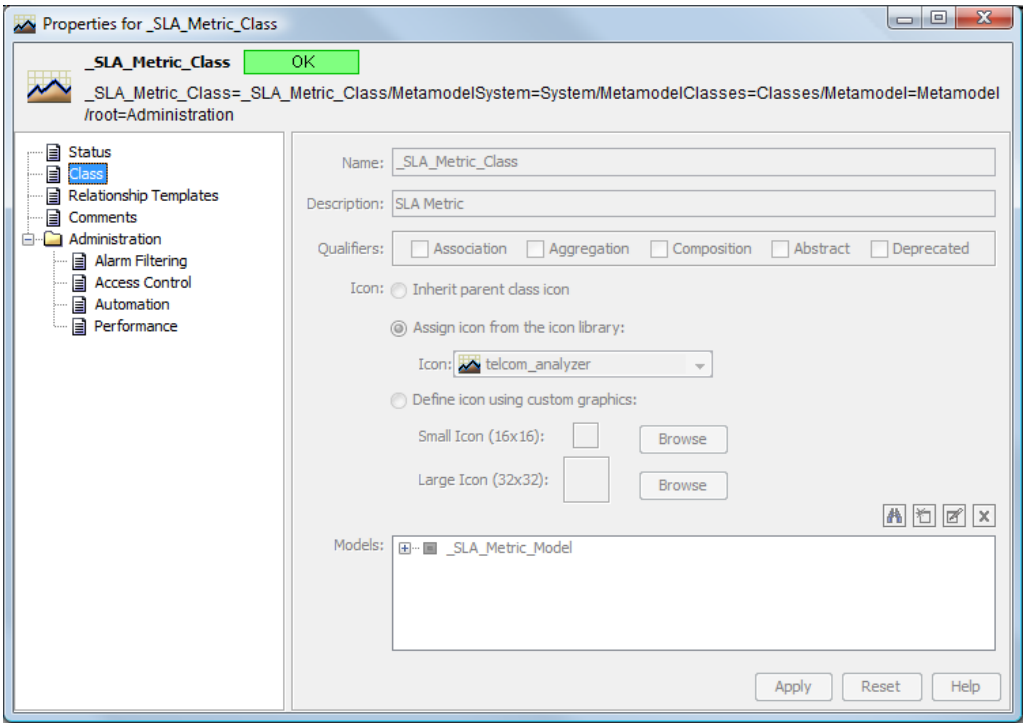
1 Expand *Enterprise* > *Administration* > *Metamodel* > *Behavior Models* > *System*, right-click *_SLA_Metric_Model*, then select *Properties* > *Model*:



The SLA Metric Class is a new system type class represented by the icon  . All elements assigned to this class are assigned to the SLA Metric Model and have the SLA Metric Computed property page. This new class cannot be edited.

Viewing the Properties of the SLA Metric Class

Expand *Enterprise* > *Administration* > *Metamodel* > *Classes* > *System*, right-click *_SLA_Metric_Class*, then select *Properties* > *Class*:



3.2.2 Using the SLA Metric Computed Property Page

The SLA Metric Computed property page is a new system property page that is assigned to all elements in the SLA Metric Model.

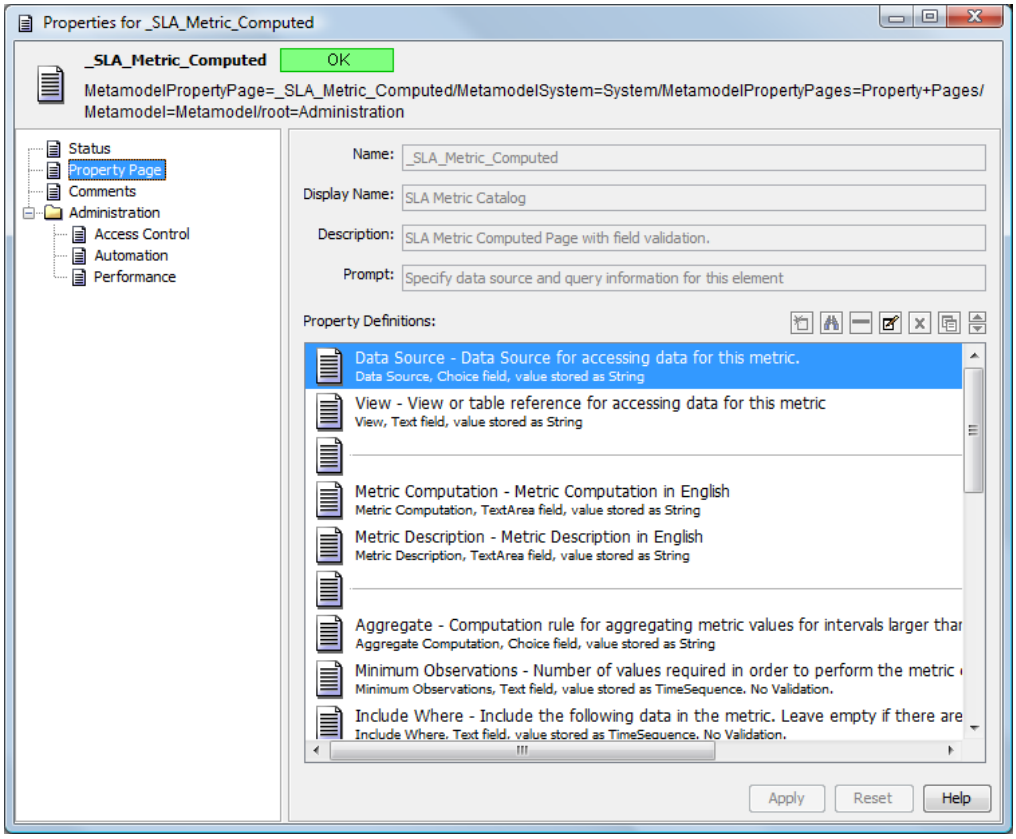
- "Accessing the SLA Computed Property Page" on page 42
- "Adding a Property" on page 42

Accessing the SLA Computed Property Page

To access the SLA Computed property page:

1 In the *Explorer* pane, expand *Enterprise* > *Administration* > *Metamodel* > *Property Pages* > *System*, right-click *_SLA_Metric_Computed*, then select *Properties* to open the properties page.

2 In the left pane, click *Property Page*:



Property names for all properties on the SLA Metric Computed property page are reserved and must be unique. All these property names begin with "SLA_" If you create a different property with the same name as a property in the SLA metric catalog, Operations Center does not behave as expected.

Properties cannot be added to this page, but they might be modified.

Adding a Property

1 Click (*Edit the Selected Property*).

When this page is assigned to an element, the values for each of these properties appear on the SLA Metric Catalog properties for an element. The SQL Monitor property shows the *SQL Monitor* option on the SLA Metric Catalog properties page of an element.

For more information on property pages, see "Viewing Element Properties" the *Operations Center 5.5 User Guide*.

3.2.3 Managing the SLA Metric Catalog Properties

The SLA Metric Catalog properties create an SQL statement that Operations Center uses to acquire custom properties for the element from an external data source and evaluate the properties to determine a key metric. The key metric can then be used to determine SLA compliance by defining a calculation objective for the element based on the SLA Metric Catalog properties.

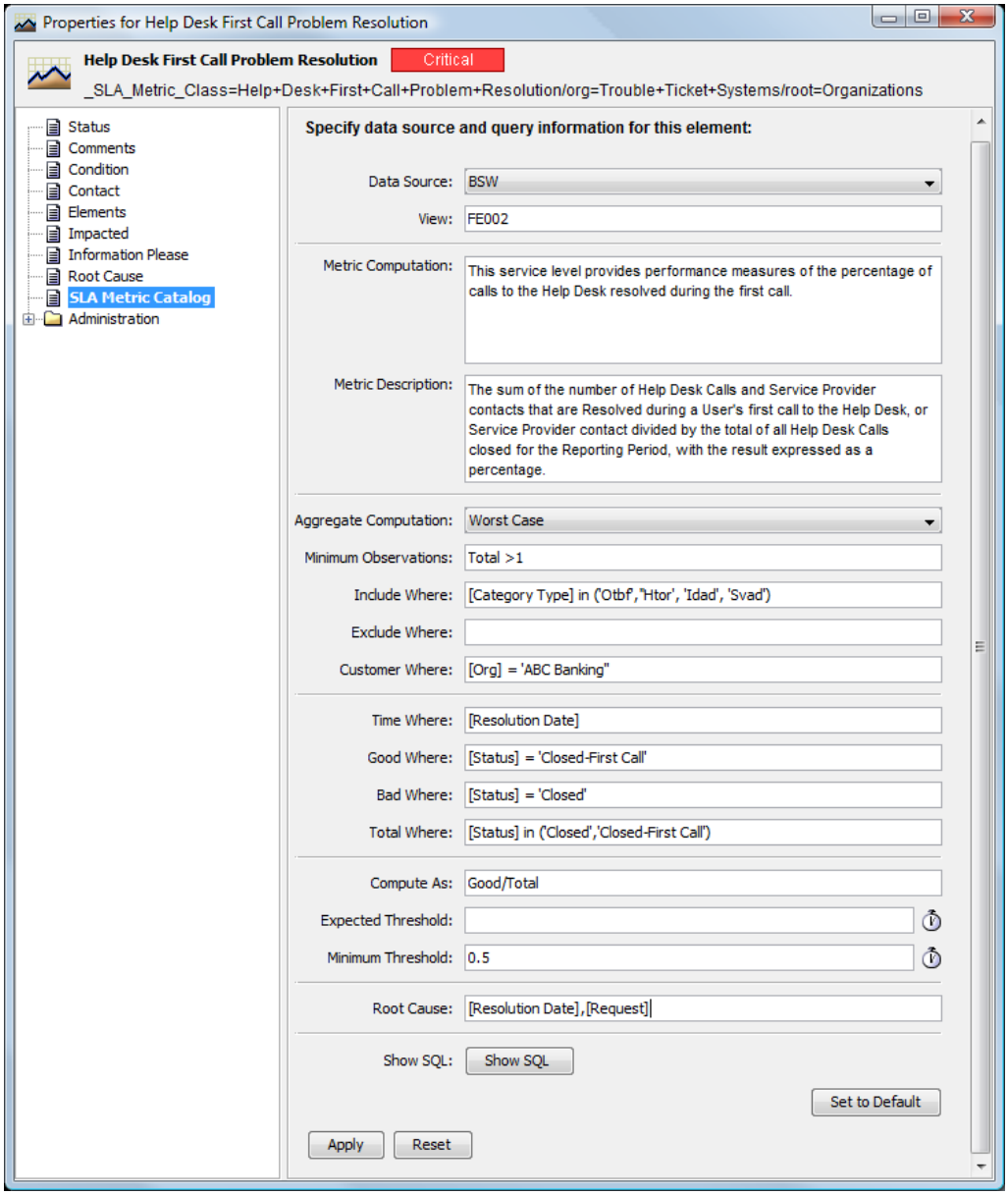
Property pages are not inherited, so each element for which you want to set a calculation objective based on the SLA Metric Catalog properties must have the SLA Metric Catalog properties assigned to it.

- "Accessing the SLA Metric Catalog Properties" on page 44
- "Viewing the SQL Statement and Results" on page 47
- "Executing the SQL Statement" on page 47

Accessing the SLA Metric Catalog Properties

To access the SLA Metric Catalog properties for an element:

1. Locate that element in the hierarchy in the Operations Center console, right-click it, then select *Properties*.
2. In the left pane of the properties page, click *SLA Metric Catalog*:



The SLA Metric Catalog properties are defined as follows by default:

Property Field	Definition
Data Source	The data source for calculating the metric. Select a value from the drop-down list, which includes all databases connections defined in Operations Center, such as all the Database Definitions listed under *Administration* in the hierarchy in the Operations Center console. This field is required.
View	The view or table for accessing the data for calculating the metric. This field is required.
Metric Computation	A text description of how the metric is calculated. This field is required.
Metric Description	A text description of what the metric is calculating. This field is required.
Aggregate	Computation rule for aggregating metric values for intervals larger than the objective interval, which is monthly. This field is required.
Minimum Observations	Number of values required before the metric can be calculated. For example: `[property name COUNT] > 3` Leave empty if no minimum is required.
Include Where	The columns and sets of values that must be met in order to include the data in the metric calculation. Leave empty if there are no inclusions.
Exclude Where	The columns and sets of values that must be met in order to exclude the data in the metric calculation. Leave empty if there are no exclusions.
Customer Where	The columns and sets of values that determine the relevant customer (for example, organization or business unit). Leave empty if there are no inclusions.
Time Where	The columns that should be used to select metric data for calculating results during a time period. For example, the calculation might be performed based on the time that a trouble ticket is closed or a transaction completes. Between is not supported. This field is required.
Good Where	The set of values that are considered good or successful.

Property Field	Definition
Bad Where	The set of values that are considered bad or failures. Used to determine Root Cause failures. This field is required.
Total Where	All the values (good and bad) that are included in the metric calculation.
Compute As	Computational algorithm for the actual metric calculation. It can reference other properties on the page and combine those properties with standard SQL functions to perform a calculation. Use {property} with SQL computations, such as {Good COUNT}. This field is required.
Expected Threshold	Computational algorithm that defines the expected threshold that the computed results must meet or exceed or the metric is breached. Use {property} with SQL computations, such as {Good COUNT}. This field supports multiple values over time.
Minimum Threshold	Minimum acceptable value for this metric. If not met, the objective fails. This field supports multiple values over time. This field is required.
Root Cause	Root cause detailed list of failures for this metric. Specify column values to include. This field is required.

For fields that support multiple values over time (such as *Expected Threshold* and *Minimum Threshold*), the field displayed in the SLA Metric Catalog properties is the current value of that property.

3 To set additional values, click  to the right of the property field to open a dialog box.

4 To define a new interval value and specify in which objective interval the new value is applicable, click  (*New*).

For example, specify one threshold to apply for the first objective interval or month and a second threshold to apply after the first interval completes. When defining a new interval value, enter either a number to indicate the month or an actual date in the format of mm/dd/yyyy. The system calendar is referenced to determine the start of the interval.

5 After defining SLA Metric Catalog properties, review the SQL code that Operations Center created to determine if there are any errors.

Also view the results that Operations Center receives from the SQL query.

Viewing the SQL Statement and Results

To view the SQL statement and results, click *Show SQL*.

The *Show SQL* button is available by default and is specified as the SQL Monitor property on the SLA Metric Computed property page.

The *SQL* tab of the SQL Console dialog box shows the SQL statement. Any errors in the statement appear in red. The amount of time the query took is also stated.

Executing the SQL Statement

1. To execute the SQL statement, select one of the following for the time frame:
   - *Today*
   - *Yesterday*
   - *This Week*
   - *Last Week*
   - *This Month*
   - *3 Months* (includes the current month)
   - *6 Months* (includes the current month)
   - *Custom*, then select a start date and end date
2. On the *Rows* tab, specify the number of rows to be displayed.

   The default is 100. The rows display the good, bad, and total values returned from the query.

   The display of all numeric data is precise to 8 digits to the right of the decimal place. However, the calculation is precise down to the full data precision. Therefore, sometimes the results might not look correct because the display shows numbers that have been rounded.

4 Defining SLAs

A Service Level Agreement (SLA) is an agreement to meet a specific level of service for a business service.

A health grade is calculated for an SLA to determine compliance. The health grade is based on requirements or objectives that have quantifiable measurements. For more information on how to define objectives, see Chapter 5, "Defining Objectives," on page 61.

Define and maintain SLAs in the Operations Center console. It is possible to use SLAs defined on other Operations Center servers; these are called remote SLAs (see Chapter 8, "Remote SLA Reporting," on page 119). It is possible to override SLA settings for child elements, if necessary.

After an SLA is defined, there are options for monitoring its status and reporting its metrics:

Note that users must have *Define* permissions to create or modify SLAs. For more information about permissions, see the *Operations Center 5.5 Security Management Guide*.

4.1 Defining SLAs

SLAs are defined based on elements in Operations Center.

4.1.1 Defining, Viewing, and Editing SLAs for an Element

To define or access SLAs for an element:

1. In the *Explorer* pane, right-click an element, then select *Properties*.
2. In the left pane of the properties page, expand *Administration* > *Service Level Agreements*.

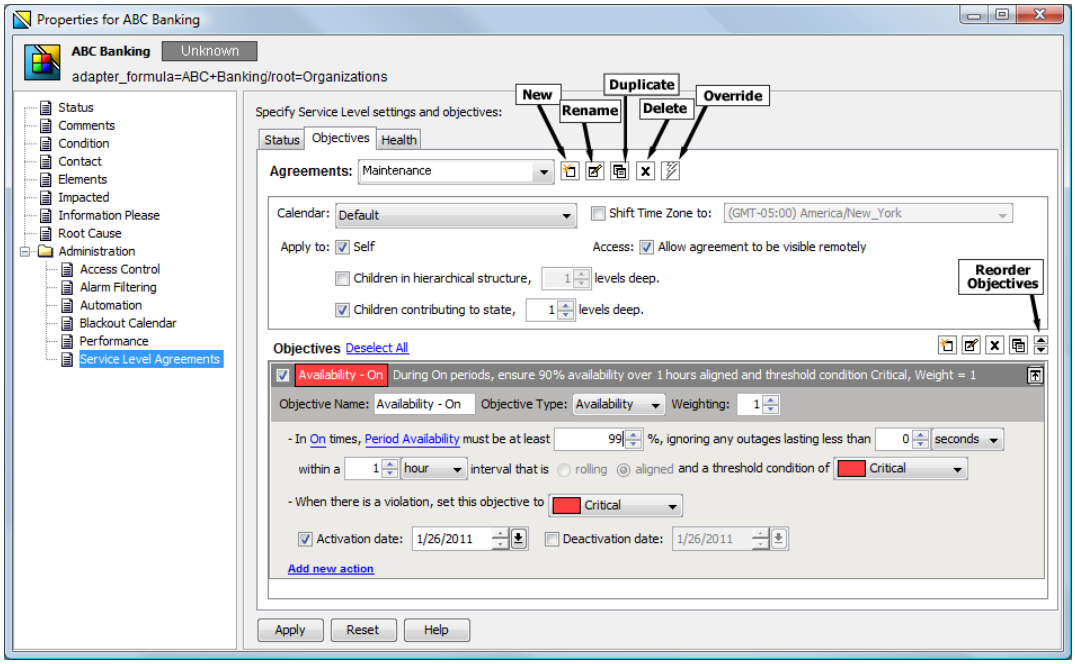
   A list of existing agreements displays in the right pane.

   In addition to the property page of elements, all existing SLAs are displayed in the *Explorer* pane under *Enterprise* > *Service Level Agreements*.

4.1.2 Creating an Agreement

To create an agreement:

1. Click the *Objectives* tab:



2. Click *New* next to *Agreements* to start a new agreement using default values.
3. When prompted for the new agreement name, think carefully before creating one.

   Duplicate agreement and objective names are allowed, so consider how the objective and SLA should appear in a report. Also, it is possible to rename an agreement during its creation. After an agreement is created, it cannot be renamed.
4. To define the following settings on the *Objectives* tab:
   - Click the *Calendar* drop-down list, then select a calendar to apply to the agreement.

     For more information, see Section 4.1.3, “Calendar,” on page 51.
   - Select a time zone to apply to the agreement, if a different one than the default is required.

     For more information, see Section 4.1.4, “Setting Time Zones,” on page 51.

- Specify the elements to which the SLA applies.

  For more information, see Section 4.1.5, “Selecting Elements,” on page 52.
- Define the objectives and the order of the objectives to be evaluated.

  For more information, see Section 4.1.6, “Ordering of Objectives,” on page 52 and Chapter 5, “Defining Objectives,” on page 61.

5 Specify health calculation rules on the *Health* tab.

6 Click *Apply*.

4.1.3 Calendar

The selected calendar is applied to the agreement and all its objectives to calculate real-time service level health and metrics. A different calendar can be applied.

For each objective, assign a time category from the calendar to indicate when collected data is used to measure that objective.

4.1.4 Setting Time Zones

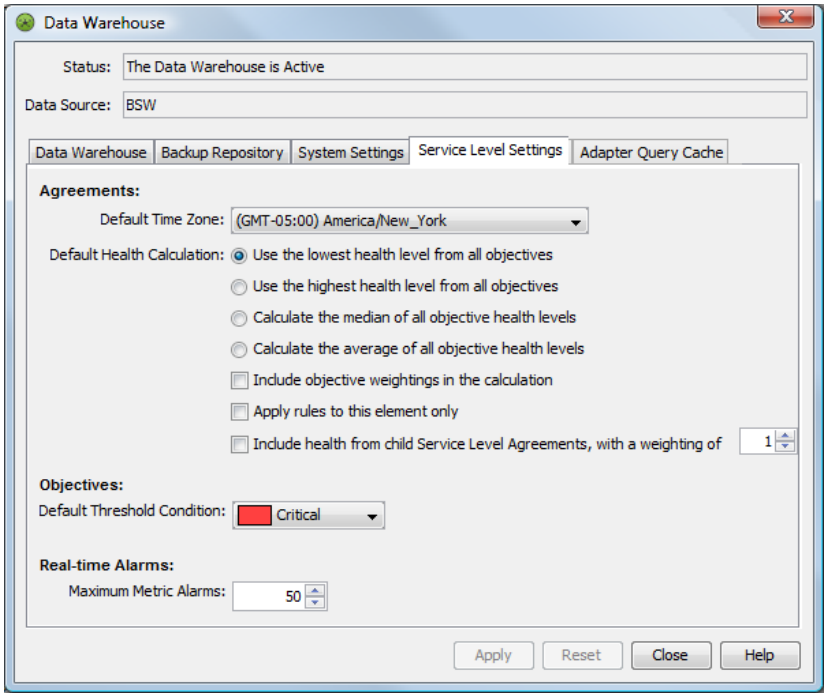
The time zone is set by default for all SLAs in the Business Service Warehouse. It is possible to override the time zone for a particular agreement by selecting the *Shift Time Zone To* check box, then selecting a different time zone.

To set the time zone global default setting:

1 Expand *Enterprise* > *Administration*, right-click *Data Warehouse*, then select *Properties*.

2 Click *Data Warehouse*.

3 In the Data Warehouse property page, click the *Service Level Settings* tab.



4 Select a time zone for the *Default Time Zone* option.

5 Click *Apply*.

4.1.5 Selecting Elements

When defining the SLA, select the elements to which it applies.

The options to apply the SLA to the element on which it is defined and its children are as follows:

- **Selected element (Self):** By default, the SLA applies to the element on which it is created. If the SLA is not applied to this element, then SLA data, such as outages, do not include the element even if the element's children are included.
- **Children in hierarchal structure:** If the agreement is defined for an element in the *Services* hierarchy, then this agreement applies to all elements that naturally exist in the hierarchy, regardless of whether they contribute to the state of the parent element. If the agreement is on an element in the *Elements* hierarchy, then this agreement applies to all elements that are natural children of the parent element. Select the number of levels in the hierarchy to apply the agreement.
- **Children contributing to state:** This agreement applies to all elements that have been matched or linked under the element and those elements that contribute to state but are not natural children of the element. Select the number of levels in the hierarchy to apply the agreement.

If you select both children in hierarchal structure and children contributing to state, then the children in the hierarchal structure are evaluated first followed by the children contributing to state.

4.1.6 Ordering of Objectives

Creating objectives requires understanding the various objective types and options. For more information, see Chapter 5, "Defining Objectives," on page 61.

After creating and assigning objectives to an SLA, consider the order of the objectives. Objectives are applied in the order they are listed on the *Objectives* tab. After an objective is found in violation, the agreement condition is updated without regard to remaining objectives. When ordering objectives, place the most restrictive (most likely to be violated) objectives first, followed by increasingly broader objectives. This way, service level breaches and breach warnings are issued in a timely manner prior to evaluating all objectives.

Use the  up and down arrow icons to reorder objectives in the *Objectives* section of the Service Level Agreements property page.

4.2 Defining Health

Operations Center uses health as a measurement for whether the SLA is in or out of compliance.

4.2.1 Understanding Health

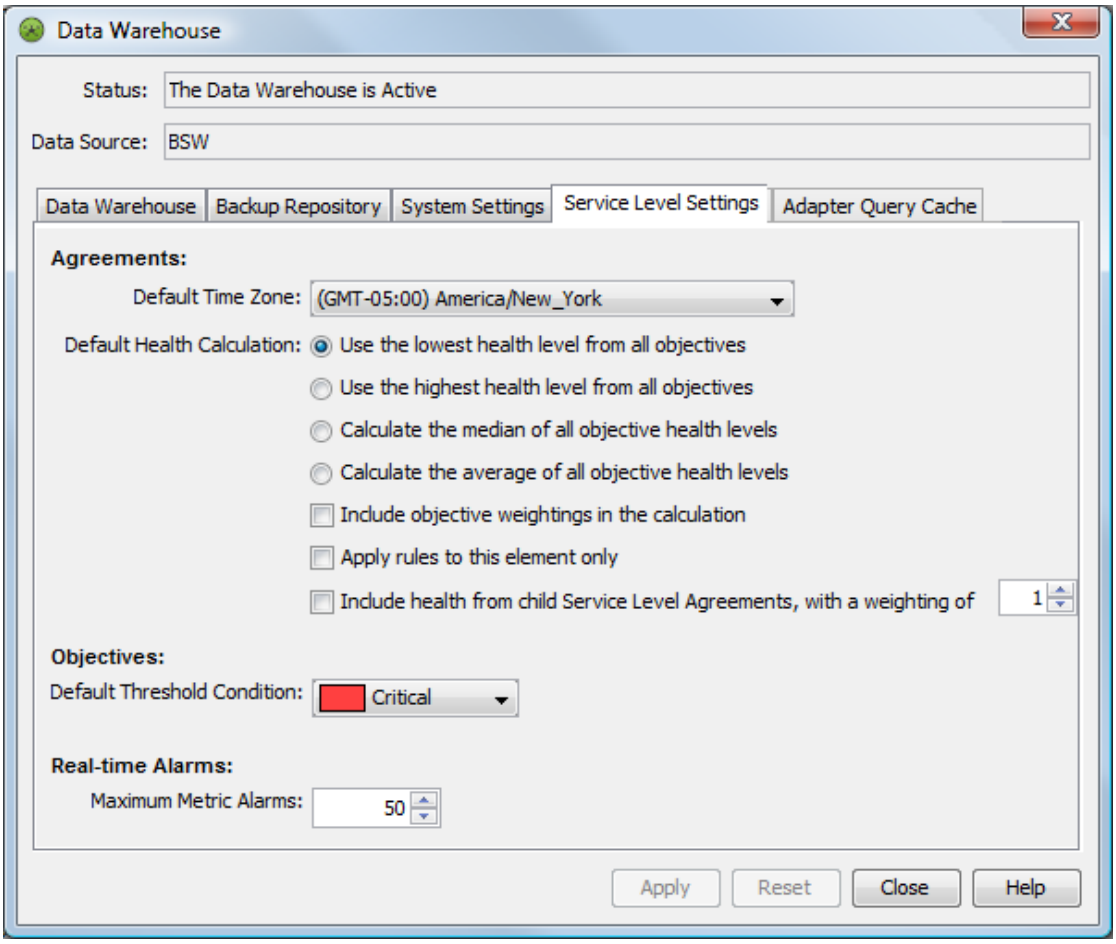
Agreement health is like a car's gas gauge. Rather than just notify you that the gas tank is empty, it indicates how much gas remains in the tank and provides key information, alerting you when you are running low on gas and need to fill up.

Compliance is considered in violation when agreement health is at 49%. Before a violation occurs without any indication, a warning breach alarm is issued at 75% so that appropriate measures can be taken to avoid the violation.

Health of the SLA is based on the health of the objectives. There are rules for calculating health of the SLA as well as factors that influence the calculation.

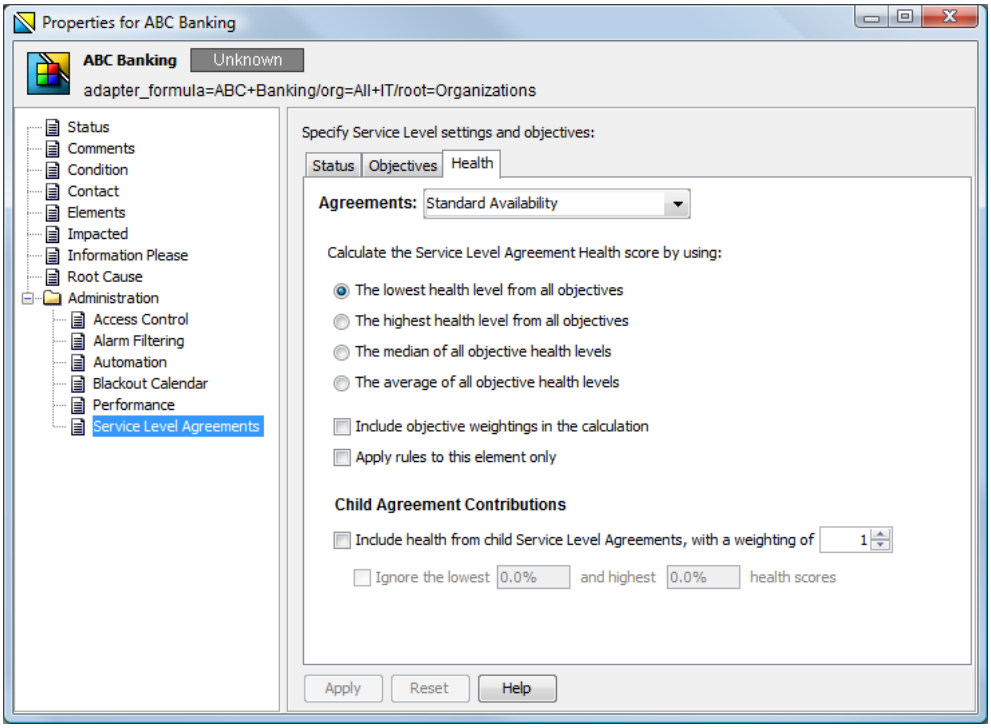
Global default health rules can be set that apply to all SLAs on the Operations Center server. These rules are set in the properties of the Data Warehouse. In the Explorer, expand *Enterprise* > *Administration*. Right-click *Data Warehouse* and select *Edit Data Warehouse Settings*. Click the *Service Level Settings* tab.

Figure 4-1 *Set Global Default Rules in Data Warehouse Settings*



Health calculation rules can also be set for each SLA. Rules that are set on the individual SLA override the global health calculation rules. Health calculations are set on the *Health* tab of the Service Level Agreements property page in the element's *Properties*.

Figure 4-2 *Health Calculation Rules on the Health Tab of a Service Level Agreement Property Page*



4.2.2 Understanding the Mathematical Functions

Health for an SLA is calculated based on the health of all its objectives. The mathematical function for the calculation can be one of the following:

- **Lowest:** Takes the lowest health calculation from all objectives and uses it for the agreement health score
- **Highest:** Takes the highest health calculation from all objectives and uses it for the agreement health score
- **Median:** Calculates the median from all objectives and uses it for the agreement health score
- **Average:** Calculates the average from all objectives and uses it for the agreement health score

By default, lowest is used.

4.2.3 Setting Objective Weightings

Some objectives in the SLA might have greater importance than others. To reflect this in the health calculation, assign weight values to each objective. On the *SLA Health* tab, select the check box to include the objective weightings in the calculation.

For example, if there are three objectives with a weighting of 1 set for two objectives and a weighting of 2 set for the third objective, start by looking at the health and applied weighting of all:

- Objective A's health = 95 (weighting = 1)
- Objective B's health = 99.6 (weighting = 2)
- Objective C's health = 98.5 (weighting = 1)

Next, apply the weightings to the objective health, then divide by the sum of the weightings to calculate the average health score, as follows:

((1 * 95) + (2 * 99.6) + (1 * 98.5)) / (1 + 2 + 1) = 98.175

To set weighting values on an objective:

1. On the Service Level Agreements property page of an element, click the *Objectives* tab.
2. In each objective, find the *Weighting* option.
3. Set the option to a whole number.

4.2.4 Understanding Child SLA Health

The health scores of agreements assigned to all child elements of the parent element can be included in the health calculation for the parent agreement. The impact on the calculation is as follows:

- **Lowest:** The lowest child agreement health is evaluated against the health of the objectives on the parent to determine lowest health score.
- **Highest:** The highest child agreement health is evaluated against the health of the objectives on the parent to determine the highest score.
- **Median:** The median is calculated based on all child agreement health scores and the health of the objectives on the parent.
- **Average:** The average is calculated based on all child agreement health scores and the health of the objectives on the parent.

The health score for each child objective can be assigned a weighting value, similar to the weighting values for the objectives on the parent.

Exclude a range of values in the child agreements from the health calculation by specifying the lowest and highest health scores to ignore. The health scores should be a percentage.

4.2.5 Applying Rules

To prevent health rules set on the current element from applying to other elements in the hierarchy, select the *Apply Rules to This Element Only* check box.

4.2.6 Configuring Health Grades

Agreement and objective health are mapped to a health grade, which gives a clearer indication of the state of health. The health grade gives some idea of whether the objective is fully in compliance or getting close to failure. The health grade for objectives is reflected in service level metric and breach alarms, and in some service level reports where agreement and objective health are mapped to a health grade.

The default grade mappings are as follows (the upper bounds are not inclusive):

- A+ 93.3 – 100 (inclusive)
- A 86.6 – 93.3
- A- 80 – 86.6
- B+ 76.6 – 80
- B 73.3 – 76.6
- B- 70 – 73.3
- C+ 66.6 – 70
- C 63.3 – 66.6
- C- 60 – 63.3
- D+ 56.6 – 60
- D 53.3 – 56.6
- D- 50 – 53.3
- F <50

To customize these ranges:

1. In a text editor, open the */OperationsCenter_install_path*`/config/Formula.custom.properties` file.
2. Add the `Formula.GradeString` parameter and customize as necessary.

   For example, the above default settings is set with the following definition:

   ```
   Formula.GradeString="A+ 93.3 A 86.6 A- 80 B+ 76.6 B 73.3 B- 70 C+ 66.6 C 63.3
   C- 60 D+ 56.6 D 53.3 D- 50 F"
   ```

   As another example, the following could also be defined:

   ```
   Formula.GradeString="Good 80 Acceptable 70 Poor 60 Unacceptable 50 Failed"
   ```
3. Stop and restart the Operations Center server for the changes to take effect.

For information on creating and editing the `Formula.custom.properties` file, see "Making Custom Changes" in the *Operations Center 5.5 Server Configuration Guide*

4.3 Copying SLAs

To copy an SLA to create a new SLA:

1. In the *Explorer* pane, right-click an element, then select *Properties*.
2. Under *Administration*, click *Service Level Agreements*.
3. In the Service Level Agreements property page, click the *Objectives* tab.

4 Click the *Agreement* drop-down list, then select an agreement.

All agreement settings and objectives display in the *Objectives* tab.

5 Click *Duplicate Agreement*.

A duplicate agreement is created.

6 To rename the agreement, click *Rename Agreement*.

7 Specify a name for the agreement in the *Agreement* field.

8 Make the necessary changes to the settings and objectives.

9 Click *Apply* to save the new agreement.

4.4 Overriding SLAs

Because requirements for an agreement might vary (or be more or less demanding) for child elements, it is possible to adjust agreement settings at a selected level with an agreement override.

For example, you might want to change the calendar and/or time zone associated with a portion of the hierarchy, or you might want to add or remove objectives for a portion of the hierarchy.

To override agreement settings for a specific element:

1 In the *Explorer* pane, right-click an element in the *Elements* or *Services* hierarchy, then click *Properties*.

2 Under *Administration*, click *Service Level Agreements*.

3 In the Service Level Agreements property page, click the *Objectives* tab.

4 Click the *Agreement* drop-down list, then select an agreement.

All agreement settings and objectives display in the *Objectives* tab, but are dimmed out (unavailable for editing).

5 Click *Override Agreement*.

6 Make the necessary changes to the agreement and/or objectives.

If necessary, define new objectives.

7 Click *Apply* to save the override for the agreement.

4.5 Understanding Deleting SLAs and Elements with SLAs

You can delete an SLA that is applied to an element. You can also delete elements to which SLAs are applied. Because of the deletion, service level reports might have difficulty accessing the information.

- Section 4.5.1, "Understanding Deleting Agreements or Objectives," on page 58
- Section 4.5.2, "Understanding Deleting Elements with Agreements," on page 58

4.5.1 Understanding Deleting Agreements or Objectives

When an agreement definition is modified or deleted, existing service level data is retained in the Business Service Warehouse. However, because service level reports are run only on current or active service level definitions, any deleted agreement or objective definitions are not displayed in the service level reports.

In order to reproduce the previous service level reports for the deleted agreement, re-create the agreement or objective definition using its preexisting settings. Because reports are generated based solely on the settings of the current agreement or objective definition if new settings differ from the preexisting agreement, the report results are different because they are based on the new and current settings.

All service level metric data previously captured (for example, availability, downtime, outage, key performance metric values) is retained in the database and can be referenced again when the agreement or objective definition is recreated.

However, as no new data is captured from the point when the agreement or objective definition is deleted until it is re-created, gaps can exist when no data is available—particularly for key service level metric data (such as data evaluated using a custom objective). Availability, downtime, and outage data might be available if another agreement exists on the element.

4.5.2 Understanding Deleting Elements with Agreements

When an element with an applied agreements is deleted, existing service level data is retained in the Business Service Warehouse. However, the element must exist in order for the data to appear in service level reports. Recreating the deleted element with its preexisting name enables the service level reports to display any existing service level data in the Business Service Warehouse.

When using Business Service Configuration Manager (BSCM), be careful not to define agreements directly on the elements produced by BSCM, unless BSCM is set to not delete the elements during a scheduled generation process. Otherwise, the agreements are deleted whenever BSCM executes.

4.6 Viewing SLAs and Understanding the SLA Hierarchy

SLAs display in the Operations Center console both in the hierarchy under *Service Level Agreements* and as a property of the elements to which they are applied.

Although agreements and objectives are set at the element level, the Service Level Agreements root element displays defined agreements and objectives. The *Service Level Agreements* hierarchy shows all service agreements, all objective definitions, all overrides, and all elements under the agreement's umbrella.

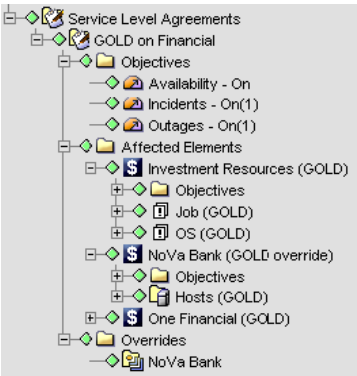
For each agreement, there are three branches that provide different ways of monitoring the status of the SLA. They include:

- **Objectives:** Each objective defined in the agreement regardless of where in the hierarchy it is defined.
- **Affected Elements:** The complete element structure for all elements contained within the agreements umbrella. As you drill-down through the hierarchy, each element has an *Objectives* folder showing all objectives that apply to it.
- **Overrides:** Any change (or override) made on any objective on any point of the hierarchy. This change affects elements in the *SLA* hierarchy from that point down.

Each element shown in the *Affected Elements* branch of the *Service Level Agreements* root element has a unique naming convention of: `AgreementName on elementName`.

This naming syntax clearly shows which instance of the element is being viewed. This is useful in a Business Service View where an element from the *Service Level Agreements* tree was dragged and dropped into a view. The naming syntax indicates the status and information is related to the agreement and not to the element itself.

Figure 4-3 *Hierarchy in Explorer Pane in Operations Center console*



In Figure 4-3, GOLD is the only Service Level Agreement that was set up on the *Financial* element. It has three objectives at this time—one for availability, one for incidents, and one for outages.

Under the *Financial* element, there are three children included in the agreement (*Investment Resources*, *NoVa Bank*, and *One Financial*), as well as their children, which are technology elements from adapters. There is one override on the agreement, set on the *NoVa Bank* element.

Table 4-1 lists useful options that are available on the *Service Level Agreements* elements' right-click menu.

Table 4-1 *Element Right-Click Options*

Option	Available on…	Description
Go To Element	Agreements, objective, overrides, and affected elements	Shifts *Explorer* pane focus to the element where the agreement, objective, or override was set.
Show Details	Agreements, objectives, and overrides	Opens agreement, objective or override properties.
Show Root Cause	Affected elements	Opens Root Cause information.

5 Defining Objectives

An objective, formally known as an Operational Level Agreement (OLA), is a requirement that must be met. A series of objectives make up a Service Level Agreement (SLA).

To define objectives:

5.1 Understanding Objectives

To determine whether a requirement has been met, the requirement must be evaluated using measurable data. Generally, the types of data are:

- Availability
- Downtime
- Outages
- Incidents

In Operations Center, you can define an objective for each of these, as well as for any piece of data on which you can perform a calculation. In addition, you can use the health of an SLA as an objective to consider in another SLA. Table 5-1 summarizes objectives.

Table 5-1 *Objective Types*

Type	Specifies…
Availability	A threshold minimum that availability must be equal to or above in order to be compliant within the selected interval of time. The threshold setting defaults to Critical.
Downtime	An acceptable level of total time down within the selected objective interval of time. The threshold setting defaults to Critical.
Incidents	The maximum number of incidents (of specified duration) allowed to be compliant within the selected objective interval of time. The threshold setting defaults to Critical.
Outages	The maximum number of outages (of specified duration) allowed to be compliant within the selected objective interval of time. The threshold setting defaults to Critical.
Agreement	An aggregate type calculation for agreement health that factors in health values from another Service Level Agreement, where applicable for associated elements. Select from other Service Level Agreements defined for that branch of elements.
Calculation	The Calculation objective either performs a mathematical calculation to determine if a property is compliant, or determines if a key metric based on custom properties of an element in an external data source is compliant.

You select the type of objective when you create or edit an objective.

The common features of all objective types are:

- Activation and deactivation dates
- Time intervals
- Threshold condition

5.2 Creating an Objective

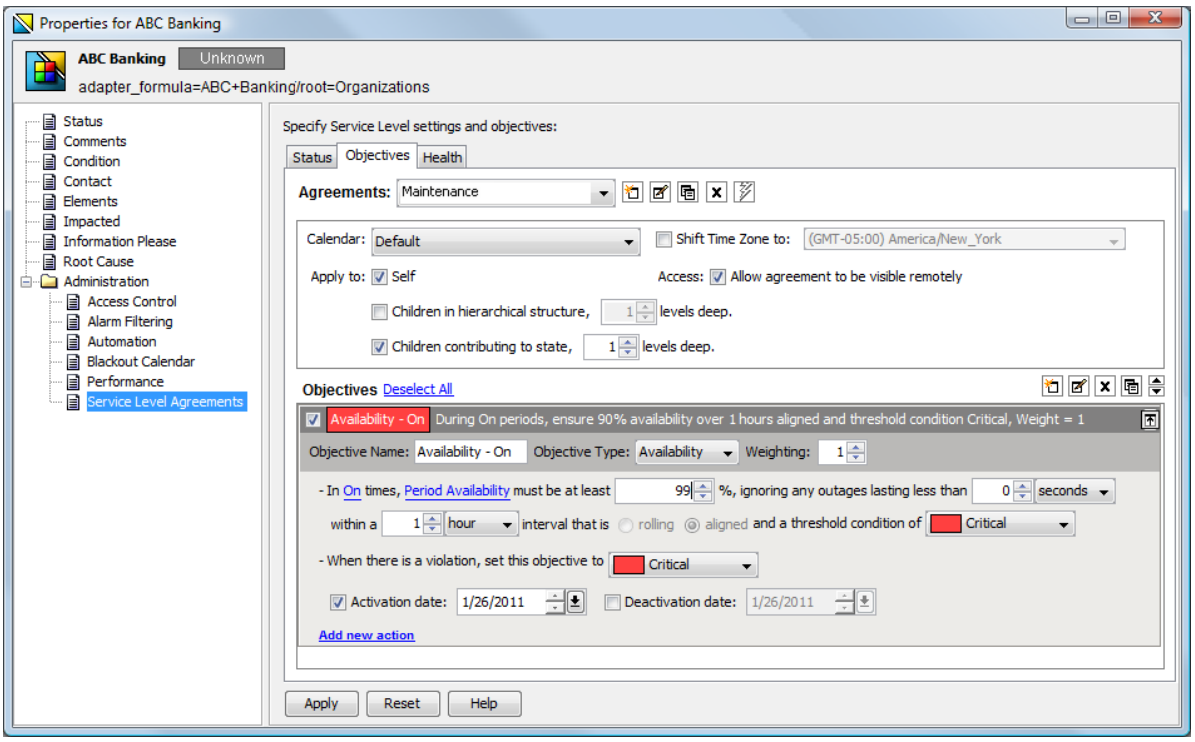
Objectives are created as part of SLAs. Carefully consider the name of the objective before creating it. It is possible to rename an objective while creating it, but renaming is not allowed after it is saved.

After an objective is named and saved, the name cannot be changed.

Poorly defined objectives can result in an infinity value for service level metrics. For example, assume an objective is defined to calculate a percentage and the threshold is set as greater than 1.0 or 90.0. The threshold is illogical because the results should always be between 0 and 1. However, configuring the threshold to be greater than 100% or 90% makes sense. Operations Center can convert a percentage value to 1.0 or .90.

After an objective is created, it is possible to disable it, edit it, or make a duplicate copy to use as the basis for creating a new objective. These functions are accessed through icons on the *Objective* tab in the Service Level Agreements property page.

Figure 5-1 *Objectives Tab of Service Level Agreements Property Page Showing One Existing Objective*

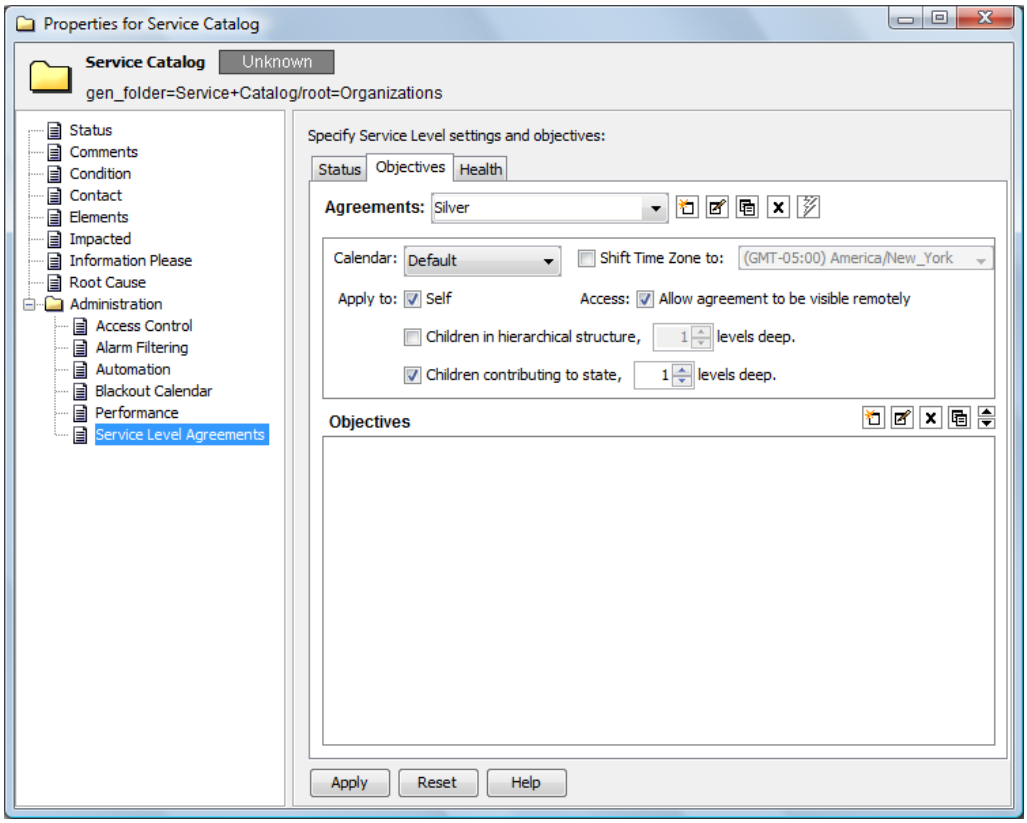


After an objective has been defined, it appears on the *Objectives* tab of the Service Level Agreement property page for the element for which the SLA applies. To show and hide the details of objectives, double-click the title bar of the objective.

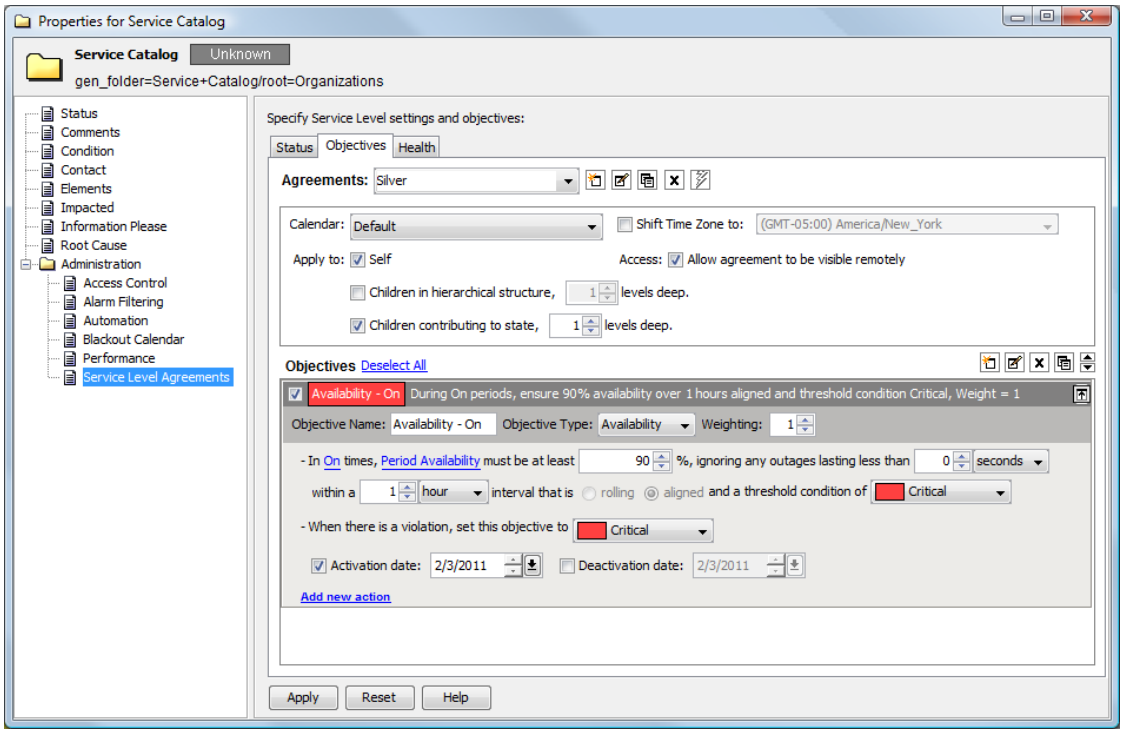
For information on the options to select when defining a new objective or editing an objective, see the section below for the specific type of objective.

To create an objective:

1. In the *Explorer* pane, browse to an element, right-click the element, then select *Properties*. The Properties dialog opens.
2. Under *Administration*, click *Service Level Agreements*.
3. In the Service Level Agreements property page, click the *Objectives* tab.



4 On the *Objectives* toolbar, click *New Objective*.



5 Complete the settings for the new objective, as applicable for the objective type.

6 Click the *Threshold Condition* drop-down list, then select the condition level that the element must reach before outage calculations begin.

7 Click the *Add New Action* link to define actions that are performed when a violation occurs for the objective.

8 Use the up and down arrow icons to reorder objectives.

9 To save changes at any time, click *Apply*.

5.3 Understanding Activation and Deactivation Dates

All objectives have an optional activation and deactivation date. The activation date specifies when the objective is active (or started). The deactivation date specifies when the objective is inactive (or ended). In essence, the activation and deactivation dates are the effective start and end dates, respectively.

The activation/deactivation dates allow creating objectives to match the start and end dates specified in the contract for the SLA. It is possible to create objectives before you need to begin monitoring the SLA by setting the activation date.

A deactivation date, in essence, retires an objective. After retired, an objective no longer executes and real-time data is no longer generated. However, historical data related to the objective is retained and can be used in reports in the Operations Center dashboard. In contrast, when an objective is deleted, the historical data related to that objective is also deleted and is no longer available for reporting purposes.

By default, the activation and deactivation dates show the current date, but are not selected. These fields are not required. If the activation and deactivation dates are not set, then the current objective definition settings are always applied.

The activation date can be set in the past, as the present day, or in the future. If the activation date is set to a date in the past, Operations Center attempts to generate the objective status based on past data already collected. If the activation date is set in the future, then until that date occurs the objective does not fire in real time and reports for data related to the objective show `NA` (not applicable). If only an activation date is set, then the current objective definition settings are used until the objective definition is updated with a new activation date.

An activation date must be selected for a deactivation date to be selected. The deactivation date can be a past day, the present day, or a future day. If the deactivation date is set in the past, then the objective never fires in real time and reports for data related to the objective always show `NA` (not applicable).

If both the activation and deactivation dates are set, then the objective definition is applicable only between those two dates. The last version of the objective definition settings apply for the entire period specified.

5.4 Understanding Time Intervals

For all objectives except the Agreement objective, it is necessary to specify a time interval.

The time interval is the span of time during, which the objective measures and calculates values.

The interval can be 1 or more minutes or hours, 1 day, 1 week, or 1 month. The interval must be a positive number greater than zero. If specifying minutes, 60 must be evenly divisible by the specified number of minutes. For example, 5 minutes is valid, but 7 minutes is not. If the interval is hours, 24 must be evenly divisible by the specified number of hours. For example, 12 hours is valid, but 13 hours is not.

There are two considerations when setting the objective time interval:

- Reporting intervals (see Section 5.4.1, “Reporting Intervals,” on page 66)
- Starting and stopping calculations (see Section 5.4.2, “Aligned vs. Rolling,” on page 67)

5.4.1 Reporting Intervals

Objectives are usually created with a consideration of how the data needs to be reported. If you need to report on availability for the day, week, and month, you could create three different objectives. However, this could result in creating many objectives, which might be confusing when reviewing agreements.

In its reporting capability, Operations Center has an option to select a smaller interval than the one used for the objective. For example, assume an objective is defined using the month interval. When viewing an SLA Status report in the Operations Center dashboard, you can view the availability for a week or day.

5.4.2 Aligned vs. Rolling

Aligned objectives automatically reset when the specified interval completes. For instance, to look at performance for each month, starting at the beginning of the calendar month (the 1st) and ending with the last calendar day of that month, set the interval to 1 month aligned. The objective resets at the beginning of each month. Other aligned objective examples include:

- 1 hour aligned starts at 12:00 and resets at 1:00
- 1 day aligned starts on March 1st at 12:00 AM and resets on March 2nd at 12:00 AM
- 1 week aligned starts on Sunday at 12:00 AM and resets on the next Sunday at 12:00 AM
- 1 month aligned starts on March 1st at 12:00 AM and resets on April 1st at 12:00 AM

Rolling objectives are currently not supported.

Unlike aligned intervals, rolling objectives are continuously evaluated for a specified interval of time. Therefore, to always view the last 24 hours, set the interval to 24 hours rolling, which starts at the present time and ends 24 hours earlier. Rolling objectives reset only when the interval no longer includes conditions that cause the objective to fail. For example, if the service availability is 94.8% for the last 24 hours because of an outage that occurred May 28, from 10:11 AM to 11:26 AM, then the availability objective resets after May 29, 11:26 AM.

5.4.3 Customizing the Weekly Time Interval

By default, the time interval for week starts on Sunday. This can be configured to start on Monday if required.

To customize the start of the week interval:

1. In a text editor, open the `/OperationsCenter_install_path/config/Formula.custom.properties` file.
2. To set the time window to start on Monday, add the following parameter:

   ```
   performance.timewindow.rolltosunday=false
   ```

   Setting this parameter to `true` reverts behavior back to the default of Sunday being the first day of the week.
3. Stop and restart the Operations Center server for the changes to take effect.

For information on creating and editing the `Formula.custom.properties` file, see "Making Custom Changes" in the *Operations Center 5.5 Server Configuration Guide*

5.5 Setting the Threshold Condition

Some objectives (Availability, Downtime, Outages, and Incidents) provide the ability to define a threshold condition at which the objective considers any measured elements or contributing agreements as unavailable (such as the outage conditions).

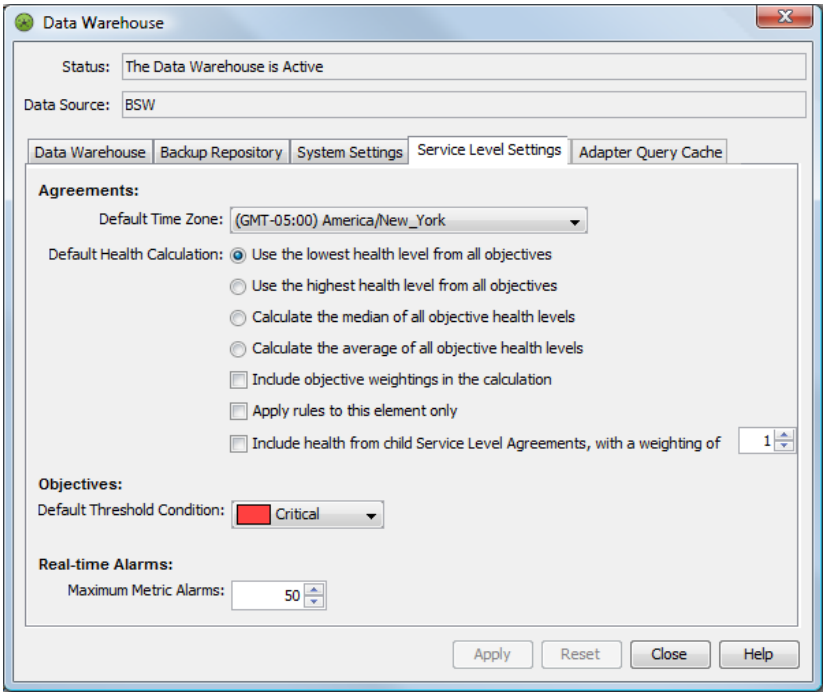
Unknown and unmanaged conditions are treated as available when calculating SLA metrics.

The default threshold condition is Critical for all objectives except incident objectives, and can be modified for each objective based on requirements.

For example, the threshold condition can be set to Major for a service where the service is considered unavailable when the service's condition is Major or Critical.

The global default setting used for threshold condition can be changed in the *Data Warehouse* element's properties.

Figure 5-2 *Global Threshold Condition Setting on Data Warehouse Properties*



To set the threshold condition global default setting:

1. Expand *Enterprise* > *Administration*, right-click *Data Warehouse*, then select *Properties*.
2. In the left pane, click *Data Warehouse*.
3. In the Data Warehouse property page, click the *Service Level Settings* tab.
4. Edit the *Default Threshold Condition* property.

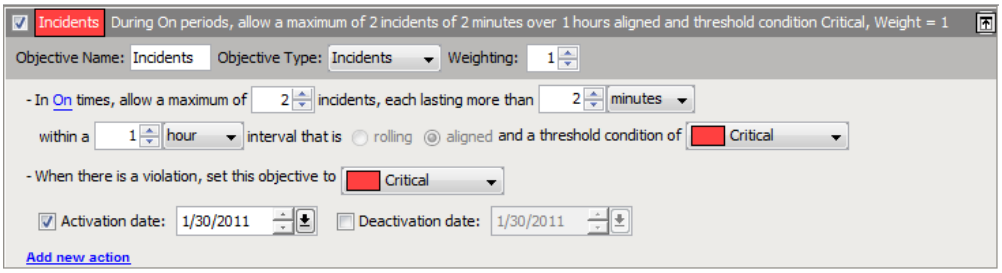
5.6 Defining an Incidents Objective

An incident occurs when an elements condition remains greater than or equal to the threshold condition. By default the threshold is Critical.

The Incident objective specifies the maximum number of incidents and their duration that are allowed for the objective to still be compliant within the selected objective interval of time.

For example: In Peak times, allow a maximum of 10 incidents, each lasting no more than 60 seconds within a 2 hour interval that is aligned and a threshold condition of Major.

Figure 5-3 *Incidents Objective with Default Options*



To define an Incident objective, set the following:

1. **Time Category:** Select a time category during which data is analyzed to determine if an incident occurs. The time category is associated with the calendar for the SLA for which the objective applies.

   Threshold Number: Set the number of incidents allowed before the objective is out of compliance.

   Time for Compliance: For an incident to be counted as part of the objective, it must last a specified amount of time; in other words, the element must be at the specified condition for equal to or greater than the specified amount of time. The default is 15 seconds. You can change this time, which is set as a whole number of seconds, minutes, or hours.

   This option allows discounting minor and occasional blips in performance and target True performance issues.

   Time Interval: The interval in which to calculate incidents. For more information, see Section 5.4, “Understanding Time Intervals,” on page 66.

   Threshold Condition: The element must be at the condition or greater than the condition specified as the threshold for an incident to occur.

Violation Condition: When the objective is out of compliance, the condition of the objective is Critical. You can change this condition. However, changing this condition has absolutely no impact on the state of the objective at any other time (for example, when it is halfway to the failure state). The state of a failed objective has absolutely no impact on the state of the SLA, which is determined by health scores of objective and not state of objectives.

When an objective is halfway to failure, the state of the objective always defaults to Major. For example, if 6 incidents are allowed, when the 3 incident occurs, the objective state changes to Major.

Activation and Deactivation Dates: (Optional) Indicates when the objective starts and ends. For more information, see Understanding Activation and Deactivation Dates (page 65).

5.7 Defining an Outages Objective

An outage occurs when an element goes below a specified condition for a specified amount of time during a period specified. An outage continues as long as the element condition remains equal to or greater than the threshold condition.

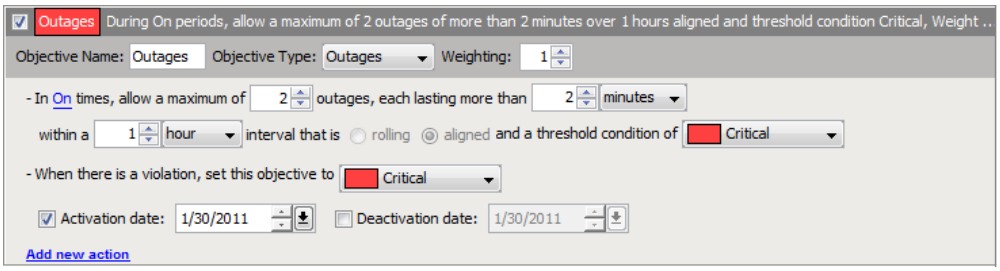
Typically when an element's condition becomes critical, an outage occurs.

If an element reaches or exceeds the threshold condition when the element is scheduled to be unavailable, then the incident is not counted as an outage.

The outages objectives sets the maximum number of outages (of specified duration) allowed to be compliant within the selected objective interval of time. The threshold setting defaults to Critical.

For example: In Peak times, allow a maximum of 10 outages, each lasting no more than 60 seconds within a 1 hour interval that is aligned and a threshold condition of Major.

Figure 5-4 *Outages Objective with Default Options*



When defining the Outages objective, set the following:

1 **Time Category:** Time category specifies when to collect data to use to define outages. The actual time associated with the time category is specified in the calendar defined for the SLA with which the objective is associated.

Threshold for Compliance: The threshold for compliance is the number of outages allowed for the objective to still be in compliance. If that number is exceeded, then the objective might be out of compliance. The default is 0, which means that any time there is an outage it is counted against compliance.

Outages Ignored: By default, every outage regardless of the amount of time it lasts is considered against compliance. Specify an amount of time that an outage must meet or exceed to be counted as an outage for compliance. Specify a whole number of seconds, minutes, or hours.

This option allows discounting minor and occasional blips in performance and target True performance issues. However, if every outage is important and should result in a breach alarm, then leave the default of 0 outages lasting 0 seconds.

Time Interval: The time period in which to calculate availability. For more information, see Section 5.4, "Understanding Time Intervals," on page 66.

Threshold Condition: The threshold is the condition at which the objective considers the element to be unavailable or out. That is, the time that the element is at or below this condition is considered an outage.

The default is Critical. This default can be changed.

When an element has a condition of either `Unknown` or `Unmanaged`, then it is treated as available and not experiencing an outage.

Violation Condition: When the objective is out of compliance, the condition of the objective is Critical. You can change this condition. However, changing this condition has absolutely no impact on the state of the objective at any other time (for example, when it is halfway to the failure state). The state of a failed objective has absolutely no impact on the state of the SLA, which is determined by health scores of objective and not state of objectives.

When an objective is halfway to failure, the state of the objective always defaults to Major. For example, if 6 outages are allowed, when the 3 outage occurs, the objective state changes to Major.

Activation and Deactivation Dates: (Optional) Indicates when the objective starts and ends. For more information, see Understanding Activation and Deactivation Dates (page 65).

5.8 Defining the Downtime Objective

Downtime is the amount of time measured in days, hours, minutes, and seconds (to the thousandths of a second) that an element remains at a specified condition for a specified time interval. That is, downtime is the total elapsed time during an outage.

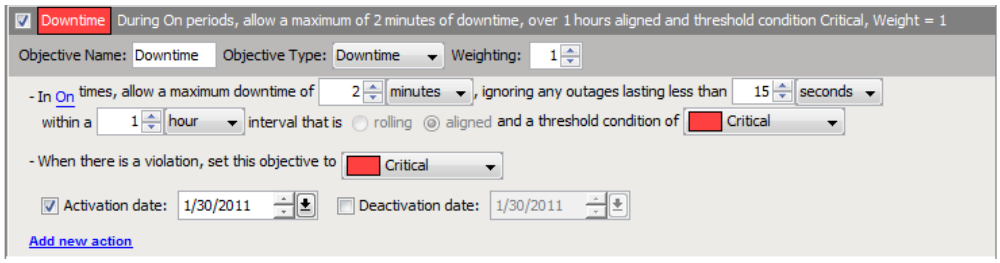
If an elements condition is greater than or equal to the threshold condition, then it is considered down or unavailable. Otherwise the element is considered available. The amount of time that an element is scheduled to be unavailable is not factored into the downtime.

When downtime is calculated for an element based on impact to service, only those outages on child elements that impacted the service for the element are considered.

The downtime objective defines an acceptable level of total downtime within a selected interval of time. Downtime is defined by a threshold condition; the default is Critical.

For example, in On times, allow a maximum downtime of 15 minutes within a 2 hour interval that is aligned and a threshold condition of Critical.

Figure 5-5 *Downtime Objective with Default Options*



To define the Downtime objective, set the following:

Time Category: The time category specifies when to collect data to use to determine the amount of downtime. This time category is associated with a calendar that is specified during the creation of the SLA to which this objective belongs.

Compliance Threshold: The threshold compliance is the maximum amount of downtime that is allowed for the objective to be still in compliance. Designate a whole number of seconds, minutes, or hours.

Outages Ignored: By default, all outages are considered toward downtime.

(Optional) Specify that outages lasting a whole number of seconds, minutes, or hours not be considered part of downtime.

Time Interval: The time period in which to calculate downtime. For more information, see Section 5.4, “Understanding Time Intervals,” on page 66.

Threshold Condition: The threshold is the condition at which the objective considers the element to be down or experiencing an outage. That is, the time that the element is at or below this condition is considered downtime calculation.

The default is Critical. This default can be changed.

When an element has a condition of either `Unknown` or `Unmanaged`, then it is treated as available or up.

Violation Condition: When the objective is out of compliance, the condition of the objective is Critical. You can change this condition. However, changing this condition has absolutely no impact on the state of the objective at any other time (for example, when it is halfway to the failure state). The state of a failed objective has absolutely no impact on the state of the SLA, which is determined by health scores of objective and not state of objectives.

When an objective is halfway to failure, the state of the objective always defaults to Major. For example, if 5 minutes of downtime is allowed, when the outage reaches 2.5 minutes, the objective state changes to Major.

Activation and Deactivation Dates: (Optional) Indicates when the objective starts and ends. For more information, see Section 5.3, “Understanding Activation and Deactivation Dates,” on page 65.

5.9 Defining the Availability Objective

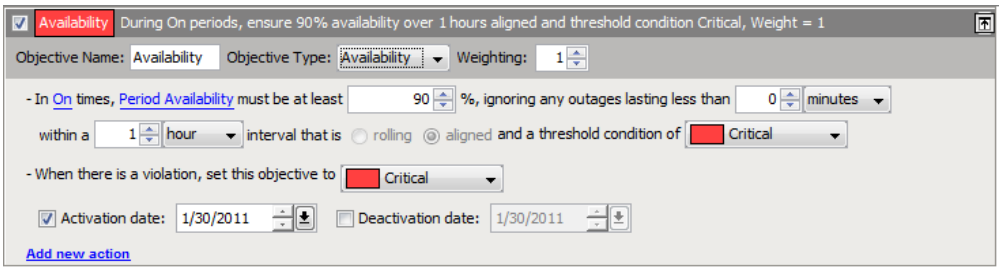
Availability is the amount of time when the condition of the element is not below a specified threshold. It is expressed as the percentage of uptime in comparison to total time as follows:

Availability = (total time-downtime)/total time x 100

The Availability objective defines a threshold minimum that availability must be equal to or above in order to be compliant within the selected interval of time. The threshold setting defaults to Critical.

For example: In On times, the availability basis must be at least 90% within a 1 hour interval that is aligned and a threshold condition of Major.

Figure 5-6 *Availability Objective with Default Options*



When defining the Availability objective, set the following:

Time Category: Time category specifies when to collect data to use to calculate the availability. The actual time associated with the time category is specified in the calendar defined for the SLA with which the objective is associated.

Total Time: Based on either a period or the calendar:

- **Availability:** This is a percentage based on total time. The total time can be calculated one of two ways:
- **Period:** The total is the amount of time in the time category only. In other words, if the objective is monthly and the time category is set to On, then the total time is the amount of time in the On time category, it is not the total time in the month.
- **Calendar:** The total time is the amount of time in the time interval regardless of time categories. In other words, if the time interval is one month and the month has 30 days, then the total time is 720 hours (or 43200 minutes). For the periods not in the time category specified, the availability is considered to be 100%.

Threshold for Compliance: The threshold for compliance is the percentage that the availability can be at or above for the objective to still be in compliance. The default is 90 percent.

For example, if the default is 90 percent and the availability falls below 90 percent than the objective is in violation.

Outages Ignored: An outage occurs when an element goes below the specified threshold condition. By default all outages are considered to contribute to downtime.

(Optional) Remove outages of a specified length from the availability calculation for the objective. Specify a whole number of seconds, minutes, or hours.

Time Interval: The time period in which to calculate availability. For more information, see Section 5.4, “Understanding Time Intervals,” on page 66.

Threshold Condition: The threshold is the condition at which the objective considers the element to be unavailable or down. That is, the time that the element is at or below this condition is considered downtime for the availability calculation.

The default is Critical. This default can be changed.

When an element has a condition of either Unknown or Unmanaged, then it is treated as available for the calculation of availability.

Violation Condition: When the objective is out of compliance, the condition of the objective is Critical. You can change this condition. However, changing this condition has absolutely no impact on the state of the objective at any other time (for example, when it is halfway to the failure state). The state of a failed objective has absolutely no impact on the state of the SLA, which is determined by health scores of objective and not state of objectives.

When an objective is halfway to failure, the state of the objective always defaults to Major. For example, if availability must be above 95%, when the availability slips to 95% or below, the objective state changes to Major.

Activation and Deactivation Dates: (Optional) Indicates when the objective starts and ends. For more information, see Section 5.3, "Understanding Activation and Deactivation Dates," on page 65.

5.10 Understanding the Calculation Objective

The Calculation objective has two purposes:

- To perform a mathematical calculation to determine if a property is compliant or to compare a property value with the threshold value to return a result
- To determine if a key metric defined by an SLA metric catalog using data from an external data source is compliant

For health and compliance, the Calculation objective returns only breaches. Unlike other objectives, the Calculation objective does not produce values for outage counts, outage duration, availability, downtime, or health.

5.11 Calculation Objective for Property or Alarm Severity

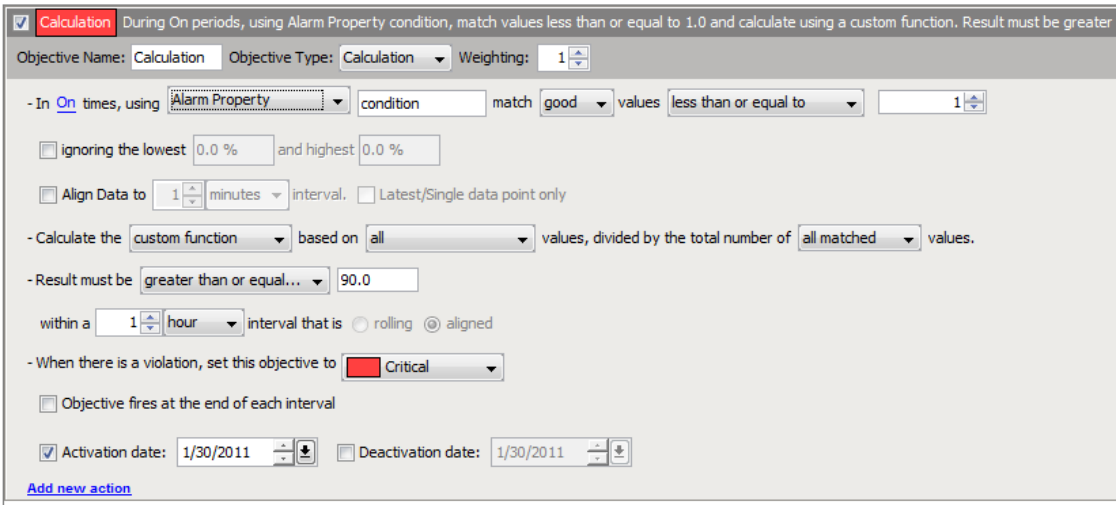
When a Calculation Objective is set for an element property, alarm property, or alarm severity, it uses a mathematical calculation to determine of the element is compliant.

Some general example uses of the Calculation objective's mathematical functions are:

- In Peak times, allow no more than a 5% failure rate on scheduled jobs within a 1 month interval that is aligned (measures Critical alarms issued from scheduled jobs).
- In On times, 80% of employees must be participating in the corporate benefits plan within a 1 month interval that is aligned (measures an alarm property that indicates employee participation in benefits plan).
- In Peak times, average Response Time must be at least 10 seconds within a 1 day interval that is aligned.
- In On times, no more than 20% of Critical alarms must have a trouble ticket issued after 10 minutes within a 1 month interval that is aligned (measures an alarm property that indicates the length of time taken to create the trouble ticket after the alarm was issued).
- Average response time metrics are measured on a daily basis. Monitor that daily average response time must stay under 5 minutes within a month.

- Trading volume metrics are measured on an hourly basis. Monitor that hourly trading volume must exceed 350 trades per hour at least 80% of the time within a month.
- Lag time of payroll processing (e.g. 5 days late) is measured on a monthly basis. Monitor that at least 90% of payroll items are processed in less than 5 days in a month.
- A trouble ticket must be opened against a Critical alarm within 10 minutes. Monitor that at least 95% of trouble tickets are opened in 10 minutes or less within a week.
- Server availability is measured on a daily basis by an availability objective. Monitor that the daily availability objective is met at least 99% of the time within a month.

Figure 5-7 *Calculation Objective with Default Options for Alarm Property*



In setting the Calculation objective for a mathematical function, define the following:

- Time during which to collect data for the calculation (see Section 5.11.1, "Time Category," on page 76)
- Data to be used in the calculation: element property, alarm property, or alarm severity (see Section 5.11.2, "Property or Alarm Severity," on page 76)
- Data to ignore and not use in the calculation (see Section 5.11.3, "Ignored Data," on page 76)
- Data alignment, particularly how to handle discontinuity data (see Section 5.11.4, "Data Discontinuity and Alignment," on page 76)
- Mathematical function to perform to return a data value (see Section 5.11.5, "Mathematical Function to Return Data Value," on page 77)
- Threshold to determine data to use for the objective (see Section 5.11.6, "Results Threshold," on page 77)
- A time interval to set the time period in which to calculate values for the objective (see Section 5.4, "Understanding Time Intervals," on page 66)
- Condition at which to set the objective when it is out of compliance and in violation (see Section 5.11.7, "Violation Condition," on page 78)
- Time when the objective is fired (see Section 5.11.8, "Objective Firing," on page 78)
- (Optional) Activation and deactivation dates to indicate when the objective starts and ends (see Section 5.3, "Understanding Activation and Deactivation Dates," on page 65)

For alarm calculation examples, see:

- Section 5.11.9, “Alarm Property Calculation Example,” on page 78
- Section 5.11.10, “Alarm Severity Calculation Example,” on page 80

5.11.1 Time Category

Time category specifies when to collect data to use for the calculation. The actual time associated with the time category is specified in the calendar defined for the SLA with which the objective is associated.

5.11.2 Property or Alarm Severity

The calculation is performed against an element property, an alarm property, or alarm severity on data collected. The element and alarm properties must be numeric.

Specify the data to collect for use in the calculation. Ranges of values can be discarded and not used in the calculation.

For alarm property and element property, specify the property name, which must have numeric data. The default is to use all values in the calculation. Change this to specify a comparison, a number to which to compare, and whether the comparison is negative (bad) or positive (good). The comparisons are:

- *Less Than or Equal To*
- *Greater Than or Equal To*
- *Between*
- *Not Between*
- *Equal To*
- *All Values (Match)*

For alarm severity, the default is to include all elements with the condition equal to Critical. Select a condition and, then one of the following comparisons:

- *Equal To*
- *Worse Than*
- *Better Than*

5.11.3 Ignored Data

By default, the calculation is based on all data collected for the time interval based on the property or severity options selected. Opt to ignore some of the data based on the lowest or highest values. These values can be expressed as a percent or a decimal.

5.11.4 Data Discontinuity and Alignment

Data is collected once a minute for element properties and the state of the property is recorded once a minute for evaluation. Data for alarm properties is collected when an alarm is received or updated.

Discontinuity data typically indicates when the server does not collect real-time data, when the database is unavailable, when the warehouse/profile is not running, when the integration adapter is not running, and when the server is not running. When using the Calculation objective, the processed

data differs from other data (such as real-time condition data), because the Calculation objective typically processes historical data that is received in batches or that is fed in real time, but represents a span of time, such as the last 15 minutes.

The Calculation objective allows defining point data or aligned data. Point data assumes that data is received randomly and that data is always available regardless of whether there is a data point in a given time interval. In this case, there is no discontinuity or missing data.

For example, assume the first data value is received on January 15, then no additional data is received until March 15. This means all days from January 15 forward show 100% data available. If a monthly objective is defined, then the months of January and March show valid key metric results, but February shows N/A. All three months show 100% data available, however.

Aligned data assumes that at least one data value must be received within the aligned data interval; otherwise, no data is available and the data interval is marked as a discontinuity interval. For example, if data is aligned to daily and a daily value is not received on a given day, that day is marked as a discontinuity period and SLA reports show 0% data available during that day.

5.11.5 Mathematical Function to Return Data Value

The mathematical calculations available are:

- **Custom:** Returns a ratio, or percentage value. Uses a custom calculation that can divide a selected dividend by a selected divisor. All, matched, unmatched, matched/unmatched equal to a value (dividend only), or an expected number of values can be used in the equation.
- **Minimum:** Returns the minimum of all matched values.
- **Maximum:** Returns the maximum of all matched values.
- **Average:** Returns the average of all matched values.
- **Median:** Returns the median of all matched' values.
- **Sum:** Returns the sum of all of matched values.
- **Count:** Returns the total number of matched values.

The property value option simply returns the most recent property value or current value to compare against the threshold to determine the key metric during the objective interval.

Percentage and ratio calculations work best with historical data.

5.11.6 Results Threshold

The value returned by the calculation must meet a specified threshold to determine if the objective is in compliance. For an element property or alarm property, the default is for the threshold to be greater than or equal to 90. Set the number, then select one of the following comparisons:

- *Less Than or Equal To*
- *Greater Than or Equal To*
- *Between*

For alarm severity, the result of the calculation must be worse than Critical to meet the threshold. Select a different condition and one of the following comparisons:

- *Worse Than*
- *Better Than*
- *Equal To*

5.11.7 Violation Condition

When the objective is out of compliance, the condition of the objective is Critical. You can change this condition. However, changing this condition has absolutely no impact on the state of the objective at any other time (for example, when it is halfway to the failure state). The state of a failed objective has absolutely no impact on the state of the SLA, which is determined by health scores of objective and not state of objectives.

When an objective is halfway to failure, the state of the objective always defaults to Major.

5.11.8 Objective Firing

For the Calculation objective to return breaches correctly, it should be set to run at the end of the interval to calculate compliance. If it is not run at the end of the interval, it might show a violation early in the interval if the objective is out of compliance but ultimately by the end of the interval the objective might be in compliance. Note that if the calculation executes at the end of the interval, no real-time calculations are performed.

5.11.9 Alarm Property Calculation Example

An employer needs to maintain an 80% participation rate for their employee Life Insurance plan. The Calculation objective can be used to help them monitor percentage of participation.

The calculation needs to measure the percent of employees that are eligible but not participating, based on the total number of eligible employees. Mathematically, this can be calculated with the following equation:

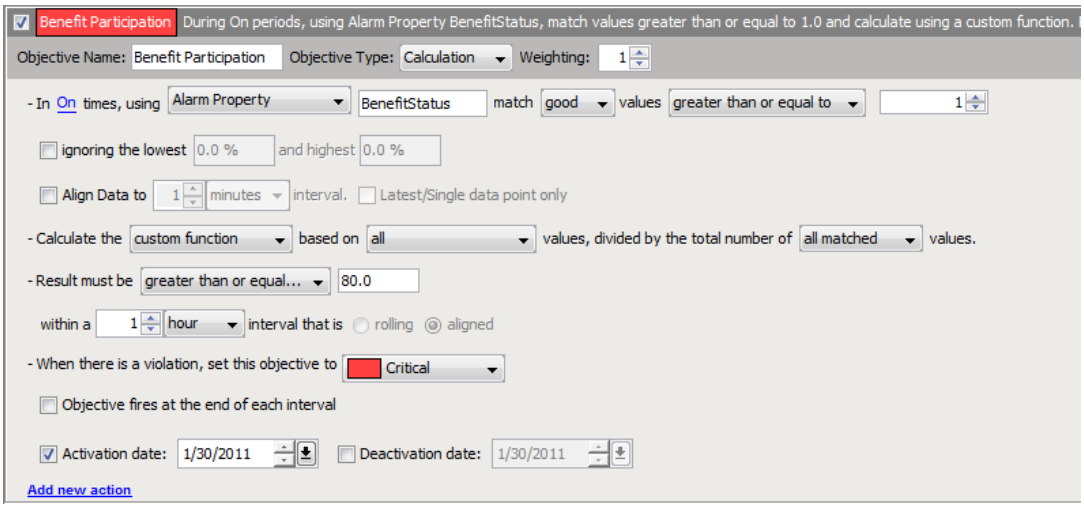
```
% Eligible but NOT     =    --          (Eligible Not Participating)                _
   Participating                      (Participating) + (Eligible Not Participating))
```

The employee participation information is stored in a database and is surfaced in Operations Center using a Data Integrator adapter. An informational alarm is created for each employee with a code for benefits participation.

- **0:** The employee is not eligible to participate and therefore is not participating in the plan.
- **1:** The employee is eligible and is participating in the plan.
- **2:** The employee is eligible but is not participating in the plan.

Figure 5-8 shows the selections necessary to set up the objective:

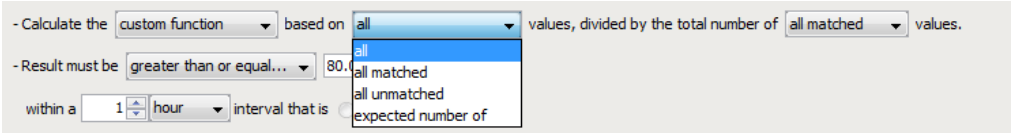
Figure 5-8 *Example Calculation Objective for Alarm Property*



To define an objective:

1. Specify the matched values in the dataset:
   - *Calculation* is the selected objective type.
   - *Alarm Property* is selected because the information to be evaluated is contained in an alarm. In the example above, BenefitStatus is the relevant alarm property.
   - The example above calls for matching values greater than 1 (to return alarms with a value of 1 or 2 — all employees that are eligible). The options are:
     - *All Values*
     - *Less Than or Equal To*
     - *Greater Than or Equal To*
     - *Between* (is inclusive >= and <=)
     - *Not Between* (is exclusive < and >)
     - *Equal To* (one value x)
2. Select a standard function, such as maximum or average, or use a custom function for the equation, based on all or a subset of matched values.

   Select from the drop-down list:



3. Set up the divisor in the equation.

   Select the *Divided by the Total Number* check box to indicate there is an equation to calculate the percent value:

4. Specify the goal of the objective.

   Results should be greater than 80.0 (the calculation returns a percent) or the objective fails, as more than 80% of employees must participate in the benefits plan.

   Enter either a decimal or percentage; for example, .90 and 90% are valid entries.

   When using custom functions, it is necessary to enter a number and the percentage symbol (%).

5.11.10 Alarm Severity Calculation Example

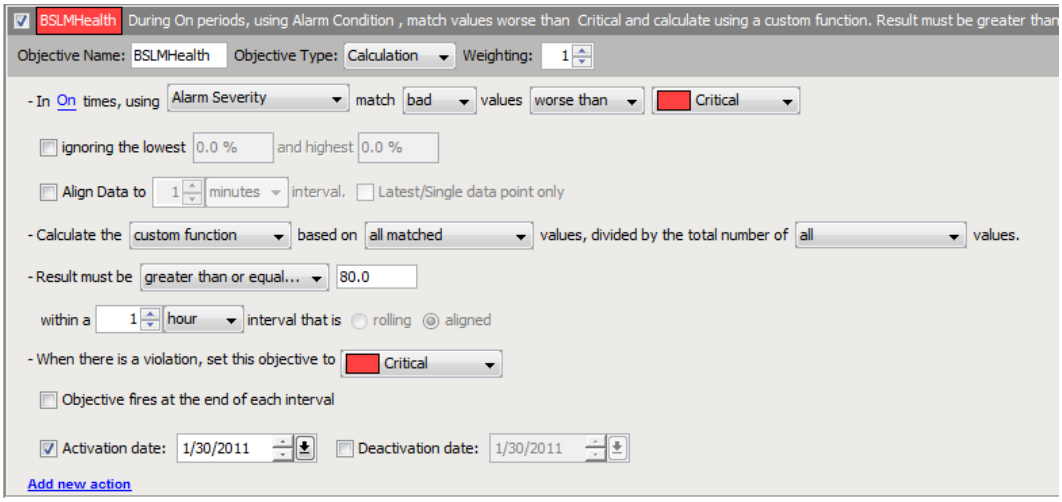
A company wants to monitor the performance of SLM jobs. An alarm fires when certain jobs are executed and indicates the success or failure of the job. In order to monitor the jobs, a Calculation objective can be setup to alert when a threshold is reached for job failure.

If the job failure rate is over 5% in any given month, it is unacceptable, and administrators want to be alerted. Mathematically, this can be calculated with the following equation:

```
% failure     =    --(number of critical jobs)
                                  (all jobs)
```

Figure 5-9 shows the selections necessary to set up the objective.

Figure 5-9 *Example Calculation Objective for Alarm Severity*



To define the objective:

1. Specify the matched values in the dataset:
   - *Calculation* is selected as the objective type.
   - *Alarm Severity* is selected because we are concerned about failing alarms.
   - We are interested in matching values worse than Critical (to return the number of alarms that are Critical).
2. Set up the mathematical equation:

   Use a custom function for the equation.
   - Set up the dividend of the equation. We want the number of Critical alarms (all matched values).
   - Set up the divisor of the equation. Select the check box to indicate that there will be an equation to calculate the percent value. We are interested in all values (the total number of alarms including Critical alarms).

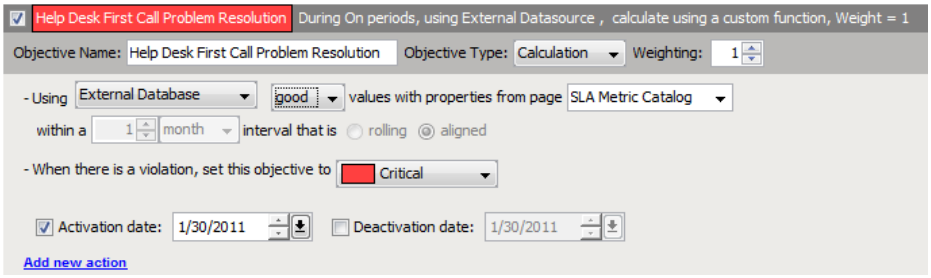
3 Specify the goal of the objective.

We need results to be less than 5.0% or the objective fails because 5% of the jobs are allowed to fail.

5.12 Calculation Objective for External Database

The Calculation objective measures compliance based on a key metric that is defined in the SLA Metric Catalog properties of an element. These properties are defined by generating a query against data in an external database.

Figure 5-10 *Calculation Objective with Default Options for External Database*



In setting the Calculation objective for a mathematical function, define the following:

- Condition at which to set the objective when it is out of compliance and in violation (see Section 5.11.7, “Violation Condition,” on page 78)
- (Optional) Activation and deactivation dates to indicate when the objective starts and ends (see Section 5.3, “Understanding Activation and Deactivation Dates,” on page 65)

Each element can have only one calculation objective that uses the SLA metric catalog defined for it. Operations Center does not support an element with multiple SLA Metric Catalog properties associated with multiple calculation objectives using an external database.

Because property pages are not inherited, every child element for which you want to define a calculation objective using an external database must have SLA Metric Catalog properties defined for it.

When set to use the SLA metric catalog, the calculation objective only fires monthly. The objective can only be defined for a monthly interval based on historic data. The time interval displays in the objective but cannot be changed.

No real-time data is collected and processed for the calculation objective when it is based on an external database and SLA Metric Catalog properties of an element. Therefore values are as follows in real time:

- Severity is unknown or NA (not applicable)
- Health, health grade, and compliance are null
- Violation is null

The calculation objective produces a key metric, which is displayed in the SLA Status Report in the Operations Center dashboard. For more information about the key metric and SLA reports, see the *Operations Center 5.5 Dashboard Guide*.

The *Status* tab lists any existing objectives. For calculation objectives based on the SLA metric catalog, the status is unknown (shown as a gray box) because no real-time data is collected.

5.13 Agreement Objective

An Agreement objective is an aggregate type calculation for agreement health that factors in health values from another Service Level Agreement, where applicable for associated elements. It applies only to the agreement health score calculation.

Figure 5-11 *Agreement Objective*

Select from other Service Level Agreements defined for that branch of elements. Also select a activation and deactivation dates (see Understanding Activation and Deactivation Dates (page 65)).

When defining agreement objectives, it is imperative that the agreement itself must include children that participate in the selected aggregate agreement.

For example, if a Routers SLA is applied to all routers, and router elements are 5 levels below the element where an Email SLA is defined, then the Email SLA must include an objective for the Routers agreement and the Email SLA must be applied to at least 5 levels of children. Otherwise, the health of the Routers SLA has no affect on the Email SLA.

If an agreement objective is applied to an element, but the agreement doesn't include the element, the agreement objective is ignored.

All calculations are based on the agreement's settings where originally defined. Only the health value, reason, and root cause are rolled up to the aggregate agreement.

6 Monitoring

After defining Service Level Agreements and their objectives, it is critical to proactively monitor and manage them. Operations Center can monitor the following in real time:

- Breach warning and alarms for objectives and SLAs
- Metric alarms for objectives and SLAs
- Outages
- Status and state of the elements, objectives, and SLAs

Various tools can be used to monitor SLAs:

- Operations Center console (for more information, see the *Operations Center 5.5 User Guide*)
- Operations Center dashboard (for more information, see the *Operations Center 5.5 Dashboard Guide*)

For breach warnings and alarms, you can also set up automated actions to alert you or perform a specified action.

6.1 Setting Up Breach Alarms

Breaches can be either alarms or warnings. Breach warnings are automatically issued prior to the violation of an objective. They indicate when the health of an objective or SLA is trending toward a service violation.

6.1.1 Understanding Breach Alarms

Breach alarms can be issued for either objectives or SLAs independently. A breach alarm is issued for an SLA when health rules that determine the health of the SLA is in violation. A breach alarm is issued for an objective when the objective is out of compliance (for example, it fails).

When an objective is halfway to a breach condition, the condition of the objective is Major (warning). This occurs even if you specify `Minor` as the option for what the objective should be when a violation is reached.

Breach alarms can show the following:

- Severity
- Element
- Date/Time
- ID
- Status
- Agreement name
- Objective name
- Applied agreement, which shows element path based on the point at which the SLA was evaluated to issue the breach alarm
- Metric key, which is the current measurement based on objective type
- Reason
- Comments
- History

Breaches are displayed as long as the breach condition applies within a measured interval. Alarm data can be filtered based on severity.

Breach alarms can be viewed in the *Alarms* view of the Operations Center console, and in the Alarms portlet in the Operations Center dashboard.

6.1.2 Actions on Breaches

For breach alarms, the following actions are available:

- *Clear the Breach*
- *Add a Comment to the Alarm*
- *Show the Root Cause*

Perform these actions in the Alarms portlet in the Operations Center dashboard or in the Operations Center console *Alarms* view, by right-clicking the alarm.

Another option is to set up an automatic action by configuring the automation function in Operations Center by setting up a script to execute when a breach occurs.

6.1.3 Automating Notice of Breaches

In addition to monitoring breach warning and alarms in a Operations Center tool, you can also receive automatic notice or have an action performed for breach warnings or alarms for an objective or an SLA.

- "Understanding Automation of Notices" on page 85
- "Adding an Automated Action to an Objective" on page 86
- "Adding Automation to a Service Level Agreement" on page 87

Understanding Automation of Notices

To receive automated notice for an objective, add an action when the objective is defined. More than one action can be defined per objective.

Set up automation for an element so that if any of the Service Level Agreements for that element have either a violation or warning, the automated action occurs. Automation for an element is defined on the Automation property page for the element's properties.

The automated actions available are:

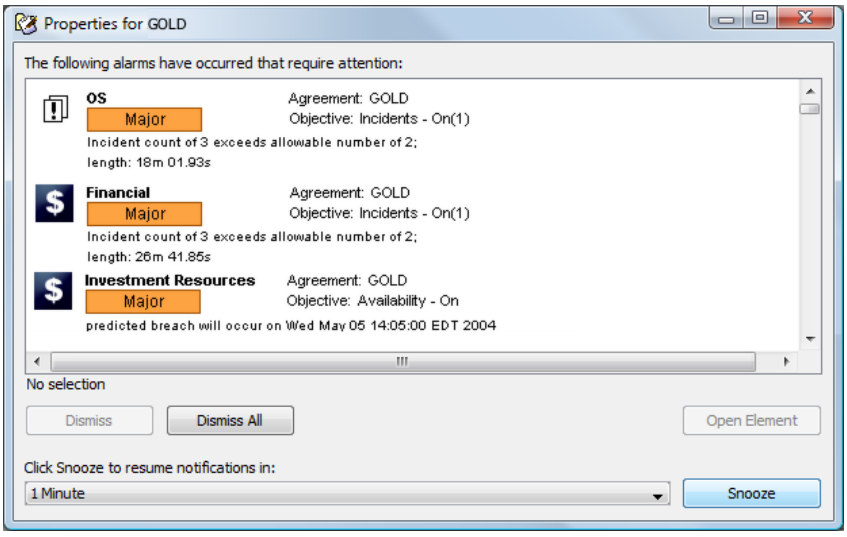
- Open an alarm pop-up dialog box.
- Play or stop a noise, such as an audio clip, gong, chirping, or a computer-generated noise.
- Send an e-mail with alarm and element information.
- Send a page with element information.
- Post an alarm to the IBM Tivoli Enterprise Console (T/EC).
- Run a script, either one configured specifically for this automation action or one from the script library.

In the alarm pop-up dialog box, the agreement and objective names display if agreement and objective are specified in the Alarm's detail fields for the automation definition.

A predicted time for the violation message displays (as shown in the highlighted item in Figure 6-1) if predict.* is specified for the *Alarm Message* field in the automation definition and the alarm contains a predicted time for failure. Predicted failure is only available for alerts pertaining to Availability objectives.

It is possible to clear an alert from this dialog box:

Figure 6-1 *Alarm Pop-up Dialog Box*

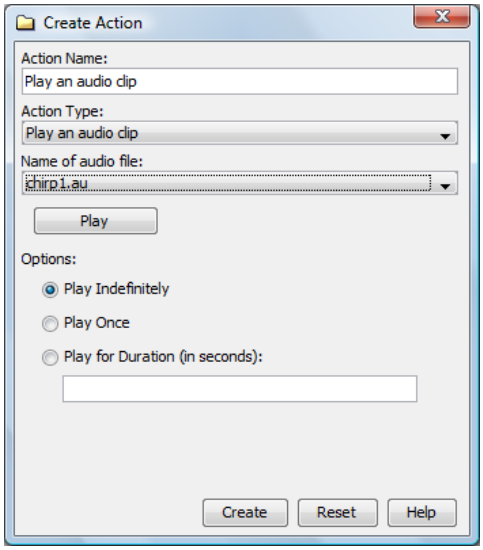


For more information on automated action and automation in general, see "Defining and Managing Automation Events" in the *Operations Center 5.5 Server Configuration Guide*

Adding an Automated Action to an Objective

To add an automated action to an objective:

1 When defining or editing an objective, click the *Add New Action* link found at the bottom of the objective definition.



2 Specify the name for the action in the *Action Name* field.

3 Click the *Action Type* drop-down list, then select an action.

Other options display, depending on the type selected.

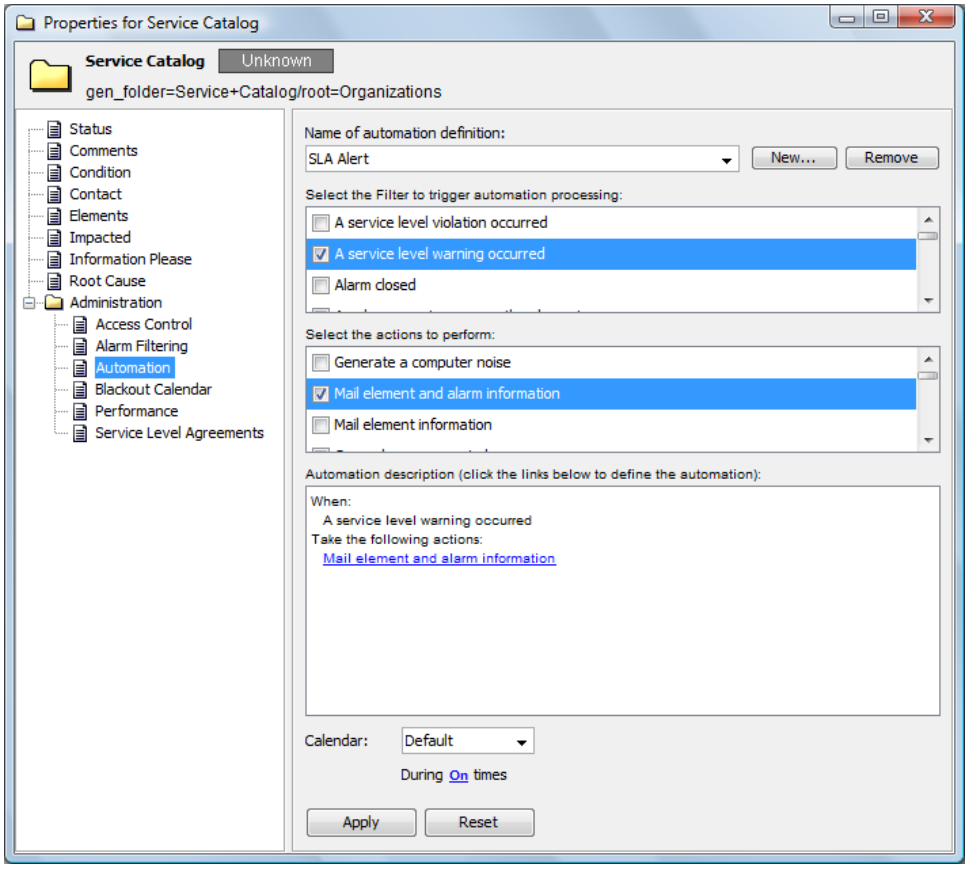
4 Click *Create* to save the action.

A link to the new action displays at the bottom of the objective definition.

Adding Automation to a Service Level Agreement

To add an automation to an agreement:

1. At the highest applicable level in the *Services* hierarchy, right-click the top element, then select *Properties*.
2. Click *Automation*:



3. In the *Name of Automation Definition* drop-down list, select a definition, or click *New* to specify a new name.
4. Under *Select the Filter to Trigger Automation Processing*, select the appropriate check box.
5. Under *Select the Actions to Perform*, select the appropriate check boxes.
6. Complete the other fields, which can vary, depending on the action selected.

6.2 Setting Up Metric Alarms

Metric alarms are issued for an element to provide information about changes to an agreement or any objectives, including changes that can affect health, such as element state change or a parameter value change.

- Section 6.2.1, "Understanding Metric Alarms," on page 88
- Section 6.2.2, "Setting the Service Level Metrics Alarm Limit," on page 89

6.2.1 Understanding Metric Alarms

Service level metric alarms are unique in that they are never saved for historical purposes, nor persisted when the Operations Center server is restarted. Metric alarms are always real time and there is a limit to the number of alarms that can be issued per element, per objective, and per agreement.

This limit is set in the settings of the BSW. The default is 50 but it is advisable to set a lower number (such as 5 or 10). If there is one agreement with two objectives applied to five elements, using the default value of 50 no more than 500 metric alarms are held in memory. Older metric alarms are removed from memory when the measured interval ends or a condition change occurs producing a new metric alarm.

Metric alarms can be viewed in the Operations Center console in the *Alarms* view by selecting *Service Level Metrics* as the alarm type. They are also available in the *Alarms* portlet in the Operations Center dashboard.

Metric alarms can show the following information and changes:

- Severity
- Element
- Date/Time
- ID
- Transition: Previous state and the current state
- Compliance: Agreement health score, which indicates how well the element is doing in respect to the associated objective
- Grade: Letter grade based on the compliance score; this letter grade is mapped to the agreement health score
- Agreement
- Objective
- Applied agreement: Element path based on the point at which the agreement was evaluated to issue the metric alarm
- Violation
- Metric key: Current measurement based on objective type
- Uptime: Amount of time available in the current interval for the calendar applied to the SLA
- Downtime: Amount of time unavailable in the current interval for the calendar applied to the SLA
- Element downtime
- Unknown
- Predict warning: Predicted amount of time until a breach warning occurs based on the prediction ratio (if performance continues at the same level)
- Predict violation: Predicted amount of time until a breach or violation occurs based on the prediction ratio (if performance continues at the same level)
- Worst warning: Predict time of warning if failure occurred now
- Worst violation: Predicted time of violation if failure occurred now
- Time included: Total amount of time included in the interval period
- Period start: Date and time when the interval period started (sets the interval for uptime and downtime)

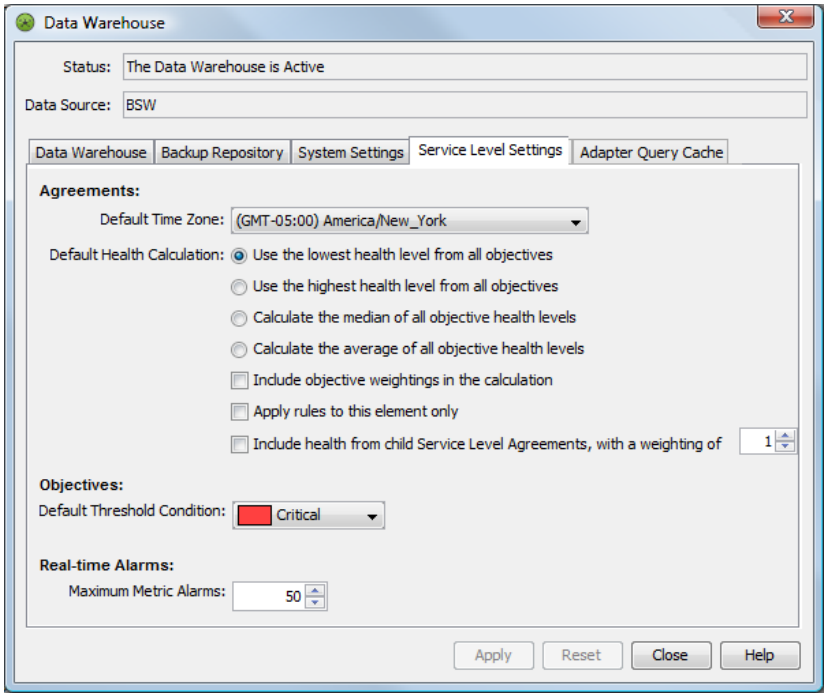
- Period end: Date and time when the interval period ended (sets the interval for uptime and downtime)
- Prediction ratio: Ratio measurement based on amount of time in compliance vs. amount of time element was noncompliant
- Points captured: Number of data points measured and stored
- Low: Minimum constraint if set by the objective
- High: Maximum constraint if set by the objective
- Reason: Description of why the metric was recorded

The only actions to perform on service level metric alarms are to save them to a file or add a comment in the *Alarms* portlet in the Operations Center dashboard or in the Operations Center console *Alarms* view by right-clicking the alarm. Note, that as metric alarms are not persisted after a server restart, nor are comments on metric alarms.

6.2.2 Setting the Service Level Metrics Alarm Limit

To set the alarm limit for metric alarms:

1. In the Operations Center console, open Enterprise > Administration.
2. Right-click *Data Warehouse*, then select *Edit Data Warehouse Settings*:



3. Click the *Service Level Settings* tab.
4. Under *Real-Time Alarms*, select a number for *Maximum Metric Alarms*.

6.3 Monitoring SLAs, Breaches, Outages and Element Statuses

The status of elements and SLAs can be monitored in both the Operations Center console and dashboard:

- Section 6.3.1, “Operations Center Console,” on page 90
- Section 6.3.2, “Operations Center Dashboard,” on page 91

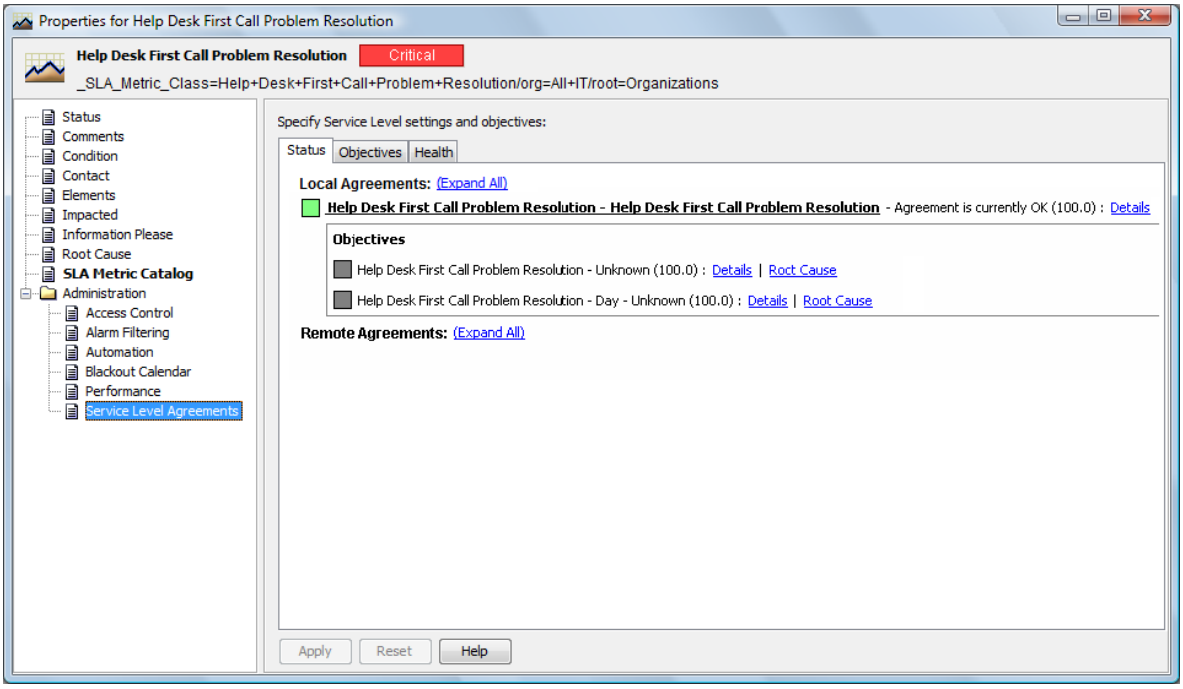
6.3.1 Operations Center Console

The Operations Center console provides two options for monitoring the status of SLAs:

- Service Level Agreement property page
- *Network* view

The property pages for an element include a Service Level Agreement page. The *Status* tab of the Service Level Agreement property page displays a status summary for the SLA status, as well as its objectives:

Figure 6-2 *Status on the Service Level Agreements Property Page*



Obtain additional details for each and view the details for the root cause of any warnings or violations.

The *Network* view is available for any element in the *Operations Center* hierarchy. View the relationships for an element or a Service Level Agreement. Service Level Agreement and objectives are located in the hierarchy under *Enterprise*.

6.3.2 Operations Center Dashboard

The Operations Center dashboard has portlets that display basic data about elements, such as status, root cause of the current condition, and other elements impacted by the element, as well as SLA reporting portlets:

- **SLA Compliance Portlet:** View health, downtime, availability, outages, and breaches related to SLAs for specified elements over a specified interval of time.

  For more information about SLA compliance reporting, see Chapter 7, "SLA Reporting," on page 93, or "SLA Reporting Portlets" in the *Operations Center 5.5 Dashboard Guide*.

- **SLA Status Portlet:** View compliance/availability from a status or summary perspective with links to SLA Compliance reports.

  For more information about SLA reporting, see Chapter 7, "SLA Reporting," on page 93, or "SLA Reporting Portlets" in the *Operations Center 5.5 Dashboard Guide*.

- **Alarms Portlet:** View Service Level breaches or Service Level metrics depending on portlet configuration.

  For more information about the Alarms portlet, see "Configuring the Alarms Portlet" in the *Operations Center 5.5 Dashboard Guide*.

- **Status Portlet:** Shows a list of elements with the current status and can show additional information such as the date and time that the element was last updated, notes for the element, and links to other components..

  For more information about the Alarms portlet, see "Configuring the Status Portlet" in the *Operations Center 5.5 Dashboard Guide*.

- **Root Cause Portlet:** Provides information about why the element is at its current condition. When reporting on the compliance and health of an objective or SLA with an SLA Compliance Report, also obtain information on root cause. The root cause information can include such information as the current availability compared to what it should be, the dates and times of all violations, and the number of relevant outages.

  For more information about the Alarms portlet, see "Configuring the Root Cause Portlet" in the *Operations Center 5.5 Dashboard Guide*.

- **Show Impacted Portlet:** Provides information about how the element is affecting other elements.

  For more information about the Alarms portlet, see "Configuring the Show Impacted Portlet" in the *Operations Center 5.5 Dashboard Guide*.

7 SLA Reporting

Operations Center offers tools to generate predefined and custom reports on Service Level Agreement (SLA) data. Most reports typically use data from the local Operations Center server and therefore use local SLA data. But Operations Center reports can also include SLA data from other Operations Center servers by using the Remote SLA function.

Operations Center offers two tools for creating custom reports:

- **Operations Center SQL Views:** Can extract SLA-related data from tables and use it in a custom reporting tool, such as Crystal Reports.

  For more information, see the *Operations Center 5.5 SQL Views Guide*.
- **Operations Center Web Services Application Programmer Interface (WASPI):** Also known as Web Services, allows remote applications to query Operations Center data, including SLA-related data.

  For more information, see the *Operations Center 5.5 Web Services Guide*.

For predefined reports, the main reporting tool is the Operations Center dashboard, a custom portal tool. The dashboard also has additional portlets for presenting data from Operations Center. For more information about the dashboard, including how to set it up and use it, see the *Operations Center 5.5 Dashboard Guide*.

Some reports can be localized for a specific language, scheduled to run at a specific time, and exported as either an Excel spreadsheet or a PDF.

Review the following sections to understand and configure SLA reporting:

7.1 Understanding Data Types

Table 7-1 lists the types of data available in reports and the tool in which it appears.

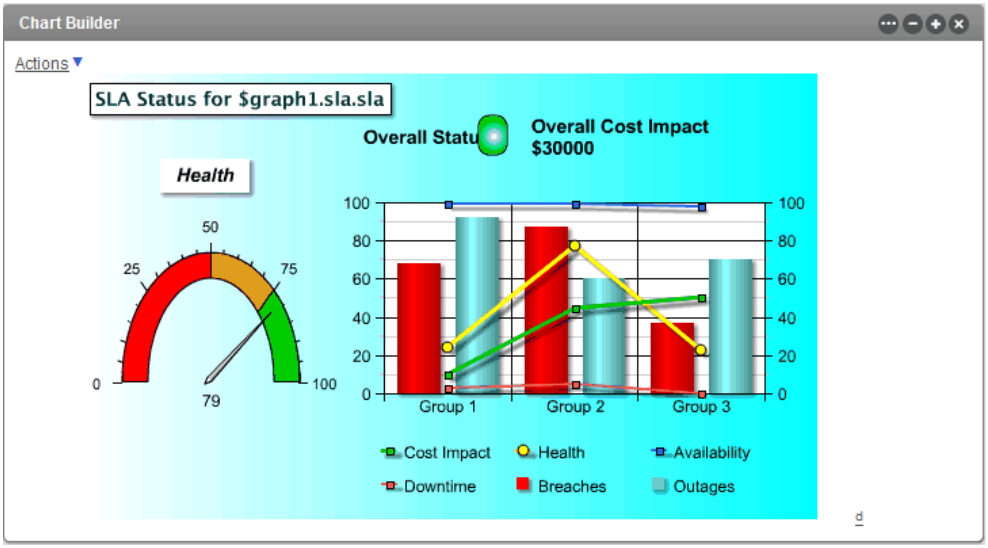
Table 7-1 *SLA Reporting Options*

Data	Reports	Operations Center Tools
Compliance (health)	SLA Status Report	Dashboard
	SLA Compliance Report	Dashboard
Breaches	SLA Compliance Report	Dashboard
	Alarms View	Console
	Alarms Portlet	Dashboard
Availability	SLA Status Report	Dashboard
	SLA Compliance Report	Dashboard
Downtime	SLA Status Report	Dashboard
	SLA Compliance Report	Dashboard
Outages	SLA Compliance Report	Dashboard
	Alarms View	Console
	Alarms Portlet	Dashboard
Key metric	SLA Status Report	Dashboard
	SLA Compliance Report	Dashboard

Element and SLA status data is also available in the Operations Center dashboard. For more information, see Chapter 6, “Monitoring,” on page 83.

Charts containing SLA data can also be built in the Operations Center dashboard and used as a different way to visual the data. Figure 7-1 shows a created SLA status dashboard:

Figure 7-1 *SLA Status Dashboard*



This chart as well as other types of charts are available in the Operations Center dashboard using the Chart Builder portlet. For more information, see the *Operations Center 5.5 Dashboard Guide*.

Performance information is also available in the Operations Center console and dashboard. For more information, see Chapter 9, "Analyzing Performance," on page 125.

7.2 Understanding Reports and Their Uses

7.2.1 Report Descriptions

Table 7-2 describes reports and lists the possible users of each report.

Table 7-2 *Report Uses and Descriptions*

Report	Uses	Description
SLA Compliance Report	Operators to view declining health of a service to avoid SLA breaches. Customers and/or internal management to view SLA data on a weekly or monthly basis.	Displays agreement and objective health, downtime, outage, and availability information for the element during the specified time frame. Includes charts for condition and availability/compliance as well as information regarding outages, root cause, and breaches. The *Reason* field includes information indicating whether agreement or objective health is in violation or not, what the current health is, and how health was determined. The *Root Cause* link displays root cause data for the selected objective or agreement.
SLA Status Report	Managers to view current day, week, or month and compare it to the previous day, week, or month.	Displays a health/availability/downtime status summary for an element and all its children, the children of a selected element, or a specified list of elements during selected time frames. Expand the tree to a full *SLA Compliance Report* for the associated element. Unique to the Status report is the ability to calculate smaller intervals independently of the objective interval. For example, with monthly objectives, run independent health calculations on daily, weekly, and monthly, instead of showing a cumulative report.

7.2.2 Report Uses

Table 7-3 describes the use of reports for specific requirements.

Table 7-3 *Reporting Needs*

Requirement	Use Report
Calendar views (such as weeks, months)	SLA Compliance
Quick status review with an option for more information	SLA Status
Detailed list of outages and/or breaches	SLA Compliance (*Breaches*, *Outages* tabs) Alarms Listing (for Breaches and Metrics)
Quick status list for multiple elements	SLA Status
Chart agreement or objective compliance condition or health	SLA Compliance (*Chart* tab) Performance

Requirement	Use Report
Chart availability	SLA Compliance (*Chart* tab)
	Performance
Chart downtime	Performance
Chart outage counts or duration	Performance

7.3 Understanding Time Intervals

SLA reports in the Operations Center dashboard allow reporting on a specific time interval. Create reports with varying time intervals to meet the needs of different users as described in Table 7-4.

Table 7-4 *Time Control Options*

Option	Description	Useful for
Use Interval	Reports with nonspecific date/time ranges. Report on the last x hours, days, weeks, months, or this hour, day, week, month. This is a rolling setting that is updated each time the report display changes or refreshes. This is treated as an inclusive option, so that the current date/time is included in the results. For example, this month as of 3:06 PM on May 14 includes data from May 1, 12:00 AM to May 14, 3:06 PM. Last is treated as an exclusive option, so that the following apply: ◆ Last 60 minutes includes the 60 minutes prior to the minute when the report is generated. ◆ Last hour includes the last complete hour prior to the hour when the report is generated. ◆ Last day includes the last full day ending at midnight prior to the day the report is generated. ◆ Last week includes the last complete Sunday to Saturday week, prior to and not including the day the report is generated. For details on customizing the week interval to start on Monday instead of Sunday, see Section 5.4.3, “Customizing the Weekly Time Interval,” on page 67. ◆ Last month includes the last full month of data prior to the month in which the report is generated. For inclusive reporting, such as the last 3 months including this month as one of the 3 months, use Last 90 days displayed in months.	◆ Executives who want to know what happened for trending purposes, or what is currently happening for business services. ◆ Publishing results to customers for a specific time period. ◆ Monthly and Weekly reports are the most common selections.

Option	Description	Useful for
Use Date Range	Reports on a date range that includes a specific start date and time with a specific end date and time (or uses the current date and time at report run time).	◆ IT managers who want to know what happened and perform detailed trend analysis during a specific date and time period. ◆ Publishing results to customers or executives for a specific time period, such as May 1–15.
Use Real-Time	Reports on the system data in real time. This option does not apply to Availability reports.	◆ IT managers and administrators who need current operational information.

7.4 Understanding Reports on Compliance and Health

Operations Center uses health as a measurement for whether the SLA is in or out of compliance. The health of the SLA depends on the health of each objective.

7.4.1 Types of Reports

SLA reports available in the Operations Center dashboard are for an element and its children. You can view compliance and health data in three reports:

- **SLA Status Report:** Shows summary data for a specific objective or SLA applied to the element.
- **SLA Compliance Report:** Shows detailed data for a specific objective or SLA applied to the element. This report is also available by clicking metrics in the SLA Status Report.

If an objective is disabled, then the reports shows `N/A`.

7.4.2 Report Content

Reports show the following:

- **Health Grade As a Number:** The SLA Compliance Report also shows additional details, such as availability, when a violation occurred, availability required, and number of relevant outages.
- **Data Available:** Amount of data available for the measured period of time as measured in a range of the following values:
  - 0%
  - 0.1%–33%
  - 33.1%–65.9%
  - 66%–99.9%
  - 100%
- **Compliance Grades:** Level of compliance as correlated to a letter grade for health and indicated by a color as follows:
  - **Green:** 90–100%
  - **Blue:** 70–89%
  - **Yellow:** 60–69%
  - **Orange:** 50–59%
  - **Red:** less than 50%
- **Data Relevance:** Relevancy of data to the reported period of time. For example, there can be data available but it is not considered (not relevant) if the associated time category is filtered out. It is indicated by the following range:
  - 0%
  - 0.1%–33%
  - 33.1%–65.9%
  - 66%–99.9%
  - 100%

When reporting agreement health and compliance, blackout dialog boxes are excluded from the SLA Health and Compliance report, because any outages that occur during regularly scheduled maintenance or blackout periods are typically not counted against the agreement's health and compliance.

When viewing health or compliance reports, filtering of blackout periods does not affect the health or compliance values; unless an objective is actually established for blackout periods. In other words, if your objectives are established to not include Blackout periods, then the health of an objective or an agreement is never impacted by an outage that occurs during a blackout period. The only visual indication of the filtering of Blackout periods (or any other time category) for Health and Compliance reports is through the Data Relevance square icon in the SLM reports. The Data Relevance shows an empty square icon with a value of 0 when a time period is not affecting the health of an agreement or objective.

7.4.3 Report Options

Options for a report include:

- **Reporting:** On either a specific objective or all the objectives. All the objectives provide the compliance and health for the SLA. Aggregate agreements defined using Agreement objectives. This objective type is included with and listed as any other objectives.
- **Calculating Health:** Using the time defined in the objective or using the time control as selected to be displayed in the report. The time specifies the interval over which the objective is evaluated to determine compliance. By default, the time defined in the objective is used to calculate compliance.
- **Time Control:** For displaying the time period in the report: an interval, a data range, or real time.
- **Time Categories:** For which you want data to be considered when calculating health and compliance. The time categories related to the calendar defined for the SLA.

The *Roll Up Children in Calculation* option allows you to report on the SLA status of a given element. By default, children are always rolled up in the calculation; in other words, SLA or objective health includes data from the children of the element. If not checked, it produces the values for the SLA on that element only and ignore any child SLAs that might normally apply (or roll up) into the overall agreement. Rollup children in calculation should always be selected for agreement and objective health reports so that the children are included in the health calculation. Otherwise, breaches, outages, and health metrics for element children that contribute to the SLA are not included, thereby producing incomplete and inaccurate results.

7.4.4 SLA Compliance Report

The SLA Compliance Report also has two formats:

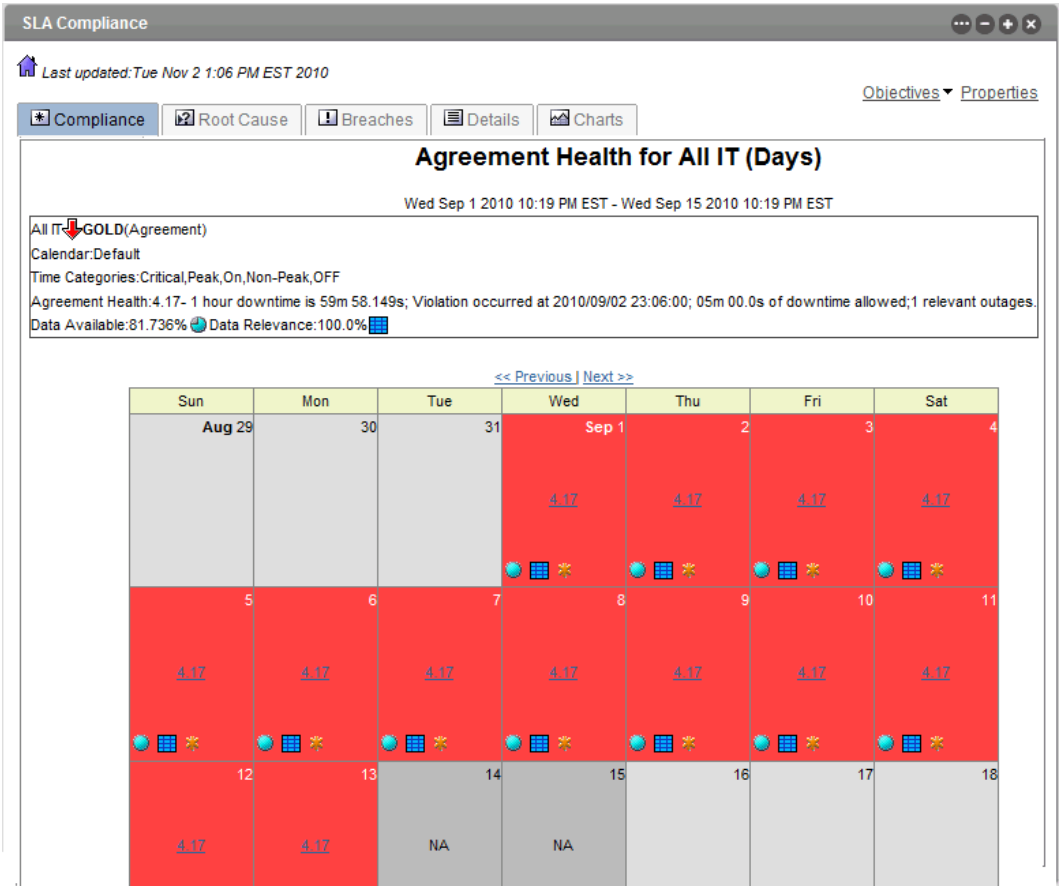
- **Calendar view:** Displays SLA or objective compliance per day in a calendar format.
- **Chart view:** Displays the same data as the calendar view, but in a chart format.

The SLA Compliance report has the following tabs:

- "Compliance Tab" on page 101
- "Details Tab" on page 102
- "Chart Tab" on page 103

Compliance Tab

Figure 7-2 *SLA Compliance Report: Compliance Report, Compliance Tab*



Details Tab

Figure 7-3 *SLA Compliance Report: Compliance Report, Details Tab*

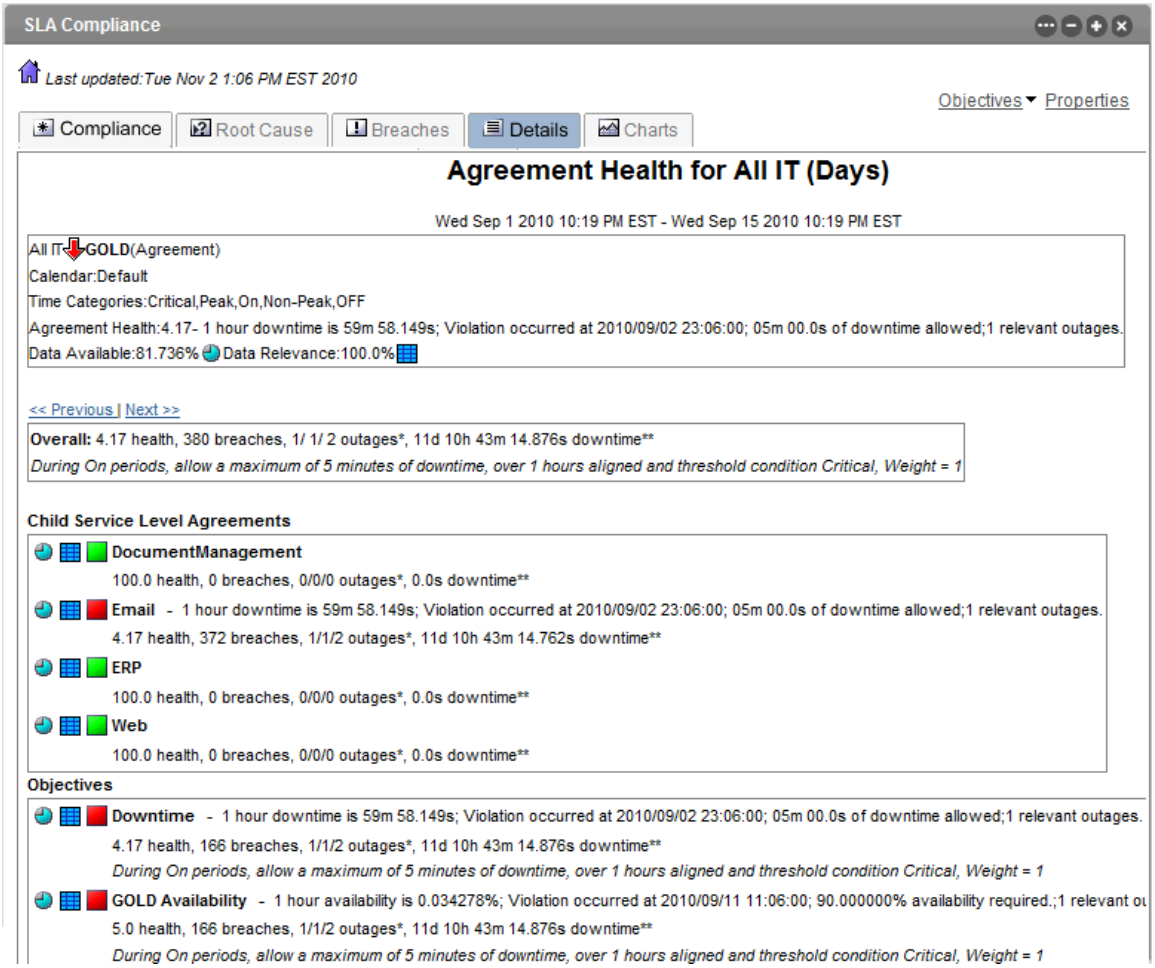
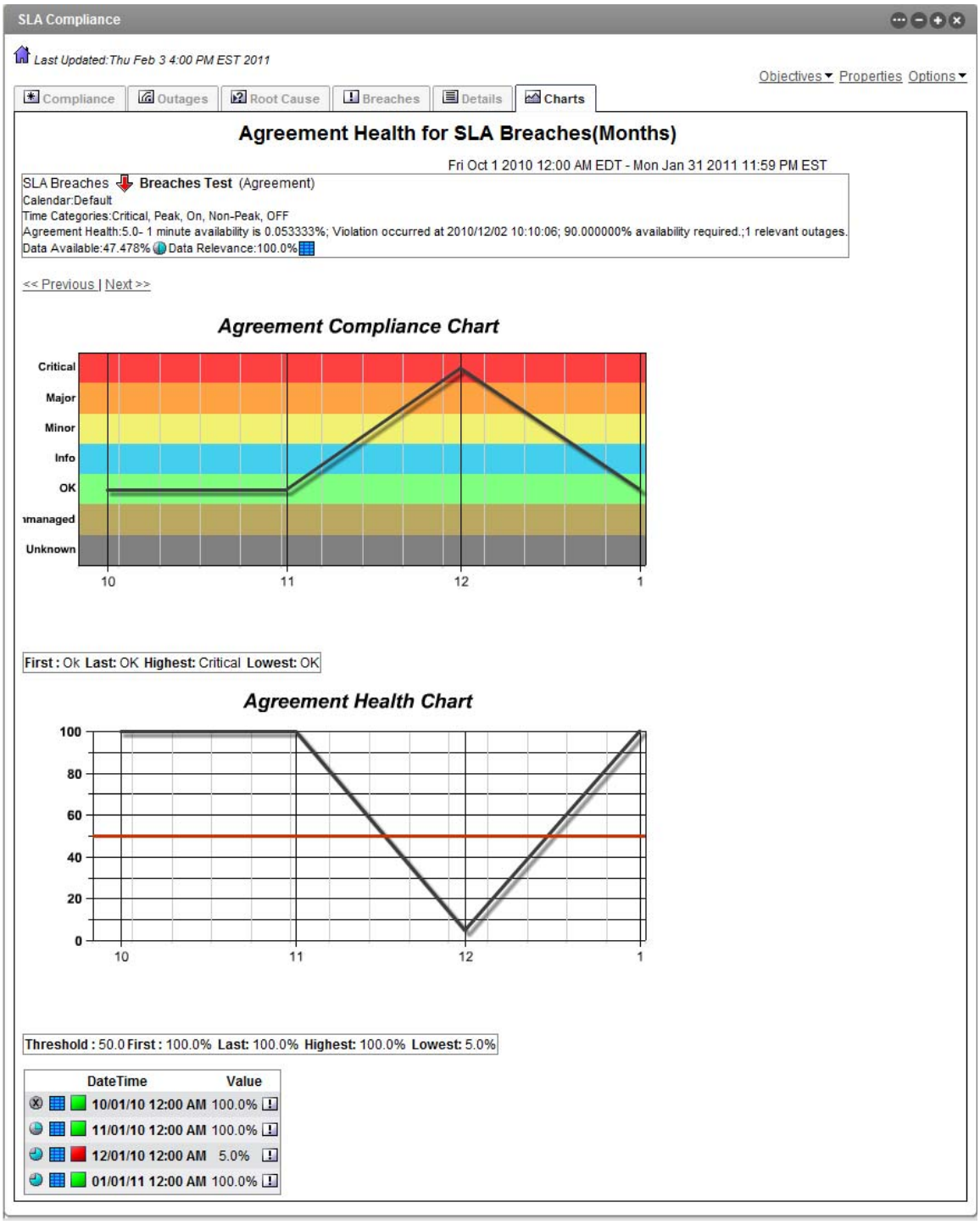


Chart Tab

Figure 7-4 *SLA Compliance Report: Compliance Report, Chart Tab*



7.5 Understanding Breaches

A breach indicates that either an objective or an SLA is out of compliance, that is, it failed. Information on historical breaches is available as alarms and also as data in compliance reports. Breaches can also be viewed in real time as alarms.

- Section 7.5.1, "Historical Breach Alarms," on page 104
- Section 7.5.2, "Breaches in Compliance Report," on page 105

7.5.1 Historical Breach Alarms

Historical alarm data can be viewed in the Operations Center console and in an Alarms portlet in the Operations Center dashboard.

A cleared breach can display without showing that it has been cleared if the action to clear it was taken after the selected time range being viewed. Also, a cleared alarm can display without any information about its original occurrence if it occurred outside the time range being viewed.

Existing historical breach information is not further updated if an agreement of definition is changed after the real-time data is calculated. For example, if data is imported that includes outages that have already occurred, Operations Center never has the opportunity to create a breach alarm that it would have if the outages were system generated in real time.

In the Operations Center console, historical data on service level breaches can be viewed in the *Alarms* view by selecting *Historical: Service Level Breaches* as the data type to view. Unlike real-time alarms, you must select a time period to view, then click *Retrieve*. The *Alarms* view shows the same types of data for historical alarms as it does for real time alarms.

The Alarms portlet in the Operations Center dashboard has the option to display historical data including service level breaches. The same data as displayed in the Operations Center console is displayed in a report on service level breaches. No actions can be taken on these breaches from this report.

Select the time period and the columns of data to be displayed. The report has the following options to filter out data according to severity type:

- **Show Major Breaches.**
- **Show Cleared Breaches:** By default, cleared breaches including all warning and violation alarms associated with these breaches are not shown. Opt to include them in the report.
- **Roll Up Children Breaches:** By default, all breach alarms issued by the element's children that contribute to the objective or SLA are included in the report. They can be excluded.

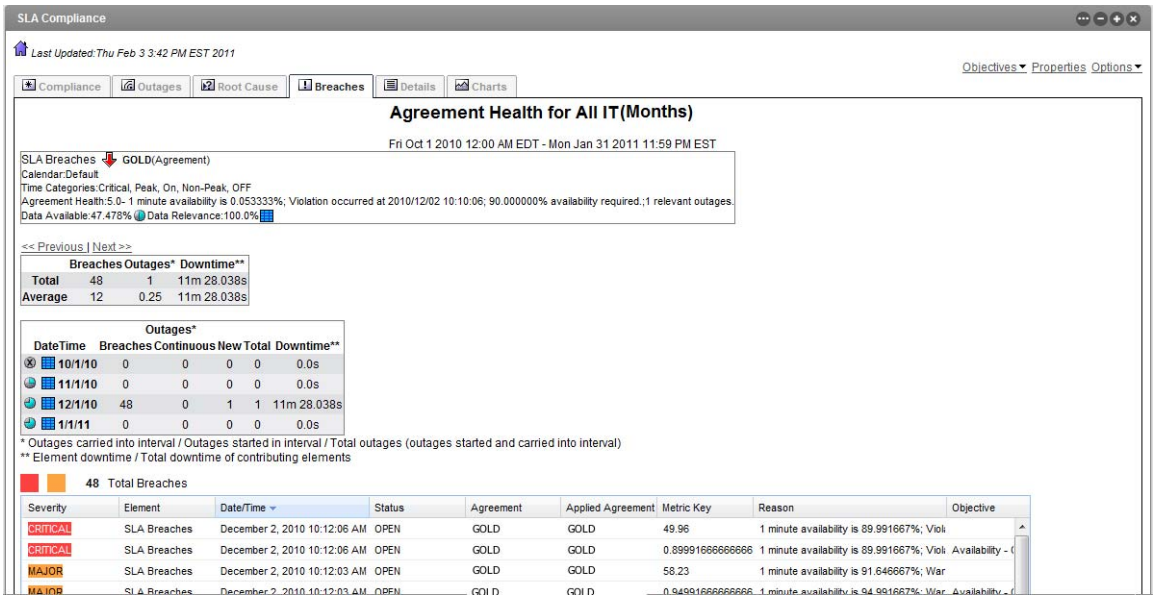
Historical breaches are unavailable for manual outages as breaches are not created for manual outages as they would be for real-time outages. However breaches are simulated and included for manual outages in SLA reports. For more information, see Section 10.3, "Understanding Manual Outages in Breach Reporting," on page 137.

7.5.2 Breaches in Compliance Report

When running a compliance report using the SLA Compliance Report, opt to view breaches. By default, the report does not include objective breaches, major breaches, or cleared breaches, but you can opt to view these.

The *Breaches* tab of the report shows the number of breaches per selected interval, total number of breaches for the whole time period, and the average number of breaches over the whole time period. It also shows outages and downtime:

Figure 7-5 *SLA Compliance Report: Compliance Report, Breaches Tab*



Breaches are measured on the following:

- **Data Available:** Amount of data available for the measured period of time as measured in a range of the following values:
  - 0%
  - 0.1%–33%
  - 33.1%–65.9%
  - 66%–99.9%
  - 100%
- **Data Relevance:** Relevancy of data to the reported period of time. For example, there can be data available but it is not considered (not relevant) if the associated time category is filtered out. It is indicated by the following range:
  - 0%
  - 0.1%–33%
  - 33.1%–65.9%
  - 66%–99.9%
  - 100%

7.6 Understanding Outages

An outage occurs when an element reaches or goes below a specified condition. Outages are defined within objectives.

Outages are rolled up from child elements to parent elements based on algorithms and their relationships. When viewing outages in reports, outage counts can indicate multiple outages when a single outage occurred because the outage affected each of its parent elements. This does not affect SLA compliance calculations.

Historical outages can be viewed as alarms or with compliance and availability in the SLA Compliance Report.

- Section 7.6.1, "Outage Alarms," on page 106
- Section 7.6.2, "Outages in SLA Compliance Report," on page 106

7.6.1 Outage Alarms

The *Alarms* view in the Operations Center console shows historical outages by selecting *Historical: Outages* as the alarm type, selecting a time interval to view the outages, then clicking *Retrieve*. The *Alarms* view shows the following by default:

- Severity
- Element
- Date/Time
- ID
- End time
- Duration
- Type
- Origin
- Comment

An alarm can be exported to a .csv file by right-clicking the alarm, then selecting *Export to File*.

The Alarms portlet in the Operations Center dashboard shows the same data as the *Alarms* view in the Operations Center console.

7.6.2 Outages in SLA Compliance Report

While reporting on SLA compliance or availability, also view outages in the SLA Compliance Report in the Operations Center dashboard.

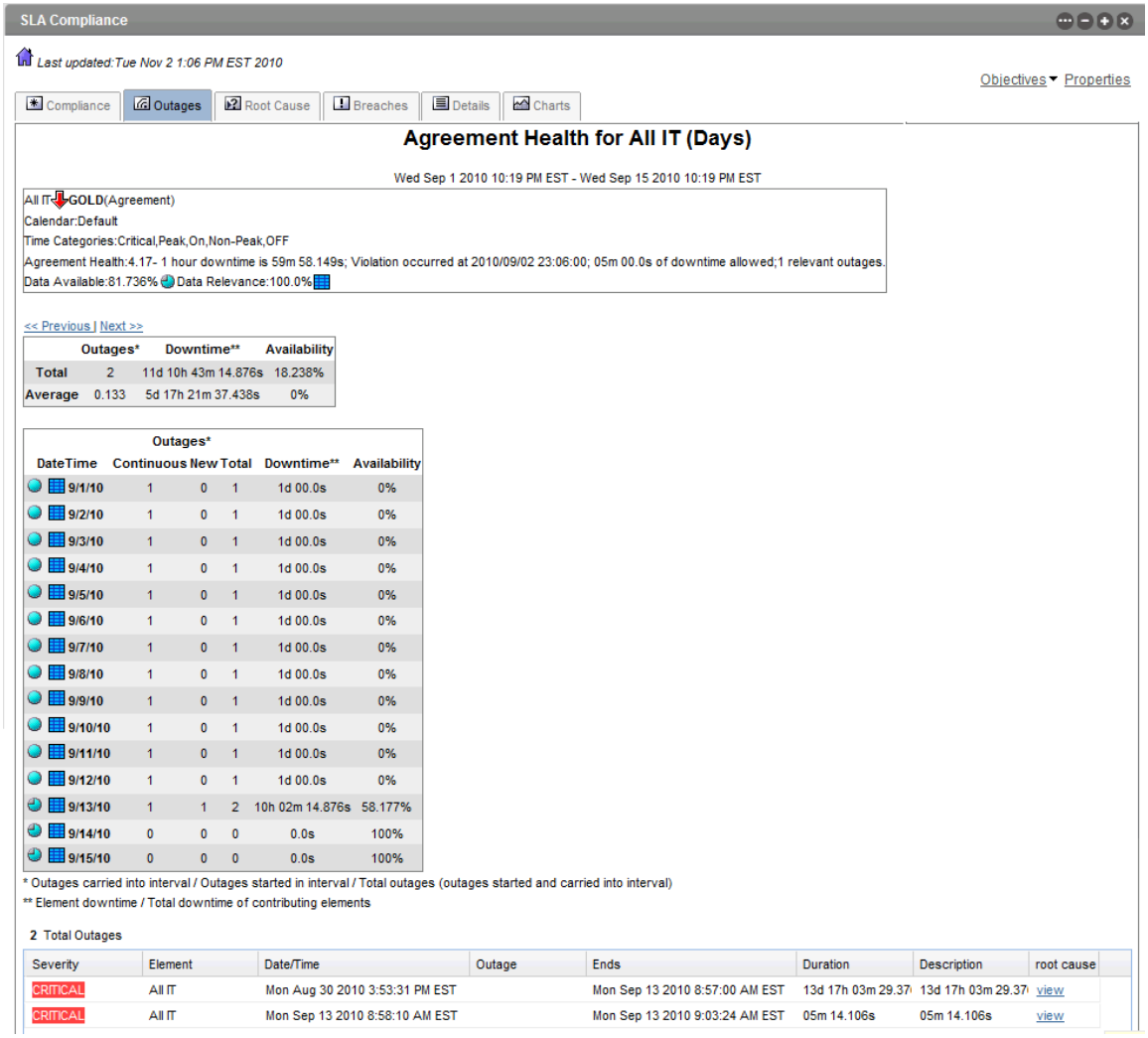
The report shows the following for outages according to the time interval selected:

- **Continuous:** Outages being carried into the interval.
- **New:** Outages that started in the interval.
- **Total:** All outages (continuous + new).
- **Average:** Average of the total outages.

As outage start and end times are rounded to seconds, adding the outage duration to the start date/time might not match the end date/time and be off by milliseconds, because of the math rounding. Also, because of this, the outage data display can indicate that an outage did not take up the entire interval (such as an hour). However, the math rounding might show an end date/time that ends on the interval (for example, 12:00:00 PM).

The report also shows the downtime for the element and total downtime of contributing elements and availability:

Figure 7-6 *SLA Compliance Report: Compliance Report, Outages Tab*



At the bottom of the report is a link to obtain more details that are similar to outages in the Alarm portlet.

7.7 Understanding Downtime

Downtime is the amount of time measured in days, hours, minutes, and seconds (to the thousandths of a second) that an element remains at a specified condition for a specified time interval. That is, downtime is the total elapsed time during an outage.

Disabled objectives have no impact on downtime calculations.

7.7.1 Downtime Reports

You can report on downtime in the following reports:

- SLA Status Report
- SLA Compliance Report

The SLA Status Report offers a summary view, whereas the SLA Compliance Report provides more details. Both reports show the following:

- Condition of the element based on its downtime
- Amount of downtime in hours, minutes, and seconds

Click either report for a more detailed view, which is the same as the SLA Compliance Report. The status report can show data in the following units of time:

today
yesterday
this week
last week
this month
last month

The multiple service report allows selecting an interval specified in a date range, or in months, weeks, days, hours, or minutes.

7.7.2 Downtime Data Availability and Relevance

The SLA Compliance Report also allows selecting between an interval and a date range and shows the downtime status as indicated by a color in a calendar view. It also indicates the data available and data relevance, which are defined as:

- **Data Available:** Amount of data available for the measured period of time as measured in a range of the following values:
  - 0%
  - 0.1%–33%
  - 33.1%–65.9%
  - 66%–99.9%
  - 100%
- **Data Relevance:** Relevancy of data to the reported period of time. For example, there can be data available but it is not considered (not relevant) if the associated time category is filtered out. It is indicated by the following range:
  - 0%
  - 0.1%–33%
  - 33.1%–65.9%
  - 66%–99.9%
  - 100%

7.7.3 Outages

When running any of the reports on downtime in the Operations Center dashboard, specify how an outage is determined, which impacts the downtime calculation as follows:

- **Element Outages:** An outage occurs when the condition of an element is Critical. The amount of time that the element spends in this condition is the downtime.
- **Specified Duration:** Define the threshold condition for an element at which point an outage occurs. Also specify that the amount of time that the element must be at this condition or worse before an outage occurs. By default, the default is for the element to experience an outage when the condition is Critical for 0 seconds. The downtime is the amount of time the element is experiences an outage.
- **SLA or Objective Based:** Outages are defined in objectives in SLAs. Opt to calculate the downtime based on outages as defined in a specific objective in an SLA or for the whole SLA, such as all of the objectives in an SLA.

7.7.4 Calendar

For downtime reports, specify a calendar.

The ability to apply a calendar at report time allows:

- Reporting on downtime for an element using any calendar and time category definition
- Viewing downtime that was excluded from an SLA based on the SLA calendar and specified objective time categories

Downtime is not calculated during periods on the calendar when an outage is scheduled to occur (such as blackout periods).

If you specify a different calendar when viewing downtime and availability than that used by an SLA, the downtime and availability results might differ from those used to perform the SLA calculations. Outages also respect the SLA calendar, so you might see zero outages but also see downtime if you specify a different calendar. Therefore, be consistent when specifying the calendar to use for a report so that you do not see availability and downtime numbers that do not coincide with the SLA outage and health calculations.

Table 7-5 lists some uses of the calendar options.

Table 7-5 *Implementing Scenarios for SLA Reporting*

Requirement	Then…
Ignore all blackout calendars and dialog boxes in reports	When selecting the calendar to use for the downtime reports, do not select the *Include Blackout* option for time categories.
Include all blackout calendars and dialog boxes in reports	When specifying the calendar for the downtime reports, be sure to select the *Blackout* option for time categories. Element blackout calendars are applied, as well as the specified report calendar.
Ignore a scheduled maintenance dialog box in availability and downtime reports	Create a new calendar that matches the agreement calendar but doesn't include the maintenance dialog box, then configure the report to use the new calendar for downtime. Be sure to select the time categories to report on. Element blackout calendars are applied, as well as the specified report calendar.
Ignore an outage in reports	Do one of the following: ◆ Update the calendar used by the agreement to include a maintenance dialog box when the outage occurred. Select this calendar for the SLA reports. The New Maintenance dialog box is applied to all elements under the agreement. ◆ Create a blackout calendar on the element where the outage occurred and for every parent element that it impacted. If breaches were issued during the New Blackout dialog box, be sure to clear the breaches so that they do not appear in SLA reports.

7.7.5 Time Categories

In the report, specify which time categories from the calendar are to be displayed in the report.

Downtime reports appear to filter out time categories, but the summary metrics do not exclude outages that occur during Blackout periods or any other time periods that are excluded based on *Time Category* selections.

When viewing downtime reports, filtering of time categories is independent of any agreement or objective, thereby allowing IT to assess what availability and downtime are during specific time categories, such as peak hours. For example, Blackout periods (and other time categories) can be included in an Internal IT report, in order to analyze whether service outages are occurring during scheduled maintenance periods, for example. Thus, Internal IT might decide to include/exclude Blackout periods from the availability report.

In the downtime report, the availability and downtime data values are filtered out based on the selected time categories. The Data Relevance shows an empty square icon with a value of 0 when a time period is not included in the availability and downtime metrics. In addition, an NA appears in the time periods that are filtered out of the report. Note that outage counts and durations, and the actual outage alarms are still visible in the *Outage* tab (if the display options are set to show this data) to illustrate when outages did occur. However, these outages are not affecting the availability and downtime data.

7.8 Understanding Child Downtime

Child downtime is based on the downtime of leaf children, which are defined as one of the following:

- Children with no children of their own (such as the end of a branch of the hierarchy tree)
- The lowest level specified during configuration of the report in the portlet
- The lowest level specified in the SLA definition itself

The leaf children of an element include both children in the hierarchal structure and children that contribute to the state of the parent element. For example, a parent has two children and the second child has two children of its own. From the perspective of the parent, the hierarchy looks like this:

When the SLA Status Report is configured, the level of children contributing to the data calculations is set at 3. Therefore, the parent availability is based on the availability of Child 1, Grandchild A, and Grandchild B. The availability of Child 2 is based on the availability of Grandchild A and Grandchild B. In addition to availability, the report shows the percent of outages and the percent of downtime that each leaf element contributed to its parent. Grandchild A and Grandchild B contributes to Child 2. Child 2 and Child 1 contributes to the Parent.

Child downtime is available in the SLA Status Report. This report can show daily details for today and yesterday, this month and last month, this quarter and last quarter, and monthly for this year and last year. It displays the following:

- Section 7.8.1, “Outages,” on page 111
- Section 7.8.2, “Outages Contributed,” on page 112
- Section 7.8.3, “Downtime,” on page 112
- Section 7.8.4, “Downtime Contributed,” on page 112
- Section 7.8.5, “Committed Time,” on page 112
- Section 7.8.6, “Availability,” on page 112

7.8.1 Outages

Typically when calculating the number of outages for a service, all the outages of the children are considered only in terms of their functional impact on the parent. When considering the impact of leaf children on a parent, the outage of each leaf child contributes directly to the number of outages for the parent.

Outages can be calculated based on one of the following:

- Element outages
- Outage duration and threshold

  A change in condition is considered an outage if both the minimum outage duration and the outage threshold condition are met. The minimum outage duration is the number of seconds that the element must be at the outage threshold condition for it to be considered an outage. The

outage threshold condition is the condition that the element must reach to be calculated as part of the outage. For example, if the duration of an incident is 10 seconds and the threshold condition selected is *Critical*, then the element must have a condition of `Critical` for a minimum of 10 seconds for it to have an outage.

7.8.2 Outages Contributed

Expressed as a percent, outages contributed are the number of outages that the leaf child had that impacted the parent element in comparison to the total number of outages for the parent. It is expressed as a percent. For example, if a parent had 100 outages and a child had 10 outages, then the outages contributed for the child is 10 percent.

7.8.3 Downtime

When downtime is calculated for an element based on impact to that element, only those outages on child elements that impacted the service for the element are considered. When downtime is calculated for an element based on its leaf children, all the downtime for each leaf child is factored into the downtime for the parent. Downtime can be shown in seconds, minutes, days, weeks, months, or years.

7.8.4 Downtime Contributed

Expressed as a percentage, downtime contributed is the amount of downtime that a leaf child had that impacted the parent element in comparison to the total amount of downtime for the parent. It is expressed as a percent. For example, a parent has 10 hours of downtime and a child had 1 hour of downtime, then the downtime contributed by the child is 10 percent.

7.8.5 Committed Time

To calculate the committed time of a parent based on its leaf children, the committed time of each leaf child is cumulative. For example, if a service has two servers that are leaf children and each server has a committed time of 7 days a week, then the service has a committed time of 14 days per week.

7.8.6 Availability

Availability is the amount of uptime in comparison to the committed time and is expressed as a percent. Uptime is the amount of committed time minus the amount of child downtime.

7.9 Understanding Availability

Availability is the amount of time when the condition of the element is not below a specified threshold. It is expressed as the percentage of uptime in comparison to total time as follows:

Availability = (total time downtime)/total time x 100

Disabled objectives have no impact on availability calculations. Availability is rounded so it is possible for the report to show 100% availability when it is actually between 99% and 100%. There is an option in the reports to indicate this negligible impact and if this option is used, when availability is less than 100% but not exactly 100%, the availability displays as <100% (with a down arrow).

7.9.1 Availability Reports

Availability based on objectives is available in the following reports:

- SLA Status Report
- SLA Compliance Report

For availability based on an objective, as of the first day the availability is 100% and declines over the interval specified.

Run the SLA reports only for elements that have an SLA defined. If the element does not have an SLA defined for it, no data appears in the report.

7.9.2 Availability Data Availability and Relevance

The SLA Status and SLA Compliance reports have options for calculating downtime. The downtime calculation impacts how availability is calculated. Downtime can be calculated using the element outages, outages for a specified threshold and duration, or outages as defined in an objective or SLA.

The SLA Status Report shows a summary overview of availability. They show the condition as well as the availability percentage. From within these reports click a specific piece of data and obtain more detailed information, which is the same as the SLA Compliance Report.

The SLA Compliance Report shows availability on a chart and include summary information, such as averages or first, last, highest, and lowest data. They also show data availability and data relevance, which are defined as follows:

- **Data Available:** Amount of data available for the measured period of time as measured in a range of the following values:
  - 0%
  - 0.1%–33%
  - 33.1%–65.9%
  - 66%–99.9%
  - 100%

- **Data Relevance:** Relevancy of data to the reported period of time. For example, there can be data available but it is not considered (not relevant) if the associated time category is filtered out. It is indicated by the following range:
  - 0%
  - 0.1%–33%
  - 33.1%–65.9%
  - 66%–99.9%
  - 100%

The availability and downtime data values are filtered out based on the selected time categories. Filtering of time categories is independent of any agreement or objective, thereby allowing IT to assess what availability and downtime are during specific time categories, such as peak hours. For example, Blackout periods (and other time categories) could be included in an internal IT report in order to analyze whether service outages are occurring during scheduled maintenance periods, for example. Thus, Internal IT might decide to include/exclude Blackout periods from the availability report.

The Data Relevance shows an empty square icon with a value of 0 when a time period is not included in the availability and downtime metrics. In addition, an `NA` appears in the time periods that are filtered out of the report. Note that outage counts and durations, and the actual outage alarms are still visible in the *Outage* tab (if the display options are set to show this data) to illustrate when outages did occur. However, these outages are not affecting the availability and downtime data.

7.9.3 Time-Related Options

For all availability reports, select the following time-related options:

- **Calendar:** Defines when data is collected for the availability calculation.
- **Time Categories:** Defines the periods in the calendar for which data is collected for the availability calculation.
- **Time Control:** For either an interval or date range, further defines when data is collected for the availability calculation and the time period displayed in the report.

The ability to apply a calendar at report time allows:

- **Reporting:** Reporting on downtime for an element using any calendar and time category definition.
- **Viewing:** Viewing downtime that was excluded from an SLA based on the SLA calendar and specified objective time categories.

Downtime is not calculated during periods on the calendar when an outage is scheduled to occur (such as blackout periods).

If you specify a different calendar when viewing downtime and availability than that used by an SLA, the downtime and availability results might differ from those used to perform the SLA calculations. Outages also respect the SLA calendar, so you might see zero outages but also see downtime if you specify a different calendar. Therefore, be consistent when specifying the calendar to use for your report so that you do not see availability and downtime numbers that do not coincide with the SLA outage and health calculations.

7.9.4 Calendar Option Uses

Table 7-6 lists some uses of the calendar options.

Table 7-6 *Implementing Scenarios for SLA Reporting*

Requirement	Then…
Ignore all blackout calendars and dialog boxes in reports	When selecting the calendar to use for the availability reports, do not select the *Include Blackout* option for time categories.
Include all blackout calendars and dialog boxes in reports	When specifying the calendar for the availability reports, be sure to select the *Blackout* option for time categories. Element blackout calendars are applied, as well as the specified report calendar.
Ignore a scheduled maintenance dialog box in availability and downtime reports	Create a new calendar that matches the agreement calendar but doesn't include the maintenance dialog box, then configure the report to use the new calendar for availability. Be sure to select the time categories to report on. Element blackout calendars are applied, as well as the specified report calendar.
Ignore an outage in reports	Do one of the following: ◆ Update the calendar used by the agreement to include a maintenance dialog box when the outage occurred. Select this calendar for the SLA reports. The new maintenance dialog box is applied to all elements under the agreement. ◆ Create a blackout calendar on the element where the outage occurred and for every parent element that it impacted. If breaches were issued during the new blackout dialog box, be sure to clear the breaches so that they do not appear in SLA reports.

7.10 Understanding Child Availability

Child availability is availability that is calculated based on leaf children. It is available in the SLA Status Report. For more information about child availability, see Section 7.8, "Understanding Child Downtime," on page 111.

7.11 Understanding the Key Metric

The key metric is available in the SLA Status Report and SLA Compliance Report.

These reports can include values, such as average response time, percentage of tickets closed, and so on. The value of the key metric depends on the type of objective defined in the SLA.

Table 7-7 describes how you can determine the key metric depending on the type of objective.

Table 7-7 *Determining the Key Metric*

Objective Type	Key Metric
Calculation	Calculated result (such as average, sum, count, ratio, percentage, and so on) of values meeting the criteria as a percent or result of a query on data in an external database specified in the SLA Metric Catalog properties of an element.
Availability	Availability value as a percent.
Downtime	Total downtime that has occurred so far in during the measured objective interval.
Outage	Total outage count for outages that have occurred so far during the measured objective interval.
Incident	Total incident count for incidents that have occurred so far during the measured objective interval.
Agreement	Agreement health value for specified objective.

If an objective is disabled, then the reports shows NA.

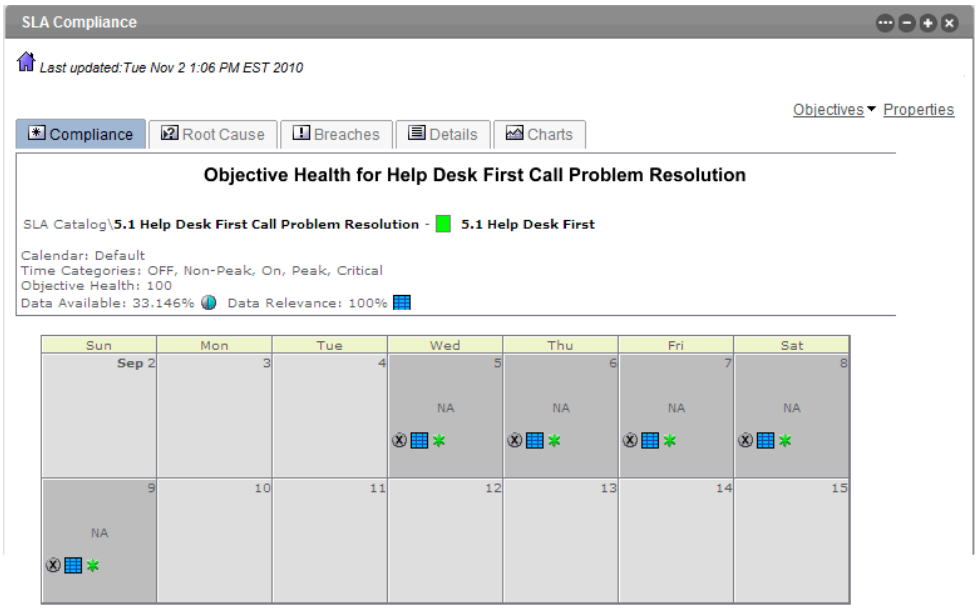
Show the key metric value for a specific objective for an SLA. In addition to displaying the value, there are the following options:

- Key metric as a percentage, which is the key metric value multiplied by 100
- Inverse of the key metric, which is 1-key metric value

If the key metric is the value from an availability objective, the availability is calculated based on either the period availability of the calendar availability (whichever was specified in the objective definition) and the calendar applied to the SLA.

If the key metric is based on a Calculation objective using an external database, then the real-time status always shows NA. The objective only fires on a monthly interval.

Figure 7-7 *SLA Compliance Report for Key Metric on Element with SLA Metric Catalog*



7.12 Understanding Exception Reporting

Exception-based reporting generates a report that only shows data when the health of an element, objective, or agreement is anything other than 100, or when availability is less than 100%. These exceptions indicate one or more of the following:

- There is a risk in meeting compliance
- The selected agreement or objective has already failed
- The element is not 100% available
- The data is not available

The SLA Compliance Report can be used for exception reporting. Only the *Details* tab and the *Chart* tab displays are affected by this option. This option does not affect the downtime report.

To report on elements that are not in full health for an SLA Compliance Report, select the *Show Only Exceptions* check box.

7.13 Understanding Report Usage Options

The following options are available for the reports on SLA information in the Operations Center dashboard:

- **Localization:** The time zone in which data appears can also be changed; the default is the time zone of the Operations Center server.
- **Schedule to Run:** The report can be configured to include live data at all time; however, this could take a lot of bandwidth. The report can also be scheduled to run on a regular basis.

For more information about these options, see the *Operations Center 5.5 Dashboard Guide*.

8 Remote SLA Reporting

Typically, reports include data from the local Operations Center server. The Remote SLA Reporting function can consolidate reporting on SLAs stored on multiple servers. Locally view SLA data from remote servers, as well as configure reports that include SLA data from remote servers and the local server.

The ability to access and use remote SLA data locally makes it possible to have multiple data warehouses for performance reasons and avoid redundant data storage by not requiring all SLA data to be stored in a single, centralized database.

The Remote SLA Reporting function enables managing data for multiple customers, both internal and external, on multiple servers in possibly varied locations while providing a mechanism to consolidate all the data for reporting purposes. You are able to set security permissions.

Consider the example of a company that uses two Operations Center server with SLM to monitor internal IT services both for their own internal IT and for a remote customer site. A single IT manager is responsible for all the IT services at both sites where each have specific Service Level Agreements (SLAs). So he wants to be able to open his dashboard connected to his local Operations Center server and view a report that contains information related to compliance on all SLAs, both those stored locally and those stored remotely. The Remote SLA Reporting function allows creating such a report for that manager's dashboard.

To use the Remote SLA Reporting function, first configure the remote SLA data so it can be viewed in the Operations Center console, then generate reports on the remote SLA data by using the reports in the Operations Center dashboard.

8.1 Configuring Remote SLA Data

Before you can view remote SLA data in the console of the local Operations Center server or use the remote SLA data in reports, you must do the following:

8.1.1 Configuring Server Communication

For a local Operations Center server to use data on another Operations Center server, communication must be established between the servers. An InterCommunication adapter is required on both the local and remote servers for a local server to access remote elements. For steps to create an adapter, see the *Operations Center 5.5 Adapter and Integration Guide*.

In addition, both the local and remote servers must be licensed for both Operations Center and SLM.

8.1.2 Enabling SLA to Display Remotely

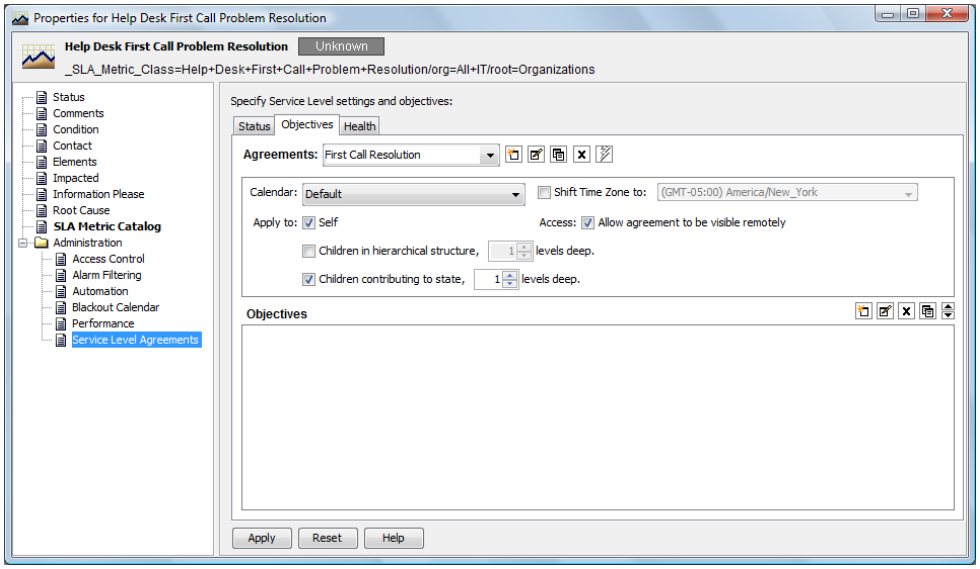
In order to collect data for both local and remote elements, it is necessary to define and set local SLAs.

Note that SLA definitions support inclusion of local agreements and objectives only. Remotely defined agreements and objectives are not included in local SLA calculations. The Agreement objective and Calculation objective cannot reference remotely defined agreements or objectives. For example, you must define a local router agreement on a remote router element in order for the router agreement to be included in another local service agreement via the Agreement objective.

To make SLA data for an element remotely accessible, use the following steps while working in the SLA objectives for that element.

To make SLA data available remotely:

1. On each server, locate the elements whose SLA data should be available remotely.
2. In the *Explorer* pane, right-click an element, then select *Properties*:
3. In the left pane, click *Service Level Agreements*.
4. Click the *Objectives* tab to display the agreements and objectives.



5. Select an agreement in the *Agreements* drop-down list.
6. In the *Agreements* section, select the *Allow Agreement to Be Visible Remotely* check box.
7. Click *Apply* to save changes.

8.1.3 Setting Data Security

Security permissions set on remote servers can allow local users/customers to view only those elements and SLAs that are relevant to the local users/customer. Security permissions set on the local server can further restrict access to SLA data and portal pages/views. For more information about security permissions, see the *Operations Center 5.5 Security Management Guide*.

8.2 Viewing Remote SLA Data

After your local server has been configured to access remote SLA data, view the specifics of the remote agreements in the property page of the elements. Also display performance data for elements based on these agreements in the *Performance* view.

- Section 8.2.1, "Viewing Remote Service Level Agreements," on page 121
- Section 8.2.2, "Viewing Remote SLA Data in the Performance View," on page 121

8.2.1 Viewing Remote Service Level Agreements

To see if an element has remote agreements applied to it, access the Service Level Agreement property page for the element's properties. On this page, use the Details and Root Cause links to identify factors contributing to the agreement status.

To view the details of both local and remote SLAs on a specific element:

1. In the *Explorer* pane, expand *Elements*, right-click an element, then select *Properties*.
2. Under *Administration*, click *Service Level Agreements*.

   All SLAs set on the element display under *Local Agreements* or *Remote Agreements*.

8.2.2 Viewing Remote SLA Data in the Performance View

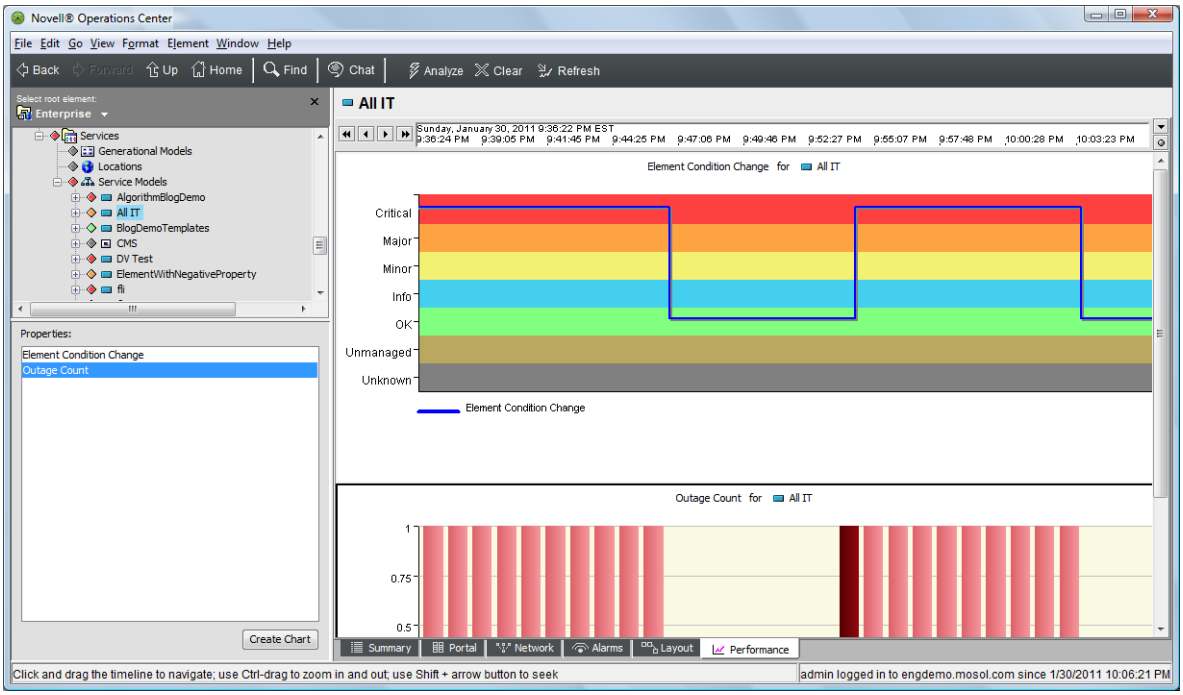
From the *Performance* view in the Operations Center console, view performance data for a specific element or multiple elements.

All Performance charts in the *Performance* view support user selection of remote elements for viewing the following SLA data:

- Agreement and objective availability (not element availability)
- Agreement and objective downtime (not element downtime)
- Agreement and objective outage counts (not element outage counts)
- Agreement and objective health
- Agreement and objective breach counts
- Element condition change data
- Performance metrics (alarm or element properties)

Figure 8-1 shows an Element Condition Change line chart for a remote element:

Figure 8-1 *Performance View*



The chart tracks condition changes for the remote element Test 2, which displays beneath the InterCommunication adapter, and which connects the local and remote servers.

8.3 Generating Reports on Remote SLA Data

When generating SLA reports in the dashboard, the portal/query engine can make requests that are routed to either local or remote servers in order to report on all relevant SLA data that a user has permissions to access and view.

- Section 8.3.1, “SLA Metrics,” on page 122
- Section 8.3.2, “Troubleshooting Remote SLA Data Access Problems,” on page 123

8.3.1 SLA Metrics

The following SLA metrics are available for remote elements for SLA compliance reports:

- Agreement and objective availability (not element availability)
- Agreement and objective downtime (not element downtime)
- Agreement and objective outages and outage counts (not element outages and outage counts)
- Agreement and objective health
- Agreement and objective key metric
- Agreement and objective breach alarms and breach counts
- Agreement and objective service level metric alarms

- Element condition change data
- Performance metrics (alarm or element properties)

For all Alarms listings, select the following data for elements with remote SLAs:

- Outages
- Service Level Breaches (Agreement and Objective)
- Service Level Metrics (Agreement and Objective)

Similar to SLA reports for local data, all queries for SLA reports support filtering options, such as time intervals, calendars, time categories, warnings, and so on. However, it is not possible to view remote time category names over the InterCommunication connection. Therefore, only the local time category names display. If a remote SLA has a remote calendar definition, the SLA engine calculates the appropriate values based on the remote time categories, but the local portal displays time category names based on the local server definition only.

When creating an SLA report, both the local and remote agreements and objectives display in the portal selection list. The remote agreements begin with the word "Remote."

8.3.2 Troubleshooting Remote SLA Data Access Problems

If you experience problems accessing remote SLA data, the following common reasons might prevent viewing all remote SLAs for a remote element:

- **Check box not selected:** Open the remote element's Service Level Agreements property page. In the SLA's *Objectives* tab, the *Allow Agreement to Be Visible Remotely* check box should be selected.
- **Missing permissions:** Verify the InterCommunication adapter user has appropriate permissions on the remote server to access the SLA on the remote element.

9 Analyzing Performance

Performance metrics can be charted to provide an indication of how an element is performing. Performance metrics can be any property that is captured via a profile and expression in Operations Center.

For information on configuring performance metrics and basic charting instructions, see "Charting Performance Data" in *Operations Center 5.5 User Guide*.

By default, when you create a Service Level Agreement for any element, the service level profile is automatically applied to it and element condition change including outages is captured as part of this profile. You can also apply other profiles and expressions to an element that are predefined or define your own profiles and expressions.

9.1 Understanding Property Types

You can create charts to analyze performance metrics over time. The types of charts available are stacked bar charts, condition charts, and line charts. The type of chart available depends on the property being analyzed. Table 9-1 lists the chart types available for various property types.

Table 9-1 *Alarm History and Historical Performance Property Types and Corresponding Chart Types*

Property Type	Chart Type
Alarm Column	Varies by data type. Line Chart created for most columns, except for Severity, which creates a Condition Line chart.
Alarm Severity Counts	Stacked Bar
Child Condition Counts	Stacked Bar
Element Condition	Condition
Element Condition Change	Condition.
Element Property	Varies by data type. Line chart created for most properties; Condition chart created for some properties.
Performance Series	Line
Script	Varies by data type.

Other properties are also available to chart, depending on the properties captured, or if a Service Level Agreement is defined. For example, when a Service Level Agreement is applied with an availability objective, `Availability` and `Outage Count` metrics are often available to chart.

Table 9-2 lists the chart types available for SLA property types.

Table 9-2 *SLA Property Types and Corresponding Chart Types*

Property Type	Chart Type
Availability	Line
Outage Count	Stacked Bar

When charting SLA metrics in the Operations Center console's Performance view, it can take up to several minutes before a refreshed or new chart registers an update, while updates for other property types are received and charted in near-real-time. In this case, the server has not yet recorded update data for `Availability` and `Outage Count` properties.

When charting metrics, if there is no data for the time range selected, the chart displays with no data.

Charts can be created using the following tools:

- Section 9.3, "Viewing Performance and Performance Analysis in the Operations Center Console," on page 129
- Section 9.4, "Using the Performance Portlet in the Dashboard," on page 130

9.2 Understanding Chart Types

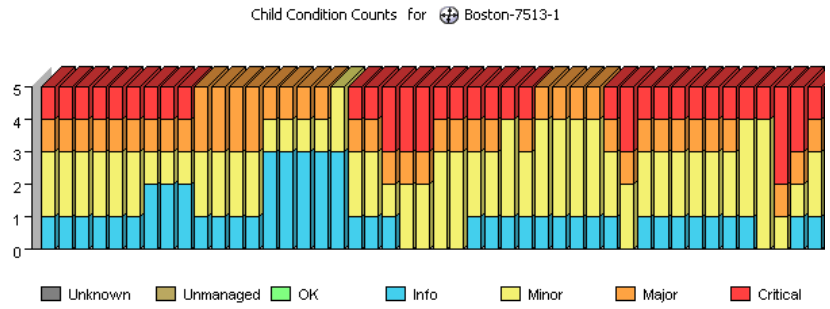
The type of charts available depends on the property for which you are analyzing performance. Three main types of charts are available: stacked bar charts, condition charts, and line charts. The chart type is automatically selected based on the type of property selected.

- Section 9.2.1, "Understanding Stacked Bar Charts," on page 127
- Section 9.2.2, "Understanding Condition Charts," on page 127
- Section 9.2.3, "Understanding Line Charts," on page 128

9.2.1 Understanding Stacked Bar Charts

Stacked Bar charts are normally used for alarm severity counts or child condition counts. They provide the alarm totals by severity for an element at a given point in time. Figure 9-1 shows the child condition counts for an element:

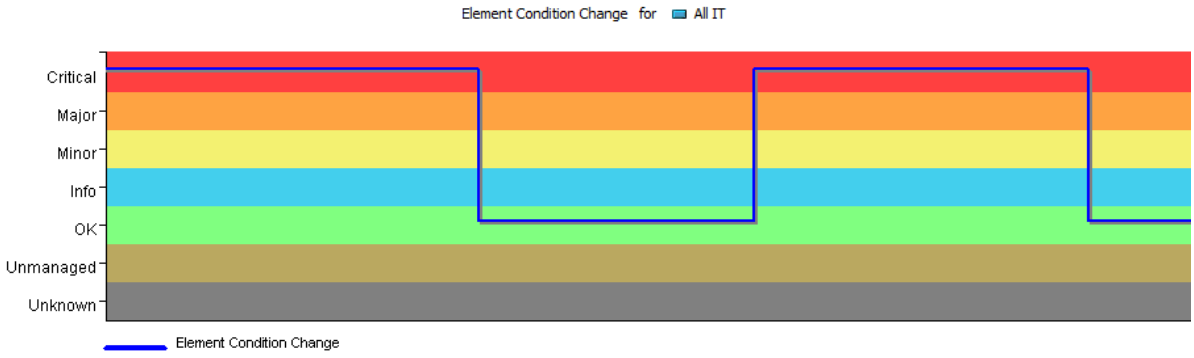
Figure 9-1 *Stacked Bar Chart*



9.2.2 Understanding Condition Charts

Condition charts use one or more lines to track element conditions over time. The background band of condition colors helps you identify the changes. The chart in illustrated in Figure 9-2 tracks changing conditions for an element.

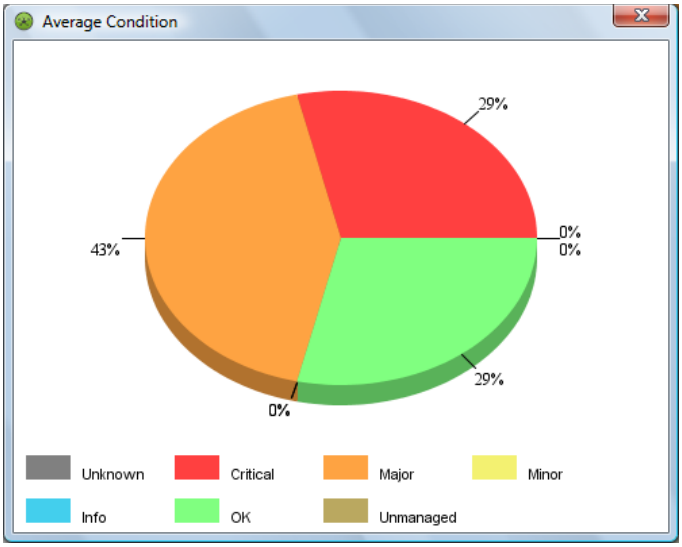
Figure 9-2 *Condition Line Chart in the Operations Center Console*



When charting condition changes for performance metrics or SLAs, the chart render in the Performance report in Operations Center dashboard is a typical line chart and looks different from the stepped line chart that is available in the Operations Center console.

Average condition information is available in a pie chart from the Condition Line chart in the Operations Center console. The pie chart identifies the percentage of time that the element was in each condition (Critical, Major, Minor, and so on) for the given time period. The chart in Figure 9-3 shows the element was in Critical and Major condition for equal percentages of time, and in OK condition for the remaining 20 percent of the time:

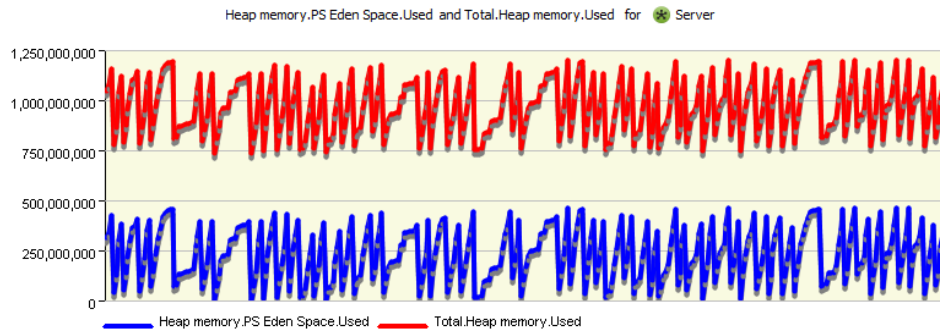
Figure 9-3 *Average Condition Pie Chart*



9.2.3 Understanding Line Charts

Line charts use lines to connect property value data points over time. The chart illustrated in Figure 9-4 tracks two properties, the percentage of CPU utilization and idle time, for two elements. Different colored lines are used for each combination of property and element.

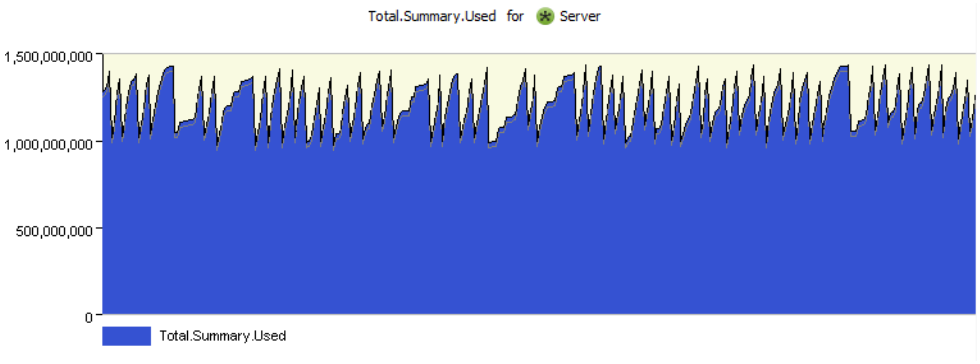
Figure 9-4 *Multielement Line Chart*



If only one element is charted, a single line can be displayed or an area line chart can be displayed in the Operations Center console. The area line chart fills in the range between zero and the line value to improve the visual presentation of data changes and trends.

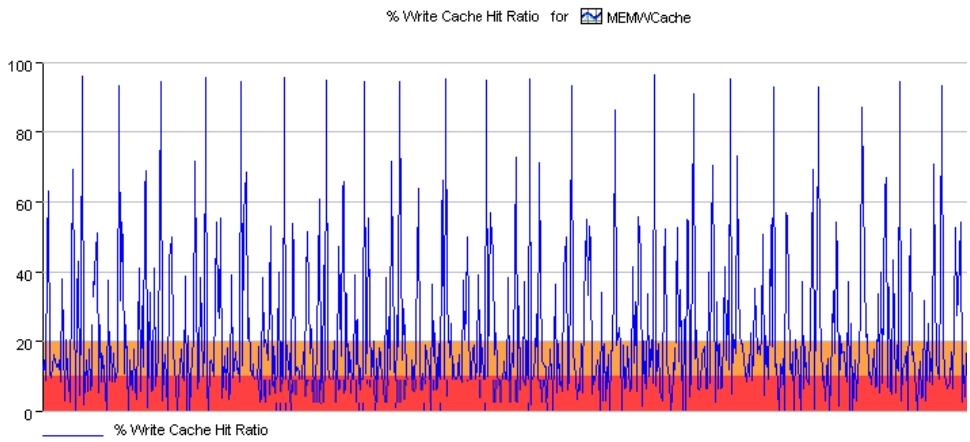
The area line chart illustrated in Figure 9-5 tracks the % Write Cache Hit Ratio property values every five minutes for one element, MEMWCache.

Figure 9-5 *Area Line Chart*



When available from the native element (on some *Event Manager* and *PATROL* elements), the performance chart renders both warning and alarm thresholds visually. For example, in Figure 9-6 where the Write Cache Hit Ratio falls below 20, it is considered to be at warning level, and when falling below 10 it is a Critical violation:

Figure 9-6 *Line Chart Including a Warning and Critical Threshold*



9.3 Viewing Performance and Performance Analysis in the Operations Center Console

The *Performance* view and the *Performance Analysis* view in the Operations Center console allow you to create performance charts for a single element. In the *Performance Analysis* view, chart multiple elements as a means of comparison.

Both the *Performance* view and the *Performance Analysis* view have similar functionality. However, in addition to comparing metrics for multiple elements, the *Performance Analysis* view displays alarm information in a format that is the same as the *Alarms* view.

When charting SLA metrics, it can take up to several minutes before a refreshed or new chart registers an update, while updates for other property types are received and charted in near-real-time. In this case, the server has not yet recorded update data for `Availability` and `Outage Count` properties.

To view performance metrics:

1 Do one of the following to view *Performance* metrics:

   1a Select the element in the hierarchy in the Operations Center console, then click the *Performance* tab along the bottom of the window.

   If you do not wish to compare performance metrics on more than one element, skip to Step 3.

   1b From within the *Performance* view, click *Analyze* on the top menu bar to open the *Performance Analysis* window.

   The properties of the element for which you can create charts on is listed in the Properties dialog box in the bottom left.

2 If working from the *Performance Analysis* window, select any additional elements that you wish to chart data for.

   An element name, in bold typeface, indicates active performance profiles are collecting data for that element. Even if an element does not have active performance profiles, you can chart any historical data collected for them.

3 Select a property, then click *Create Chart*.

4 To set the time interval to chart, use the bar at the top of the window.

5 In a condition chart, such as an Element Condition chart, view the average condition in a pie chart by right-clicking in the condition chart, then selecting *Show Average Condition* in pie chart.

6 In a line chart, fill the area between zero and the line for better visual representation by clicking the line chart, then selecting *Fill*.

7 Export the data in a specific chart by right-clicking the chart, then selecting *Export Performance*.

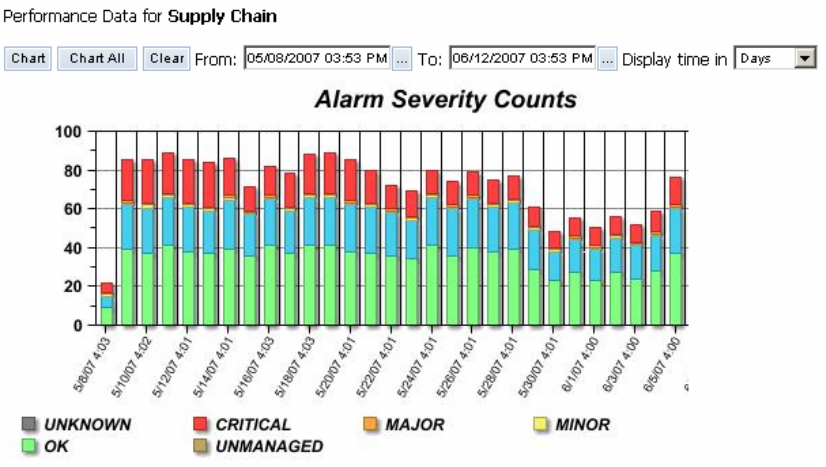
8 Save your settings in the *Performance Analysis* view by clicking *Save*.

For more information about the *Performance* view, see the *Operations Center 5.5 User Guide*.

9.4 Using the Performance Portlet in the Dashboard

The Performance portlet in the Operations Center dashboard can create a chart to show alarm severity counts or child condition counts on a chart.

Figure 9-7 *Performance Component Showing Alarm Severity Counts*



To create a chart to show alarm severity counts or child condition counts on a chart in the Dashboard:

1. Select either *Alarm Severity Counts* or *Child Condition Counts*, or both.

   If the data is incompatible, nothing displays on the chart.

2. To display the time (minutes, hours, days, weeks, months, or years), select the time period to chart.

   For each time period, there is a maximum amount of data that can be displayed.

   For more information see the *Operations Center 5.5 Dashboard Guide*.

10 Adjusting Data

Operations Center provides a way to enter outages for an element. For example, a device can be down, but data for this outage might not be available in the Business Service Warehouse. An outage that lasted 6 minutes was only recorded as lasting 1 minute. These types of discrepancies might occur when the Operations Center server is down or when data is not fed directly to Operations Center in real time. Manual outages can be used to record these untracked outages.

There are two methods for entering element outages:

- Create an outage for a specific element in the Operations Center console
- Use a JavaScript to create outages

Manually creating an outage has an impact on SLA calculations in terms of when the outage is calculated and how the outage interacts with other system-generated outages if there is an overlap. There is a way to create outages so they have no impact on SLAs.

10.1 Entering Outages in the Console

Manual outages can be created on any specific element by right-clicking the element, then selecting *Create Outage*.

After an outage is manually created, it can be edited and cleared at any time through options available directly on the outage in the *Alarms* view while viewing *Historical* > *Outages*. Manual outages entries are bolded by default for easy identification and have an *Alarm Type* value of `Manual`. As a manual outage is updated and edited, the history is retained and can be viewed in alarm properties.

Manual outages are stored in the Service Warehouse. If you suspect a manual outage is not applied immediately to agreement real-time calculations, you might need to perform a manual calculation on agreements.

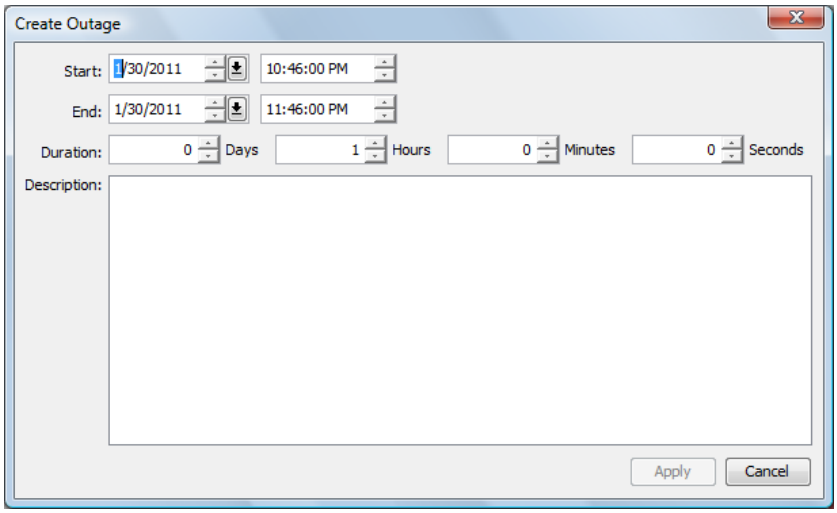
NOTE: Real-time breaches are not created for manual outages as they would for real-time outages. However breaches are simulated and included for manual outages in SLA reports. For more information, see Section 10.3, “Understanding Manual Outages in Breach Reporting,” on page 137.

Only the most current entry of a manual outage is included in Service Level Agreement calculations. Cleared outages are excluded from all Service Level Agreement calculations.

10.1.1 Specifying a Manual Outage for an Element

To specify a manual outage:

1 In the *Explorer* pane, right-click an element, then select *Create Outage*.



2 Specify the Start date and time of the outage.

3 Specify the End date and time of the outage.

or

Specify the Duration of the outage in days, hours, minutes, and/or seconds.

If the Duration is specified, the End date and time is automatically updated.

4 Specify a description in the *Description* field.

This descriptive text displays as part of the outage alarm in the *Comment* column.

5 Click *Apply* to save and apply the manual outage to the associated element.

10.1.2 Editing a Manual Outage

To edit a manual outage:

1 In the *Explorer* pane, navigate to and click an element.

2 In the view pane, click the *Alarms* tab to open the *Alarms* view.

3 On the toolbar, click *Alarms*, then click *Historical* > *Outages*.

4 Adjust the timeline selector to show the time range that includes the manual outage.

5 Click *Retrieve*.

6 Right-click the manual outage, then select *Edit Outage*.

7 Update the outage as required.

8 Click *Apply* to save the outage settings.

10.1.3 Clearing a Manual Outage

To clear a manual outage:

1 In the *Alarms* view, right-click the outage, then select *Clear Outage*.

A confirmation message asks for you to confirm the deletion.

2 Click *Yes* to confirm the deletion.

The outage receives a deletion entry and displays in the *Historical Alarms Outage* view as a strikethrough entry.

10.1.4 Viewing Manual Outages

To view manual outages:

1 In the *Explorer* pane, navigate to and click an element.

2 In the view pane, click the *Alarms* tab to open the *Alarms* view.

3 On the toolbar, click *Alarms*, then click *Historical* > *Outages*.

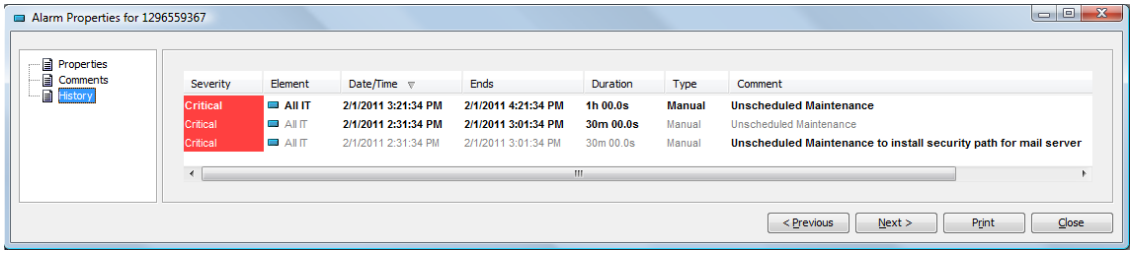
4 Use the timeline selector to select the time range, then click *Retrieve*.

All generated and manual outages for the selected time range display in the *Alarms* view. Manual outages display as bolded entries.

10.1.5 Viewing the History of a Manual Outage

To view manual outage history:

1 In the *Alarms* view, right-click the outage, then select *Properties*:



2 In the left pane, click *History*.

Each change in the outage is listed as a line item. Changed or updated items are bolded, as shown in the *Ends* and *Duration* columns in the illustration in Step 1.

10.2 Entering Outages by JavaScript

JavaScript can be used to create outages via a client automation script or custom client operation. This can be useful when outage data is obtained from an external source, such as a service provider, on a regular or scheduled basis.

NOTE: Real-time breaches are not created for manual outages as they would for real-time outages. However breaches are simulated and included for manual outages in SLA reports. For more information, see Section 10.3, "Understanding Manual Outages in Breach Reporting," on page 137.

The following script snippet illustrates how a script automation can create outages based on alarm information. This script expects a start and end date as alarm columns (*mDateTimeOpened* and *mDateTimeClosed*) as these are required for a manually created outage. alarm is any alarm passed as a parameter when the automation script is executed. The element on which the outage is created is defined by alarm.element and is the affected element of the alarm.

```
rootorg="root=Elements";
formula.log.info("autooutage starts " );
dateformat="yyyy-MM-dd hh:mm:ss";
var formatter=new java.text.SimpleDateFormat(dateformat);

ticketnumber=alarm.originating_event_id;
startdate=alarm.mDateTimeOpened;
try {
     startdated=formatter.parse(startdate);
} catch (Exception) {
     formula.log.error("Error parsing startdate " + Exception);
     startdated=new Date();
}
enddate=alarm.mDateTimeClosed;
try {
     enddated=formatter.parse(enddate);
} catch (Exception) {
     formula.log.error("Error parsing enddate " + Exception);
     enddated=new Date();
}

TTwhoPerform="AutomationOutager";
TTreason=alarm.msg;
TTreason="res:" + alarm.getField('Description');
myelement=alarm.element;

var alarmFields=new java.util.Hashtable;
alarmFields.put("myDate", new java.util.Date())
alarmFields.put("myOS", "Windows XP")
alarmFields.put("myID", "101")
var alarmFieldbyteArray = null
var bos = new java.io.ByteArrayOutputStream();
var oos = new java.io.ObjectOutputStream(bos);
oos.writeObject(alarmFields);
oos.close();
alarmFieldbyteArray = bos.toByteArray();

var from = new java.util.Date()
var to = from.getTime() + 100000

// (required) params[0] -> dname as string (required)
// (required) params[1] -> from date as long
// (required) params[2] -> to date as long
// (required) params[3] -> type as int (0 = GENERATED, 1 = SUPPRESS, 2 = OUTAGE)
// (required) params[4] -> reason as string
// (optional) params[5] -> extra alarm columns/values as serialized HashTable key/
value pairs.

try {
```

```
  myelement.perform( session, "Create|Outage", [],
       [myelement.getDName(), startdated.getTime(), enddated.getTime(), 2,
TTreason, alarmFieldbyteArray ])
} catch (Exception) {
   formula.log.error("Error adding outage 1 " + Exception);
   try {
      myelement.perform( server.automationSession, "Create|Outage", [],
            [myelement.getDName(), startdated.getTime(), enddated.getTime(), 2,
TTreason, alarmFieldbyteArray ])
   } catch (Exception) {
        formula.log.error("Error adding outage 2 " + Exception);
   }
}
formula.log.info("autooutage ends " + TTreason + " " +  alarm);
```

10.3 Understanding Manual Outages in Breach Reporting

The SLA engine does not process manual outages in the same way as it does for real-time outages. While a real-time breach is created when real-time outage occurs, a breach is not created as a result of a manual outage. Therefore, there are no breaches corresponding to manual outages listed in *Alarms* view while viewing *Historical* > *Outages*.

However, manual outages are considered when calculating the SLA reports. Because manual breaches are simulated during report generation, and not queried breaches saved in the Service Warehouse, they are included in the SLA reports for any manual outages.

10.4 Understanding Impact on SLA Calculations and Recalculating

When Operations Center receives manual or imported alarms, it perceives them as historical alarms that should not affect the element's real-time state. However, all outages or metric alarms do affect the real-time condition of related elements because they are perceived as new alarms for those elements.

- Section 10.4.1, "Understanding Outage Calculations," on page 137
- Section 10.4.2, "Forcing Recalculation," on page 138

10.4.1 Understanding Outage Calculations

Manual outages or imported historical outages or metric data affecting objectives within the current measured interval might not be applied immediately to SLA's real-time calculations. The real-time state reported in the Operations Center console and reports in the Operations Center dashboard could be inaccurate unless a manual calculation is performed. The Operations Center dashboard's SLA reports automatically detect new metric and/or condition data and reports correctly.

Manual outages, alarms, and metrics for future intervals are also not automatically reflected in real-time SLA calculations. To apply them to real-time state, health, and metrics, you must perform a manual calculation on SLAs after the date and time of the alarm has been reached.

Alarms not being applied to SLAs can occur because of timing issues between time to write to the BSW and when the next calculation of state occurs. If the outage data is not received by the BSW before a calculation process, it must wait for the next calculation.

Note that data in the BSW is not read except on server restart, warehouse or profile restart, or when saving an SLA definition.

Running a manual calculation of agreements runs a recalculation of agreement real-time state, health, and metrics (including metric properties), and includes all agreements and objectives applied to the element.

10.4.2 Forcing Recalculation

To force a recalculation of agreement state, health, and metrics:

1. Right-click any element that is measured by the agreement, then select *Recalculate Real-Time Agreements*.
2. Perform this operation on the same element where the manual outage was created or for which historical data was imported.

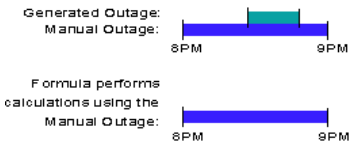
   All agreements and objectives applied to the selected element are recalculated.

10.5 Understanding Outage Overlap Issues

Because manual outages can be created at anytime and affect any range of time, it is possible that they can overlap a generated outage caused by real-time condition changes. Manual outages always take precedence over generated outages.

Occasionally, a manual outage totally contains a generated outage. One example is when the generated outage occurs within the same time as the manual outage, but the manual outage starts prior to the generated outage and ends after the generated outage — the manual outage take precedence over the generated outage. Figure 10-1 shows an example:

Figure 10-1 *Manual Outage Graph*



When a manual outage only partially overlaps a generated outage, Operations Center creates multiple outage entries as a result of allowing the manual outage to take precedence for the duration of the manual outage.

When generated outages partially overlap, the outage type displays as Partial. In this case, the original system generated outage displays as a historical outage entry in the *Alarms* view (but not in the alarm History property page).

However, when a generated outage exists within a manual outage, the generated outage appears as a historical outage entry for the manual outage with the outage type of Full overlap.

10.6 Understanding Outages with No Impact on SLAs

To create a manual outage or to import outage and metric data without affecting the element's state in Operations Center, consider the following strategies:

- Import the metric data with all alarm severities set to OK. Calculations are not affected if all severities are set to OK.
- Use the element's condition algorithm to set its condition to OK. After the import or manual update is complete, change the algorithm to its original settings.

When historical metric data is fed to Operations Center using either strategy, SLA availability, downtime and outage data based on element condition change data do not accurately reflect the state of a business metric because all condition data display as OK.

A Service Level Management Demo

A demo database adapter, BusinessMetricDemo, showcasing business-based metrics, such as number of invoices processed and number of invoices rejected, is installed with Operations Center in the `/OperationsCenter_install_path/demos` directory. This demo system is customizable to leverage virtually any business metric data.

In order to use the Business Metric demo adapter, first create the demo database. After the database is created, the adapter is created to surface business data in Operations Center.

To demonstrate business-based service level objectives, such as number of invoices processed per hour or revenue generated daily, a database definition needs to be created for the Business Service Warehouse (BSW). The database definition must be created for the Data Warehouse Engine as well as the SLM Engine to run. After the database definition is created and configured, the SLM Engine starts to collect and measure against defined Service Level Agreements (SLAs) and objectives, and the Data Warehouse Engine starts to store all collected data.

Operational Level Agreements are defined in the Operations Center browser. This demo creates simple SLAs. After data is captured, the SLA data can be viewed in the Operations Center console and the dashboard.

A.1 Before You Start

This demo assumes that:

- Microsoft SQL Server is installed.

  When installing, use all defaults.

  If you want to use a different DBMS, you must manually edit the `BusinessMetroDemo.sql` file and make the necessary changes to support the selected DBMS.
- Operations Center has a Service Warehouse database definition created and enabled, and the Data Warehouse is running.

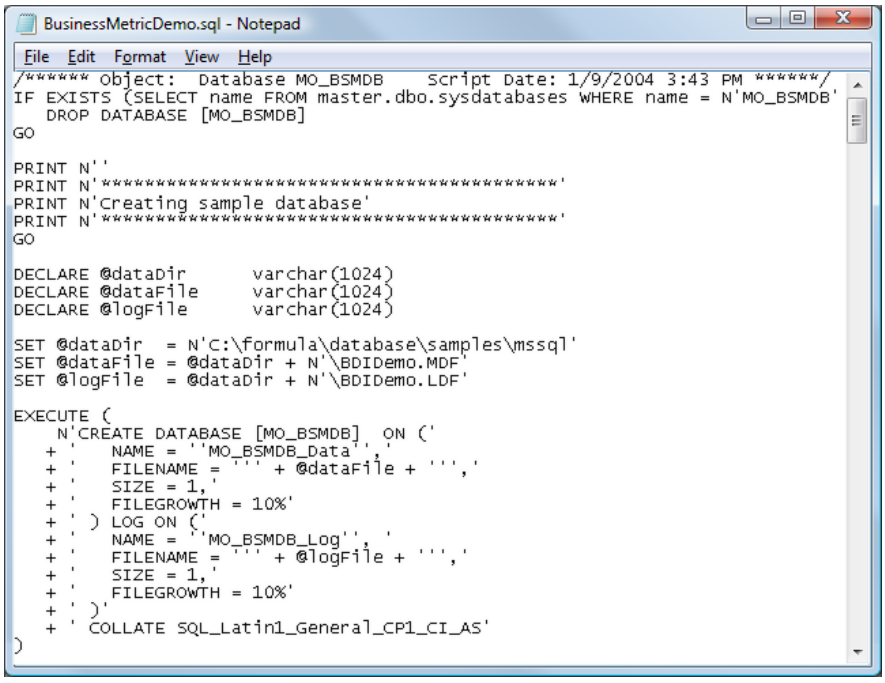
  For more instructions on setting up a Service Warehouse database definition, see the *Operations Center 5.5 Server Configuration Guide*.

A.2 Step 1. Create the Business Metric Demo Database

The SLA Demo utilizes the `BusinessMetricDemo.sql` script to create a database demo. The first steps are to access the demo script in order to make changes to it, then execute the script to create the demo database.

To customize the demo script:

1 Open the */OperationsCenter_install_path*`/demo/template/BusinessMetricDemo.sql` file in a text editor.



2 To use a different name for the database, replace the database name, MO_BSMDB, with the new database name, for all occurrences in the script.

The database name is listed in several places in the script.

3 If you change the database demo name, be sure to change the database name in the adapter properties.

For more information, see Section A.3, “Step 2. Create a Business Metric Demo Adapter,” on page 143.

4 (Optional) Change the directory to store the data in a different location.

The data directory is the directory where the demo data, BDIDemo.MDF and BDIDemo.LDF is created.

5 Save the script file with a unique name.

Then using your SQL Server tools, execute the modified */OperationsCenter_install_path*/demo/template/BusinessMetricDemo.sql script to create the demo database and populate it with demo data.

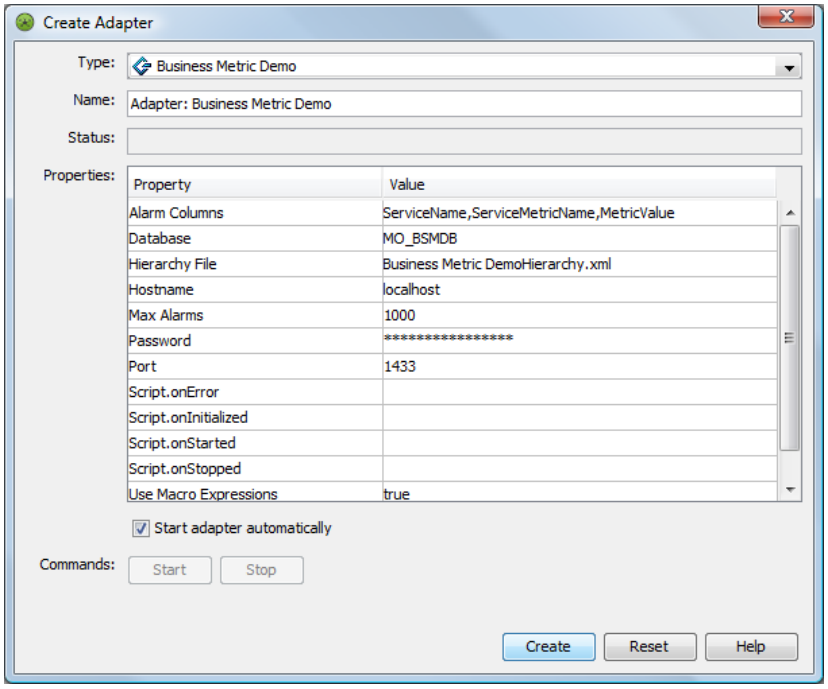
A.3 Step 2. Create a Business Metric Demo Adapter

After the demo database is created, a Data Integrator adapter needs to be created to tap into the database. A Data Integrator definition, Business Metric Demo adapter already exists.

- Section A.3.1, "Creating the Business Metric Demo Adapter," on page 143
- Section A.3.2, "Generating Data," on page 145

A.3.1 Creating the Business Metric Demo Adapter

1. In the *Explorer* pane, expand the *Administration* root element.
2. Right-click *Adapters*, then select *Create Adapter* to open its dialog box:



3. Click the *Type* drop-down list, then select *Business Metric Demo*.
4. Edit the Database property value if not using the default the demo database name.
5. If necessary, specify the host name.

   The host name defaults to localhost, assuming your local machine is running Operations Center.

   The Port connects to the database and the default SQL server port, 1433, displays.
6. If necessary, change the port number.
7. If necessary, specify new user name and password, as defined by your administrator.

   The Username and Password are the defaults used to connect to the database.

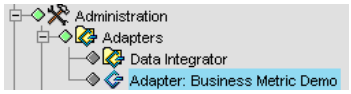
   The user must have appropriate SQL permissions to read from the demo database. The default user is `sa` and the default password is `admin`.

8 Select the *Start Adapter Automatically* check box to start the adapter automatically after it has been created.

Otherwise, you must start the adapter manually each time.

9 Click *Create* to create the adapter.

The adapter starts automatically if the *Start Adapter Automatically* check box was selected:

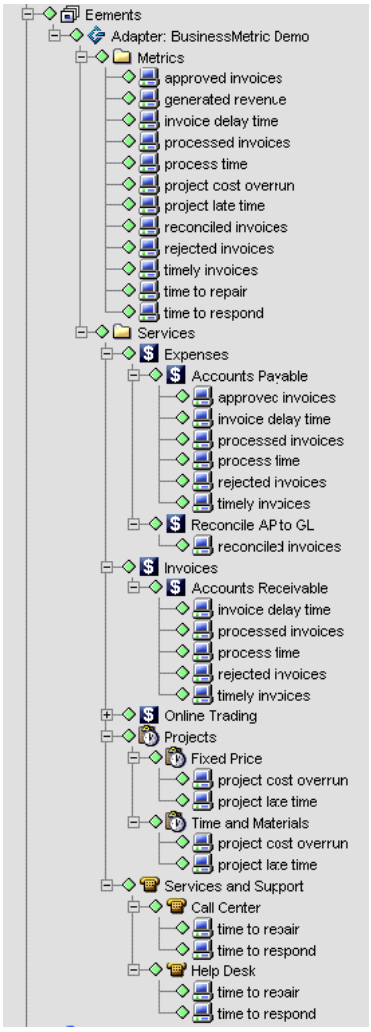


The adapter displays elements from the demo database in the *Explorer* pane.

10 In the *Explorer* pane, expand *Elements* > *Adapter: BusinessMetric Demo* > *Metrics*.

11 Double-click *Services*.

Figure A-1 *Explorer Pane. Elements from the Demo database display.*



The Business Metric Demo adapter is a Data Integrator adapter definition that instructs Operations Center to pull data populated in the BusinessMetric database to produce a demo hierarchy for metrics and services.

Each *Services* branch contains elements that represent services (such as *Expenses*, *Invoices*, *Online Trading*, *Projects*, and *Services and Support*), which contain specific business metrics as modeled by elements (such as time to repair or invoice delay time). For example, the Expense service contains child services, Accounts Payable and Reconciled AP to GL.

Their state or condition is fed by alarms that are created for business metrics. For example, if 950 invoices approved per hour, then the condition is in an OK state.

The hierarchy produced represents the metrics as a top-level objects as well as specific elements underneath the services.

A.3.2 Generating Data

The Business Metric adapter is set to poll hourly for updates from the database.

A batch data fill utility, `/ManagedObjects/demo/BusinessMetricGenData.bat`, to generate new data on minute or hourly intervals. We recommend setting it for Hourly intervals, which allows state changes in the data over time.

The Business Metric Demo performs a query on adapter start that reads data that is current as of the last hour.

If the adapter or your server is restarted after the initial install, there might not be any alarms, unless the restart/start occurs within an hour of the last alarms being generated for the MO_BSMDB database.

This means that the `BusinessMetricDemoGenData.bat` file must be run to generate new alarms. The adapter polls the database hourly for any updates or deletions, and adds and removes alarms from the Operations Center server based on the changes to the database. The alarms held in memory are automatically removed after the total number of alarms exceeds the max alarm limit as defined in the adapter properties, which is by default set to 1K.

If the demo being utilized for an extended amount of time, it is a good idea to rerun the `BusinessMetricDemo.sql` script on occasion to clear the database and start over. The demo database can become very large as there is currently no mechanism to delete records and in this case, records are continually being added to when the `BusinessMetricDemoGenData.bat` is run to insert new records.

A.4 Step 3. Create a Service Hierarchy

After the database connection is established and the Business Metric Demo adapter is running, the next step is to set up a service hierarchy that you can define SLAs on.

For demo purposes, the organizational structure is very simple and requires the creation of two elements that have element children.

- Section A.4.1, “Creating the Service Hierarchy,” on page 146
- Section A.4.2, “Linking the New Elements,” on page 146

A.4.1 Creating the Service Hierarchy

1. In the *Explorer* pane, expand *Enterprise* > *Services*.
2. Right-click *Service Models*, then select *Add Element* to open its dialog box.
3. Enter Customers in the *Title* field.
4. Click *Finish* to add this element.
5. Right-click *Customers*, then select *Add Element* to add *Customer2*.

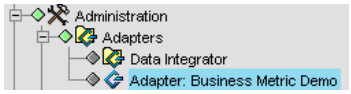
A.4.2 Linking the New Elements

After creating the elements, you should link them to the elements pulled from the demo database.

To link the new elements:

1. In the *Explorer* pane, click *Customer2*.
2. In the view pane, click the *Layout* tab.
3. In the *Explorer* pane, navigate to *Adapter:Business Metric Demo* without selecting it.

   To do this, click the plus sign next to *Elements* > *Adapter:Business Metric Demo*:



4. Drag the *Services* folder to the open *Layout* view for the *Customer2* element.

   A relationship between the *Customer2* and the *Services* folder is created. Elements in the *Services* folder now drive the condition of the *Customer2* business view.

A.5 Step 4. Define Service Level Agreements and Objectives

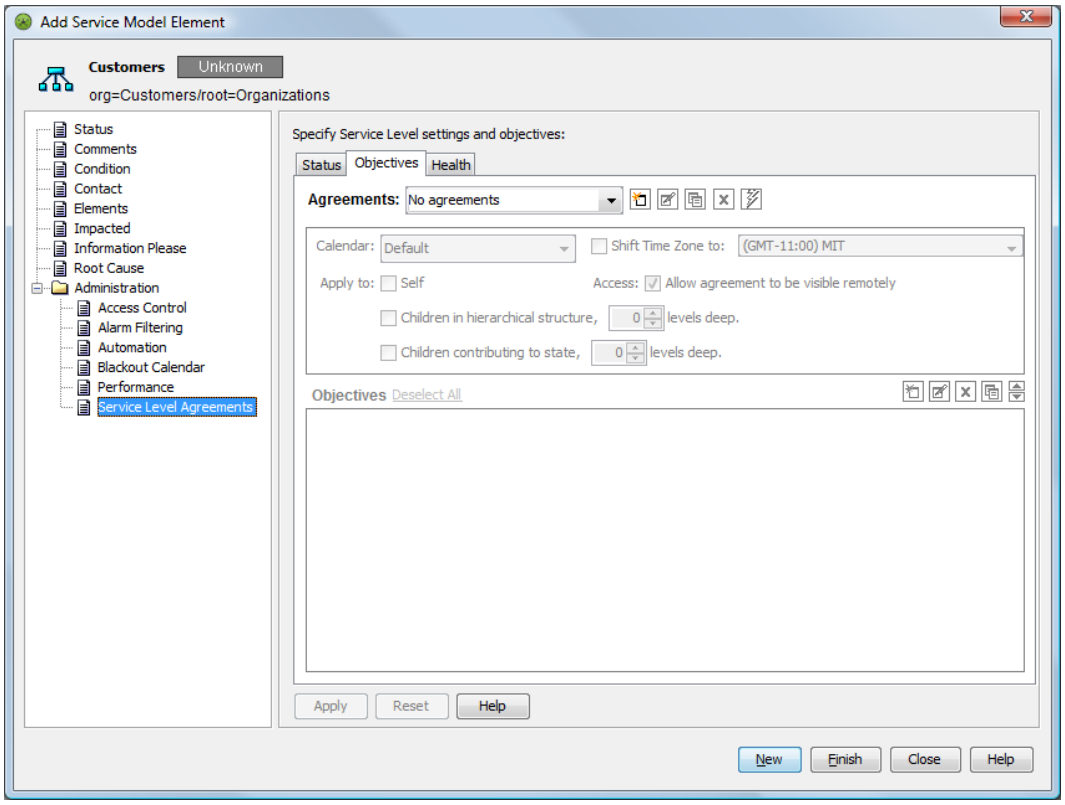
Use the top level element property pages to start defining the Service Level Agreement and standard objectives.

- Section A.5.1, “Defining the Service Level Agreement,” on page 146
- Section A.5.2, “Creating an Objective,” on page 148
- Section A.5.3, “Verifying the Results,” on page 149
- Section A.5.4, “Overriding Agreements,” on page 149

A.5.1 Defining the Service Level Agreement

1. In the *Explorer* pane, expand *Enterprise* > *Services* > *Service Models*.
2. Right-click *Customers*, then select *Properties* to open the Status property page.
3. In the left pane, expand *Administration*.
4. Click *Service Level Agreements* to open its property page.

5 In the Service Level Agreements property page, click the *Objectives* tab.



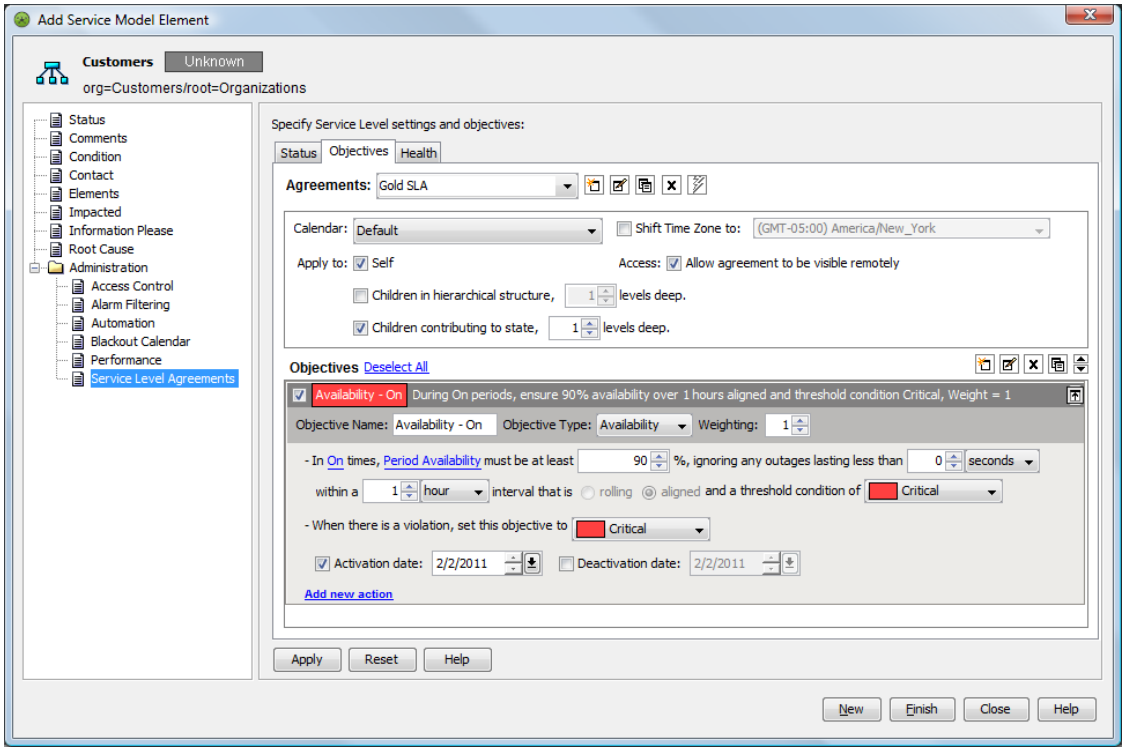
6 On the *Agreements* toolbar, click *New Agreement* to open its dialog box:

7 Enter `Gold SLA` in the field to name the Service Level Agreement.

8 Click *OK* to create the agreement.

A.5.2 Creating an Objective

1 On the *Objectives* toolbar, click *New Objective* to display the default objective values in the *Objectives* pane:



2 Create a new calendar for a service to define operational windows of time.

3 Set different objectives for each time category, such as operational and nonoperational hours.

The Calendar setting is `Default`. The default calendar is set to `ON`, 24 hours, 7 days a week. The objectives for this SLA are applied 24 hours, 7 days a week, provided the `ON` time category is used in the objective definition.

4 In the *Apply To* section, select the *Self* check box.

5 Select the *Element Children* check box.

6 Select 4 for the number of levels deep.

All child elements four levels down from Customers inherit the SLAs and objectives.

7 Select the *Organizational Children* check box.

8 Select 4 for the number of levels deep.

9 Click *Apply* to save the objective.

10 Verify that the child element, *Customer2*, inherited the objective just created.

A.5.3 Verifying the Results

1. In the *Explorer* pane, expand *Enterprise* > *Services* > *Customers*.
2. Right-click *Customer2*, then select *Properties* to open the Status property page.
3. In the left pane, expand *Administration*.
4. Click *Service Level Agreements* to open its property page.
5. In the Service Level Agreements property page, click the *Objectives* tab.

   The Gold SLA displays as inherited.

   Also, the objective displayed is the same one added to the *Customers* element.

A.5.4 Overriding Agreements

It is possible to override an agreement and its objectives. For example, the objectives for a specific branch of a hierarchy might require more specific objectives that do not apply elsewhere.

The following is an example of how to override the agreement settings that were made with the steps above.

To override the agreement:

1. In the *Explorer* pane, expand *Enterprise* > *Services* > *Customers* > *Customer2* > *Invoices* > *Accounts Receivable*.
2. Right-click processed invoices, then select *Properties* to open the Status property page.
3. In the left pane, expand *Administration*.
4. Click *Service Level Agreements* to open its property page.
5. In the Service Level Agreements property page, click the *Objectives* tab.
6. Click  *Override Agreement* to create a new SLA override.
7. Click  *New Objective* to specify an objective for the agreement override.
8. Enter `Number of Approved Invoices` in the *Objective Name* field.
9. In the *Objective Type* drop-down list, select *Custom*.
10. In the *Property* drop-down list, select *Alarm Property*.
11. Enter `Metric Value` in the property field, then select *Be Less Than* from the drop-down list.
12. Enter `950` in the value field, then select 2 in the occurrences selector.
13. Click *Apply* to save the SLA override and its new objective.

A.6 Step 5. View and Report on Service Level Agreements

There are several ways to view SLA data. Through Operations Center, it is easy to view what is happening in real time, because service level breaches and metrics are issued as performance is being evaluated based on the objectives set.

Then, results and statistics can be published to the Web using Operations Center dashboard's SLA-related reports.

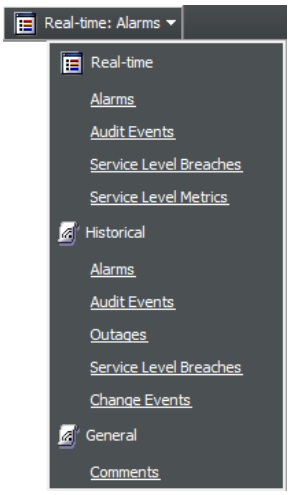
- Section A.6.1, "Viewing SLA Breaches and Metrics," on page 150
- Section A.6.2, "Viewing the Service Level Agreements Hierarchy," on page 151
- Section A.6.3, "Viewing Service Level Data in the Dashboard," on page 152

A.6.1 Viewing SLA Breaches and Metrics

To view SLA Breaches and Metrics:

1. In the *Explorer* pane, expand *Enterprise* > *Services*.
2. Click *Customers*.
3. Click the *Alarms* tab in the view pane to display the *Alarms* view.

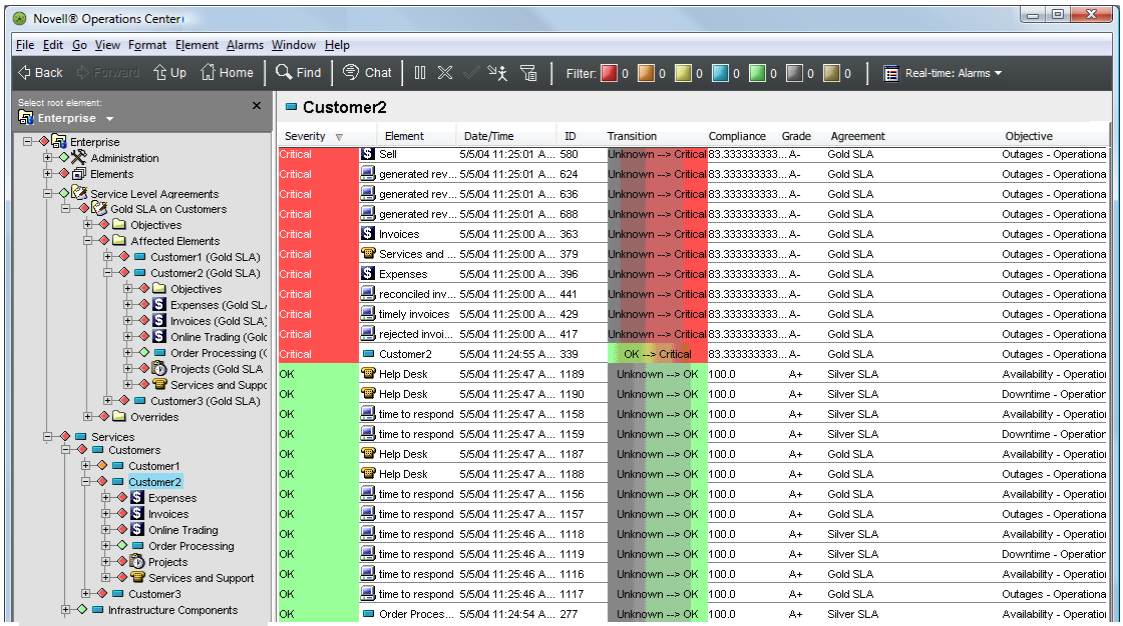
   In the toolbar, the *Alarms Selector* button provides several options to view SLA data, in real time or historically:



4. To view Service Level Breaches, click *Real-Time* > *Service Level Breaches*, or click *Historical* > *Service Level Breaches*.

   For information on Service Level Breaches and alarm column types, see Section 6.1.1, "Understanding Breach Alarms," on page 83.

5 To view Service Level Metrics, click *Real-Time* > *Service Level Metrics*.

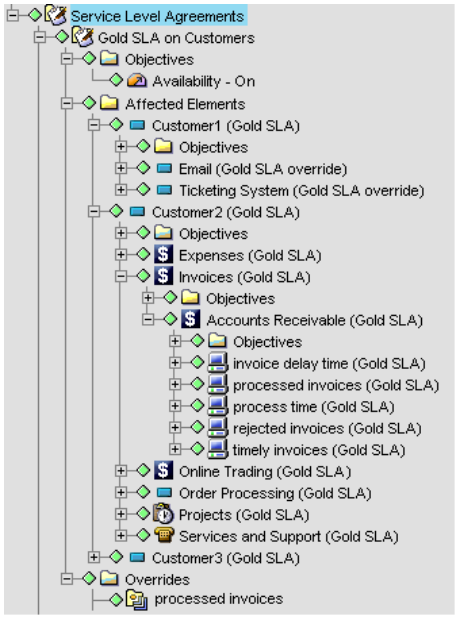


For information on Service Level Metrics and alarm column types, see Section 6.2.1, "Understanding Metric Alarms," on page 88.

A.6.2 Viewing the Service Level Agreements Hierarchy

1 In the *Explorer* pane, expand *Enterprise* > *Service Level Agreements*:

Figure A-2 *Service Level Agreements Hierarchy*



A.6.3 Viewing Service Level Data in the Dashboard

Portal pages can be created to display historical and real time SLA data. The *Operations Center 5.5 Dashboard Guide* is a useful reference that provides detailed information on how to create your portal and configure the views and reports.

Figure A-3 *Portal Pages: Pages display historical and real time SLA data.*