****

**Specification**

**for**

**11/17/09**

IderaLogo

Proprietary and Confidential to BBS Technologies, Inc.

**© 2009 BBS Technologies, Inc.; all rights reserved.**

# Revision history:

|  |  |  |
| --- | --- | --- |
| **When?** | **Who?** | **What?** |
| 11/13/2009 | Robert | First Draft |

# Table of Contents

1. Revision history: ii

2. Table of Contents iii

3. Requirements 1

3.1. Overview/Purpose 1

3.1.1. Related Customer Requests 1

3.2. Use Cases 1

3.3. Feature/Function Market Requirements 2

3.3.1. Required Functions 2

3.3.2. Non-Supported Functions 3

3.4. Open Questions 4

4. Functional Design 5

4.1. User Interfaces 5

4.2. Installation and Upgrade 9

4.3. Permissions and other Required Configuration 9

4.4. Licensing Issues 9

4.5. Dependencies 9

4.5.1. Dependencies on Idera Software 10

4.5.2. Third-Party Software Required on the Customer Machine 10

4.5.3. Third-Party Software Required Internally 10

5. Internal Design 10

5.1. Architecture 10

5.2. Installation Issues 11

5.3. Schedule 11

5.3.1. Work Breakdown and Sizings 11

5.3.2. Areas of Risk 11

6. Quality Assurance Considerations 11

6.1.1. Overview 11

7. Documentation Considerations 11

8. Bibliography 12

# Requirements

## Overview/Purpose

Many customers have requested the ability to setup alerts based on the operation of the product. For example, when the collection services loses contact with the agent or the agent trace directory is full, the user is not notified and does not discover that event tracing/processing has stopped. This feature will provide notification when something is wrong with the operation of SQL compliance manager.

### Related Customer Requests

9397 – FRQ:Alerts from SQLcompliance when Agent has lost contact for X days.

Lots of customers (too many to count) want an alert when an operational error occurs such as trace directory full or collection services lost contact with an agent.

10565 – FRQ: Email alerting for errors from the Agent and Collection Services

This is a clone from 9397.

10356 - FRQ: Add “Delete Rule” button to “Alert Rules” ribbon

This Alert ribbon in the Administration view will be modified for this feature. It will be very simple to include a Delete button.

## Use Cases

1. Users should receive alerts when something is wrong with the operation of SQL compliance.
2. Users should be able to view these operational alerts in the alerts view.
3. Users should be able to create and configure these alerts from the Alerts ribbon in the Administration view.
4. Users should receive an alert when the collection service loses contact with an agent.
5. Users should receive an alert when the collection service trace directory is greater than a certain percentage full.
6. Users should receive an alert when the monitored server’s repository database grows greater than a certain size.
7. Users should receive an alert when the sum of all event repository databases and archived event databases is greater than a certain size.
8. Users should receive an alert when an agent’s trace directory is greater than certain percentage full.
9. Users should receive an alert when an agent cannot communicate with a monitored instance.

## Feature/Function Market Requirements

### Required Functions

#### Collection Server Alerts

* The collection server currently heartbeats every 15 minutes but only writes a timestamp to the repository. This heartbeat will be changed to generate the operational alerts outlined below. Also, the heartbeat time will be decreased to a default of six minutes. This value will now be user configurable and will be maintained in the Collection Server Status dialog. See Figure 3 in Section 4.
* **Trace File Directory Full Alert**– Every collection server heartbeat, the collection server will look at the trace file directory. When it reaches or goes above a certain size, an alert will be generated. The size will be user configurable and the default will be 10GB. No action will be performed other than sending the alert. Because there is no maximum value and no additional action, this is just an alerting threshold and does not need a percentage of max warning. This alert can be disabled.
* **Unable to connect to an agent/not receiving heartbeats** –Every collection server heartbeat, the collection server will look in the repository for all of the agent heartbeats. If the difference between the current time and the last agent heartbeat is greater than the agent heartbeat interval, an alert will be generated. A separate alert will be generated for every agent that has failed to update their heartbeat in the repository. This alert can be disabled.
* **Monitored Server’s repository database grows too big** – Every collection server heartbeat, the collection server will check all of the monitored server’s repository databases. If a database has reached or is above a certain size, an alert will be generated. The default for this value will be 20GB. This will be a global value. It will apply to all monitored server repository databases. This alert can be disabled.
* **Total Size of All Event Repository Database Greater Than Size X** - Every collection servier heartbeat, the collection server will get the total of all the repository event databases and all archived event databases. If the size is greater than a certain value, an alert will be generated. The default total size will be 100GB. The SQLCompliance database will not be included because the size of this database is not affected by an increase or decrease in the number of events processed. This alert can be disabled.

#### Agent Alerts

* **Trace Directory Full –** Every agent heartbeat, the trace file directory’s size is checked. When it reaches the trace directory size limit, it is reported during the heartbeat and all tracing stops. An alert will be generated when the trace directory reaches a certain percentage of the trace directory size limit. The default will be 80%.
* **Agent unable to communicate with SQL Server –** Currently, when a compliance agent is unable to communicate with its monitored instance, it adds an entry to the repository. In addition, an alert will be genterated. (See open question 2)

#### Changes to the Alerting Framework

Operational alerts are generated based on the operation of the product and not on events generated on the monitored SQL Server. They have very little in common. Therefore, generation of the rules and viewing of the alerts will be separated for the different types.

* The current alerts will be renamed “Event Alerts”. Every place in the console that currently uses the word “Alert” will be changed to “Event Alert”.
* The Alert Rule ribbon is being redesigned to accommodate the separation of the two event types. See option 1 and option 2 in Section 4.
* A new wizard is being created to maintain operational alert rules. See Figure 2 in Section 4.
* The operational alerts will apply to either all audited servers or the collection server only. A new tab for viewing the operational alerts will be added to the Audited SQL Servers Ribbon. See Figure 1 in Section 4.

### Non-Supported Functions

1. This feature will not include alerts when an agent cannot communicate with the collection service.
2. Operational Alerts will not be included in the Activity Report Card or Auditing Thresholds

#### PRs Related to Alerting

Here are the PRs that are related to alerting that should be considered for future releases.

Threshold based alerting

10655

10584

10533

10432

9047

Alert on compliance errors

10565    - mentioned in Specs

Enable/Disable alerting on a schedule

10561

10510

Configure Alert Rules from user file or table

10654

Alert on any trace column

10549

Alert on data changes

10541    - already in POR

More alerting configuration options

10452

10438

10434

9424

8903       - Delete of alert rules (this one should be added to the specs)

Alert on SQLcompliance events

10467    - Alert if integrity check fails (and schedule integrity check from the console which would go well with grooming/archiving scheduling)

10428    - Alert when audit configuration changes

9685       - Alert on change log events like integrity check, grooming, etc.

9353       - Alert on trace tampering detection

6904       - No msg if integrity check fails

6558       - no msg if archive fails

6160       - Alert when application event log is full (not really a compliance event, but it fits the model of these)

Alert on BAD changes

10322    - Note this was a QA PR

Consolidate multiple events into one alert

10320    - Note this was a QA PR

9390

Configuring email notifications

10319    - Make sure email is configured properly when creating email alerts . Note this was a QA PR

9813       - Notify user when email address is removed from an alert rule

9554       - Changing settings does not generate change log event

Alert processing

10250    - Handle bad email address in Send To field correctly and still send to good ones

9317       - log if alert email fails

9013       - alert if stops processing dml or ddl

Acknowledge Alerts

9511

Create an alert rule from an event

9371

## Open Questions

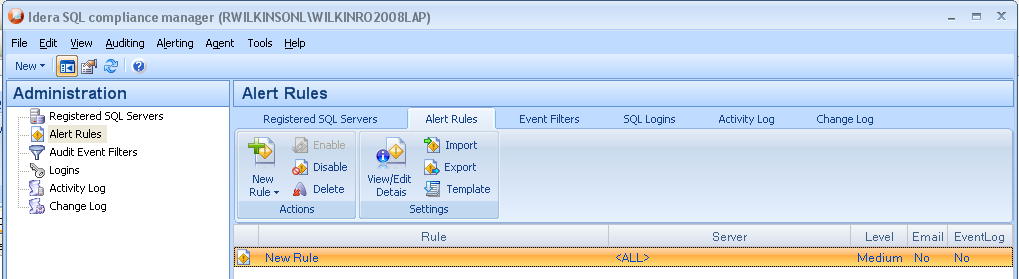
1. Which version of the Alert Rules ribbon do we want to use, option 1 or option 2?
2. The agent currently logs error events (trace directory full, unable to communicate to sql server, etc) to the repositiory. The agent log two entries, when the issue occurred and when it was resolved. Should the alerts be generated when the entry is made in the repository or every collection server heartbeat, have the collection server look in the repository for the events and create alerts in they exist?

# Functional Design

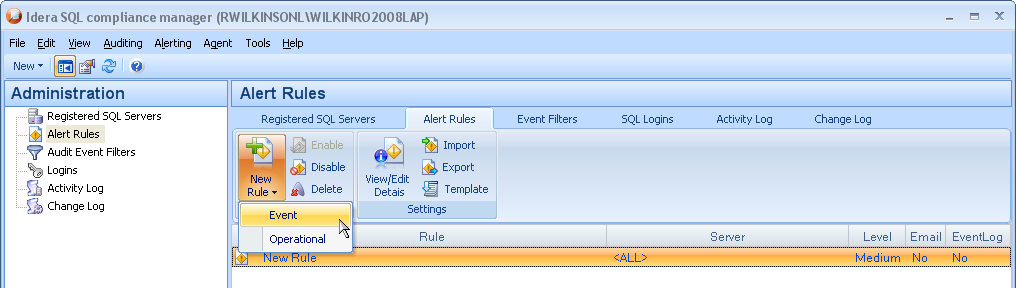
## User Interfaces

These are the two possible options of the redesigned Alert Rules ribbon. This first is more compact but less obvious and vice versa for the second option

Option 1



Option 1 with menu expanded



Option 2

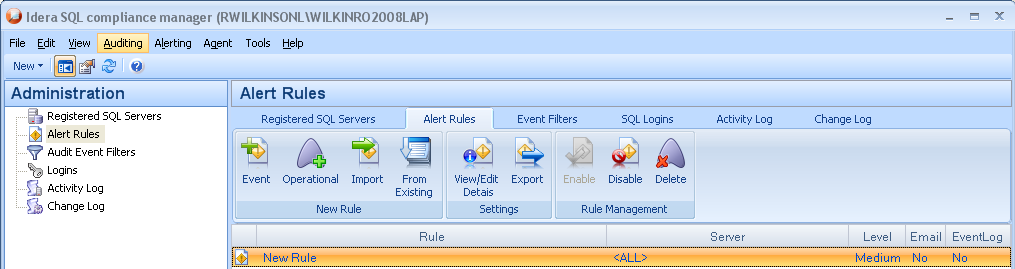


Fig 1. The event alerts and operational alerts will each be displayed on separate tab. The tabs will be identical except for the columns displayed in each view.

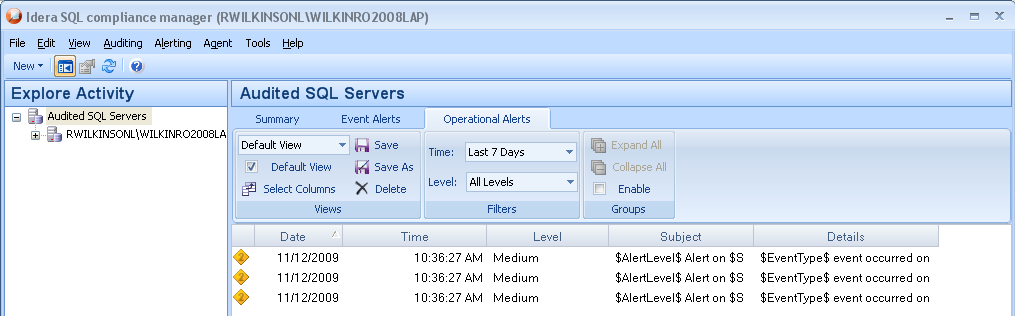
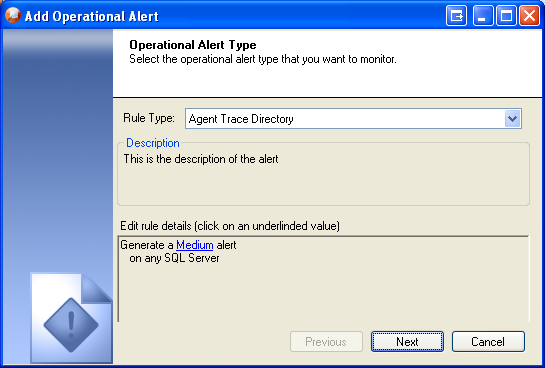
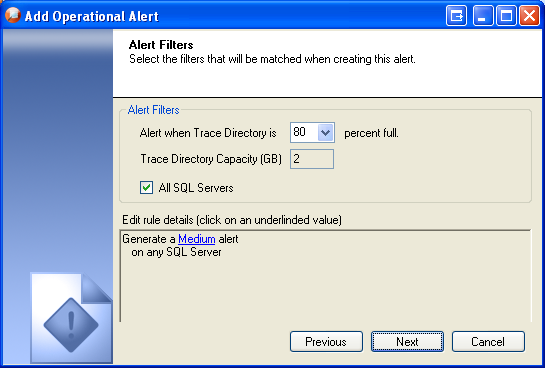
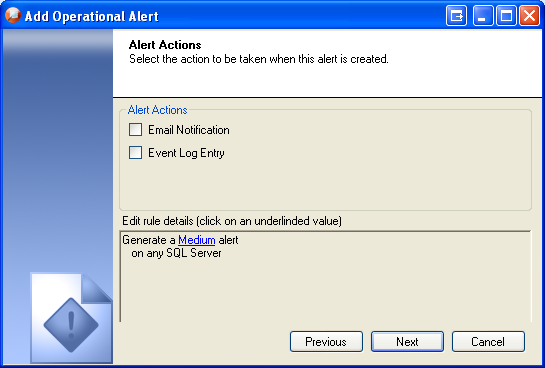
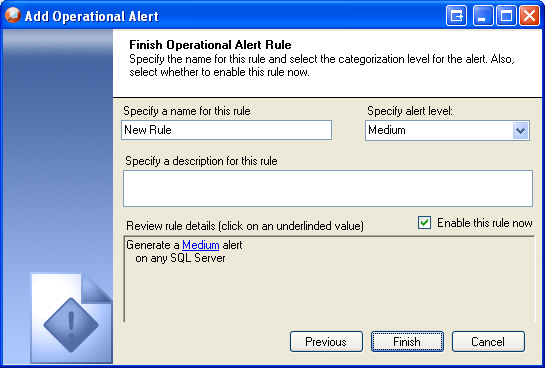


Fig 2. This is the Add an operational Alert wizard. The first page lets the user select an alert type. When they select a type, a description of the type will be displayed.



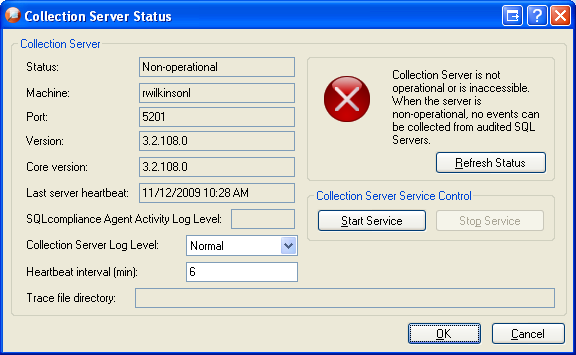






The collection server log level is now modifiable and the heartbeat interval has been added.

Fig 3.



## Installation and Upgrade

None

## Permissions and other Required Configuration

The user must have modify rights to add alert rules. Otherwise, everything will be read only.

## Licensing Issues

None

## Dependencies

None

### Dependencies on Idera Software

None

### Third-Party Software Required on the Customer Machine

None

### Third-Party Software Required Internally

None

# Internal Design

## Architecture

An overview of the architecture behind this feature – how it works, components, communication between components etc

* Collection Service Alerts
  + Trace Directory Full - just get the disk size and compare. The value will be stored in the registry here :HKLM\Software\Idera\SQLcompliance\CollectionServer

DWORD – Heartbeat Value = 6

* + Not getting agent heartbeats – just get the last heartbeat, the current date/time and compare.
  + Repository db too full - sp\_spaceused (maybe)
* Agent Alerts
  + Trace directory full – need to pass the percentage to the agent in the settings (i.e. when the agent gets the settings from the repository, it needs to look at the percent full value.
  + Can’t talk to SQL server – keep everything the same.
* Repository Changes – Where to store the alert information – It will fit in the current alert stuff.
* Places that Alert needs to change to Event Alert – Pretty much everywhere. Only lables in the console will be changed.

## Installation Issues

None.

## Schedule

### Work Breakdown and Sizings

|  |  |  |
| --- | --- | --- |
| Component | Who | Sizing (Days) |
| Add new Alerts (1.5days x 5alerts) | Robert | 7.5 |
| Changes to the existing alerting frame work | Robert | 5 |
| Add Operational Alert Wizard | Robert | 3 |
| Repository Changes | Robert | .5 |
| **Total** |  | **16** |

### Areas of Risk

None

# Quality Assurance Considerations

### Overview

Need to verify existing alerting doesn’t have problems with the new alerting rules.

Need to make sure operational alerts don’t show in event alerts grids or reports.

# Documentation Considerations

* The new alerts will need to be documented in the help and descriptions created for the New Operational Alert Wizard.
* There will be a new wizard and ribbon UI changes that will need to be reviewed for proper grammar, wording, etc.

# Bibliography