****

**Specification**

**for**

**12/13/11**

IderaLogo

Proprietary and Confidential to BBS Technologies, Inc.

**© 2011 BBS Technologies, Inc.; all rights reserved.**

# Revision history:

|  |  |  |
| --- | --- | --- |
| **When?** | **Who?** | **What?** |
| 12/13/2011 | Robert | First Draft |
| 01/13/2011 | Robert | Added Reports |

# 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 1

3.3.1. Required Functions 1

3.3.2. Non-Supported Functions 3

3.4. Open Questions 3

4. Functional Design 4

4.1. User Interfaces 4

4.2. Installation and Upgrade 8

4.3. Permissions and other Required Configuration 8

4.4. Licensing Issues 8

4.5. Dependencies 8

4.5.1. Dependencies on Idera Software 8

4.5.2. Third-Party Software Required on the Customer Machine 8

4.5.3. Third-Party Software Required Internally 8

5. Internal Design 9

5.1. Architecture 9

5.2. Installation Issues 9

5.3. Schedule 9

5.3.1. Work Breakdown and Sizings 9

5.3.2. Areas of Risk 9

6. Quality Assurance Considerations 10

6.1.1. Overview 10

7. Documentation Considerations 10

8. Bibliography 10

# Requirements

## Overview/Purpose

This feature will implement Data Alerts. These are alerts genterated based on reading data or changing data. This has many uses from detecting unauthorized price and salary changes to unauthorized changes to stock trades and bank transactions. This feature will add two data alerts – alert when a numerical column value changes and alert when selecting a Sensitive column.

### Related Customer Requests

PR 11286 – Provide an alert for Sensitive Column Access

PR 10541 – Alert when a numeric value changes

## Use Cases

1. Users should receive alerts when data values change.
2. Users should be able to view these data 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 value of a column changes.
5. Users should receive an alert when a sensitive column is read.

## Feature/Function Market Requirements

### Required Functions

#### Data Alerts

Data Alerts are a new type of alerts that will be created based on data instead of events. This feature include two new alerts – alerting when the value of a column changes and reading a sensitive column.

##### Alert When a Column Value Changes

###### Alert Description

This new data alert will be generated when the value of a column changes. The user will selected a column to be monitor, a comparison operator and a value for comparison. The only columns available for this alert will be numeric columns that have set up for Before and After Data Auditing. The comparison operators will be: =, <, >, <=, >=, !=.

Alert Rule Creation

1. The user will click New Data Rule from the Alert Rules tab on the Administration ribbon.
2. A New Data Alert Rule wizard will be displayed.
3. The first page of the wizard will display list of available alerts. (see Section 4.1) Only columns that have been setup for BAD auditing will be available to data alerting. If a desired column is missing from the data alert wizard, it needs to be added to the BAD auditing before it will be available for data alerting.
4. The user will select a column, a comparison operator and a value for comparison against. The only columns that will be available are ones that a numeric (tinyint, int, bigint, etc.) and are setup for BAD auditing.
5. The following information will be just like the status alerts. Alert level, email and event log will all be options.
6. The alert rule will be displayed on the alert rules tab along with staus rules and event rules.

Alert Generation

The data alerts will be processed along with the event alerts. But instead of using the data in the events table, it will use the data in the DataChanges and ColumnChanges tables. Just like the event alerts, the data alerts will be processed in blocks of 5000 events at a time. There is consideration being given to removing that limit but that is not a part of this feature.

When processing the BAD events for the new data alert, it will compare the column value to the comparison value in the data alert rule. If that comparison is true, an alert will be generated.

Here is an example default message for the alert. “The value of column [column] in [Instance], [Database], [Table] is [comparison operator] [value from the alert rule]. This was changed by user: [username]”

##### Alert When a Sensitive Column is read.

###### Alert Description

This new data alert will be generated when a sensitive column is read. The user will select a column to monitor. The only columns available for this alert will be columns that have set up for Sensitive column auditing.

Alert Rule Creation

1. The user will click New Data Rule from the Alert Rules tab on the Administration ribbon.
2. A New Data Alert Rule wizard will be displayed.
3. The first page of the wizard will display list of available alerts. (see Section 4.1) Only columns that have been setup for Sensitive Column auditing will be available to data alerting. If a desired column is missing from the data alert wizard, it needs to be added to the Sensitive Column auditing before it will be available for data alerting.
4. By default, all columns from any instance that have been setup for Sensitive Column auditing will apply to this alert. However, the user drilldown and select and instance, database, table and column if desired., a comparison operator and a value for comparison against.
5. The following information will be just like the status alerts. Alert level, email and event log will all be options.
6. The alert rule will be displayed on the alert rules tab along with staus rules and event rules.

Alert Generation

The data alerts will be processed along with the event alerts. But instead of using the data in the events table, it will use the data in the SensitiveColumns table. Just like the event alerts, the data alerts will be processed in blocks of 5000 events at a time. There is consideration being given to removing that limit but that is not a part of this feature.

An alert will be generated when a Sensitive column is accessed

Here is an example default message for the alert. “Sensitive Column [column] in [Instance], [Database], [Table] was accessed by user: [username].”

#### Changes to the Alerting Framework

Event Alerts and Status Alerts will stay the same.

* A new Data Alert button will be added to the Alert Rules ribbon
* A new wizard is being created to maintain Data Alert rules. See Figure 2 in Section 4.

#### Reports

There will be a new report, Alert Activity – Data and the existing Alert Rules report will be changed to include data alerts.

### Non-Supported Functions

* The alert when a numeric value changes will not include alerts on string data or blog data. The Sensitive column alert will include it.

## Open Questions

1. Should the Data Alerts be displayed with the Event Alerts? Unlike the Status Alerts, they are similar and have similar data.

# Functional Design

## User Interfaces

Fig 1. The data alert rules will be added in the via the Alert Rules tab in the Administration view.

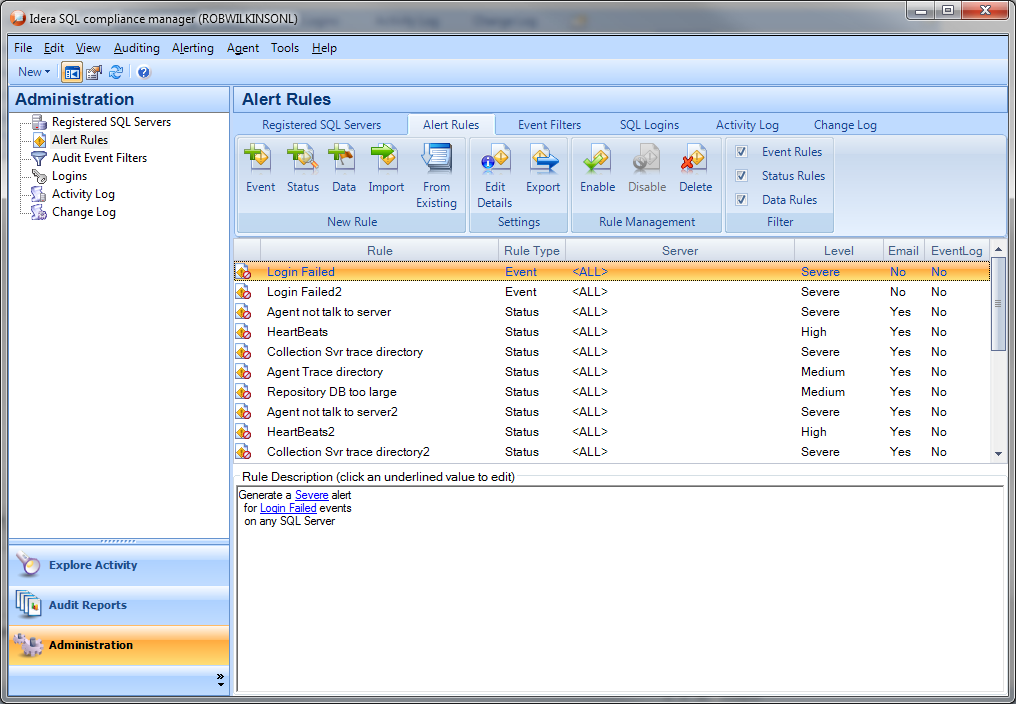
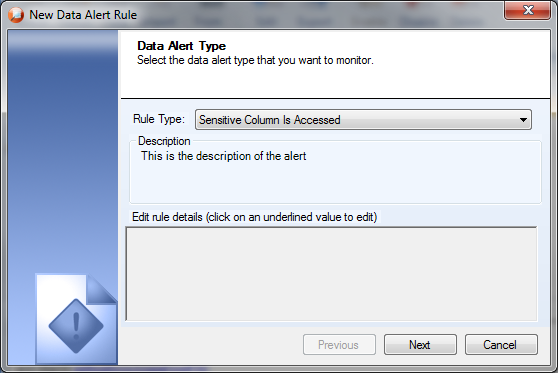


Fig 2. This is the Add a Data Alert wizard. Currently there is only one alert of this type so the first page of the wizard will have a description of the alert. 

Below is a basically what the text will look like when selecting a Sensitive column alert. It will default to any SQL Server. They user will click on the link to select a specific SQL Server. That will then default to any Database on that SQL Server. The user will then click on the database link to select a specific database, etc.

Generate a Medium Alert when **a Sensitive column** **is accessed** on any SQL Server.

Generate a Medium Alert when **a Sensitive column** **is accessed** on any Database on robwilkinsonl\sql2008r2.

Generate a Medium Alert when **a Sensitive column** **is accessed** on any Table on Envision on robwilkinsonl\sql2008r2.

Generate a Medium Alert when **a Sensitive column** **is accessed** on any Column on tblInfo on Envision on robwilkinsonl\sql2008r2.

This it the text for the numeric value alert. It will have the same logic for the Instance/DB/Table/Column as the Senetive Column alert. It will also have a link that users can click to select the comparison operator and comparison value. The comparison operator will be spelled out in the alert rule.

We will use:

equal to

less than

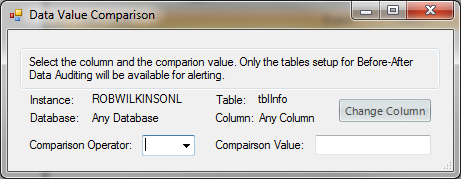
greater than

equal to or less than

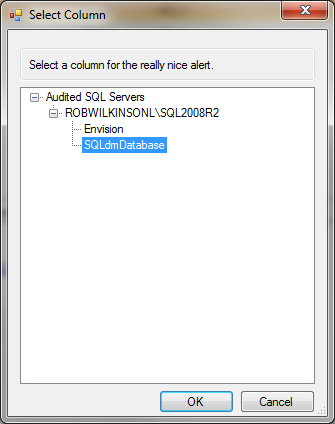
equal to or greater than

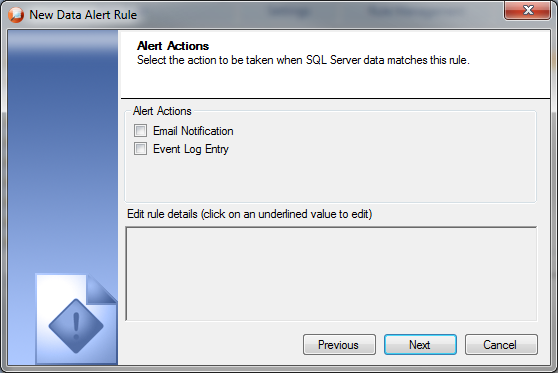
not equal to

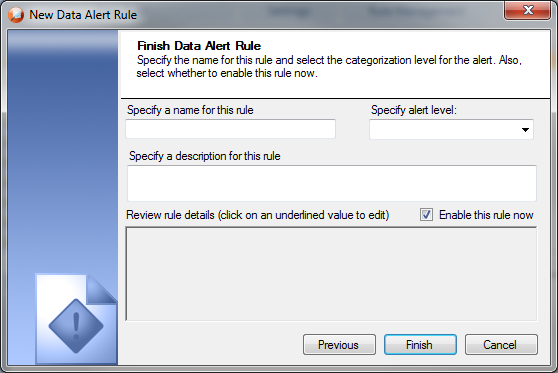
Generate a Medium Alert when **the value of a numeric column changes** to equal5000 on any SQL Server.



This is the dialog users will use to select a column Instance/Database/Table/Column. The title will change as appropriate and it will only list what is being selected. Only Instance for instance, only databases for the selected instance, only tables for the selected database, etc.







## 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 Server Changes
  + The Data Alert processing will be done with the Event Alert processing.
  + Repository Changes –
    - Add a new Alert Rule type to AlertTypes.
    - Need to create a new table to hold the Data Alert Rules since the rules are not just tied to an instance but also a database, table and column.
    - The indexes on the ColumnChanges, DataChanges and Sensitive Column tables will need to be looked at and possibly changed. The clustered index on the ColumnChanges table is the columned. This is a very bad decision because there will be very few unique entries in this column. The clustered index will be changed to be a combination of the columnId and the dcId. The dcId is the unique Id from the DataChanges table..

## Installation Issues

None.

## Schedule

### Work Breakdown and Sizings

|  |  |  |
| --- | --- | --- |
| Component | Who | Sizing (Days) |
| Repository Changes | Robert | 1.5 |
| Collection Server Changes to process the alert | Robert | 3 |
| Data Alert Wizard | Robert | 3 |
| New Data Alert View | Robert | 2 |
| Reports | Robert | 2 |
| Testing | Robert | 1.5 |
| **Total** |  | **13** |

### 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 data alerts don’t show in event alerts grids or reports.

# Documentation Considerations

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

# Bibliography