

# Requirements Analysis

## Smarter Balanced Assessment Consortium Test Delivery System

### Component: Monitoring and Alerting

#### Revision History

Revision Description	Author/Modifier	Version	Date
Initial Revision	David Lopez de Quintana		August 27, 2012
Additional Detail added	Michael Stern		September 27, 2012
Formatting	Kevin Ptak		October 15, 2012
Updated **Note, section 2	Russ Hammond		November 12, 2012
Section 2 – Workflow – removed silencing or acknowledging alerts	Russ Hammond		November 16, 2012

<ul style="list-style-type: none"> <li>• Section 2 – revised statements about workflow alerts based on conversations with David. M&amp;A will not send workflow alerts.</li> <li>• Section 2 – changed reports to include printed displays, and reports offered by the off-the-shelf M&amp;A package selected</li> <li>• Section 2 – added statements about creating a custom code UI for some M&amp;A users</li> <li>• Section 2 – removed Component Admin, Security Auditor, Proctor roles from table, added Business user role</li> <li>• Section 4 – added requirements 118, 120, 122 from the RFP</li> <li>• Section 7 – added reqt 121 from the RFP</li> <li>• Section 8 – removed Error api, Errors are reported through logging.</li> </ul>		1.1	
<ul style="list-style-type: none"> <li>• Cleaned up typos</li> <li>• Removed reference to CSV file export</li> </ul>	Russ Hammond	1.2	April 29, 2013

# Contents

1. Component Name: Monitoring and Alerting .....	5
2. Component Description .....	5
3. Responsible Organization.....	6
4. Functional Requirements from SMARTER Balanced RFP-11 .....	6
5. Detailed Requirements from RFP-11 and/or Architecture Document.....	6
6. Additional Requirements from Technical Proposal.....	6
7. Non-Functional Requirements .....	7
8. Data Utilized .....	7
9. Data Dependencies .....	8

## 1. Component Name: Monitoring and Alerting

## 2. Component Description

Monitoring and Alerting is a shared set of services that allow components to communicate important system events to a centralized location in a consistent manner. Monitoring and Alerting accepts events, and errors from components, which are then processed, and if appropriate, routed to various audiences. A component also has the ability to send alerts directly to Monitoring and Alerting for routing. Alerts are available for consumption by the intended audience(s) and can be acted upon in a consistent manner. Monitoring and Alerting allows vendors to develop add on applications and features to use and act on these alerts.

Monitoring and alerting acts as a centralized system log configuration tool and log repository to be used by system administrators for error investigation, telemetry and reporting.

(3/20/13) The primary purpose of Monitoring and Alerting is to identify situations where the system is experiencing problems which require intervention to keep the system operational. Monitoring and Alerting is not intended to issue alerts regarding workflow events.

### SUMMARY OF CAPABILITIES:

#### Workflow

~~There will be integration with workflow components. Components that utilize a workflow will have the ability to create or elevate an Alert based on a workflow event.~~

(3/20/13) Monitoring and Alerting will not be used to send workflow notifications; its purpose is to identify problem areas in the system and warn personnel so that action can be taken to keep the system operational.

#### Reporting

Reports can contain summary information regarding errors, performance metrics and other information captured by the system components. Reports differ from alerts in that they will be created and delivered in an offline manner. The delivery method and audience will be configurable in an interface consistent with the real time alerts configuration interface. ~~Report content will not be customizable beyond the features available in the third-party, open-source component.~~

(3/20/13) Reporting will be limited to the ability to print Monitoring and Alerting displays, and any reporting functions which can be performed by the selected Monitoring and Alerting off-the-shelf product.

#### User Interfaces

All user interfaces will be accessed via the Portal, which provides SSO, authentication and grants Authorization following the standard Portal methods. The off-the-shelf UI will be used for viewing server health information. Another user interface will be coded to allow searching on logs and alerts, and to allow business users to see the results of tasks they have submitted. (3/20/13) Interfaces have been defined to allow a variety of audiences to consume and act upon the Alerts. The following is a list of audiences that will be consuming Alerts and the associated interface via the Portal:

	<u>Audience/Actor</u>	<u>Interface</u>	<u>Requirement</u>
1.	Support Personnel	(System Administrator) Dashboard (Hyperic dashboard)	Real time preventive monitoring
2.	<del>Component Administrator</del>	<del>(System Administrator) Dashboard</del>	<del>Centralized component log level configuration and viewing</del>
3.	<del>Security Auditor</del>	<del>(System Administrator) Dashboard</del>	<del>Auditing of security and access logs, with Alerts of suspicious activity generated for administrator investigation</del> (3/20/13) – The system should allow messages to be sent to groups specified by the administrators of the system. The roles of Component Administrator and Security Auditor are not required.
4.	All Dashboard users	Dashboard settings	configuration for notification options including distribution list, notification method, as well as the potential for modification of rule based notification thresholds.
5.	System Administrator	** (System Administrator) Dashboard (Hyperic dashboard)	Monitor component status, this status may include simple information such as up/down count of instances of each component
6.	<del>Proctor</del>	<del>(Proctor) Dashboard</del>	<del>Ability to see real time events relating to the test delivery, including monitoring of student progress</del> The proctor workstation will receive messages through test delivery rather than from Monitoring and Alerting (3/20/13)
7.	Business users	Custom code interface	Business users require the ability to see the results of tasks they have submitted.

\*\* NOTE: The Portal referred to a “dashboard” of component status. The Monitoring and Alerting component will provide to the portal the necessary services to display a dashboard.

### 3. Responsible Organization

DRC is responsible for developing the Monitoring and Alerting component.

### 4. Functional Requirements from SMARTER Balanced RFP-11

The following requirements are numbered in the same way as in RFP-11

88	System includes a suite of alerts to the test administrator and Consortium delegates if there appears to be a testing irregularity.
118	Sufficient audits must be available to identify the source and time of data changes related to system components. (3/20/13)

119	System must ensure that it logs system activity necessary to monitor and debug the system in a timely and accurate manner.
120	System must ensure that all errors are written to an error log. (3/20/13)
122	System must allow for a system administrator to view, filter, sort, and search the error log. (3/20/13)

## 5. Detailed Requirements from RFP-11 and/or Architecture Document

1.	Provide a framework for other components' log information.
2.	Allow components to write log and tracing information in a consistent and configurable way.
3.	Operational parameters are actively monitored - runtime metrics and dashboards.
4.	Provide an API for collecting log information and alerts.
5.	Provide the ability to expose information as to the status of a component
6.	Provide the ability for machine or VM monitoring events experiencing low-memory issues, disk-full issues, processor overloading issues and exceptions to cause alerts which notify support personnel of possible issues. NOTE: the alerting urgency must be able to vary depending upon the availability category (High or Medium) for the component being monitored.
7.	Provide the ability to alert other components and possibly other vendor components accordingly.
8.	Provide an interface for all system components' log and alert messages.

## 6. Additional Requirements from Technical Proposal

1.	Provide a user interface for configuring alerts and rules that allow the component to make decisions based on the information collected from the other components of the system.
2.	Provide a user interface capable of producing reports that indicate the overall health of the system, including performance metrics and error reports.
3.	The monitoring and alerting component needs to provide capabilities to monitor server information as well as the software applications running on the servers.
4.	The monitoring and alerting component will support a custom monitoring and alerting center. The system will be designed to receive information from a variety of sources, which might include <ul style="list-style-type: none"> <li>third-party server monitoring software that monitors resource usage and raises alerts if resources approach critical levels</li> <li>internal event monitoring built into component systems.</li> </ul>
5.	The monitoring and alerting component will provide the ability for a component to report performance metrics, error logging, and workflow alerts

## 7. Non-Functional Requirements

RFP 121	Errors to the end user must be communicated in plain language with an explanation of required action. (3/20/13)
1.	See Section 7 Non-Functional Requirements in the General Requirements document for up-time requirements as well as additional non-specific non-functional requirements..
2.	See Section 7 Non-Functional Requirements in the General Requirements document for up-time requirements as well as additional non-specific non-functional requirements..
3.	Monitoring and Alerting, like most other identified components, is prescribed a minimum component server count of two (2) to maintain up-time requirements as well as accessibility in a single node failure. The architecture report was less prescriptive in the minimum data server count, specifying that it depends on application architecture.
4.	The Technical Proposal recommends that Monitoring and Alerting should be built upon a customized off the shelf commercial product. A competitive analysis cross matrix will be included as appendix A to the level II requirements document.
5.	Infrastructure monitoring is a functional requirement, specifying, there must be 'actionable' items taken from the alert. The implied non-functional requirement is that when an alert is received regarding an infrastructure component nearing or exceeding an acceptable threshold that an administrator be provided the opportunity to provision more hardware. The actual means for such provisioning will depend upon hosting solution chosen. However, a standard interface for taking action must be defined, the message must contain some amount of context and event identifier. See reqt 121 from the RFP above.
6.	XML is the format recommended by the Technical Proposal, with no mention of a required schema.
7.	HTTP is the delivery protocol recommended by the Technical Proposal recommends with a presumably RESTful API.
8.	As with all other components, is is required that Monitoring and Alerting be built with open-source technology, and the component be open sourced when completed.
9.	Proper logging configuration guidance is an important deliverable for the Monitoring and Alerting, given that the component will responsible for keeping a centralized log for each component, it is highly important that the client components are logging only appropriate events to the Monitoring and Alerting component. This configuration can be controlled via the user interface listed above.

## 8. Data Utilized

1.	The Monitoring and Alerting component will use a centralized log configuration tool to specify logging level.
2.	The Monitoring and Alerting component will persist individual log events for reporting purposes.
3.	<p>The Monitoring and Alerting component will be responsible for aggregation of monitoring events. The aggregation of events will enable the generation of alerts from centralized business rules. Events will consist of the following sub types:</p> <ul style="list-style-type: none"> <li>• <b>Metric:</b> key metrics (ex: number of connected students) generated by client components. Also generated from hardware monitoring of operational parameters and run time metrics, note that these events may be sourced from third party monitoring software</li> <li>• <b>Error:</b> generated from system monitoring, such as application errors</li> </ul>
4.	The Monitoring and Alerting component will provide the ability to configure an alert rule that will generate an alert based on criterion such as count of a specific event in a given time period, severity of the event, and the threshold of events. Additionally each component has been categorized as a High or Medium availability component, and for each respective category, there will be differing alerting needs.

5.	<p>The Monitoring and Alerting component will send alert notifications to an end user in a variety of formats and delivery mediums.</p> <ul style="list-style-type: none"> <li>Generated by the Monitoring and Alerting component based off of events</li> <li>Sent directly to the Monitoring and Alerting component from client components</li> </ul>
----	---

## 9. Data Dependencies

Start Point	Input	Output	End Point
All components	Alert	Persisted Alert, Alert Message	Monitoring and Alerting
All components	Metric	Persisted Metric, Metric Message	Monitoring and Alerting
All components	Error	Persisted Error, Error Message	Monitoring and Alerting Error endpoint removed, errors are recorded through logging api
All components	Log entry	Persisted log entry	Monitoring and Alerting
Monitoring and Alerting	Alert Message	Notification to user	User Interface
Monitoring and Alerting	Metric Message	Notification to user	User Interface
Monitoring and Alerting	Error Message	Notification to user	User Interface Error endpoint removed, errors are recorded through logging api
Monitoring and Alerting	Log Message	Notification to user	User Interface
Monitoring and Alerting	Alert Message	Notification to Admin	Admin Interface
Monitoring and Alerting	Metric Message	Notification to Admin	Admin Interface
Monitoring and Alerting	Error Message	Notification to Admin	Admin Interface Error endpoint removed, errors will not be visible in Hyperic console
Monitoring and Alerting	Alert Message	Workflow event	Workflow System
Monitoring and Alerting	Metric Message	Workflow event	Workflow System
Monitoring and Alerting	Error Message	Workflow event	Workflow System Workflow alerts removed per discussion with David 3/20/13

NOTE: This table is does not represent the final API between the Monitoring and Alerting component and other components/interfaces. The specifics of the API will be further described as we move from high-level requirements into design.