Sentinel Internal Audit Events

Sentinel 7.0.1

April 2012

Legal Notices

For more information, please contact NetIQ at:

1233 West Loop South, Houston, Texas 77027

U.S.A

www.netiq.com

Contents

About This Guide

This section lists the various internal events generated in Sentinel.

Audience

This guide is intended for Sentinel users.

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.

Contacting Novell and NetIQ

Sentinel is now a NetIQ product, but Novell still handles many support functions.

- Novell Web site (http://www.novell.com)
- NetIQ Web site (http://www.netiq.com)
- Technical Support (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup)
- Self Support (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Patch download site (http://download.novell.com/index.jsp)
- Sentinel Community Support Forums (http://forums.novell.com/netiq/netiq-product-discussion-forums/sentinel/)
- Sentinel TIDs (http://support.novell.com/products/sentinel)
- Sentinel Plug-in Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html)
- **Notification Email List:** Sign up through the Sentinel Plug-in Web site

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team.

Worldwide: NetIQ Office Locations (http://www.netiq.com/about_netiq/officelocations.asp)

United States and Canada: 888-323-6768

Email: info@netiq.com

Web site: www.netiq.com

1 Internal Audit Events

This section lists the various internal events that are generated by the various components in Sentinel, such as Event Source Management, User Management, Report definitions, and report results. The events are grouped by component.

1.1 Active Views

Below listed is about Active views.

1.1.1 Active View Created

DAS_Binary sends this event when an Active View is created.

Tag	Value
Severity	1
Event Name	RtChartCreated
SentinelServiceName	RealTimeSummaryService
SentinelServiceComponent	ChartManager
Message	Creating new Active View with filter <filter> and attribute <attribute> for users with security filter <security filter>. Currently <n> Active View(s) Collecting.

1.1.2 Active View Joined

DAS_Binary sends this event when a user connects to an existing Active View.

Tag	Value
Severity	1
Event Name	RtChartJoiningExistingData
SentinelServiceName	RealTimeSummaryService
SentinelServiceComponent	ChartManager
Message	`Joining existing Active View with filter <filter> and attribute <attribute> for users with security filter <security filter>. Currently <n> Active View(s) Collecting.`

1.1.3 Active View No Longer Permanent

DAS_Binary sends this event when it detects a formerly permanent Active View that is no longer permanent. This check happens periodically, so it can be several minutes after an Active View is removed from preferences before this event is generated.

Tag	Value
Severity	1
Event Name	RtChartNotPermanent
SentinelServiceName	RealTimeSummaryService
SentinelServiceComponent	ChartManager
Message	`Active View with filter <filter> and attribute <attribute> for users with security filter <security filter> is no longer permanent.`

1.1.4 Active View Now Permanent

DAS_Binary sends this event when it detects an Active View as newly permanent. This check happens periodically, so it can be several minutes after an Active View is saved to preferences before this event is generated.

Tag	Value
Severity	1
Event Name	RtChartIsNowPermanent
SentinelServiceName	RealTimeSummaryService
SentinelServiceComponent	ChartManager
Message	`Active View with filter <filter> and attribute <attribute> for users with security filter <security filter> is now permanent.`

1.1.5 Idle Active View Removed

DAS_Binary sends this event when a non-permanent Active View is removed because of inactivity.

Tag	Value
Severity	1
Event Name	RtChartInactiveAndRemoved
SentinelServiceName	RealTimeSummaryService
SentinelServiceComponent	ChartManager
Message	`Removed idle Active View with filter <filter> and attribute <attribute> for users with security filter <security filter>. Currently <n> Active View(s) Collecting.`

1.1.6 Idle Permanent Active View Removed

DAS_Binary sends this event when a permanent Active View is removed because of inactivity. Permanent Active Views are ones saved in user preferences and timeout after several days of inactivity by default.

Tag	Value
Severity	1
Event Name	RtPermanentChartRemoved
SentinelServiceName	RealTimeSummaryService
SentinelServiceComponent	ChartManager
Message	`Removed idle permanent Active View with filter <filter> and attribute <attribute> for users with security filter <security filter>. Currently <n> Active View(s) Collecting.`

1.2 Activities

Below listed are relevant to Activities.

1.2.1 Creating an Activity

Tag	Value
Severity	
Event Name	createActivity
SentinelServiceName	
SentinelServiceComponent	ActivityNamespace
Message	`Creating iTRAC Activity <name>`

1.2.2 Deleting an Activity

Tag	Value
Severity	
Event Name	deleteActivity
SentinelServiceName	
SentinelServiceComponent	ActivityNamespace
Message	`Deleting iTRAC Activity <name>`

1.2.3 Saving an Activity

Tag	Value
Severity	
Event Name	saveActivity
SentinelServiceName	
SentinelServiceComponent	ActivityNamespace
Message	`Saving changes for iTRAC Activity <name>`

1.3 Advisor Audit Events

1.3.1 Advisor Update Successful

Tag	Value
Severity	1
Event Name	Advisor update succeeded
SentinelServiceName	Advisor Processor
SentinelServiceComponent	Advisor Processor

Message	If the feed file is not available, the message displayed is:
	`‘No new feed available to process’`
	If the feed file is available, the message displayed is:
	`“Number of records inserted: (value) Number of records updated (value) Processing started: (datetime) Processing ended: (datetime)’`

1.3.2 Advisor Update Failure

The events are similar for all types of failures, except that the Message field has the actual cause of error.

Tag	Value
Severity	4
Event Name	Advisor update failed
SentinelServiceName	Advisor Processor
SentinelServiceComponent	Advisor Processor
Message	`Advisor feed file advnxsfeed.1.zip could be corrupt`

1.4 Authentication Events

1.4.1 Authentication

Tag	Value
Severity	1
Event Name	Authentication
SentinelServiceName	UserAuthentication
SentinelServiceComponent	Authenticate
Message	`User <username> has passed authentication to Sentinel/ Wizard`

1.4.2 Failed Authentication

Tag	Value
Severity	4
Event Name	AuthenticationFailed
SentinelServiceName	UserAuthentication
SentinelServiceComponent	Authenticate
Message	`Authentication of user <username> with OS name <domUser> from <IP> failed`

1.4.3 Web User Interface Login

Tag	Value
Severity	1
Event Name	LoginUser
SentinelServiceName	SessionServices
SentinelServiceComponent	SessionServices
Message	`Logging in user:<username>`

1.4.4 Web User Interface Login Failed

Tag	Value
Severity	4
Event Name	LoginUser-*-Failed
SentinelServiceName	SessionServices
SentinelServiceComponent	SessionServices
Message	`Logging in user:<username>`

1.4.5 User Logged In

Tag	Value
Severity	1
Event Name	UserLoggedIn
SentinelServiceName	UserSessionManager
SentinelServiceComponent	User
Message	`User <username> with OS name <osName> at <IP> logged in; currently <number> active users`

1.4.6 User Logged Out

Tag	Value
Severity	1
Event Name	UserLoggedOut
SentinelServiceName	UserSessionManager
SentinelServiceComponent	User
Message	`Closing session for <username> OS name <osName> from <IP> was on since <date>; currently <number> active users`

1.5 Correlation Engine

Below listed are relevant to correlation engine.

1.5.1 Correlation Action Definition

Tag	Value
Severity	
Event Name	New/Update/Remove
SentinelServiceName	Correlation
SentinelServiceComponent	CorrelationActionDefinition
Message	`Action Name: <name> with Id: <ID>`

1.5.2 Correlation Engine Configuration

Tag	Value
Severity	
Event Name	New/Update/Remove
SentinelServiceName	Correlation
SentinelServiceComponent	CorrEngineConfig
Message	`Correlation Engine ID: <ID> Name: <name> Active: {2}`

1.5.3 Correlation Engine is Running

The correlation engine process can be idled by the user. Its running state determines whether the active process is processing events or not. The process starts in the idle (stopped) state and waits to retrieve its configuration from the database. This event is sent when the engine changes state from stopped to running.

Tag	Value
Severity	1
Event Name	EngineRunning
SentinelServiceName	CorrelationEngine
SentinelServiceComponent	CorrelationEngine
Message	`Correlation Engine is processing events.`

1.5.4 Correlation Engine is Stopped

This event is sent out when the engine changes state from running to stopped.

Tag	Value
Severity	1
Event Name	EngineStopped
SentinelServiceName	CorrelationEngine
SentinelServiceComponent	CorrelationEngine
Message	`Correlation Engine has stopped processing events.`

1.5.5 Correlation Rule

Tag	Value
Severity	
Event Name	New/Update/Remove
SentinelServiceName	Correlation
SentinelServiceComponent	CorrRule
Message	`Rule Name: <name> Type: <type> Rule Id: <ID>`

1.5.6 Correlation Rule Configuration

Tag	Value
Severity	
Event Name	New/Update/Remove
SentinelServiceName	Correlation
SentinelServiceComponent	CorrRuleConfig
Message	`Correlation Rule Config ID: <ID> Rule Definition ID: {1} Name: <name> Active: {3}`

1.5.7 Deploy Rules With Actions To Engine

Tag	Value
Severity	
Event Name	deployRulesWithActionsToEngine
SentinelServiceName	CorrelationManagementService
SentinelServiceComponent	CorrelationManagementService
Message	`Deploy Rules With Actions To Engine <enginId>: Rules: <ruleID> Actions: <actionID>`

1.5.8 Disabling Rule

Tag	Value
Severity	
Event Name	disableRule
SentinelServiceName	CorrelationManagementService
SentinelServiceComponent	CorrelationManagementService
Message	`Disable Rule: {ruleCfgId}`

1.5.9 Enabling Rule

Tag	Value
Severity	
Event Name	enableRule
SentinelServiceName	CorrelationManagementService
SentinelServiceComponent	CorrelationManagementService
Message	`Enable Rule: {ruleCfgId}`

1.5.10 Rename Correlation Engine

Tag	Value
Severity	
Event Name	renameCorrEngine
SentinelServiceName	CorrelationManagementService
SentinelServiceComponent	CorrelationManagementService
Message	`Rename Engine to: <name> with EngineId: <ID>`

1.5.11 Rule Deployment is Modified

This event is sent out when an engine successfully reloads a rule deployment. This message is sent out regardless of the engine running state.

Tag	Value
Severity	1
Event Name	DeploymentModified
SentinelServiceName	CorrelationEngine
SentinelServiceComponent	Deployment
Message	`Deployment <name> modified`

1.5.12 Rule Deployment is Started

This event is sent out when an engine successfully loads a rule deployment. This message is sent out regardless of the engine running state.

Tag	Value
Severity	1
Event Name	DeploymentStarted
SentinelServiceName	CorrelationEngine
SentinelServiceComponent	Deployment
Message	`deployment <name> started`

1.5.13 Rule Deployment is Stopped

This event is sent out when an engine successfully unloads a rule deployment. This message is sent out regardless of the engine running state.

Tag	Value
Severity	1
Event Name	DeploymentStopped
SentinelServiceName	CorrelationEngine
SentinelServiceComponent	Deployment
Message	`deployment <name> stopped`

1.5.14 Starting Engine

Tag	Value
Severity	
Event Name	startEngine
SentinelServiceName	CorrelationManagementService
SentinelServiceComponent	CorrelationManagementService
Message	`Start engine: <engineID>`

1.5.15 Stopping Engine

Tag	Value
Severity	
Event Name	stopEngine
SentinelServiceName	CorrelationManagementService
SentinelServiceComponent	CorrelationManagementService
Message	`Stop engine: <engineID>`

1.5.16 UnDeploy All Rules From Engine

Tag	Value
Severity	
Event Name	undeployAllRulesFromEngine
SentinelServiceName	CorrelationManagementService
SentinelServiceComponent	CorrelationManagementService
Message	`Undeploy all rules from Engine:`

1.5.17 UnDeploy Rule

Tag	Value
Severity	
Event Name	undeployRule
SentinelServiceName	CorrelationManagementService
SentinelServiceComponent	CorrelationManagementService
Message	`Undeploy Rule: {ruleCfgId}`

1.5.18 Update Correlation Rule Actions

Tag	Value
Severity	
Event Name	updateCorrRuleActions
SentinelServiceName	CorrelationManagementService
SentinelServiceComponent	CorrelationManagementService
Message	`Update Rule Config {0} by deleting Actions: <actionID> and adding Actions: <actionID>`

1.6 Data Objects

1.6.1 Configuration

Tag	Value
Severity	
Event Name	New/Update/Remove
SentinelServiceName	Core
SentinelServiceComponent	FilterConfig,GlobalFilterConfig,SEARCH_HISTORY
Message	`Updating Config Object: <name> by User: _SYSTEM`

1.7 Data Retention Policy

1.7.1 Create Data Retention Policy

Tag	Value
Severity	1
Event Name	CreateRetentionPolicy
SentinelServiceName	IndexedLog
SentinelServiceComponent	IndexedLogRetentionPolicy
Message	`Creating Data Retention Policy: <name>`

1.7.2 Update Data Retention Policy

Tag	Value
Severity	1
Event Name	UpdateRetentionPolicy
SentinelServiceName	IndexedLog
SentinelServiceComponent	IndexedLogRetentionPolicy
Message	`Update Data Retention Policy: <name>`

1.7.3 Delete Data Retention Policy

Tag	Value
Severity	1
Event Name	DeleteRetentionPolicy
SentinelServiceName	IndexedLog
SentinelServiceComponent	IndexedLogRetentionPolicy
Message	`Delete Data Retention Policy: <name>`

1.8 Disk Usage Configuration

1.8.1 Change Disk Usage Config

Tag	Value
Severity	1
Event Name	ChangeDiskUsageConfig
SentinelServiceName	Core
SentinelServiceComponent	DiskMonitorService
Message	`Changing disk usage configuration, local storage: high water mark: <high water mark in percentage>, low water mark: <low water mark in percentage> network storage: usage limit <usage limit in percentage>`

1.9 Download Manager Audit Events

1.9.1 Download Successful

Tag	Value
Severity	1
Event Name	Download Success
SentinelServiceName	DownloadFeedService
SentinelServiceComponent	DOWNLOAD
Message	`Download successful for config:<Displays download configuration>`

1.9.2 Download Failed

Tag	Value
Severity	1
Event Name	Download Failed
SentinelServiceName	DownloadFeedService
SentinelServiceComponent	DOWNLOAD
Message	`Exception for which the download failed`

1.9.3 Download Config Updated

Tag	Value
Severity	1
Event Name	Update Download Config
SentinelServiceName	DownloadFeedService
SentinelServiceComponent	DOWNLOAD
Message	`Successfully updated Download Configuration`

1.9.4 Download Config Added

Tag	Value
Severity	1
Event Name	AddDownloadConfig
SentinelServiceName	DownloadFeedService
SentinelServiceComponent	DOWNLOAD
Message	`Successfully saved Download Configuration`

1.9.5 Download Config Removed

Tag	Value
Severity	1
Event Name	RemoveDownloadConfig
SentinelServiceName	DownloadFeedService
SentinelServiceComponent	DOWNLOAD
Message	`Successfully removed Download Configuration`

1.10 Event Router

The event router is the main component of the Collector Manager. The event router performs the maps, applies event routing rules, and publishes events.

1.10.1 Event Router Is Initializing

This event is sent when an event router starts its initialization. The event router starts initializing when it has established a connection with the back end (DAS Query).

Tag	Value
Severity	1
Event Name	EventRouterInitializing
SentinelServiceName	CollectorManager
SentinelServiceComponent	EventRouter
Message	`Event router is initializing in standalone mode; reqId(1EEAD430-E790-1029-93AC-000C296FC5D4)`

1.10.2 Event Router Is Running

This internal event is sent when the event router is ready during initialization. When the Collector Manager is restarted, another event is sent when it is ready.

This event is not sent until the event router has successfully loaded all the event routing rules and map information.

Tag	Value
Severity	1
Event Name	EventRouterIsRunning
SentinelServiceName	CollectorManager
SentinelServiceComponent	
Message	

1.10.3 Event Router Is Stopping

This event is sent when a request is received by the event router to stop during shutdown.

Tag	Value
Severity	2
Event Name	EventRouterStopping
SentinelServiceName	CollectorManager
SentinelServiceComponent	EventRouter
Message	`Event router is stopping; reqId(B408EC15-F4D2-1029-A795-000C296FC5D4)`

1.10.4 Event Router Is Terminating

This event is sent when a request is received by the event router to stop during shutdown.

Tag	Value
Severity	2
Event Name	EventRouterTerminating
SentinelServiceName	CollectorManager
SentinelServiceComponent	EventRouter
Message	`Event router is terminating; reqId(B408EC15-F4D2-1029-A797-000C296FC5D4)`

1.11 Event Router

Below listed are relevant to Event router.

1.11.1 Event Router is Initializing

This event is sent when an event router starts its initialization. The event router starts initializing when it has established a connection with the backend (DAS Query).

Tag	Value
Severity	1
Event Name	EventRouterInitializing
SentinelServiceName	CollectorManager
SentinelServiceComponent	EventRouter
Message	`Event router is initializing in standalone mode; reqId(1EEAD430-E790-1029-93AC-000C296FC5D4)`

1.11.2 Event Router is Running

Event router is the main component of the Collector Manager (the one that performs the maps, applies event routing rules and publishes the events). This internal event is sent when the event router is ready during initialization. When the Collector Manager is restarted, another event will be sent when it is ready.

This event is not sent until the event router successfully loaded all the event routing rules and map information.

Tag	Value
Severity	1
Event Name	EventRouterIsRunning
SentinelServiceName	`CollectorManager`

1.11.3 Event Router is Stopping

This event is sent when a request is received by the event router to stop during shutdown.

Tag	Value
Severity	2
Event Name	EventRouterStopping
SentinelServiceName	CollectorManager
SentinelServiceComponent	EventRouter
Message	`Event router is stopping; reqId(B408EC15-F4D2-1029-A795-000C296FC5D4)`

1.11.4 Event Router is Terminating

This event is sent when a request is received by the event router to stop during shutdown.

Tag	Value
Severity	2
Event Name	EventRouterTerminating
SentinelServiceName	CollectorManager
SentinelServiceComponent	EventRouter
Message	`Event router is terminating; reqId(B408EC15-F4D2-1029-A797-000C296FC5D4)`

1.12 Event Source Management - Collectors

1.12.1 Start Collector

Tag	Value
Severity	1
Event Name	startCollector
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Start Collector: {0}`

1.12.2 Stop Collector

Tag	Value
Severity	1
Event Name	stopCollector
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Stop Collector: {0}`

1.12.3 Update Collector Configuration

Tag	Value
Severity	1
Event Name	UpdateCollectorConfiguration
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Updating collector <name> with id <id>. <updations>`

1.13 Event Source Management - Connectors

1.13.1 Start Connector

Tag	Value
Severity	1
Event Name	startConnector
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Starting Connector <name> with ID <ID>`

1.13.2 Stop Connector

Tag	Value
Severity	1
Event Name	stopConnector
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Stopping Connector <name> with ID <ID>.`

1.13.3 Update Connector Configuration

Tag	Value
Severity	1
Event Name	updateConnectorConfiguration
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Updating connector <name> with <id>. <updations>`

1.13.4 Data Received After Timeout

When the File Connector is configured with a DataTimeout greater than 0 in the `package.xml` file and no data is read from the file during the DataTimeout period, then new data is read from the file, the following internal event is generated:

Tag	Value
Severity	4
Event Name	FileUpdatedAfterTimeout
SentinelServiceName	FileConnector
SentinelServiceComponent	FileConnector
Message	`After Event source<File Event Source ID> reached time out of<Timeout Period>, file<File Location> received new data.`

1.13.5 Data Timeout

When the File Connector is configured with a DataTimeout greater than 0 in the `package.xml` file and no data is read from the file in the DataTimeout period, the following internal event is generated:

Tag	Value
Severity	4
Event Name	FileTimeout
SentinelServiceName	FileConnector
SentinelServiceComponent	FileConnector
Message	`Event source <File Event Source ID> reached time out of <Timeout Period> when processing file <File Location>.`

1.13.6 File Rotation

When the File Connector is configured to use file rotation and the Connector changes from one file to the next, the following internal event is generated:

Tag	Value
Severity	4
Event Name	RotatingFile
SentinelServiceName	FileConnector
SentinelServiceComponent	FileConnector
Message	`File rotated for event source <File Event Source ID>. Rotating file from <Previous File Location> to <New File Location>.`

1.13.7 Process Auto Restart Error

Tag	Value
Severity	4
Event Name	ProcessAutoRestartError
SentinelServiceName	ProcessConnector
SentinelServiceComponent	ProcessConnector
Message	`Process <{0}> [command: {1}] was automatically restarted more than the allowed {2} automatic restart(s) in {3} min. The process will no longer be automatically restarted. Please check process configuration.`

1.13.8 Process Start Error

Tag	Value
Severity	1
Event Name	ProcessStartError
SentinelServiceName	ProcessConnector
SentinelServiceComponent	ProcessConnector
Message	`Error starting command: {0}`

1.13.9 Process Stop

Tag	Value
Severity	1
Event Name	ProcessStop
SentinelServiceName	ProcessConnector
SentinelServiceComponent	ProcessConnector
Message	`Process <{0}> exited [command: {1}]`

1.13.10 WMI Connector Status Message

Tag	Value
Severity	4
Event Name	WMIConnectorStatusMessage
SentinelServiceName	WMIConnector
SentinelServiceComponent	WMIConnector
Message	`<Exception>`

1.14 Event Source Management - Event Source Servers

1.14.1 Start Event Source Server

Tag	Value
Severity	1
Event Name	startEventSource Server
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Start EventSource Server: <event Source Server ID>`

1.14.2 Stop Event Source Server

Tag	Value
Severity	1
Event Name	stopEventSourceServer
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Stop EventSourceServer: <eventSourceServerID>`

1.14.3 Update Event Source Server Configuration

Tag	Value
Severity	1
Event Name	UpdateEventSourceServerConfiguration
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Updating event source server <name> with <id>. <updations>`

1.15 Event Source Management - Event Sources

1.15.1 Start Event Source

Tag	Value
Severity	
Event Name	startEventSource
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Start EventSource: {0}`

1.15.2 Stop Event Source

Tag	Value
Severity	
Event Name	stopEventSource
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Stop EventSource: {0}`

1.15.3 Start Event Sources

This event is generated when multiple event sources are started at once.

Tag	Value
Severity	1
Event Name	startEventSource
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Starting event sources <names of event sources> with ids < corresponding ids of event sources>`

1.15.4 Stop Event Sources

This event is generated when multiple event sources are stopped at once.

Tag	Value
Severity	1
Event Name	stopEventSource
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Stopping event sources <names of event sources> with ids < corresponding ids of event sources>`

1.15.5 Update Event Source Configuration

Tag	Value
Severity	1
Event Name	UpdateEventSourceConfiguration
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Updating event source <name> with id <id>.<updations>`

1.16 Event Source Management - General

1.16.1 Collector Manager Initialized

Tag	Value
Severity	1
Event Name	CollectorManagerInitialized
SentinelServiceName	CollectorManager
SentinelServiceComponent	Internal
Message	`Initialized Collector Manager…`

1.16.2 Collector Manager Is Down

Tag	Value
Severity	
Event Name	CollectorManagerDown
SentinelServiceName	HealthManager
SentinelServiceComponent	CollectorManagerHealth
Message	`Collector manager <name> UUID {1} is down for {2} days {3} hrs {4} min`

1.16.3 Collector Manager Started

Tag	Value
Severity	1
Event Name	CollectorManagerStarted
SentinelServiceName	CollectorManager
SentinelServiceComponent	Internal
Message	`Started Collector Manager...`

1.16.4 Collector Manager Stopped

Tag	Value
Severity	1
Event Name	CollectorManagerStopped
SentinelServiceName	CollectorManager
SentinelServiceComponent	Internal
Message	`Stopped Collector Manager...`

1.16.5 Collector Service Callback

Tag	Value
Severity	1
Event Name	restart
SentinelServiceName	
SentinelServiceComponent	CollectorServiceCallback
Message	`Restart Collector with Id: <ID>`

1.16.6 Event Source Manager Callback

Tag	Value
Severity	1
Event Name	restart
SentinelServiceName	
SentinelServiceComponent	EventSourceManagerCallback
Message	`Restart node with Id: <ID>`

1.16.7 Initializing Collector Manager

Tag	Value
Severity	1
Event Name	CollectorManagerInitializing
SentinelServiceName	CollectorManager
SentinelServiceComponent	Internal
Message	`Initializing Collector Manager…`

1.16.8 Update Collector Manager

Tag	Value
Severity	1
Event Name	UpdateCollectorManagerConfiguration
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Updating Collector Manager <name> confgiuration with <id>. <updations>`

1.16.9 Lost Contact With Collector Manager

Tag	Value
Severity	
Event Name	LostContactWithCollectorManager
SentinelServiceName	HealthManager
SentinelServiceComponent	CollectorManagerHealth
Message	`Lost contact with collector manager <name> UUID {1}--down for {2} days {3} hrs {4} min`

1.16.10 No Data Alert

Tag	Value
Severity	1
Event Name	NoDataAlert
SentinelServiceName	CollectorManager
SentinelServiceComponent	objectName
Message	`No data received for {7} {0} (ID {1}) for last {2} days {3} hrs {4} min {5} sec (threshold {6} ms)`

1.16.11 Persistent Process Died

The Collector Engine sends this event when the persistent process Connector detects that its controlled process has stopped.

Tag	Value
Severity	5
Event Name	PersistentProcessDied
SentinelServiceName	AgentManager
SentinelServiceComponent	AgentManager
Message	`Persistent Process on port <port ID> has died.`

1.16.12 Persistent Process Restarted

the Collector Engine sends this event when the persistent process Connector can restart the controlled process that had stopped.

Tag	Value
Severity	1
Event Name	PersistentProcessRestarted
SentinelServiceName	AgentManager
SentinelServiceComponent	AgentManager
Message	`Persistent Process on port <port ID> has restarted.`

1.16.13 Port Start

The Collector Manager sends this event when a port is started.

Tag	Value
Severity	1
Event Name	PortStart
SentinelServiceName	AgentManager
SentinelServiceComponent	AgentManager
Message	`Processing started for port_<port ID>`

1.16.14 Port Stop

The Collector Manager sends this event when a port is stopped.

Tag	Value
Severity	1
Event Name	PortStop
SentinelServiceName	AgentManager
SentinelServiceComponent	AgentManager
Message	`Processing stopped for port_<port ID>`

1.16.15 Reestablished Contact With Collector Manager

Tag	Value
Severity	
Event Name	ReestablishedContactWithCollectorManager
SentinelServiceName	HealthManager
SentinelServiceComponent	CollectorManagerHealth
Message	`Reestablished contact with collector manager {0} UUID {1} after {2} days {3} hrs {4} min`

1.16.16 Restart Plug-in Deployments

Tag	Value
Severity	
Event Name	restartPluginDeployments
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Restart deployments of plug-in: {0}`

1.16.17 Restarting Collector Manager (Cold Restart)

Tag	Value
Severity	1
Event Name	CollectorManagerRestart
SentinelServiceName	CollectorManager
SentinelServiceComponent	Internal
Message	`Restarting Collector Manager (Cold restart)`

1.16.18 Restarting Collector Manager (Warm Restart)

Tag	Value
Severity	1
Event Name	CollectorManagerRestart
SentinelServiceName	CollectorManager
SentinelServiceComponent	Internal
Message	`Restarting Collector Manager (Warm restart)`

1.16.19 Start Event Source Group

Tag	Value
Severity	1
Event Name	startEventSourceGroup
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Start Connector: {0}`

1.16.20 Start Event Source Manager

Tag	Value
Severity	1
Event Name	startEventSourceManager
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Start Collector Manager: <eventSourceManagerID>`

1.16.21 Starting Collector Manager

Tag	Value
Severity	1
Event Name	CollectorManagerStarting
SentinelServiceName	CollectorManager
SentinelServiceComponent	Internal
Message	`Starting Collector Manager`

1.16.22 Stop Event Source Group

Tag	Value
Severity	1
Event Name	stopEventSourceGroup
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Stop Connector: {0}`

1.16.23 Stop Event Source Manager

Tag	Value
Severity	1
Event Name	StopEventSourceManager
SentinelServiceName	EventSourceManagement
SentinelServiceComponent	EventSourceManagerService
Message	`Stop Collector Manager: <eventSourceManagerID>`

1.16.24 Stopping Collector Manager

Tag	Value
Severity	1
Event Name	CollectorManagerStopping
SentinelServiceName	CollectorManager
SentinelServiceComponent	Internal
Message	`Stopping Collector Manager...`

1.17 General

1.17.1 Configuration Service

Tag	Value
Severity	
Event Name	saveConfig
SentinelServiceName	
SentinelServiceComponent	ConfigService
Message	`Saving configuration, unit {0} app {1} userId {2}`

1.17.2 Controlled Process Is started

Watchdog is run as a service. Its main purpose is to keep Sentinel processes running. If a process dies, Watchdog automatically restarts that process. This event is sent when a process is started.

Tag	Value
Severity	1
Event Name	ProcessStart
SentinelServiceName	Sentinel
SentinelServiceComponent	Process
Message	`Process <ProgramName> spawned (command <pID>)`

1.17.3 Controlled Process Is stopped

This event is sent out when a process is stopped. The severity is set to 5 if the process was set to respawn (that is, it is not expected to stop). The severity is set to 1 if the process was set to run once.

Tag	Value
Severity	1/5
Event Name	ProcessStop
SentinelServiceName	Sentinel
SentinelServiceComponent	Process
Message	`Process <ProgramName> exited (command <exit_code>)`

1.17.4 Importing Auxiliary

Tag	Value
Severity	
Event Name	importAuxiliary
SentinelServiceName	
SentinelServiceComponent	PluginRepositoryService (Medium)
Message	`Import auxiliary file <auxiliaryJarName> into plug-in <pluginID>.`

1.17.5 Importing Plug-in

Tag	Value
Severity	1
Event Name	importPlugin
SentinelServiceName	PluginRepository
SentinelServiceComponent	PluginRepositoryService
Message	`Import plug-in <name> (ID <ID>) of type <type>.`

1.17.6 Load Esec Taxonomy To XML

Tag	Value
Severity	
Event Name	loadEsecTaxonomyToXML
SentinelServiceName	
SentinelServiceComponent	EsecTaxonomyNodeService
Message	`Loading Esecurity taxonomy Info to an xml format:`

1.17.7 Process Auto Restart Error

This event is sent out when a process is stopped. The severity is set to 5 if the process was set to respawn (that is, it is not expected to stop). The severity is set to 1 if the process was set to run once.

Tag	Value
Severity	1/5
Event Name	ProcessAutoRestartError
SentinelServiceName	Sentinel
SentinelServiceComponent	Process
Message	`Process <{0}> [command: {1}] was automatically restarted more than the allowed {2} automatic restart(s) in {3} min. The process will no longer be automatically restarted. Please check process configuration.`

1.17.8 Process Restarts

Tag	Value
Severity	1
Event Name	ProcessRestart
SentinelServiceName	Sentinel
SentinelServiceComponent	Process
Message	`Process <`*`ProgramName`*`> spawned (command <`*`pID`*`>)`

1.17.9 Proxy Client Registration Service (medium)

Tag	Value
Severity	
Event Name	registerClient
SentinelServiceName	
SentinelServiceComponent	ProxyClientRegistrationService (medium)
Message	`Registering new client`

1.17.10 Restarting Process

Tag	Value
Severity	1
Event Name	restartProcess
SentinelServiceName	SentinelHealth
SentinelServiceComponent	SentinelHealthService
Message	`Restarting process <name> on Sentinel server <`*`name`*`> UUID {2}`

1.17.11 Restarting Processes

Tag	Value
Severity	1
Event Name	restartProcesses
SentinelServiceName	SentinelHealth
SentinelServiceComponent	SentinelHealthService
Message	`Restarting <number> processes: <`*`number`*`> name <`*`name`*`> server <name> server ID <ID>;`

1.17.12 Starting Process

Tag	Value
Severity	1
Event Name	startProcess
SentinelServiceName	SentinelHealth
SentinelServiceComponent	SentinelHealthService
Message	`Starting process <name> on Sentinel server <name> UUID {2}`

1.17.13 Starting Processes

Tag	Value
Severity	1
Event Name	startProcesses
SentinelServiceName	SentinelHealth
SentinelServiceComponent	SentinelHealthService
Message	`Starting <number> processes: <number> name <name> server <name> server ID <ID>;`

1.17.14 Stopping Process

Tag	Value
Severity	1
Event Name	stopProcess
SentinelServiceName	SentinelHealth
SentinelServiceComponent	SentinelHealthService
Message	`Stopping process <name> on Sentinel server <name> UUID {2}`

1.17.15 Stopping Processes

Tag	Value
Severity	1
Event Name	stopProcesses
SentinelServiceName	SentinelHealth
SentinelServiceComponent	SentinelHealthService
Message	`Stopping <number> processes: <number> name <name> server <name> server ID <ID>;`

1.17.16 Store Esec Taxonomy From XML

Tag	Value
Severity	
Event Name	storeEsecTaxonomyFromXML
SentinelServiceName	
SentinelServiceComponent	EsecTaxonomyNodeService
Message	`Storing Esecurity taxonomy Info:`

1.17.17 Watchdog Process Is started

As the Watchdog process starts, the following internal event is generated:

Tag	Value
Severity	1
Event Name	ProcessStart
SentinelServiceName	WatchDog
SentinelServiceComponent	WatchDog
Message	`WatchDog Service Starting`

1.17.18 Watchdog Process Is stopped

When the Watchdog service is stopped, the following internal event is generated:

Tag	Value
Severity	5
Event Name	ProcessStop
SentinelServiceName	WatchDog
SentinelServiceComponent	WatchDog
Message	`WatchDog Service Ended`

1.18 Incidents and Workflows

Below listed are relevant to Incidents and Workflows.

1.18.1 Add Events To Incident

Tag	Value
Severity	
Event Name	addEventsToIncident
SentinelServiceName	IncidentService
SentinelServiceComponent	IncidentService
Message	`User: <name> adding <number> events to incident with ID: <ID>`

1.18.2 Adding Process Definition

Tag	Value
Severity	
Event Name	addProcessDefinition
SentinelServiceName	WorkflowServices
SentinelServiceComponent	WorkflowObjectMgrService
Message	`reading iTRAC Template <name>`

1.18.3 Create Incident

Tag	Value
Severity	
Event Name	createIncident
SentinelServiceName	IncidentService
SentinelServiceComponent	IncidentService
Message	`User: <name> created incident with name: <incidentName>, state: <state>, severity: <severity>, resolution: <resolution>`

1.18.4 Creating Group

Tag	Value
Severity	
Event Name	createGroup
SentinelServiceName	WorkflowServices
SentinelServiceComponent	WorkflowObjectMgrService
Message	`Creating iTRAC Role {0} : description : <description>`

1.18.5 Creating User

Tag	Value
Severity	
Event Name	createUser
SentinelServiceName	WorkflowServices
SentinelServiceComponent	WorkflowObjectMgrService
Message	`Creating User in WorkFlow: {0} with firstname: <firstName> lastname : <lastName>`

1.18.6 Delete Incident

Tag	Value
Severity	
Event Name	deleteIncident
SentinelServiceName	IncidentService
SentinelServiceComponent	IncidentService
Message	`Delete incident with ID: <ID>`

1.18.7 Deleting Group

Tag	Value
Severity	
Event Name	deleteGroup
SentinelServiceName	WorkflowServices
SentinelServiceComponent	WorkflowObjectMgrService
Message	`Deleting iTRAC Role {0} : description : <description>`

1.18.8 Deleting Process Definition

Tag	Value
Severity	
Event Name	deleteProcessDefinition
SentinelServiceName	WorkflowServices
SentinelServiceComponent	WorkflowObjectMgrService
Message	`Deleting iTRAC Template <ID>`

1.18.9 Deleting User

Tag	Value
Severity	
Event Name	deleteUser
SentinelServiceName	WorkflowServices
SentinelServiceComponent	WorkflowObjectMgrService
Message	`Deleting User in WorkFlow: {0} with firstname: <firstName> lastname : <lastName>`

1.18.10 E-mail Incident

Tag	Value
Severity	
Event Name	emailIncident
SentinelServiceName	IncidentService
SentinelServiceComponent	IncidentService
Message	`User: <name> emailed incident with name: <incidentName>, state: <state>, severity: <severity>{2}, resolution: <resolution> to email address: <e-mailID>`

1.18.11 Get Incident

Tag	Value
Severity	
Event Name	getIncident
SentinelServiceName	IncidentService
SentinelServiceComponent	IncidentService
Message	`Get incident with ID: <ID>`

1.18.12 Save Incident

Tag	Value
Severity	
Event Name	saveIncident
SentinelServiceName	IncidentService
SentinelServiceComponent	IncidentService
Message	`Save incident with name: <name>, state: <state>, severity: <severity>, resolution: <resolution>`

1.18.13 Saving Group

Tag	Value
Severity	
Event Name	saveGroup
SentinelServiceName	WorkflowServices
SentinelServiceComponent	WorkflowObjectMgrService
Message	`Saving iTRAC Role {0} : description : <description>`

1.18.14 Saving Process Definition

Tag	Value
Severity	
Event Name	saveProcessDefinition
SentinelServiceName	WorkflowServices
SentinelServiceComponent	WorkflowObjectMgrService
Message	`Saving iTRAC Template <name>`

1.18.15 Viewing Process Definition

Tag	Value
Severity	
Event Name	getProcessDefinition
SentinelServiceName	WorkflowServices
SentinelServiceComponent	WorkflowObjectMgrService
Message	`Viewing iTRAC Template <ID>`

1.19 Mapping Service

Below listed are relevant to mapping service

1.19.1 Error

Tag	Value
Severity	
Event Name	error
SentinelServiceName	
SentinelServiceComponent	
Message	`Error while updating map data: {0}`

1.19.2 Error Applying Incremental Update

This event is sent when the mapping service fails to apply an update to an existing client map.

Tag	Value
Severity	4
Event Name	ErrorApplyingIncrementalUpdate
SentinelServiceName	MappingService
SentinelServiceComponent	ReferentialDataObjectMap
Message	`The error <error> occurred while applying updates to map <mapName> (ID <mapId>) v.<version>. Rescheduling a refresh to complete map update.`

1.19.3 Error initializing map with ID

This internal event is generated from the client side of the mapping service (the one that is part of the Collector Manager). This error is generated when the Collector Manager attempts to retrieve a map that does not exist. This should not happen but can happen if maps are created and deleted.

Tag	Value
Severity	4
Event Name	ErrorNoSuchMap
SentinelServiceName	MappingService
SentinelServiceComponent	ReferentialDataObjectMap
Message	`Error initializing map with id <ID>: no such map`

1.19.4 Error Refreshing Map

This internal event is generated from the client side of the mapping service (the one that is part of the Collector Manager). When the Collector Manager is told to refresh the map because it has been modified or its definition has changed it sends an internal event. This means that there was some unexpected non-transient error while trying to refresh a map. The Collector Manager will wait 15 minutes and will try again. If this happens during initialization the initialization will proceed and this map will be ignored until it can be successfully loaded.

Tag	Value
Severity	4
Event Name	ErrorRefreshingMapData
SentinelServiceName	MappingService
SentinelServiceComponent	ReferentialDataObjectMap
Message	`Error refreshing map <mapName>: <exc>`

1.19.5 Error Saving Data File

Tag	Value
Severity	
Event Name	ErrorSavingDataFile
SentinelServiceName	MappingService
SentinelServiceComponent	MapService
Message	`The error <error> occurred while saving data to file <fileName> (no) backup`

1.19.6 Get File Size

Tag	Value
Severity	
Event Name	getFileSize
SentinelServiceName	
SentinelServiceComponent	
Message	`Retrieving size for file <fileName>`

1.19.7 Loaded Large Map

This internal event is an information event sent by the mapping service informing that a large map was loaded to the Collector Manager. A map is considered large if the number of rows exceeds 100,000.

Tag	Value
Severity	0
Event Name	LoadedLargeMap
SentinelServiceName	MappingService
SentinelServiceComponent	ReferentialDataObjectMap
Message	`Finished loading map <name> with id <ID> and <number> entries and total size <#>Kb in <##>sec`

1.19.8 Long Time To Load Map

This internal event is an information event sent by the mapping service informing that loading a map took an unusually long time (greater than one minute).

Tag	Value
Severity	0
Event Name	LongTimeToLoadMap
SentinelServiceName	MappingService
SentinelServiceComponent	ReferentialDataObjectMap
Message	`It took <##>sec to load map <name> with id <ID> and <number> entries and total size <##>Kb`

1.19.9 Out Of Sync Detected

This event is sent when the mapping service detects that a map is out of date. The mapping service will automatically schedule a refresh.

Tag	Value
Severity	2
Event Name	OutOfsyncDetected
SentinelServiceName	MappingService
SentinelServiceComponent	ReferentialDataObjectMap
Message	`Map <mapName> detected the map data is out-of-sync, probably because of a missed update notification--scheduling a refresh`

1.19.10 Refreshing Map from Cache

This internal event is generated from the client side of the mapping service (the one that is part of the Collector Manager). When the Collector Manager is told to refresh the map because it has been modified or its definition has changed it sends an internal event. This means that its cache is up to date and is refreshing the map from cache.

Tag	Value
Severity	1
Event Name	LoadingMapFromCache
SentinelServiceName	MappingService
SentinelServiceComponent	ReferentialDataObjectMap
Message	`Loading from cache v<version> of map <mapName> (ID <id>)`

1.19.11 Refreshing Map from Server

This internal event is generated from the client side of the mapping service (the one that is part of the Collector Manager). When the Collector Manager is told to refresh the map because it has been modified or its definition has changed it sends an internal event. This means that the map was either not in the cache or the version in the cache was not up to date and the Collector Manager is retrieving the map from the server.

Tag	Value
Severity	1
Event Name	RefreshingMapFromServer
SentinelServiceName	MappingService
SentinelServiceComponent	ReferentialDataObjectMap
Message	`Refreshing from server map <name> with id <ID>`

1.19.12 Save Data File

Tag	Value
Severity	
Event Name	saveDataFile
SentinelServiceName	
SentinelServiceComponent	MapService
Message	`Saving data file {0}, backup? {1}`

1.19.13 Saved Data File

Tag	Value
Severity	
Event Name	SavedDataFile
SentinelServiceName	MappingService
SentinelServiceComponent	MapService
Message	`Saved "+fileSize+" bytes to file <fileName> with original backed up to "+backupFile:"no backup of original`

1.19.14 Timed Out Waiting For Callback

When the Collector Manager needs to refresh a map it sends a request to the backend. This request contains a callback. The backend generates the map and when it is ready it sends the map to the Collector Manager using the callback. If it takes too long for the response to arrive (more than ten minutes) the Collector Manager will submit a second request assuming the first was lost. When this occurs, the following internal event is generated.

Tag	Value
Severity	2
Event Name	TimedoutWaitingForCallback
SentinelServiceName	MappingService
SentinelServiceComponent	ReferentialDataObjectMap
Message	`Map <name> timed out waiting for callback with new map data--retrying`

1.19.15 Timeout Refreshing Map

This internal event is generated from the client side of the mapping service (the one that is part of the Collector Manager). When the Collector Manager is told to refresh the map because it has been modified or its definition has changed it sends an internal. This means that the Collector Manager attempted to retrieve the map from the server and the server never acknowledged the request and timed out. This error is considered transient and the Collector Manager will retry.

Tag	Value
Severity	4
Event Name	TimeoutRefreshingMap
SentinelServiceName	MappingService
SentinelServiceComponent	ReferentialDataObjectMap
Message	`Request timed out while refreshing map <name>: <exception>`

1.19.16 Update

Tag	Value
Severity	
Event Name	update
SentinelServiceName	
SentinelServiceComponent	MapDataCallback
Message	`Updating map data`

1.19.17 Update

Tag	Value
Severity	
Event Name	update
SentinelServiceName	
SentinelServiceComponent	(low)
Message	`Updating map data (ser)`

1.20 Report Definitions and Report Results

- Section 1.20.3, “Remove Report Result,” on page 62
- Section 1.20.4, “Remove Report Results,” on page 63

1.20.1 Remove Report Definition

Tag	Value
Severity	1
Event Name	RemoveReportDefinition
SentinelServiceName	Reporting
SentinelServiceComponent	ReportingService
Message	`Removing report definition: <name>`

1.20.2 Remove Report Definitions

Tag	Value
Severity	1
Event Name	RemoveReportDefinition
SentinelServiceName	Reporting
SentinelServiceComponent	ReportingService
Message	`Removing report definitions: <names of deleted report definitions>`

1.20.3 Remove Report Result

Tag	Value
Severity	1
Event Name	RemoveReportResult
SentinelServiceName	Reporting
SentinelServiceComponent	ReportingService
Message	`Removing report result: <name>`

1.20.4 Remove Report Results

Tag	Value
Severity	1
Event Name	RemoveReportResults
SentinelServiceName	Reporting
SentinelServiceComponent	ReportingService
Message	`Removing report results: <names of deleted report results>`

1.21 Search

1.21.1 Event Search

Tag	Value
Severity	1
Event Name	EventSearch
SentinelServiceName	Indexed Search
SentinelServiceComponent	Events
Message	`Search Started <search parameters>`

1.22 User Management

1.22.1 Create User

Tag	Value
Severity	1
EventName	CreateUser
SentinelServiceName	Config
SentinelServiceComponent	UserManagementService
Message	`Creating user account <username> with Last name: <lastname>, First name: <firstname>`

1.22.2 Create User Role

Tag	Value
Severity	1
Event Name	CreateUserRole
SentinelServiceName	Core
SentinelServiceComponent	UserGroupsPermissionService
Message	`Creating role <role_name>, users with this role can: <permissions>`

1.22.3 Add User To Role

Tag	Value
Severity	1
Event Name	AddUserToRole
SentinelServiceName	Core
SentinelServiceComponent	UserGroupsPermissionService
Message	`Adding User: <username> to Role: <role_name>`

1.22.4 Removing User From a Role

Tag	Value
Severity	1
Event Name	RemoveUserFromRole
SentinelServiceName	Core
SentinelServiceComponent	UserGroupsPermissionService
Message	`Removing User: <username> from Role: <username>`

1.22.5 Updating User

Tag	Value
Severity	1
Event Name	UpdateUser
SentinelServiceName	Config
SentinelServiceComponent	UserManagementService
Message	`Updating User: <username>`

1.22.6 Updating User Role

Tag	Value
Severity	1
Event Name	UpdateUserRole
SentinelServiceName	Core
SentinelServiceComponent	UserGroupPermissionService
Message	`Updating role: <rolename>, users with this role can now: <rolepermission>`

1.22.7 Delete User

Tag	Value
Severity	1
Event Name	DeleteUser
SentinelServiceName	Config
SentinelServiceComponent	UserManagementService
Message	`Deleting User Account: <username>`

1.22.8 Delete User Role

Tag	Value
Severity	1
Event Name	DeleteUserRole
SentinelServiceName	Core
SentinelServiceComponent	UserGroupsPermissionService
Message	`Deleting User Role: <username>`

1.22.9 Resetting User Password

Tag	Value
Severity	1
Event Name	ResettingUserPassword
SentinelServiceName	Config
SentinelServiceComponent	UserManagementService
Message	`Resetting password for User Account <username>`