# J2 Ops Monitor Thresholds and Management

## Overview

The J2 Ops Monitor is custom set of tools developed to assist in the monitoring of Cache, Ensemble, Initiate and HealthShare applications and the servers they run on. The J2 Ops Monitor consists of 2 main pieces:

-Ops Monitor Dashboard (main interface to view current status)

-Ops Monitor Client Web Services (installed on each server to be monitored)

Controlled by a set of Scheduled Jobs the Ops Monitor Dashboard connects to each monitored server and gathers information to report and alert on. The 3 Jobs are outlined below:

1. Server Tasks  
   Collects stats on:
   1. CPU
   2. Memory
   3. Disk I/O
   4. Disk Usage
2. Production Tasks  
   Collects stats on:
   1. Production Status
   2. Production Sessions
   3. Production Total Messages
   4. Production Completed Messages
   5. Production Error Messages
   6. Production Event Log Error messages
   7. Interface Status
   8. Interface Message counts
   9. Interface Last Message Time
   10. Interface Queues
   11. Interface Last Activity Time
   12. Invalid Login attempts for System Accounts
3. Send Alerts Tasks  
   Analyzes Thresholds and Status of items above and sends email alerts.

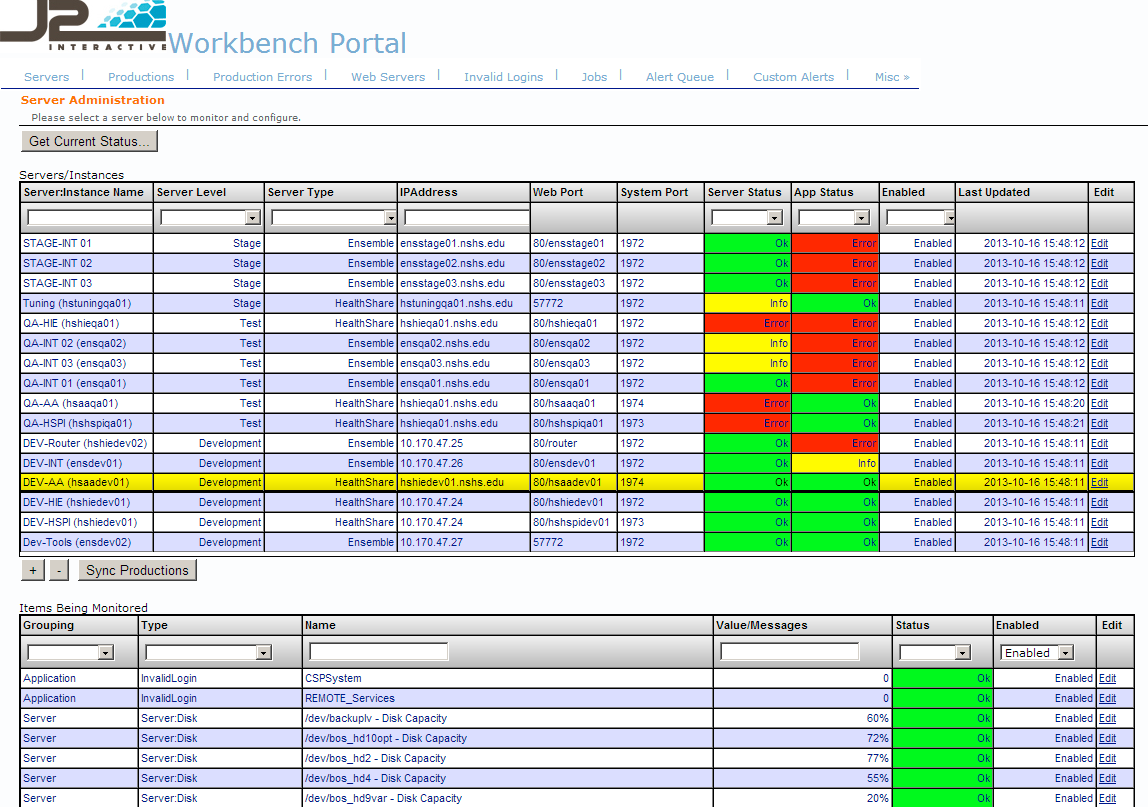
## Ops Monitor Dashboard

The J2 Ops Monitor Dashboard is a web based interface for adding servers to be monitored, viewing current status and levels of monitored items, configuring thresholds for alerts, and managing alert email settings. The Dashboard also provides an interface for researching the status of Servers, Productions, Production Interfaces, Web Servers, Invalid Logins and Custom Alerts.

Navigation/Viewing of Ops Monitor pages:

* Clicking on a Server or Production in the top table will display more detailed items being monitored in the lower table
* Clicking ‘Edit’ next to any item will allow you to enable/disable monitoring for that item as well as adjust thresholds of various alert levels.
* Using the pull down filters at the top of each column allows filtering of displayed items in the table, for instance you can choose to view only Test or Stage servers and only items that are Enabled. **NOTE: settings chosen are saved to allow per-user customization.**
* When researching Warnings or Errors on Server or Production items clicking on the ‘Alert Queue’ tab will give you a quick view of the details of the alert.

A screen shot showing the main page of the J2 Ops Monitor Dashboard is below:



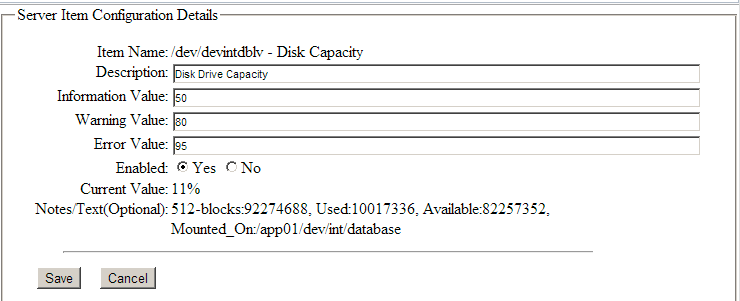
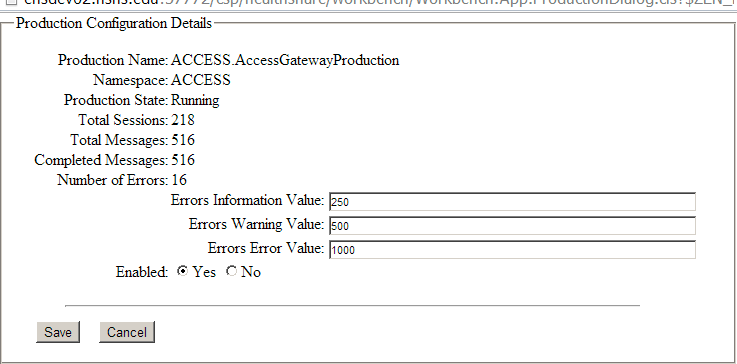
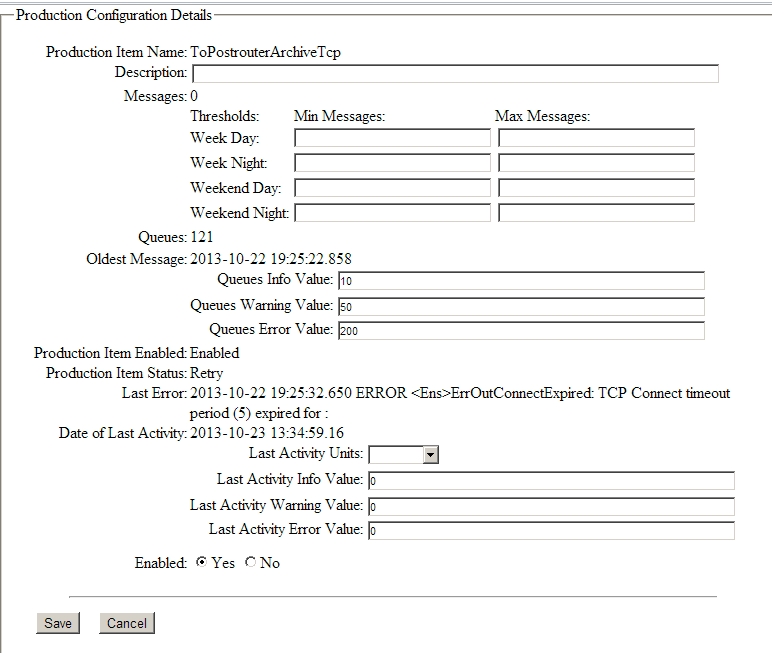
## Managing Thresholds and Alerts

After Ops Monitor is setup and running you will begin to get alerts on the monitored items. Addressing these alerts and configuring the Ops monitor to send only necessary alerts is key to using the alert system properly.

In some cases these are alerts that you will want to address on the Operating System or in the System Management portal of HealthShare/Ensemble/Cache. Examples would be: clearing or allocation proper disk space, starting a production that is not running, or addressing the cause of errors being logged to a production.

In other cases you will want to adjust the threshold of these alerts and to adjust when an item should be reported as OK, Info, Warning or Error. For example by adjusting the thresholds you can choose to change the Warning value of a particular Disk’s usage to flag Info at 80%, Warn at 85% and Error at 90%. You would adjust these based on what is considered normal for any individual item.

Thresholds that can be adjusted include:

* Server items; Disk, CPU, Memory usage. Sample of Disk Capacity thresholds are shown below:  
  
* Production Error counts (Example below):  
  
* Production Items have multiple Thresholds including Messages received during Week Day/Night and Weekend Day/Night, Messages in Queue, and Last Activity. A Sample page is showing:  
  

## Researching Alerts

The approach I often take when using Ops Monitor to research the cause of an alert is outlined below:

For Server Items:

1. Starting with the ‘Servers’ tab in the ‘Servers/Instances’ table I see there is a Server Status other then ‘OK’ for a server
2. Click on the row of that server to see the details in the ‘Items Being Monitored’ table below.
3. Find the Server item showing the status being researched. The name, current value and status should be visible.
4. Click ‘edit’ to get more details and possibly adjust the threshold to clear the alert.
5. In the ‘edit’ window you can see more details and edit the current threshold settings or disable/enable the item completely from monitoring.
6. After adjusting thresholds the next time the background tasks run the status of the item will be updated and the alert will be cleared.

For App/Production Items:

1. Starting with the ‘Servers’ tab in the ‘Servers/Instances’ table I see there is an App Status other then ‘OK’ for a server.
2. Click on the row of that server to see the details in the ‘Items Being Monitored’ table below.
3. Find the App item showing the status being researched. The name, current value and status should be visible.
4. Most times it is a **Production**, continue with the following steps:
   1. Go to the ‘Productions’ tab
   2. Check the ‘Production Stage’ column to se if it is ‘Running’
   3. Click ‘Edit Production’ to view it’s Error Threshold and current ‘Number of Errors’
   4. Close ‘Edit Production’ window
   5. Click on Production row in table to show ‘Production Items’ below.
   6. Find any items with a status other then ‘OK’
   7. Check the following columns for possible causes:  
      ‘Adapter Status’  
      ‘Last Message Time’  
      ‘Queues’
   8. Click ‘Edit’ to view/edit thresholds and to see the ‘Last Error’
   9. Adjust thresholds if needed look further into the ‘Last Error’. The causes of the last error might need to be taken to a developer or network specialist for further research.
   10. Some Adapters end up sending too many false alerts and thresholds prove difficult to adjust for them, optionally you can disable monitoring of that individual item on this screen.
5. When not a Production item it could be an **Invalid Login:**
   1. Check the item for the # of failed attempts for the given login.
   2. Often this could be sign of a configuration issue where someone provided incorrect credentials in their configuration.
   3. Go to the System Management Portal for the server in question and view the Audit Log to get more information on the Invalid Logins:  
      System Administration -> Security -> Auditing -> View Audit Database
   4. Change ‘Event Type’ to “%Login”, adjust dates as needed and click Search.
   5. Viewing details on individual items will provide value in figuring out who or what is attempting to login with invalid credentials.