Enabling Audit Logging in Uptime Infrastructure Monitor

Uptime Infrastructure Monitor can be configured to record application configuration changes in an audit log named audit.log that is found in the logs directory.

There are many uses for the audit log. For example, use the audit log to track changes to your Uptime Infrastructure Monitor environment for compliance with security or other local policies. You can also use the audit log to debug problems that may have been introduced by a specific configuration change; the audit.log enables you to determine who made the change and when it took effect.

The following is an example of an audit log entry:

2013-02-23 12:28:20,082 - dchiang: ADDSYSTEM [cfgcheck=true, port=9998, number=1, use-ssl=false, systemType=1, hostname=10.1.1.241, displayName=MailMain, systemSystemGroup=1, serviceGroup=, description=, systemSubtype=1]

Enabling the Audit Log

The audit log is disabled by default. To enable the audit log:

1. Open the uptime_install_folder\uptime.conf file in a text editor and add the following line:

   ```
   auditEnabled=yes
   ```

2. Save the file and exit the text editor.
3. Restart the Data Collector.

   On Linux or Solaris systems, enter the following commands at the command line:

   ```
   /etc/init.d/uptime_core stop
   /etc/init.d/uptime_core start
   ```

   On Windows platforms, enter the following commands at the command line:

   ```
   net stop "up.time Data Collector"
   net start "up.time Data Collector"
   ```