**Microsoft® Windows® Operating System Log Insight Content Pack**

* **Overview:**

The Microsoft® Windows® Operating System content pack is a purpose built, downloadable add on to Log Insight. Operations managers can collect, analyze, and visually sort through Windows Operating System log data (log files) for more efficient troubleshooting. Log Insight’s graphical user interface offers at a glance viewing of log files, for quickly detecting anomalies and or other behavioral issues effecting health and performance and Windows servers.

* **Highlights:**
  + Scalable log collection and monitoring of Windows Operating System servers
  + Structured collection and at a glance analytics
  + Purpose built dashboard representation of Windows OS logs for enhanced Windows OS administration
* **Description:**

The Microsoft® Windows® Operating System Log Insight content pack provides actionable data, for Windows OS operations managers, specifically for troubleshooting and pinpointing problems. With Log Insight, customers can scale for collecting up to 45K events per second, with an easy to deploy, low cost, 6-node scale out architecture. With up to 2 terabytes of searchable data, Windows admins can archive and search through hundreds of servers, historically for pattern and anomaly analysis, via a structured like database approach.

There are eleven pre-defined Windows OS specific dashboards, with total of 55 widgets, 5 query widgets and 6 alarms for helping to visualize, analyze and take meaningful action on Windows OS log information. This significantly reduces the log file data overload issues, by abstracting the log data collected into meaningful bar, line, and pie charts. Further this Windows OS content pack offers direct integration with Windows Event Log, again to simplify, and make Windows OS log data more actionable. The dashboards provided within this content pack drill into the areas of application, system and security for a more focused representation of the log data collected.

* **Tech Specs:**
  + **Compatibility:**

- Windows Desktop: Vista and newer

- Windows Server: 2008 and newer

* + **Installation**

Navigate to the "Content Pack" menu in Log Insight. Select the "Import Content Pack" button. In the "Import Content Pack" menu, do the following:

- Select the "Browse..." button and select the content pack you are trying to import

- Select the "Install as content pack" radio button

- Select the "Import" button

Alternately, you can also install the content pack from the marketplace available on Log Insight UI

-On Log Insight UI, browse to Content Pack ->Marketplace

-Click on the content pack and then click ‘Install’

* + **Configuration:**

The **"Microsoft - Windows"** content pack requires the use of the Log Insight agent with the cfapi protocol (default) and the included agent group configuration. To apply the agent group configuration:  
  
\* Go to the  **Administration -> Management -> Agents** page (requires Super Admin privileges)  
\* Select the  **All Agents** drop-down at the top of the window and select the  **“Copy Template”** button to the right of the **"Microsoft – Windows"** agent group  
\* Add the desired filters to restrict which agent receive the configuration (optional)  
\* Select the "Refresh" button at the top of the page  
\* Select the "Save Configuration" button at the bottom of the page

**IMPORTANT**: For the "Security - Object Auditing" dashboard to work in the "Microsoft - Windows" content pack, Object Access Auditing must be enabled on all Windows clients sending events. To enable object auditing you need to alter the local security policy and enable auditing on the desired object. To alter the local security policy:  
   
\* Open up Administrative Tools > Local Security Policy, or run secpol.msc  
\* Open Local Policies > Audit Policy  
\* Right-click on "Object Access Audit" and select Properties  
\* Ensure "Success" and "Failure" are checked  
\* Click on OK, and then close the Local Security Policy window

**Note**: You can also create Group Policy to enable object access auditing on multiple systems easily.  
   
Once object auditing is enabled, you need to enable auditing for a specific folder (and all its sub-folders and files):   
\* Open up the File Explorer by right-clicking and selecting Run as Administrator  
\* Browse to the folder you want to turn auditing on  
\* Right-click on the folder and select Properties  
\* Select the Security Tab  
\* Click on Advanced, then Auditing  
\* Click on Add  
\* Enter the name of the users you wish auditing, click on Find Now to ensure it is registered, and then click on OK  
\* Check the Successful and Failed boxes, and then click on OK  
\* Close the windows by clicking OK

 **Note**: You should only do this for a select few objects, since the information generated is very chatty.