# Microsoft® Active Directory® Log Insight Content Pack

- **Overview:**
  The Microsoft® Active Directory® Log Insight content pack offers customized collection, analysis, and graphical representation of Active Directory log files for efficient troubleshooting of Active Directory operation problems. By simply downloading this content pack and installing into Log Insight, system administrators can within minutes begin making sense out of their Active Directory logs files. Operation tasks including detection of anomalies, being able to wind back to yesterday's events, and/or being able to quickly sort through the logs in a more structured like manner, are several of the many features within this content pack.

- **Highlights:**
  - Comprehensive collection and monitoring of Active Directory log messages.
  - Broad Active Directory functional coverage including AD security, DNS, DS, and DFS
  - Noninvasive monitoring via Windows Event Log integration

- **Description:**
  Any Active Directory system administrator looking for a more structured approach in collecting and analyzing log files, from all the Active Directory distributed components (including AD security, Domain Name Services, Distributed File System, and/or Domain Services), should consider this content pack for Log Insight. The Log Insight simple to deploy scale out architecture is the ideal approach for collecting up to 45K messages per second, across hundreds of nodes, including all of these Active Directory components. The Active Directory content pack populates a menu bar within the product for viewing in a filtered fashion DNS, DS, DFS, and security logs within each of these respective categories.

  Log Insight offers very intuitive graphical representation, especially with regards to log events. Spikes in the number and types of messages received can be flagged as events with external notifications. System administrators can drill into these events for looking at where and why these are being generated. The Active Directory content pack includes twelve dashboards with around 65 widgets and 11 alarms for viewing and quickly analyzing Active Directory log messages.

- **Tech Specs:**
  - **Compatibility:**
    Active Directory on
    - Windows Server 2008+
    - Windows Server 2008 R2+
    - Windows Server 2012+
    - Windows Server 2012 R2+

  **NOTE:** DNS Server Auditing is not supported in this content pack version on Windows Server 2008/R2+. Only success/failure auditing is possible and the "DNSServer/Audit" channel is not available. It is however available in Windows Server 2012+

  - **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:**

1. **<u>liagent.ini configuration:</u>**

- **<u>Using agent group :</u>**

The **"Microsoft – Active Directory"** 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 – Active Directory"** 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