BLUE LANCE

Setting up LT Auditor+ App for Splunk

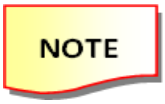
Table of Contents

Overview

This document covers the installation steps to setup the LT Auditor+ App for Splunk and the configuration needed to send monitoring and assessment data to Splunk.

Prerequisites

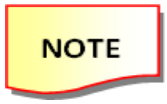
- LT Auditor+ version HF1309 or above installed on all audited servers and workstations.
- LT Auditor+ Windows Assessment has been installed in the environment
- Splunk version 6.5 or higher has been installed
- The SplunkUniversalForwarder has been installed on the machine that hosts the LT Auditor+ Windows Assessment Manager
- The following ports must be open
  - 9997
  - 1468
  - 8000



Please register with Splunk to download Splunk and the Splunk Universal Forwarder. Please remember the username and passwords used for both applications as they will required for installation steps below.

Installation Steps

1. Download the LT Auditor+ App for Splunk from www.ltauditor.com/splunk and follow www.ltauditor.com/splunk/#help for instructional video to install.
2. Download, unblock and extract the SplunkLTAAssessment.zip from https://downloads.ltauditor.com/SplunkLTAAssessment.zip
3. Use PowerShell (Admin Mode) to run the script SetupLTASplunkAssessment.ps1. Please make sure that PowerShell *Set-ExecutionPolicy Unrestricted* command has been run to allow for script execution.
4. When the script is run you will be prompted for the following parameters:
    a. *Location of Splunk Assessment Folder* – This is folder used by the Splunk Universal Forwarder to send Windows Assessment data to Splunk
    b. *Location of Selected* Splunk *Stage Folder* – Used by the LT_Sender throttle service to throttle volume of data sent to Splunk
    c. *Throttle Limit* – Volume of data in (MB) to throttle
    d. *Location of Forwarder* – Location of the where the Splunk Universal Forwarder is installed



For each of the options above click enter to accept defaults.

    e. You will be prompted for the Splunk Universal Forwarder username and password to compete the setup.

After execution of this script the following actions would have happened:

- Installation of a service called LT_Sender. This service is used to throttle data sent to Splunk primarily to avoid Splunk Licensing constraints.
- Copied new PowerShell scripts to the Assessment/PowerShellScripts folder. These new scripts need to be scheduled for execution to collect Assessment data in Splunk

PowerShell Scripts

New PowerShell Scripts	Description	Parameters
SecurityDirectories_GM_DS_M.ps1	Scanning Folders	***Start Folder*** – Set Folder to Scan ***Scan Description*** – Description ***Exclude Built-In Security Principals*** ***FullScan*** – Set to 1 ***CPUThreads*** – Set to 20 ***CPUThreadItems*** – Set to 300 ***Copy Audit Files To*** – Set to '*Splunk Assessment Folder'* defined above or Set to *Selected Splunk Stage Folder* to use the Throttle service
SecurityFiles_GM_DS_M.ps1	Scanning Files	***Start Folder*** – Set Folder to Scan ***Scan Description*** – Description ***Exclude Built-In Security Principals*** ***FullScan*** – Set to 1 ***ScanFilesModifiedBefore*** – Set to 'Today for all file' or Set Date ***ScanACLS*** – Set to 1 to collect ACLS or Set to 0 to prevent collecting ACLS ***Copy Audit Files To*** – Set to '*Splunk Assessment Folder'* defined above or Set to *Selected Splunk Stage Folder* to use the Throttle service