



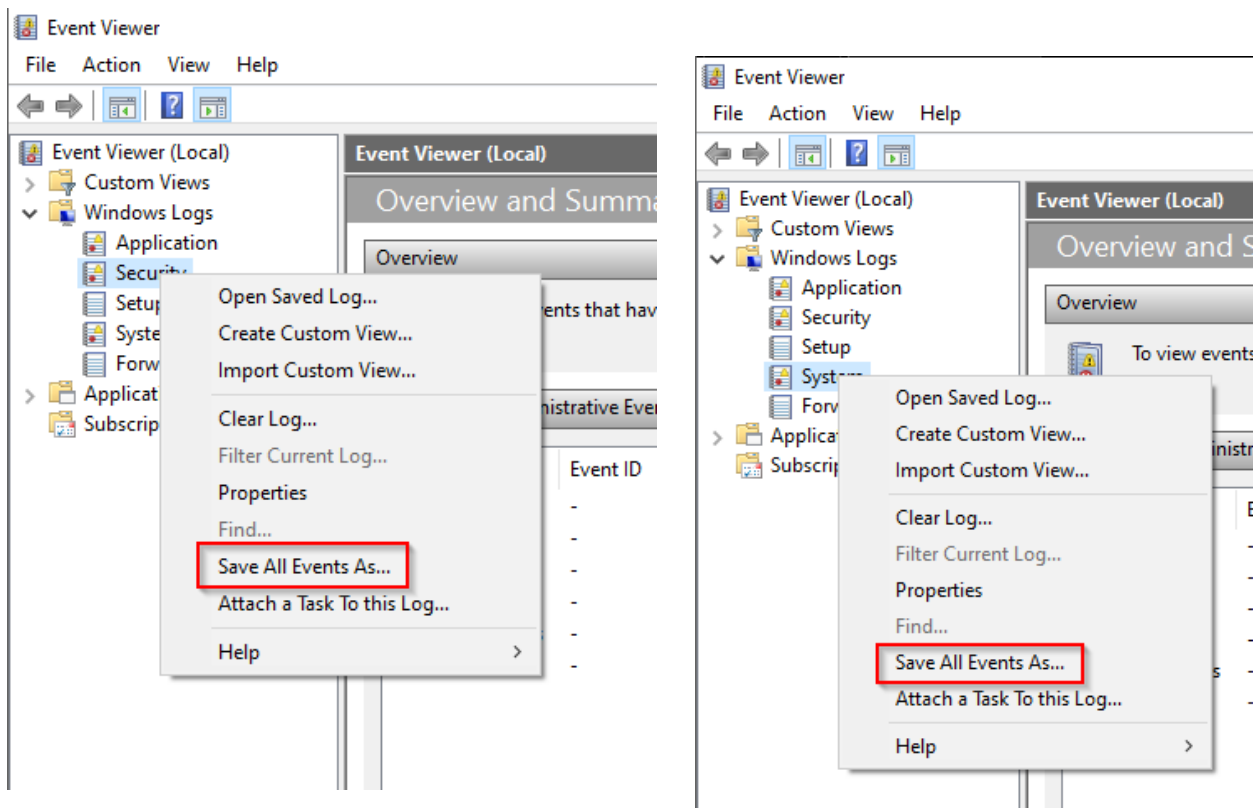
THE MANUAL UPLOAD OF LOGS AND INSTALLATION OF COLLECTORS FOR SUMOLOGIC

This document demonstrates at a basic level the steps required to manually upload logs to the Sumologic SIEM platform as well as the installation of Sumologic log collectors on both Windows and Linux

Jordan Patterson

1. Save Your Windows VM Security and system logs (separately) then upload in Sumologic.

Saving Windows Security and System Logs:



Uploading Security and System Logs to SumoLogic:

Upload Files

Uploading a static local file allows you to try Sumo Logic without configuring a Collector to ingest live, streaming data. To continuously monitor a file in your environment, configure a Collector and Source within the Sumo Logic Web Application.

1. Select the type of log files you will be uploading.

Other

2. Enter a Source Category that will help you search your logs later.

Source Category ?

uploads/other/lab/security

3. Drag and drop files below to upload, or use the button to browse. Files cannot exceed 100MB or 20 files total.

Select Files

Security Logs.evtx

4. Select a time zone for your log file.

☒ Use time zone from log file. If none present use:

(UTC) Etc/UTC

☐ Ignore time zone from log file and instead use:

(UTC) Etc/UTC

Back

Next

Upload Files

Uploading a static local file allows you to try Sumo Logic without configuring a Collector to ingest live, streaming data. To continuously monitor a file in your environment, configure a Collector and Source within the Sumo Logic Web Application.

1. Select the type of log files you will be uploading.

Other

2. Enter a Source Category that will help you search your logs later.

Source Category ?

uploads/other/lab/system

3. Drag and drop files below to upload, or use the button to browse. Files cannot exceed 100MB or 20 files total.

Select Files

System Logs.evtx

4. Select a time zone for your log file.

☒ Use time zone from log file. If none present use:

(UTC) Etc/UTC

☐ Ignore time zone from log file and instead use:




(UTC) Etc/UTC

Back

Next




SumoLogic Collection page:



Collection

+ New

CollectionOpenTelemetry CollectionStatusIngest BudgetsArchiveData Archiving

 Search for collectors and sources by name or sourceCategory

Show: All Collectors Show up to: 10 collectors Expand: All | [None](#)

Name	Health	Type	Status	Source Category
▼ File Uploads	● Healthy	Hosted		
Security Logs.evtx HTTP	● Healthy			uploads/other/lab/security
System Logs.evtx HTTP	● Healthy			uploads/other/lab/system

2. For last 3 days order each 1-hour time window with number of Security logs and system logs then create a graph for each.

3. Install SumoLogic collector in Windows and Linux

Linux:

Getting Token:

Set Up Collection

1. To download and install a Linux Collector, open a terminal, then click **Copy** to copy and paste the following code into the terminal. You'll want to run the installer on your server with root or Administrator privileges. This may take a few minutes. [?](#)

```
wget "https://collectors.sumologic.com/rest/download/linux/64" -O SumoCollector.sh && chmod +x SumoCollector.sh && sudo ./SumoCollector.sh -q -Vsumo.token_and_url=WWNLcVJCVnhoV083TVBLdHJ5OWI4d1VwQmhHRjgyb21odHRwczoVL2NvbGx1Y3RvcnMuc3Vtb2xvZ21jLmNvbQ==
```

Copy

2. Once the Collector has been installed and registered, click **Continue**.

Back

Next



Installing Collector through the Terminal:

```
ubuntu@ubuntu-VMware-Virtual-Platform: ~  
ubuntu@ubuntu-VMware-Virtual-Platform:~$ wget "https://collectors.sumologic.com/  
rest/download/linux/64" -O SumoCollector.sh && chmod +x SumoCollector.sh && sudo  
./SumoCollector.sh -q -Vsumo.token_and_url=WWNLcVJCvNhoV083TVBLdHJ5OWl4dlVwQmhH  
Rjgyb2lodHRwczovL2NvbGxLY3RvcnMuc3Vtb2xvZ2ljLmNvbQ==  
--2023-09-28 18:19:10-- https://collectors.sumologic.com/rest/download/linux/64  
Resolving collectors.sumologic.com (collectors.sumologic.com)... 54.167.221.54,  
54.236.158.108, 54.210.40.245, ...  
Connecting to collectors.sumologic.com (collectors.sumologic.com)|54.167.221.54|  
:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 100127314 (95M) [application/octet-stream]  
Saving to: 'SumoCollector.sh'  
  
SumoCollector.sh 100%[=====>] 95.49M 39.3MB/s in 2.4s  
  
2023-09-28 18:19:12 (39.3 MB/s) - 'SumoCollector.sh' saved [100127314/100127314]  
  
[sudo] password for ubuntu:  
Unpacking JRE ...  
Starting Installer ...  
The installation directory has been set to /usr/local/SumoCollector.  
WARN StatusConsoleListener The bufferSize is set to 8192 but bufferedIo is false  
: false  
Extracting files...
```

Finalizing collector installation and transferring logs through collector:

Configure Source: Linux System

1. Enter a Source Category that will help you find your metrics later.

Source Category 

linux/system/ubuntu

2. Choose any of the standard locations from which you would like to collect; you can also enter alternative or additional path expressions by clicking **Add Path Expression** one or more times, such as `/var/log/*access.log`.

☒ /var/log/auth*

[View Files](#)

[+ Add Path Expression](#)

3. Select a time zone for your log file.

☒ Use time zone from log file. If none present use:

(UTC) Etc/UTC



☐ Ignore time zone from log file and instead use:

(UTC) Etc/UTC



Back

Next

Windows:

Get installer and Token:

Set Up Collection

1. Download and install a Windows Collector by clicking the following download link 

[Windows \(64-bit\)](#)

2. When the installer package downloads, open it and follow the installation wizard prompts. Click **Copy** and then paste the Token into the installer when required. This may take a few minutes.

[> Show me how](#)

Token:

```
ejh0Y1o4RjV4dFFES1pIOGR00TNzUmFjd1lRc2RUVEVodHRwczoL2  
NvbGx1Y3RvcnMuc3Vtb2xvZ21jLmNvbQ==
```

Copy

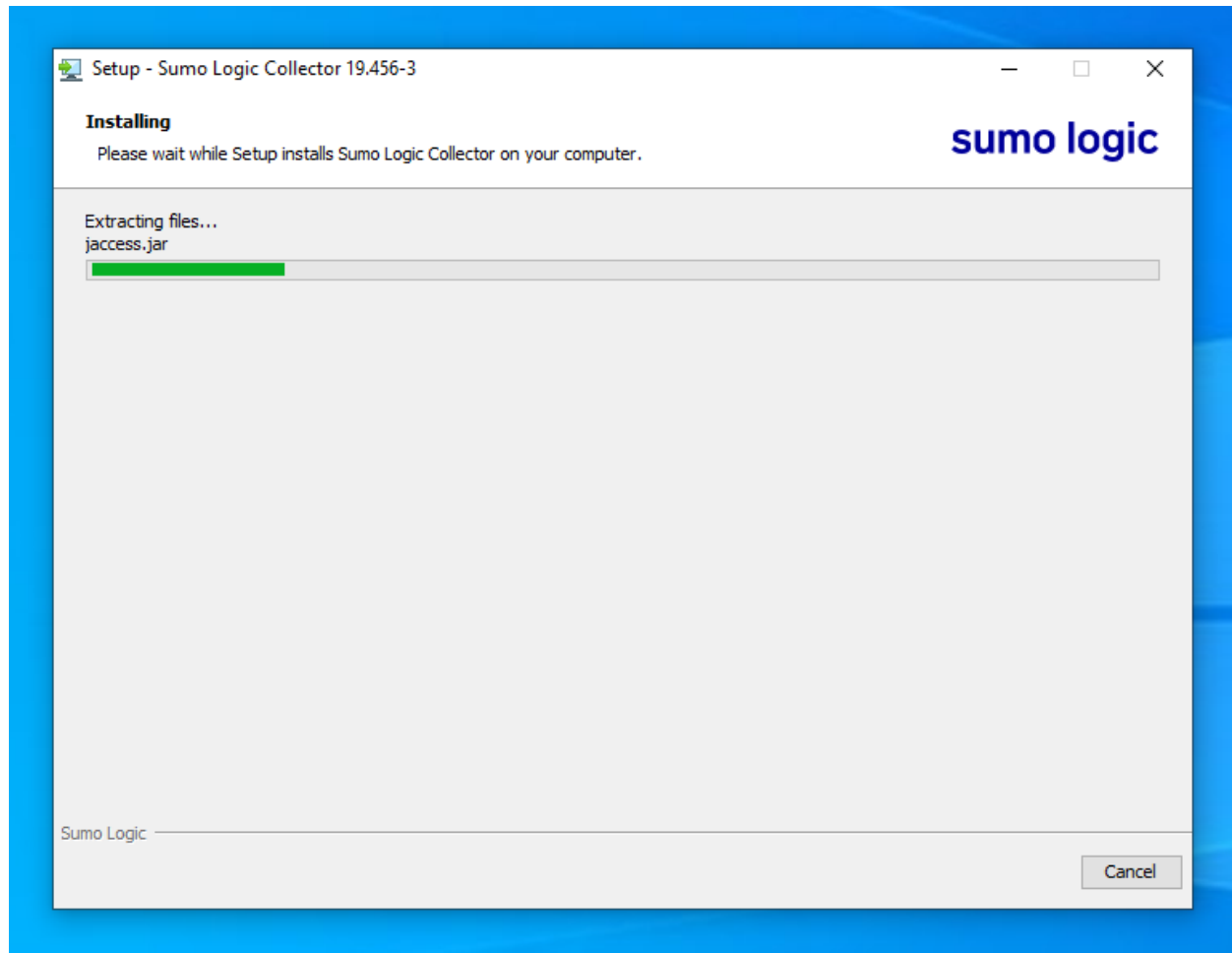
3. Once the Collector has been installed and registered, click **Continue**.

Back

Next



Installing Collector:



Configure and transfer logs:

Configure Source: Windows Events

1. Enter a Source Category that will help you find your metrics later.

Source Category 

windows/events

2. Select the Windows Events you would like to collect.

Standard Windows Events

- ☒ Security
- ☒ Application
- ☒ System

Custom Event Channels

[Select All](#) | [Select None](#)

 Filter Custom Channels

- ☒ Windows PowerShell
- ☒ Key Management Service
- ☒ Internet Explorer
- ☒ HardwareEvents
- ☒ SMCA

Back

Next