“SIEM-prove Your Security with the Google of all Logs”

Author: Michael Art Rebultan aka “Strainer”
https://www.linkedin.com/in/artrebultan/

"To my loving wife, Jennie, and my precious children, Ashera Jear and Andrei Akhira, this article is dedicated to you. Your unwavering support and love have been my driving force throughout this journey. I could not have accomplished this without your constant encouragement and belief in me. I am grateful to you for being my inspiration.

To the Supreme Being, I am eternally grateful for the talent and abilities that have been bestowed upon me. Your guidance and blessings have been invaluable in the creation of this work.

To my friends in the cyber security community, thank you for your support and for sharing in my advocacy. Your encouragement and belief in my efforts have been a source of strength and motivation. This article is a testament to the power of a supportive community. It has been a pleasure having you along on my journey."

Table of Contents

Introduction

Synopsis

The absence of logs and security monitoring in a network can present significant organizational challenges. Without this information, it can be difficult for an organization to detect and respond to security breaches, which can lead to data loss and damage to the organization's reputation. Additionally, the lack of logs and monitoring can make it difficult to troubleshoot network issues and ensure compliance with regulatory requirements. It can also make it difficult to conduct forensic investigations in the event of a security incident. Overall, the absence of logs and security monitoring can make it difficult for an organization to maintain the security and integrity of its network, which can have serious consequences for the organization and its customers.

Without logs and security monitoring, an organization may not be able to detect malicious activity, such as unauthorized access or data exfiltration, until it is too late. This can result in significant data loss and reputational damage. Additionally, without logs and monitoring, it can be difficult to identify the source of security incidents and take appropriate action to prevent future incidents.

Furthermore, the absence of logs and monitoring can make it difficult for organizations to comply with regulatory requirements. Many regulations, such as HIPAA and PCI-DSS, require organizations to maintain detailed logs of network activity and have security monitoring in place to detect and respond to security incidents. Without this information, organizations may be in violation of these regulations and face penalties.

In addition to these challenges, the absence of logs and monitoring can also make it difficult for organizations to troubleshoot network issues and identify the root cause of problems. This can lead to longer downtimes and increased costs for the organization.

Overall, the absence of logs and security monitoring in a network can have serious consequences for an organization. It can make it difficult to detect and respond to security incidents, comply with regulatory requirements, and troubleshoot network issues. It is essential for organizations to implement robust logging and security monitoring solutions to mitigate these challenges and maintain the security and integrity of their networks.

The SIEM

A Security Information and Event Management (SIEM) system can help solve the challenges associated with the absence of logs and security monitoring in a network. SIEM systems aggregate and analyze log data from various sources, such as network devices, servers, and applications, to provide a centralized view of network activity. This allows organizations to detect and respond to security incidents in a timely manner.

Here are a few ways in which a SIEM system can help solve the challenges associated with the absence of logs and security monitoring:

1. Detection and response: SIEM systems use advanced analytics and correlation rules to identify and alert on suspicious activity. This allows organizations to detect and respond to security incidents quickly, reducing the risk of data loss and reputational damage.
2. Compliance: SIEM systems can help organizations comply with regulatory requirements by collecting, analyzing, and reporting on log data. This can provide the necessary information for audits and compliance reporting.
3. Troubleshooting: SIEM systems can help organizations troubleshoot network issues by providing visibility into network activity and identifying the root cause of problems.
4. Forensics: SIEM systems store log data for a long time which allows organizations to conduct forensic investigations in the event of a security incident.
5. Correlation of events: A SIEM system can correlate events from multiple sources and provide a comprehensive view of network activity. This allows organizations to identify patterns of activity that may indicate a security incident and take appropriate action.
6. Threat intelligence: SIEM systems can integrate with threat intelligence feeds to provide real-time information about known threats and vulnerabilities. This allows organizations to proactively identify and mitigate potential security risks.
7. Automated response: Many SIEM systems come with built-in incident response capabilities that can automatically respond to security incidents. This can include actions such as blocking IP addresses or disabling user accounts.
8. User behavior analytics: SIEM systems can track and analyze user behavior to detect anomalies that may indicate malicious activity. This can include identifying patterns of activity that are outside of normal behavior or identifying unusual access patterns.
9. Customizable dashboards and reports: SIEM systems typically provide customizable dashboards and reporting capabilities that allow organizations to view and analyze log data in a way that is most relevant to their needs.

In summary, the implementation of a Security Information and Event Management (SIEM) system can provide organizations with a comprehensive view of network activity, allowing them to identify and respond to security incidents in a timely manner. SIEM systems aggregate and analyze log data from various sources, such as network devices, servers, and applications, to provide a centralized view of network activity. This allows organizations to detect and respond to security incidents quickly, reducing the risk of data loss and reputational damage. Additionally, SIEM systems can help organizations comply with regulatory requirements by collecting, analyzing, and reporting on log data. It also provides the necessary information for audits and compliance reporting. SIEM systems also have the capability to troubleshoot network issues by providing visibility into network activity and identifying the root cause of problems, conduct forensic investigations, integrate with threat intelligence feeds, automate incident response, track, and analyze user behavior, and provide customizable dashboards and reports to help organizations maintain the security and integrity of their networks.

Managed Security Services Over On-Prem SOC

An organization should opt for managed security services when it lacks the resources, expertise, or budget to build and maintain an internal Security Operations Center (SOC). Managed services can be a cost-effective solution for organizations that want to outsource their security needs.
Here are a few reasons an organization should consider managed services over building an internal SOC:

1. Lack of expertise: Building and maintaining an internal SOC requires a high level of technical expertise in areas such as threat intelligence, incident response, and security analytics. Organizations that lack this expertise may find it more cost-effective to outsource these services to a managed security provider.
2. Limited resources: Building and maintaining an internal SOC requires a significant investment in personnel, technology, and infrastructure. Organizations that have limited resources may find it more cost-effective to outsource these services to a managed security provider.
3. Compliance: Organizations that are subject to regulatory compliance requirements may find it more cost-effective to outsource these services to a managed security provider that can provide the necessary documentation and reporting.
4. Scalability: Managed services can be scaled up or down as needed, allowing organizations to adjust their security needs as their business grows or changes.
5. Cost-effective: Managed security services can be a cost-effective solution for organizations that want to outsource their security needs. By outsourcing their security needs, organizations can avoid the expenses of hiring and training staff and buying and maintaining security equipment.
6. 24/7 monitoring: Managed security services providers offer round-the-clock monitoring and protection against threats. This allows organizations to have peace of mind that their systems are being watched and always protected, even when their internal teams may be off duty.
7. Rapid response: Managed security services providers have dedicated incident response teams that can quickly respond to security incidents and minimize damage. This allows organizations to minimize downtime and reduce the impact of security breaches.
8. Automation: Managed security services providers can provide automated solutions that can help organizations with tasks such as vulnerability scanning, security patching, and compliance reporting. This can help organizations to save time and resources by automating repetitive tasks and focusing on more strategic initiatives.
9. Advanced analytics and threat intelligence: Managed security service providers often have access to advanced analytics and threat intelligence tools that can help organizations detect and respond to threats more effectively.

10. Flexibility: Managed security services providers can offer a range of services to meet the specific needs of an organization. This can include monitoring, incident response, threat intelligence, and compliance reporting. Organizations can choose the services that best meet their needs and budget.

In conclusion, organizations that lack the resources, expertise, or budget to build and maintain an internal Security Operations Center (SOC) should consider opting for managed security services. Managed services providers can offer a range of services such as expert personnel, advanced technology, 24/7 monitoring, incident response, threat intelligence, compliance reporting and automation. These services can help organizations to detect and respond to security incidents, comply with regulatory requirements, automate repetitive tasks, minimize downtime, and reduce the impact of security breaches while providing a cost-effective solution. Additionally, managed security services providers can provide organizations with the flexibility to choose the services that best meet their needs and budget. Managed services can be a valuable option for organizations looking to outsource their security needs and maintain the security and integrity of their networks.

I. Executive Summary

Disclaimer

The information and content in this article are provided solely for informational and educational purposes and is based on the author's experience and knowledge. The use of Sumo Logic as a sample for implementing a Security Information and Event Management (SIEM) system is for illustrative purposes only and does not constitute an endorsement or recommendation of the product by the author or the publisher.

Please note that the views expressed in this article are solely with the author or publisher and do not reflect the views of his current company.

Purpose of the report

The purpose of this report is to provide a comprehensive analysis of the current security environment and to recommend a solution for implementing Sumo Logic Security Information and Event Management (SIEM) to enhance the organization's security posture.

Overview of Sumo Logic SIEM

Sumo Logic SIEM is a cloud-based solution that provides real-time visibility and analytics for security and compliance. It uses machine learning and artificial intelligence to detect and respond to threats, and it can be integrated with other security tools and systems to provide a holistic view of the organization's security posture.

Benefits of implementing Sumo Logic SIEM

Implementing Sumo Logic SIEM will provide the organization with several benefits, including:

- Real-time visibility and analytics for security and compliance
- Automated threat detection and response
- Integration with other security tools and systems
- Improved incident response and forensic capabilities
- Compliance with industry and government regulations
- In summary, this report aims to provide a thorough overview of the current security environment, how Sumo Logic SIEM can be implemented and how it can benefit the organization in terms of security and compliance. This report also outlines the implementation plan, resources required, training and support, and recommendations for next steps.

II. Current Security Environment

Current security challenges and threats

The current security environment is characterized by an increasing number of sophisticated cyber threats, such as advanced persistent threats (APTs), ransomware, and phishing attacks. These threats can originate from a variety of sources, including nation-states, criminal organizations, and hacktivists. They can target any type of organization and can result in significant financial losses, reputational damage, and disruption of business operations.

Current security solutions in use

The organization currently employs various security solutions to protect against these threats, such as firewalls, intrusion detection and prevention systems, and antivirus software. However, these solutions may not provide complete protection against advanced threats and may also generate a large amount of log data that is difficult to analyze and correlate.

The organization may also have some security solutions in place like:

- Network segmentation
- Multi-factor authentication
- Security Information and Event Management (SIEM)
- Identity and Access management (IAM)
- Endpoint protection

However, these solutions may not be able to provide a holistic and real-time view of the organization's security posture and may not be able to detect and respond to advanced threats in a timely manner.

In summary, the current security environment is characterized by an increasing number of sophisticated cyber threats and the organization is currently using various security solutions to protect against these threats. However, these solutions may not provide complete protection against advanced threats and may not be able to provide a holistic and real-time view of the organization's security posture.

III. Sumo Logic SIEM Solution

Description of the Sumo Logic SIEM solution

Sumo Logic SIEM is a cloud-based solution that provides real-time visibility and analytics for security and compliance. It collects and analyzes log data from a wide range of sources, including network devices, servers, applications, and cloud platforms. It uses machine learning and artificial intelligence to detect and respond to threats, and it can be integrated with other security tools and systems to provide a holistic view of the organization's security posture.

Features and capabilities

- Real-time visibility and analytics: Sumo Logic SIEM provide real-time visibility into the organization's security posture, and it can detect and respond to threats in near real-time.
- Automated threat detection and response: Sumo Logic SIEM uses machine learning and artificial intelligence to detect and respond to threats. It can also be configured to automatically respond to certain types of threats, such as blocking an IP address or shutting down a compromised account.
- Integration with other security tools and systems: Sumo Logic SIEM can be integrated with other security tools and systems, such as firewalls, intrusion detection and prevention systems, and antivirus software.
- Improved incident response and forensic capabilities: Sumo Logic SIEM provides the ability to quickly search and correlate log data, which can help incident responders and forensic analysts to quickly identify the scope and cause of a security incident.
- Compliance with industry and government regulations: Sumo Logic SIEM can help organizations to meet various industry and government regulations, such as PCI DSS, HIPAA, and SOC 2.

Comparison with other SIEM solutions

Sumo Logic SIEM is a cloud-based solution, which means that it does not require any hardware or software to be installed on-premises. This can reduce the organization's costs and complexity. Compared to other SIEM solutions, Sumo Logic SIEM provides more user-friendly interface and more advanced analytics and machine learning capabilities. Additionally, Sumo Logic SIEM can be easily scaled up or down as the organization's needs change, and it can be integrated with other security tools and systems to provide a holistic view of the organization's security posture.

In summary, Sumo Logic SIEM is a cloud-based solution that provides real-time visibility and analytics for security and compliance. It uses machine learning and artificial intelligence to detect and respond to threats, and it can be integrated with other security tools and systems to provide a holistic view of the organization's security posture. Compared to other SIEM solutions, Sumo Logic SIEM is more user-friendly, more advanced in terms of analytics and machine learning capabilities, and it can be easily scaled and integrated with other security tools.

IV. Implementation Plan

Project scope and objectives

The scope of the project is to implement Sumo Logic SIEM to enhance the organization's security posture and to meet regulatory compliance requirements. The objectives of the project are to:

- Collect and analyze log data from a wide range of sources
- Detect and respond to threats in near real-time
- Provide real-time visibility into the organization's security posture
- Improve incident response and forensic capabilities
- Meet regulatory compliance requirements

Implementation timeline

The implementation timeline for Sumo Logic SIEM will depend on the organization's specific needs and requirements. However, a general implementation timeline could include the following phases:

- Phase 1: Planning and Preparation
  During this phase, the project team will determine the specific requirements for the organization and will develop a detailed project plan.
- Phase 2: Implementation
  During this phase, the project team will install and configure Sumo Logic SIEM, and will integrate it with other security tools and systems. The team will also test and verify that the solution is working as expected.
- Phase 3: Training and Deployment
  During this phase, the project team will provide training for staff on how to use and manage Sumo Logic SIEM and will deploy the solution to production.
- Phase 4: Ongoing Support and Maintenance
  During this phase, the project team will provide ongoing support and maintenance for Sumo Logic SIEM and will perform regular updates and upgrades as needed.

Resources required

The resources required for the implementation of Sumo Logic SIEM will depend on the organization's specific needs and requirements.

However, the following resources will likely be required:

- Project manager
- Technical lead
- Security analysts
- Network engineers
- Compliance specialist
- Training and support staff

Risk assessment and management

A risk assessment will be performed to identify potential risks that could impact the implementation of Sumo Logic SIEM. Risks will be classified based on the likelihood and impact of the risk. Mitigation strategies will be developed and implemented to minimize the impact of identified risks.

In summary, the implementation plan for Sumo Logic SIEM includes the scope and objectives of the project, the implementation timeline, resources required, and risk assessment and management. The specifics of the plan will depend on the organization's specific needs and requirements. The implementation plan is designed to ensure that the organization can achieve the goals of enhanced security posture, improved incident response and forensic capabilities, and regulatory compliance.

V. Training and Support

Training plan for staff

A comprehensive training plan will be developed and implemented to ensure that staff are able to effectively use and manage Sumo Logic SIEM. The training plan will include the following elements:

- Onboarding training for new staff
- Basic and advanced user training for all staff who will be using Sumo Logic SIEM
- Administrator training for staff who will be responsible for managing and maintaining the solution
- Refresher training for staff on a regular basis to ensure that their skills are up to date

The training will be conducted both in-person and online and will be tailored to the organization's specific needs and requirements.

Ongoing support and maintenance

Ongoing support and maintenance will be provided for Sumo Logic SIEM to ensure that the solution is functioning properly, and that staff are able to effectively use and manage the solution. This will include:

- Providing support and troubleshooting assistance to staff as needed
- Performing regular updates and upgrades to the solution
- Monitoring the solution to ensure that it is performing as expected
- Providing documentation and knowledge base articles to assist staff in using and managing the solution

In summary, the Training and Support plan for Sumo Logic SIEM includes a comprehensive training plan for staff, and ongoing support and maintenance to ensure that the solution is functioning properly, and that staff can effectively use and manage the solution. The specifics of the plan will depend on the organization's specific needs and requirements. The Training and Support plan is designed to ensure that the staff are knowledgeable and comfortable with Sumo Logic SIEM and that the organization can continue to improve the security posture and meet regulatory compliance.

VI. Conclusion

Summary of key points

- The current security environment is characterized by an increasing number of sophisticated cyber threats and the organization is currently using various security solutions to protect against these threats. However, these solutions may not provide complete protection against advanced threats and may not be able to provide a holistic and real-time view of the organization's security posture.
- Sumo Logic SIEM is a cloud-based solution that provides real-time visibility and analytics for security and compliance. It uses machine learning and artificial intelligence to detect and respond to threats, and it can be integrated with other security tools and systems to provide a holistic view of the organization's security posture.
- An implementation plan for Sumo Logic SIEM has been proposed, including the scope and objectives of the project, the implementation timeline, resources required, and risk assessment and management.
- A comprehensive training plan and ongoing support and maintenance have been proposed to ensure that staff are able to effectively use and manage Sumo Logic SIEM and that the solution is functioning properly.

Recommendations for next steps

Based on the analysis and recommendations presented in this report, the following next steps are recommended:

- Approve the implementation of Sumo Logic SIEM to enhance the organization's security posture and to meet regulatory compliance requirements.
- Establish a project team and assign roles and responsibilities for the implementation of Sumo Logic SIEM.
- Develop a detailed project plan that includes the specific requirements for the organization, the implementation timeline, resources required, and risk assessment and management.
- Implement the training and support plan for Sumo Logic SIEM to ensure that staff are knowledgeable and comfortable with the solution and that the solution is functioning properly.

In summary, the conclusion of this report provides a summary of key points, and recommendations for next steps to implement Sumo Logic SIEM, which will enhance the organization's security posture and meet regulatory compliance requirements. The report also highlights that the implementation plan, training and support plan, and risk assessment and management will be important to ensure the successful implementation of Sumo Logic SIEM.

VII. Appendices

Technical specifications

The technical specifications for Sumo Logic SIEM will include information such as hardware and software requirements, system architecture, and data retention policies. This information will be useful for system administrators and network engineers who will be responsible for installing, configuring, and maintaining the solution.

Vendor information

The vendor information will include contact details for the vendor, such as their name, phone number, email address, and website. This information will be useful for staff who will be responsible for managing and maintaining the solution, as well as for staff who will be responsible for purchasing and renewing the solution.

Additional resources and references

Additional resources and references will include relevant documents, articles, and websites that provide additional information about Sumo Logic SIEM and related topics. This information will be useful for staff who will be responsible for managing and maintaining the solution, as well as for staff who will be responsible for regulatory compliance.

In summary, the Appendices section of the report includes technical specifications, Vendor information and Additional resources and references that can be useful for the staff who will be responsible for installing, configuring, maintaining, and purchasing the solution. This information can clarify the system requirements, vendor details and other relevant resources that can be used as references.

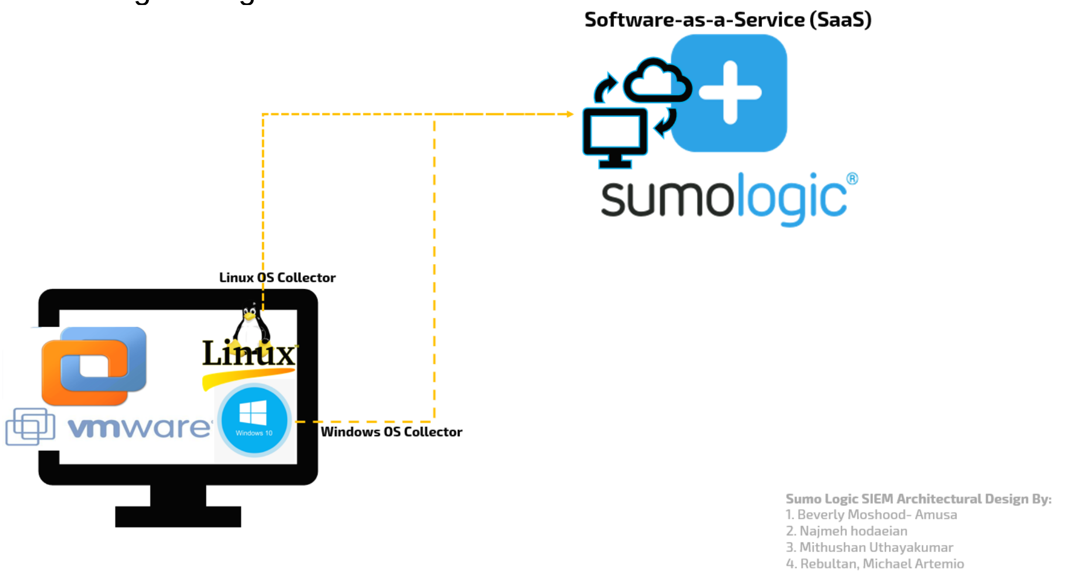
VIII. Annex

Architectural design

The architectural design for this implementation would involve several components:

1. The Sumo Logic Cloud Service: This is the central hub where all the collected log data is stored, processed, and analyzed. The Sumo Logic cloud service is a highly scalable, multi-tenant platform that can handle large volumes of log data.
2. Collectors: These are lightweight software agents that run on the Linux and Windows systems and collect log data from the specified log files. The collectors are responsible for forwarding the log data to the Sumo Logic cloud service.
3. Linux and Windows systems: These are the systems where the log data is generated. In this design, one Linux and one Windows system is being used as the source of log data.
4. Network: A reliable and secure network connection is required to transmit log data from the Linux and Windows systems to the Sumo Logic cloud service.
5. Log files: These are the files on the Linux and Windows systems that contain the log data. The collectors are configured to collect log data from specified log files.
6. Dashboards, alerts, and searches: These are the tools used to analyze and monitor the log data in the Sumo Logic cloud service. Dashboards display the log data in a visually meaningful way, alerts notify when certain conditions are met, and searches are used to extract specific information from the logs.

Overall, this design involves a distributed architecture where log data is collected from multiple systems and sent to a central location for processing and analysis. The Sumo Logic cloud service provides the necessary scalability and processing power to handle large volumes of log data, while the collectors are responsible for collecting and forwarding the log data to the cloud service.

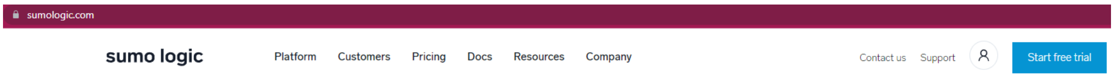


Sumo Logic SIEM Architectural Design By:
1. Beverly Moshood- Amusa
2. Najmeh hodaeian
3. Mithushan Uthayakumar
4. Rebultan, Michael Artemio

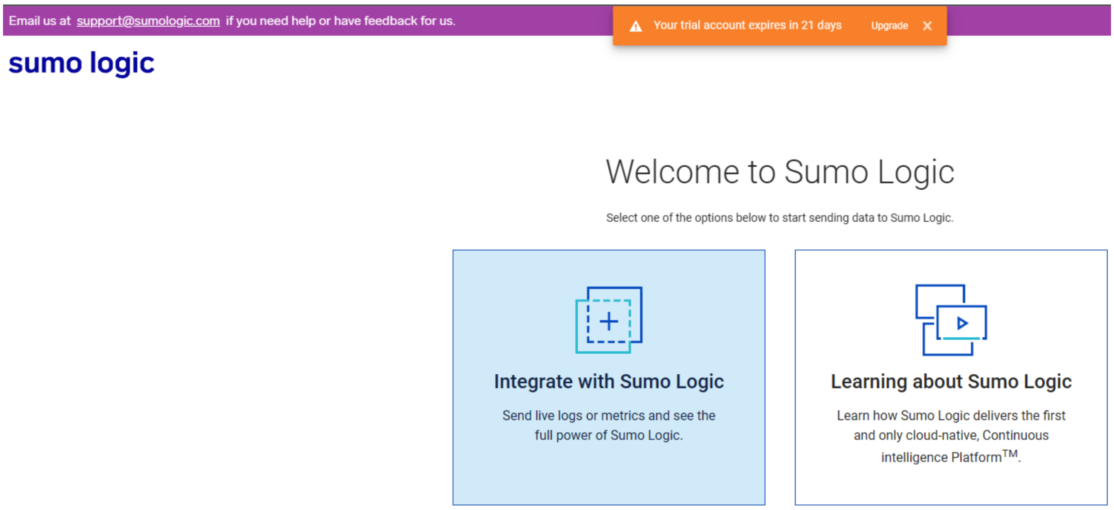
Installation steps and configurations

Here is an example of an architectural design for implementing Sumo Logic for one Linux and one Windows OS:

1. First, you will need to create a Sumo Logic account –
   - Start free trial from the Saas Portal: https://www.sumologic.com/



   - And set up a new "Collector" for each operating system you want to collect logs from.


Email us at support@sumologic.com if you need help or have feedback for us.

Your trial account expires in 21 days

Welcome to Sumo Logic

Select one of the options below to start sending data to Sumo Logic.

Integrate with Sumo Logic

Send live logs or metrics and see the full power of Sumo Logic.

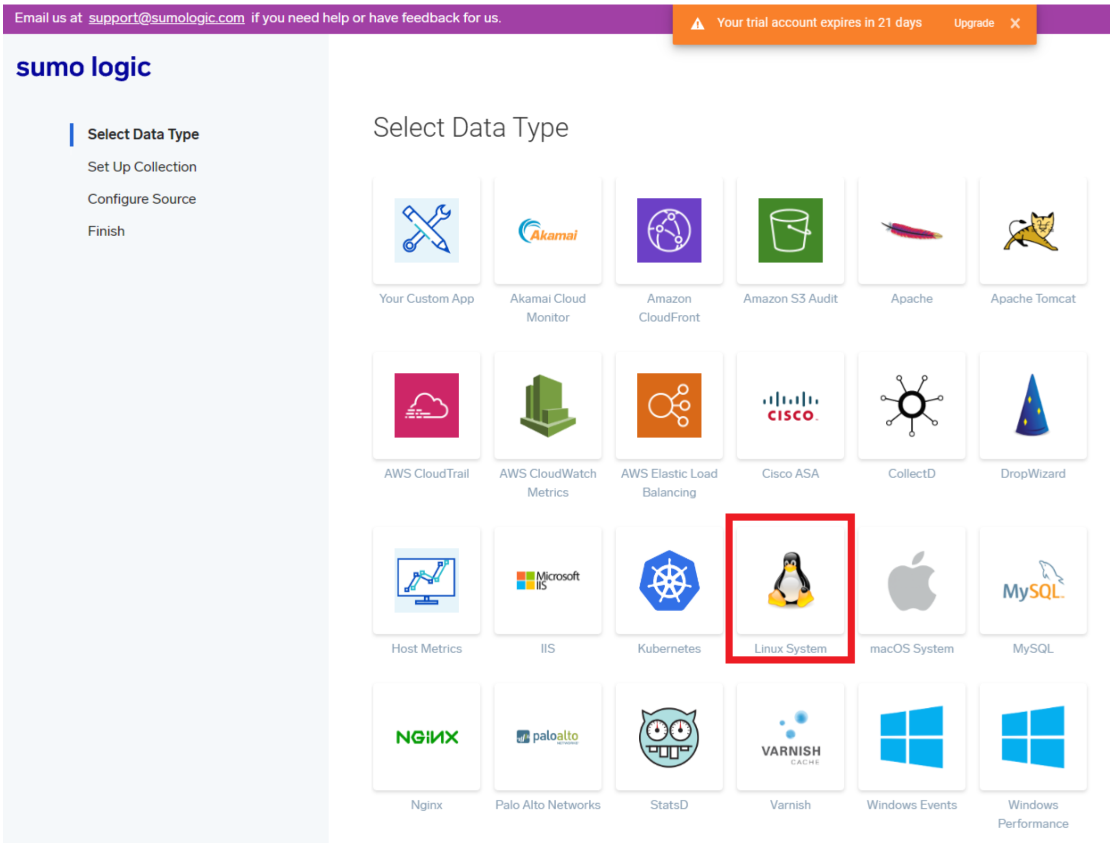
Learning about Sumo Logic

Learn how Sumo Logic delivers the first and only cloud-native, Continuous intelligence Platform^{TM}.

2. Next, you will need to install the Sumo Logic Collector on each system. The Linux Collector can be installed using a BASH script, while the Windows Collector can be installed using an MSI package.
   - Refer to the installation procedure in Page 14 (Linux) and Page 17 (Windows).
3. Once the Collector is installed, you will need to configure it to collect the specific logs you want to send to Sumo Logic. This can be done by editing the Collector's configuration file and specifying the paths to the log files you want to collect.
4. After the Collector is configured, you will need to start it and make sure it is running properly. On Linux, you can start the Collector using the command "service collector start" and on windows you can do this by running the collector as a service.
5. To verify if the collector is running and logs are being sent to Sumo Logic, you can check the Collector's log file and the Sumo Logic web interface.
6. Once data is flowing, you can start creating dashboards, alerts, and searches to monitor and analyze the log data.
7. It is also good to schedule regular monitoring and maintenance of the collectors to ensure they are running smoothly and troubleshoot any issues that may arise.

Here are the general steps to install the Sumo Logic Collector on Ubuntu Linux:

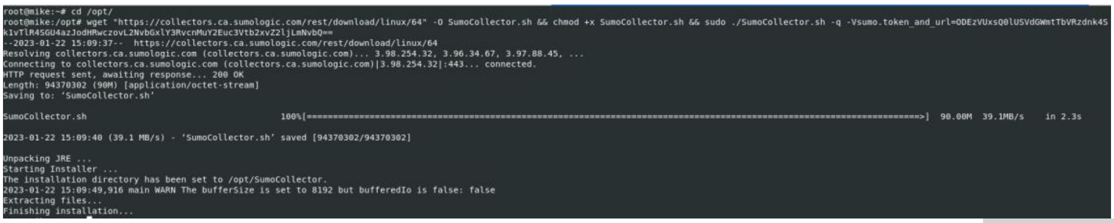
1. Select the **Linux System** collector from the Sumo Logic website.
   - ➢ https://service.ca.sumologic.com/ui/#/home



Email us at support@sumologic.com if you need help or have feedback for us.

Your trial account expires in 21 days

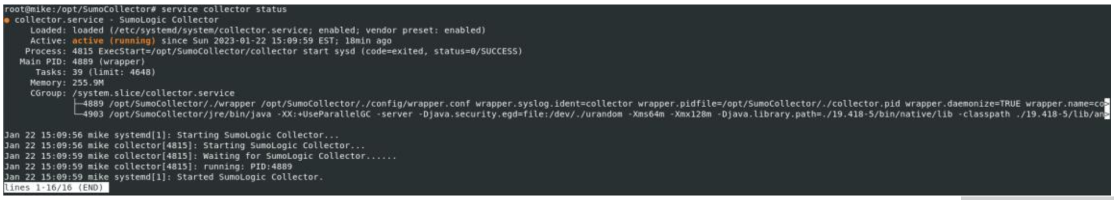
2. Dowload and install the package using the command:
   - ➢ *wget "https://collectors.ca.sumologic.com/rest/download/Linux/64" -O SumoCollector.sh && chmod +x SumoCollector.sh && sudo ./SumoCollector.sh -q -Vsumo.token_and_url=ODEzVUxsQ0lUSVdGWmtTbVRzdnk4Sk1vTlR4SGU4azJodHRwczovL2NvbGxlY3RvcnMuY2Euc3Vtb2xvZ2ljLmNvbQ==*



```
root@mike:~# cd /opt/
root@mike:/opt# wget "https://collectors.ca.sumologic.com/rest/download/linux/64" -O SumoCollector.sh && chmod +x SumoCollector.sh && sudo ./SumoCollector.sh -q -Vsumo.token_and_url=ODEzVUxsQ0lUSVdGWmtTbVRzdnk4S
k1vTlR4SGU4azJodHRwczovL2NvbGxlY3RvcnMuY2Euc3Vtb2xvZ2ljLmNvbQ==
--2023-01-22 15:09:37--  https://collectors.ca.sumologic.com/rest/download/linux/64
Resolving collectors.ca.sumologic.com (collectors.ca.sumologic.com)... 3.98.254.32, 3.96.34.67, 3.97.88.45, ...
Connecting to collectors.ca.sumologic.com (collectors.ca.sumologic.com)|3.98.254.32|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 94370302 (90M) [application/octet-stream]
Saving to: 'SumoCollector.sh'

SumoCollector.sh                        100%[================================================================================================================>]  90.00M  39.1MB/s    in 2.3s

2023-01-22 15:09:40 (39.1 MB/s) - 'SumoCollector.sh' saved [94370302/94370302]

Unpacking JRE ...
Starting Installer ...
The installation directory has been set to /opt/SumoCollector.
2023-01-22 15:09:49,916 main WARN The bufferSize is set to 8192 but bufferedIo is false: false
Extracting files...
Finishing installation...
```

Sample installation

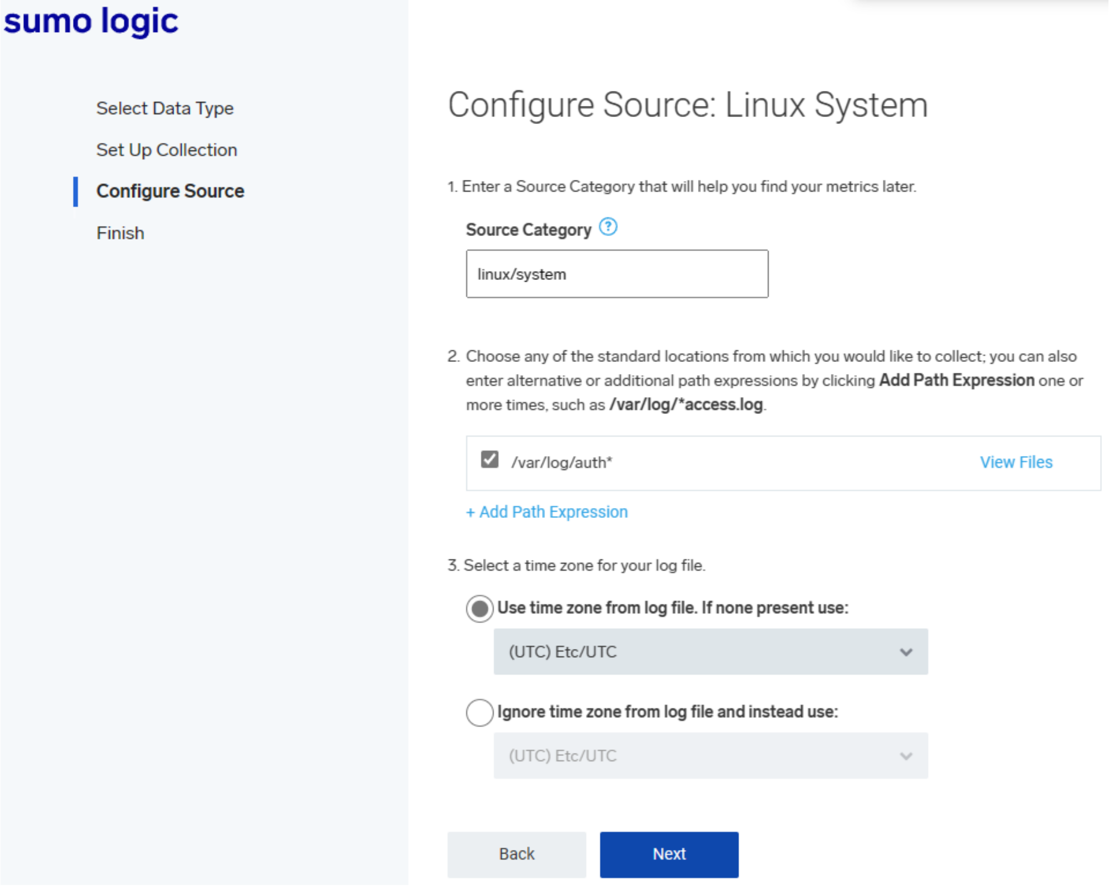
3. Verify and confirm that the "connector" has successfully installed by checking the service has started automatically with this Linux command.
   - ➢ sudo service connector status



```
root@mike:/opt/SumoCollector# service collector status
● collector.service - SumoLogic Collector
     Loaded: loaded (/etc/systemd/system/collector.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2023-01-22 15:09:59 EST; 18min ago
    Process: 4815 ExecStart=/opt/SumoCollector/collector start sysd (code=exited, status=0/SUCCESS)
   Main PID: 4889 (wrapper)
      Tasks: 39 (limit: 4648)
     Memory: 255.9M
     CGroup: /system.slice/collector.service
             ├─4889 /opt/SumoCollector/./wrapper /opt/SumoCollector/./config/wrapper.conf wrapper.syslog.ident=collector wrapper.pidfile=/opt/SumoCollector/./collector.pid wrapper.daemonize=TRUE wrapper.name=co>
             └─4903 /opt/SumoCollector/jre/bin/java -XX:+UseParallelGC -server -Djava.security.egd=file:/dev/./urandom -Xms64m -Xmx128m -Djava.library.path=./19.418-5/bin/native/lib -classpath ./19.418-5/lib/an>

Jan 22 15:09:56 mike systemd[1]: Starting SumoLogic Collector...
Jan 22 15:09:56 mike collector[4815]: Starting SumoLogic Collector...
Jan 22 15:09:59 mike collector[4815]: Waiting for SumoLogic Collector......
Jan 22 15:09:59 mike collector[4815]: running: PID:4889
Jan 22 15:09:59 mike systemd[1]: Started SumoLogic Collector.
lines 1-16/16 (END)
```

Sample status check

4. Click NEXT and configure the SOURCE in the Linux System collector.
   - ➢ Leave the default source category to "Linux/system" or create own tag.
   - ➢ Make sure all the critical logs are configured. The default for this sample is */var/log/auth** but additional path expression for the log collection from */var/log/*.log* Linux file is one of the good sources for security events to ingest in the SIEM.
   - ➢ And make sure of the time-zone is in UTC.



Configure Source: Linux System

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

Source Category: linux/system

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**.

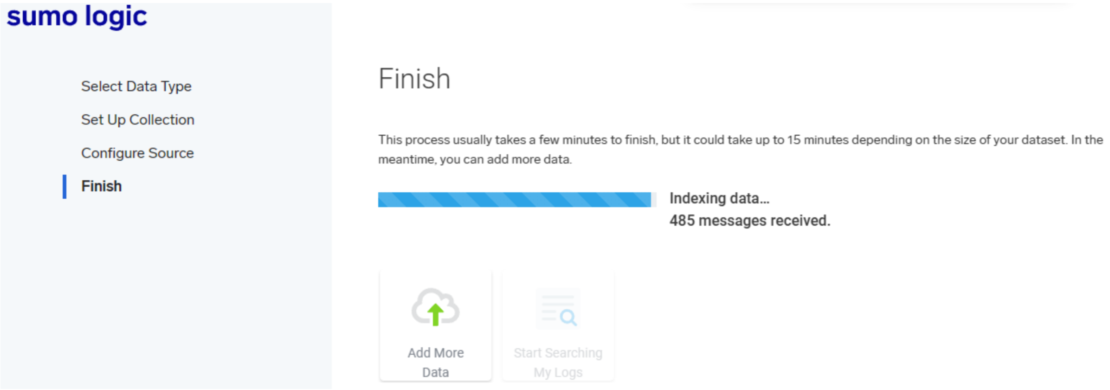
☑ /var/log/auth*

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

➢ Click NEXT to finish the Linux collector installation and configuration.

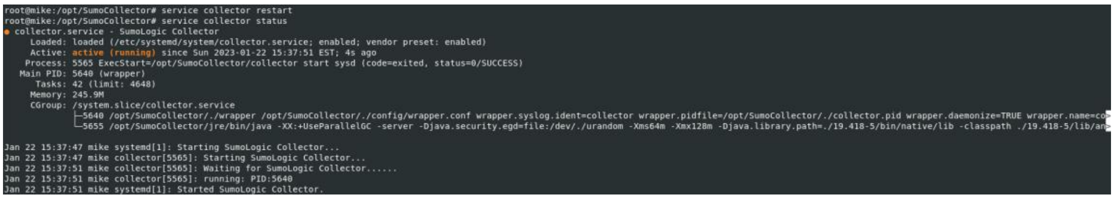


Finish

This process usually takes a few minutes to finish, but it could take up to 15 minutes depending on the size of your dataset. In the meantime, you can add more data.

Indexing data...
485 messages received.

5. Re-start the collector and check the status by running the commands below since it has started automatically on previous steps to reset the connection of the client to the Sumo Logic host in SaaS:
    - sudo service collector start
    - sudo service collector status



```
root@mike:/opt/SumoCollector# service collector restart
root@mike:/opt/SumoCollector# service collector status
● collector.service - SumoLogic Collector
     Loaded: loaded (/etc/systemd/system/collector.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2023-01-22 15:37:51 EST; 4s ago
    Process: 5565 ExecStart=/opt/SumoCollector/collector start sysd (code=exited, status=0/SUCCESS)
   Main PID: 5640 (wrapper)
      Tasks: 42 (limit: 4648)
     Memory: 245.9M
     CGroup: /system.slice/collector.service
             ├─5640 /opt/SumoCollector/./wrapper /opt/SumoCollector/./config/wrapper.conf wrapper.syslog.ident=collector wrapper.pidfile=/opt/SumoCollector/./collector.pid wrapper.daemonize=TRUE wrapper.name=co>
             └─5655 /opt/SumoCollector/jre/bin/java -XX:+UseParallelGC -server -Djava.security.egd=file:/dev/./urandom -Xms64m -Xmx128m -Djava.library.path=./19.418-5/bin/native/lib -classpath ./19.418-5/lib/an>

Jan 22 15:37:47 mike systemd[1]: Starting SumoLogic Collector...
Jan 22 15:37:47 mike collector[5565]: Starting SumoLogic Collector...
Jan 22 15:37:51 mike collector[5565]: Waiting for SumoLogic Collector......
Jan 22 15:37:51 mike collector[5565]: running: PID:5640
Jan 22 15:37:51 mike systemd[1]: Started SumoLogic Collector.
```

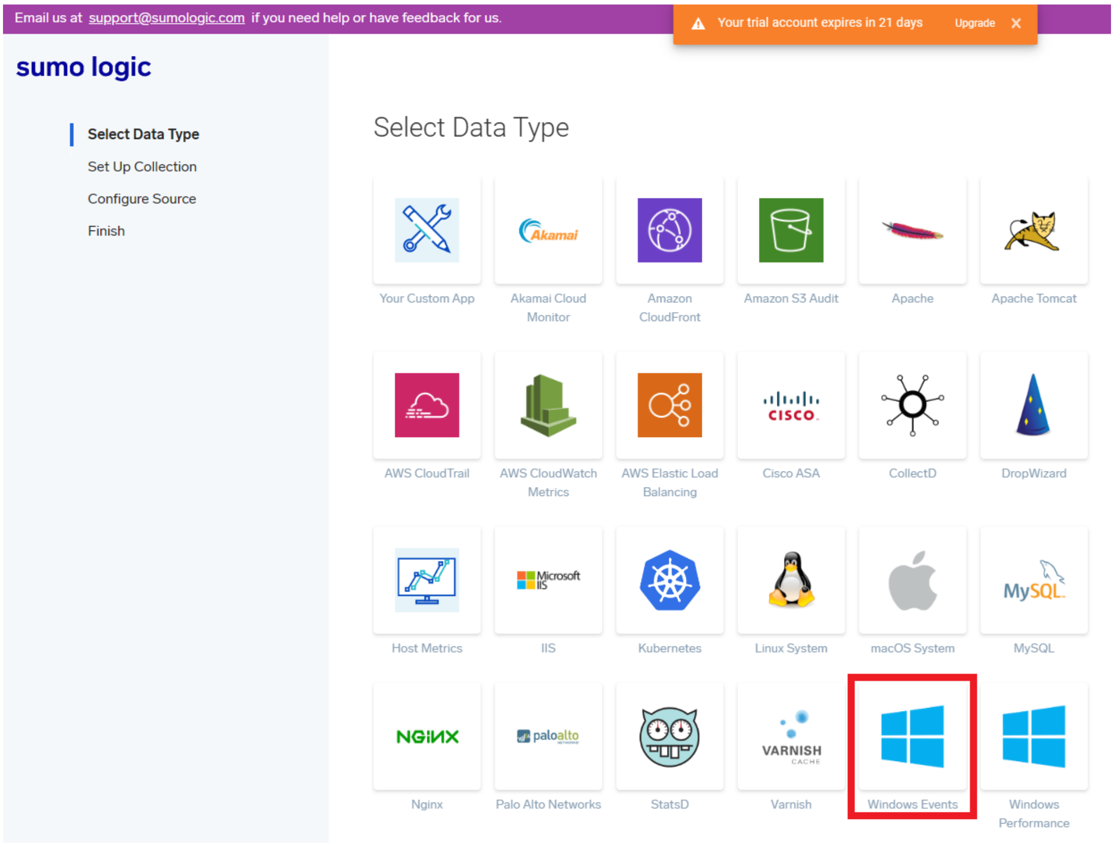
6. Once the collector is running, you can check the Sumo Logic web interface to verify if the data is being received from the collector.

Please note that these are general steps, the specific configuration and setup may vary depending on the organization environment and specific use case. Some may have a prerequisite needed such as having the correct version of Java installed before installing the collector.

It's also a good practice to keep the collector and the Sumo Logic service updated to the latest version as it will have bug fixes, performance improvements and new features.

Here are the general steps to install the Sumo Logic Collector on Windows 10:

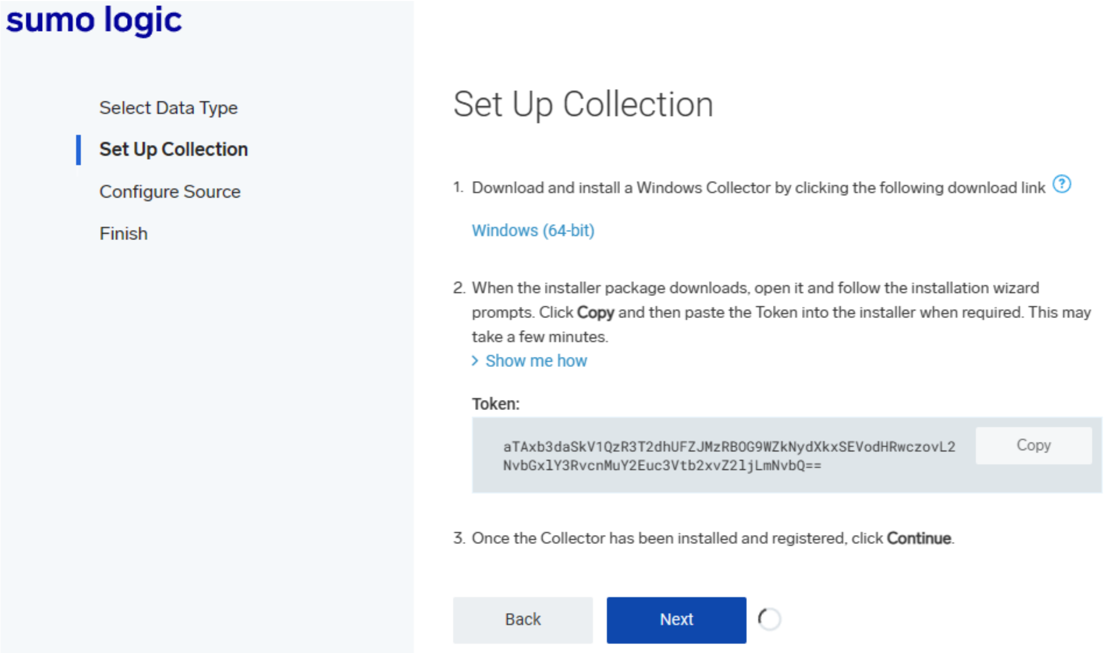
1. Download the Windows package of the collector from the Sumo Logic website.



Email us at support@sumologic.com if you need help or have feedback for us.

Your trial account expires in 21 days

2. Download the Windows 64bit collector and follow the set-up steps indicated from the next page for Windows Event logs.



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.

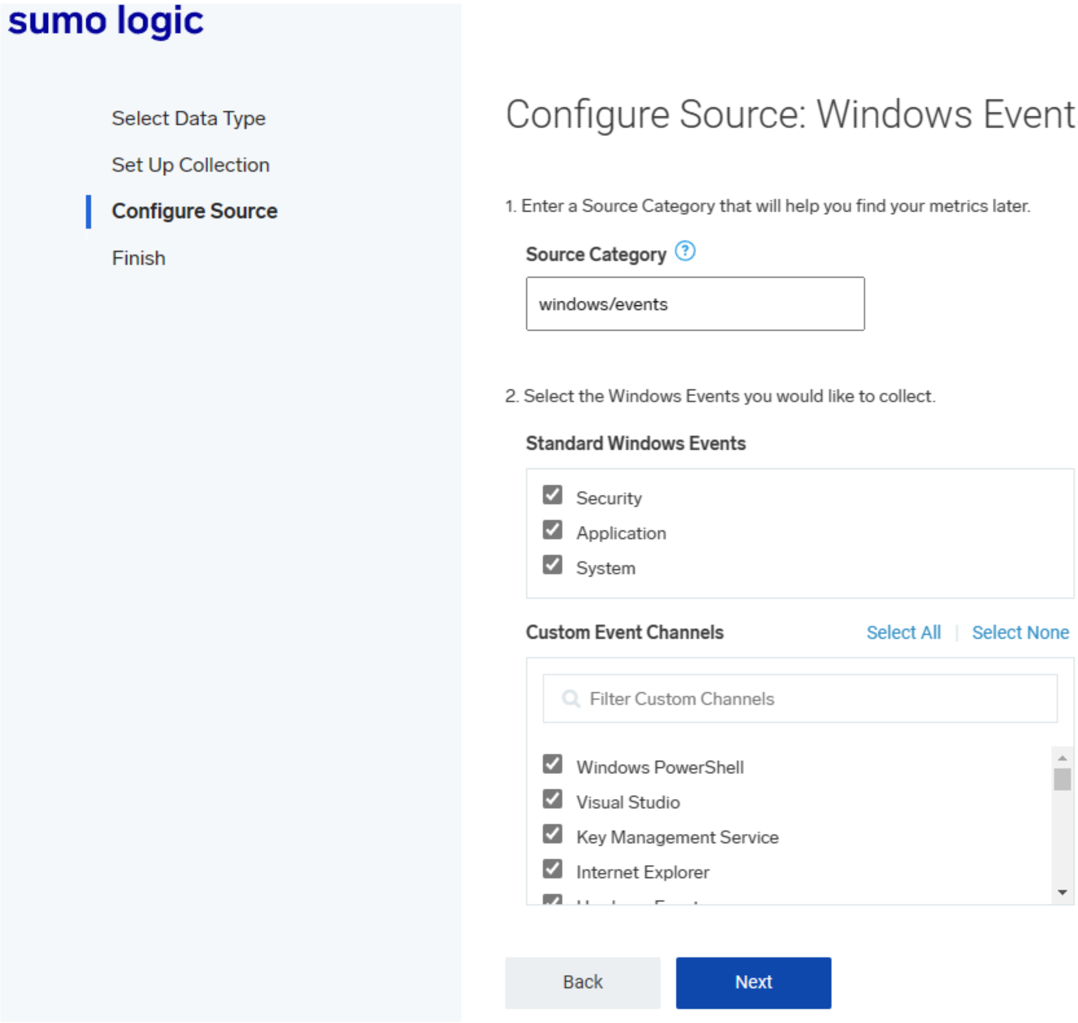
› Show me how

Token:

```
aTAxb3daSkV1QzR3T2dhUFZJMzRBOG9WZkNydXkxSEVodHRwczovL2
NvbGxlY3RvcnMuY2Euc3Vtb2xvZ2ljLmNvbQ==
```

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

3. Once the installation is complete, open the Sumo Logic Collector Manager and configure the collector. This can be done by specifying the logs you want to collect, setting up the connection to the Sumo Logic service, and configuring advanced settings if necessary.



sumo logic

- Select Data Type
- Set Up Collection
- **Configure Source**
- Finish

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.

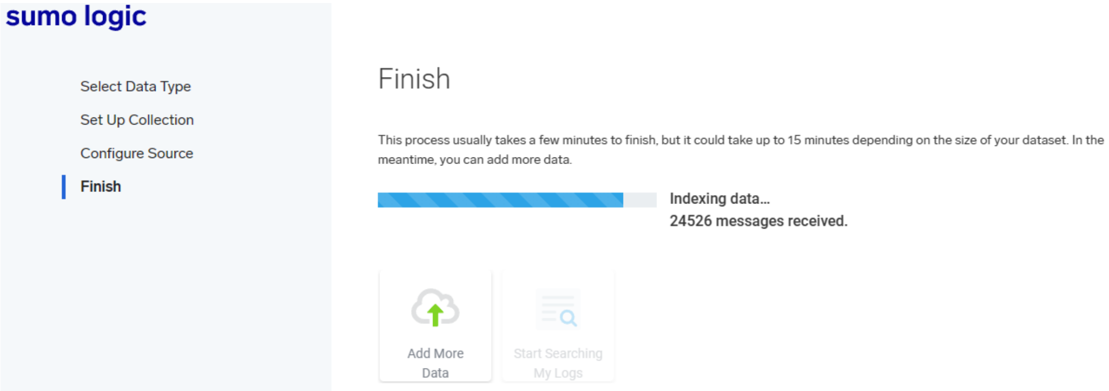
Standard Windows Events

☑ Security
☑ Application
☑ System

Custom Event Channels Select All | Select None

Filter Custom Channels

☑ Windows PowerShell
☑ Visual Studio
☑ Key Management Service
☑ Internet Explorer



sumo logic

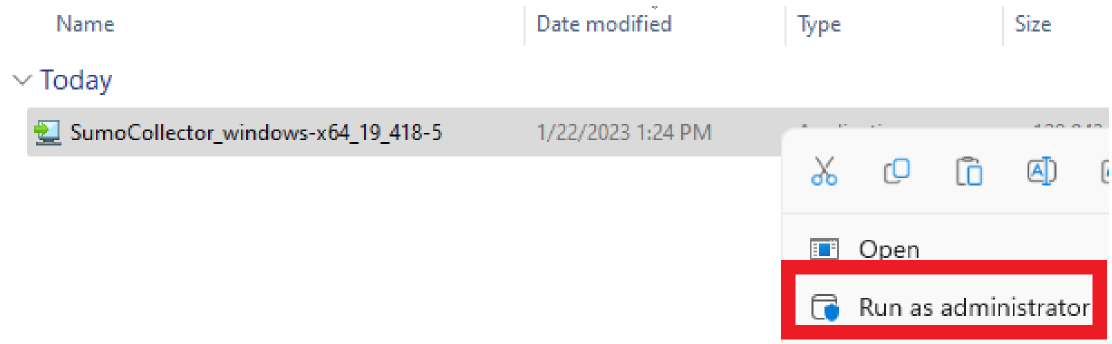
- Select Data Type
- Set Up Collection
- Configure Source
- **Finish**

Finish

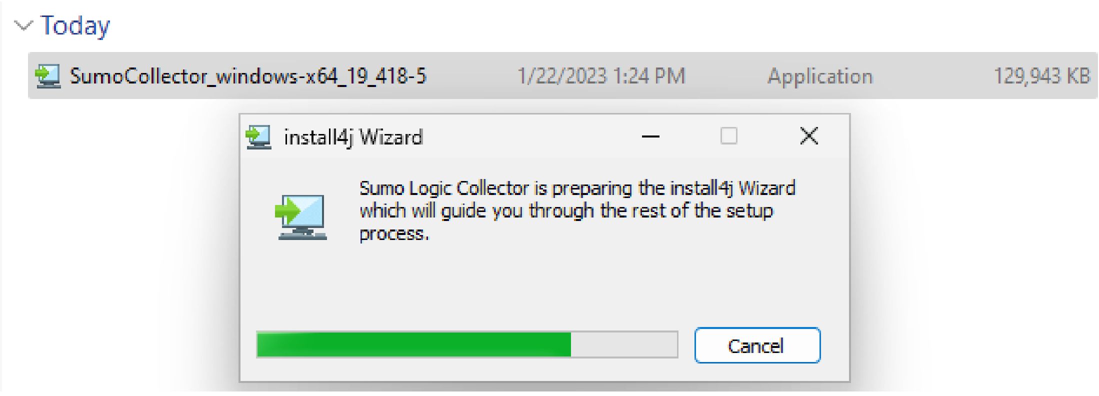
This process usually takes a few minutes to finish, but it could take up to 15 minutes depending on the size of your dataset. In the meantime, you can add more data.

Indexing data...
24526 messages received.

4. Follow the prompts to install the collector, including accepting the license agreement, specifying the installation location, and providing the token.



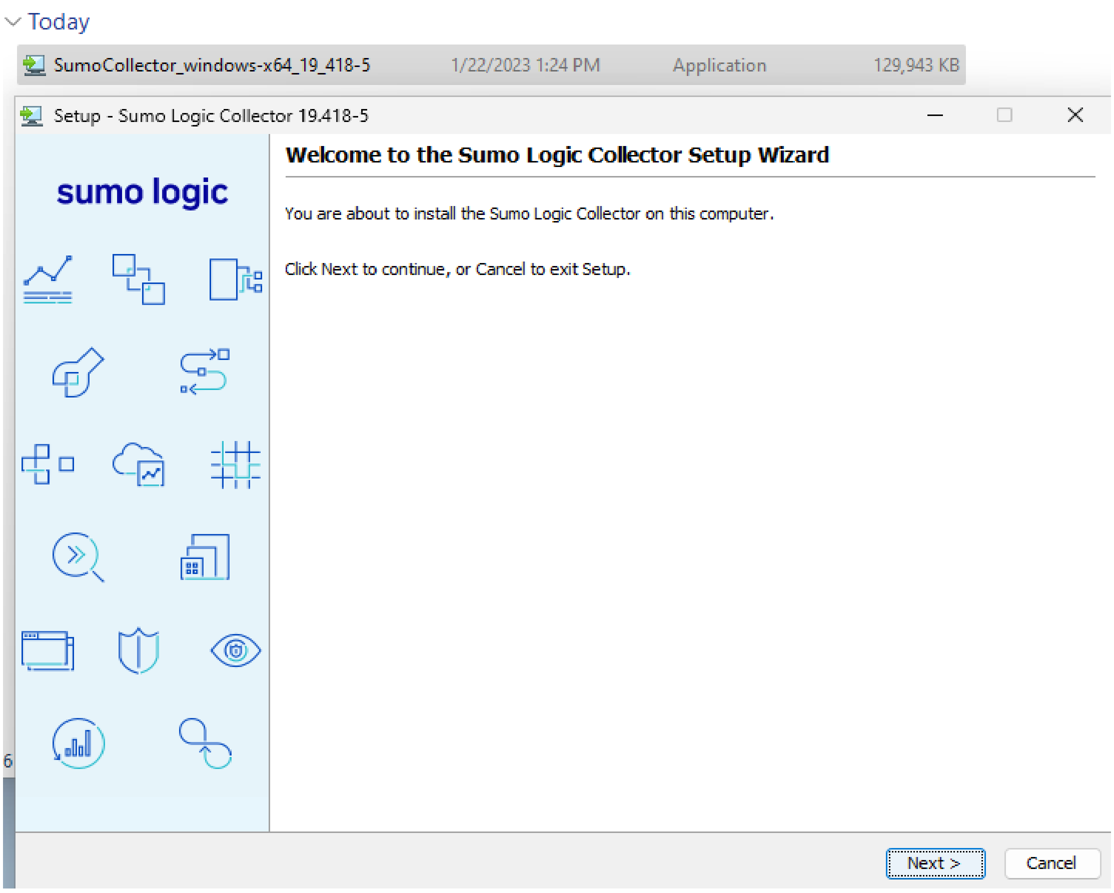
Name	Date modified	Type	Size
Today			
SumoCollector_windows-x64_19_418-5	1/22/2023 1:24 PM		



Today			
SumoCollector_windows-x64_19_418-5	1/22/2023 1:24 PM	Application	129,943 KB

install4j Wizard

Sumo Logic Collector is preparing the install4j Wizard which will guide you through the rest of the setup process.



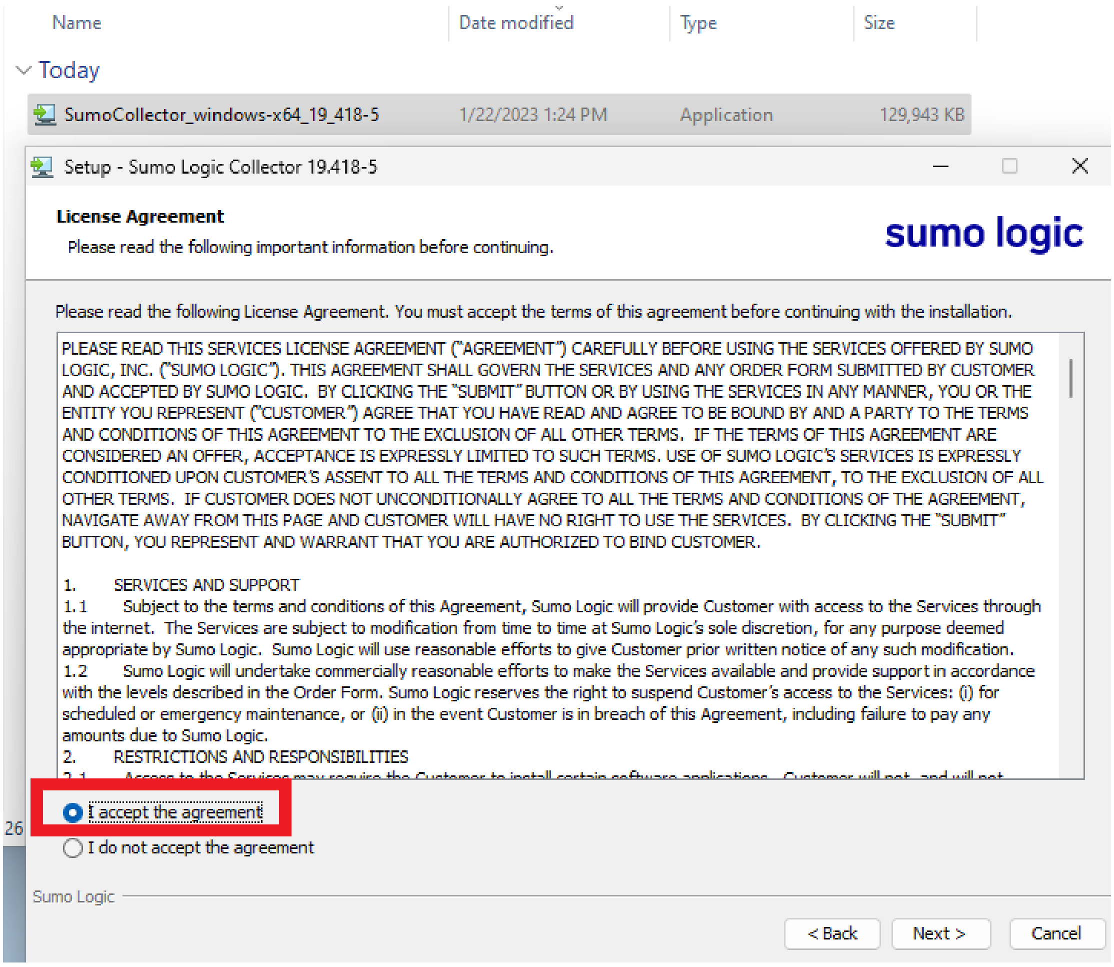
Today			
SumoCollector_windows-x64_19_418-5	1/22/2023 1:24 PM	Application	129,943 KB

Setup - Sumo Logic Collector 19.418-5

Welcome to the Sumo Logic Collector Setup Wizard

You are about to install the Sumo Logic Collector on this computer.

Click Next to continue, or Cancel to exit Setup.



Name	Date modified	Type	Size
Today			
SumoCollector_windows-x64_19_418-5	1/22/2023 1:24 PM	Application	129,943 KB

Setup - Sumo Logic Collector 19.418-5

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

PLEASE READ THIS SERVICES LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THE SERVICES OFFERED BY SUMO LOGIC, INC. ("SUMO LOGIC"). THIS AGREEMENT SHALL GOVERN THE SERVICES AND ANY ORDER FORM SUBMITTED BY CUSTOMER AND ACCEPTED BY SUMO LOGIC. BY CLICKING THE "SUBMIT" BUTTON OR BY USING THE SERVICES IN ANY MANNER, YOU OR THE ENTITY YOU REPRESENT ("CUSTOMER") AGREE THAT YOU HAVE READ AND AGREE TO BE BOUND BY AND A PARTY TO THE TERMS AND CONDITIONS OF THIS AGREEMENT TO THE EXCLUSION OF ALL OTHER TERMS. IF THE TERMS OF THIS AGREEMENT ARE CONSIDERED AN OFFER, ACCEPTANCE IS EXPRESSLY LIMITED TO SUCH TERMS. USE OF SUMO LOGIC'S SERVICES IS EXPRESSLY CONDITIONED UPON CUSTOMER'S ASSENT TO ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT, TO THE EXCLUSION OF ALL OTHER TERMS. IF CUSTOMER DOES NOT UNCONDITIONALLY AGREE TO ALL THE TERMS AND CONDITIONS OF THE AGREEMENT, NAVIGATE AWAY FROM THIS PAGE AND CUSTOMER WILL HAVE NO RIGHT TO USE THE SERVICES. BY CLICKING THE "SUBMIT" BUTTON, YOU REPRESENT AND WARRANT THAT YOU ARE AUTHORIZED TO BIND CUSTOMER.

1. SERVICES AND SUPPORT

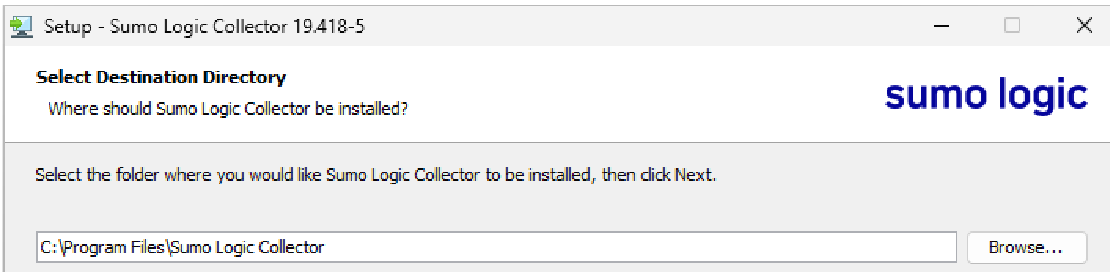
1.1 Subject to the terms and conditions of this Agreement, Sumo Logic will provide Customer with access to the Services through the internet. The Services are subject to modification from time to time at Sumo Logic's sole discretion, for any purpose deemed appropriate by Sumo Logic. Sumo Logic will use reasonable efforts to give Customer prior written notice of any such modification.

1.2 Sumo Logic will undertake commercially reasonable efforts to make the Services available and provide support in accordance with the levels described in the Order Form. Sumo Logic reserves the right to suspend Customer's access to the Services: (i) for scheduled or emergency maintenance, or (ii) in the event Customer is in breach of this Agreement, including failure to pay any amounts due to Sumo Logic.

2. RESTRICTIONS AND RESPONSIBILITIES

● I accept the agreement

○ I do not accept the agreement



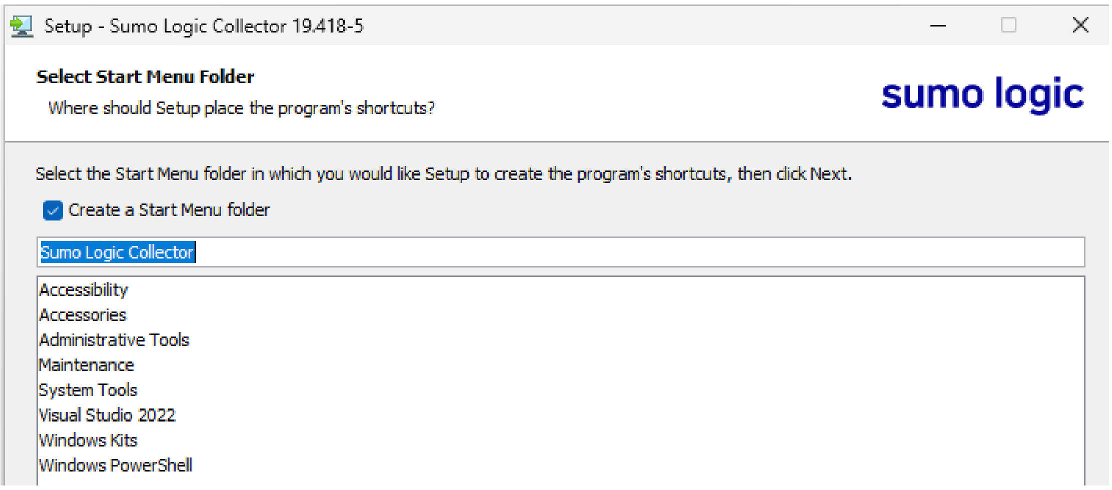
Setup - Sumo Logic Collector 19.418-5

Select Destination Directory

Where should Sumo Logic Collector be installed?

Select the folder where you would like Sumo Logic Collector to be installed, then click Next.

C:\Program Files\Sumo Logic Collector



Setup - Sumo Logic Collector 19.418-5

Select Start Menu Folder

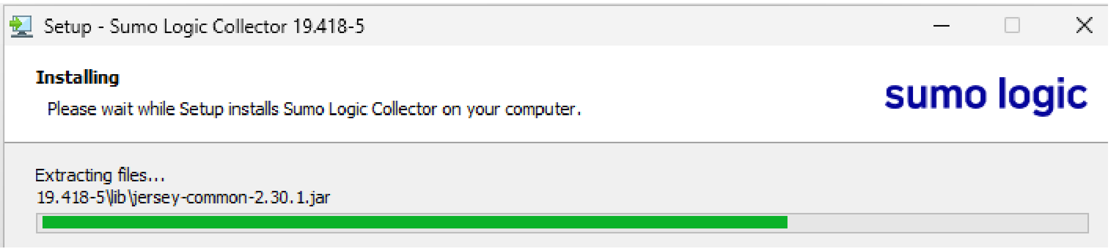
Where should Setup place the program's shortcuts?

Select the Start Menu folder in which you would like Setup to create the program's shortcuts, then click Next.

☑ Create a Start Menu folder

Sumo Logic Collector

Accessibility
Accessories
Administrative Tools
Maintenance
System Tools
Visual Studio 2022
Windows Kits
Windows PowerShell

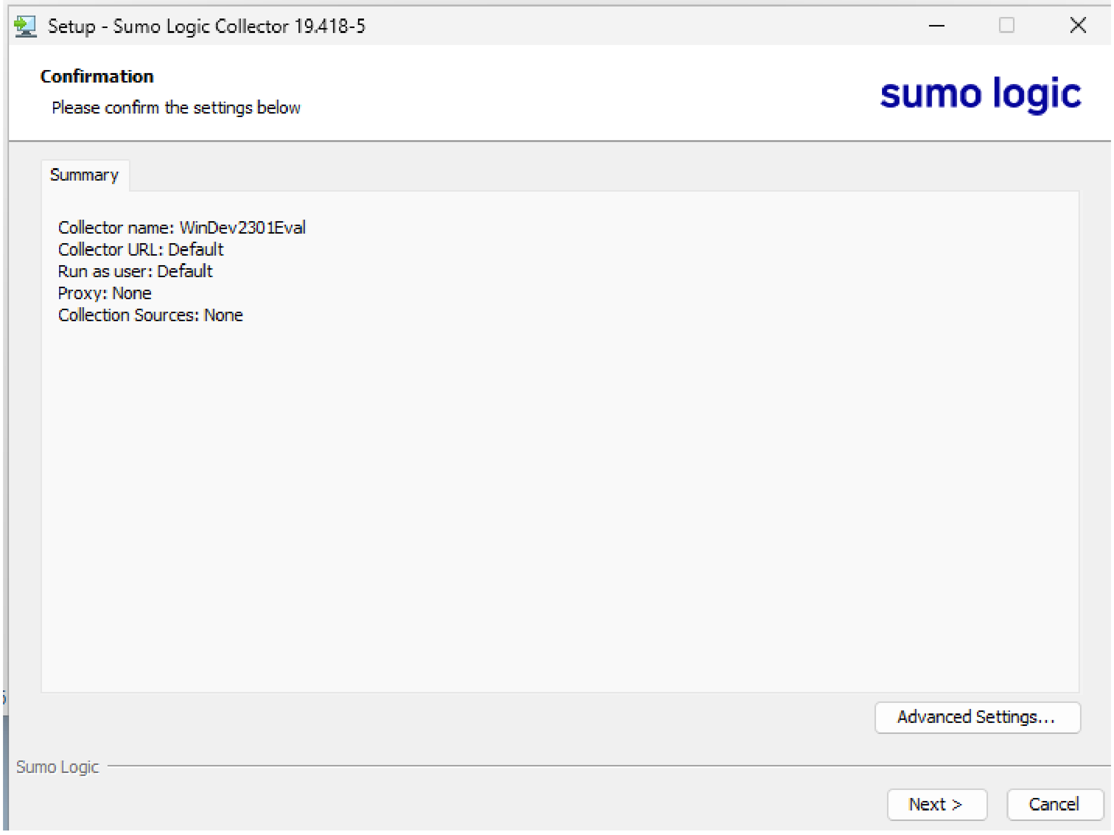


Setup - Sumo Logic Collector 19.418-5

Installing

Please wait while Setup installs Sumo Logic Collector on your computer.

Extracting files...
19.418-5\lib\jersey-common-2.30.1.jar



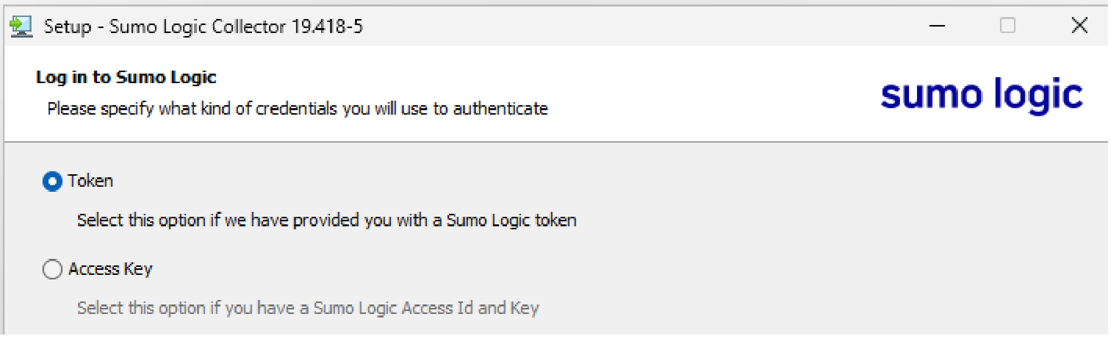
Setup - Sumo Logic Collector 19.418-5

Confirmation

Please confirm the settings below

Summary

Collector name: WinDev2301Eval
Collector URL: Default
Run as user: Default
Proxy: None
Collection Sources: None



Setup - Sumo Logic Collector 19.418-5

Log in to Sumo Logic

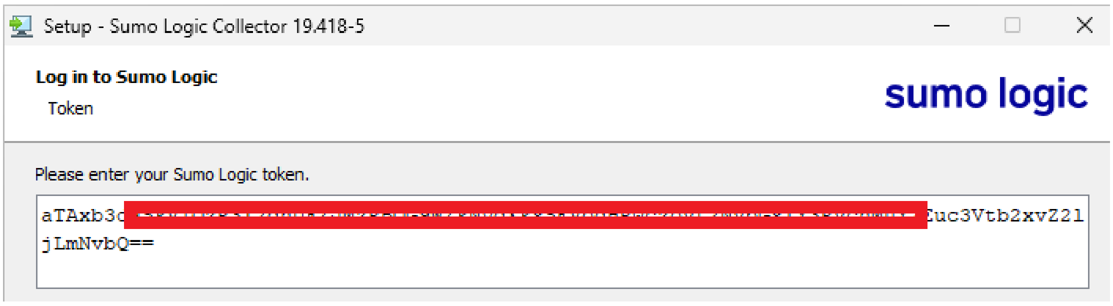
Please specify what kind of credentials you will use to authenticate

● Token

Select this option if we have provided you with a Sumo Logic token

○ Access Key

Select this option if you have a Sumo Logic Access Id and Key



Setup - Sumo Logic Collector 19.418-5

Log in to Sumo Logic

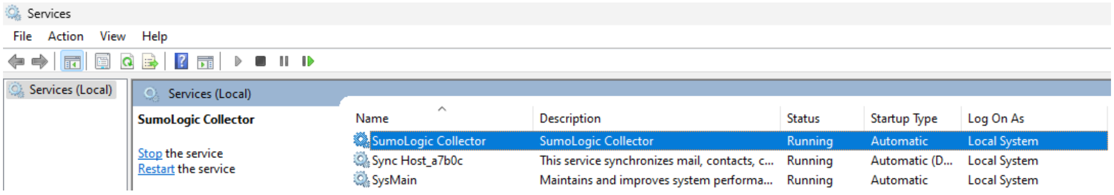
Token

Please enter your Sumo Logic token.

```
aTAxb3c[redacted]uc3Vtb2xvZ21
jLmNvbQ==
```

- Then click FINISH.

➢ Confirm is the service is running after the installation.



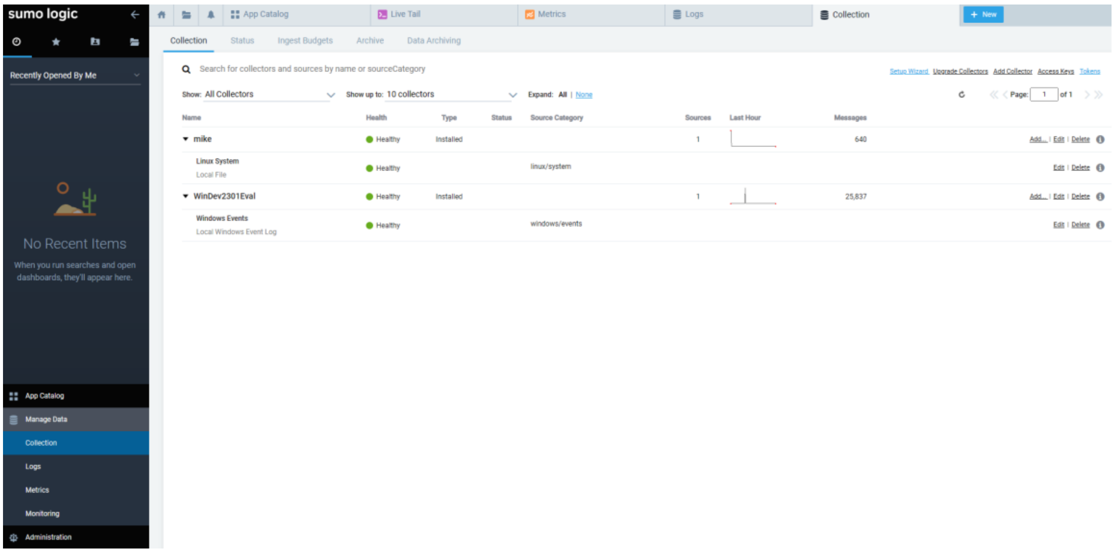
SumoLogic Collector

Stop the service
Restart the service

Name	Description	Status	Startup Type	Log On As
SumoLogic Collector	SumoLogic Collector	Running	Automatic	Local System
Sync Host_a7b0c	This service synchronizes mail, contacts, c...	Running	Automatic (D...	Local System
SysMain	Maintains and improves system performa...	Running	Automatic	Local System

5. Start the collector by clicking the "Start" button in the Collector Manager.
6. Verify the status of the collector by checking the Collector Manager for any errors or by checking the Sumo Logic web interface to see if data is being received from the collector.
7. Once the collector is running, you can check the Sumo Logic web interface to verify if the data is being received from the collector.

Successful installation and configuration of the agent host collectors will show data from the collector page from Sumo Logic Saas.



No Recent Items

When you run searches and open dashboards, they'll appear here.

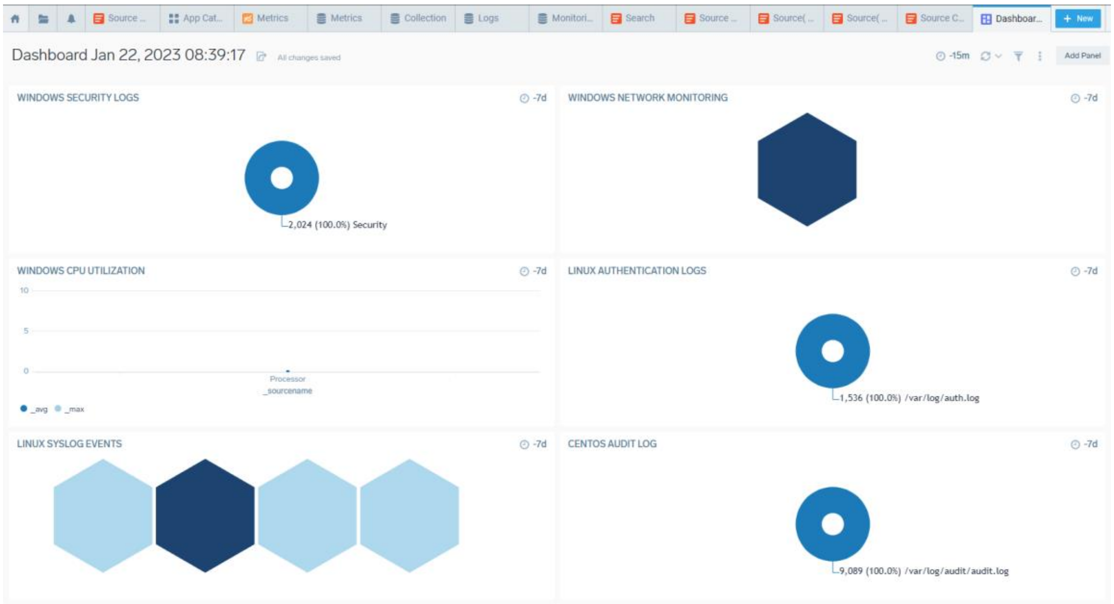
Search for collectors and sources by name or sourceCategory

Show: All Collectors Show up to: 10 collectors Expand: All | None Page: 1 of 1

Name	Health	Type	Status	Source Category	Sources	Last Hour	Messages	
mike	● Healthy	Installed			1		640	Add... | Edit | Delete
Linux System Local File	● Healthy			linux/system				Edit | Delete
WinDev2301Eval	● Healthy	Installed			1		25,837	Add... | Edit | Delete
Windows Events Local Windows Event Log	● Healthy			windows/events				Edit | Delete

Please note that these are general steps, the specific configuration and setup may vary depending on the organization environment and specific use cases. It's also a good practice to keep the collector and the Sumo Logic service updated to the latest version as it will have bug fixes, performance improvements and new features.

Sample Dashboard


Source ...
App Cat...
Metrics
Metrics
Collection
Logs
Monitori...
Search
Source ...
Source(...
Source(...
Source C...
Dashboar...
+ New
Dashboard Jan 22, 2023 08:39:17
All changes saved
-15m
Add Panel
WINDOWS SECURITY LOGS
-7d
2,024 (100.0%) Security
WINDOWS NETWORK MONITORING
-7d
WINDOWS CPU UTILIZATION
-7d
10
5
0
Processor
_sourcename
_avg
_max
LINUX AUTHENTICATION LOGS
-7d
1,536 (100.0%) /var/log/auth.log
LINUX SYSLOG EVENTS
-7d
CENTOS AUDIT LOG
-7d
9,089 (100.0%) /var/log/audit/audit.log