Cisco Catalyst SD-WAN: Microsoft Sentinel Installation, Configuration, and Usage Guide

Contents

Overview

Cisco Catalyst™ SD-WAN integration with Microsoft Sentinel brings together the capabilities of Cisco Catalyst SD-WAN and Microsoft Sentinel, a cloud-native solution offering Security Information and Event Management (SIEM) along with Security Orchestration, Automation, and Response (SOAR). Microsoft Sentinel empowers organizations with security analytics, attack detection, threat visibility, proactive hunting, and efficient threat response. With this integration, businesses can leverage the combined power of Cisco Catalyst SD-WAN and Microsoft Sentinel to enhance their security posture.

The integration between Cisco Catalyst SD-WAN and Microsoft Sentinel, which is supported starting from Cisco Catalyst SD-WAN release 17.10, enables security analytics and delivers valuable threat intelligence, enabling organizations to effectively detect and respond to security incidents. By leveraging the strengths of both solutions, this integration provides a comprehensive security solution for businesses seeking advanced threat management capabilities.

A) To begin visualizing Catalyst SD-WAN security insights, installation of a netflow collector and syslog collector is required. The following sections will outline the following:

B) **Setting up Netflow ingestion using 2 options**

    a. Option 1: Download and install a docker image

    b. Option 2: Installing Filebeat and Logstash manually

C) **Setting up an Arc Server for Syslog ingestion**

Steps to ingest NetFlow data into Microsoft Sentinel

Ingesting NetFlow data through the Docker image

To ingest NetFlow data into Sentinel through the Docker image, users simply need to download the Docker image from Docker Hub onto their VM and execute it using Docker commands. This process installs Filebeat and Logstash servers on their VM, which are responsible for receiving the NetFlow data and ingesting it into the Sentinel workspace.

Install Docker and Docker Compose

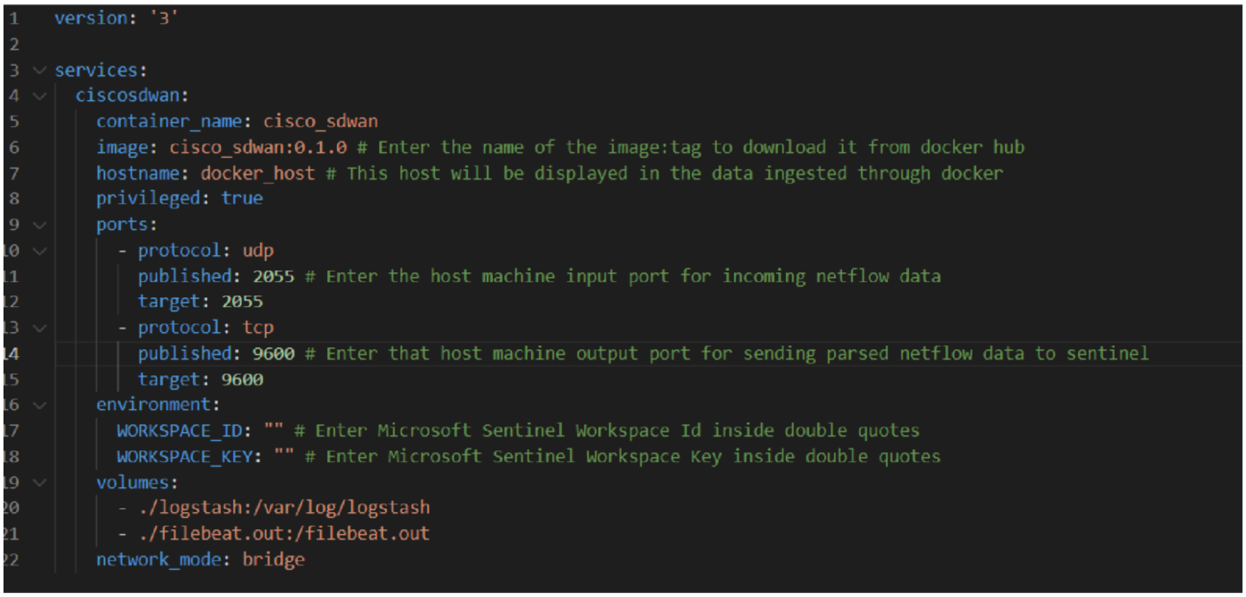
- Install Docker Engine on your preferred operating system. For Windows and Mac OS installations, you can choose between static binary installation or Docker Desktop.
    - **Link:** **https://docs.docker.com/engine/install/#server**

Run the Cisco Catalyst SD-WAN Docker image

- Open the Filebeat input port in the firewall if it is enabled. Filebeat will receive the NetFlow data sent by Cisco, parse the NetFlow fields, and send it to the Logstash server. The Logstash server will then ingest the data into the specified workspace of Sentinel.

  Example: **firewall-cmd --zone=public --permanent --add-port=2055/udp**
- Go to the **Cisco_SDWAN_Netflow_Docker** folder (shared in the Cisco_SDWAN_Netflow_Docker.zip file).

- Update the **docker-compose.yml** file and provide the following parameter values.
  - **Host machine input and output port**
  - **Microsoft Sentinel workspace ID**
  - **Microsoft Sentinel workspace key**



```yaml
version: '3'

services:
  ciscosdwan:
    container_name: cisco_sdwan
    image: cisco_sdwan:0.1.0 # Enter the name of the image:tag to download it from docker hub
    hostname: docker_host # This host will be displayed in the data ingested through docker
    privileged: true
    ports:
      - protocol: udp
        published: 2055 # Enter the host machine input port for incoming netflow data
        target: 2055
      - protocol: tcp
        published: 9600 # Enter that host machine output port for sending parsed netflow data to sentinel
        target: 9600
    environment:
      WORKSPACE_ID: "" # Enter Microsoft Sentinel Workspace Id inside double quotes
      WORKSPACE_KEY: "" # Enter Microsoft Sentinel Workspace Key inside double quotes
    volumes:
      - ./logstash:/var/log/logstash
      - ./filebeat.out:/filebeat.out
    network_mode: bridge
```

- Now open the terminal and go to the path where the **docker-compose.yml** file is located.
- To start Docker and run the application, execute the following command in the terminal:
  - **docker compose up -d**

  After 5 minutes, run the following command to verify the running state of the Docker container:
  - **docker ps**

Stop the Docker execution

- To stop the Docker execution, open the terminal and navigate to the directory where the docker-compose.yml file is located. Then run the following command.
  - **docker compose down**

Useful Docker commands

- **docker ps:** Get a list of all running Docker containers.
- **docker ps -a:** Get a list of all running and stopped Docker containers.
- **docker build -t <image_name> <location of Dockerfile>:** Build a Docker image.
- **docker system prune:** Remove all Docker cache.
- **docker exec -it <container_id> /bin/bash:** Execute commands inside the container.

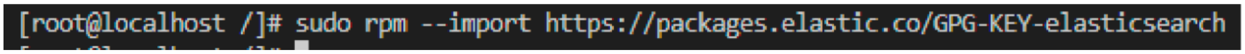
Ingesting NetFlow data through Filebeat and Logstash

To ingest NetFlow data into Sentinel using Filebeat and Logstash, you need to install and configure Filebeat and Logstash on the VM. Once properly configured, the VM will be able to receive NetFlow data on the specified port and ingest that data into the Sentinel workspace.

- To install Filebeat and Logstash using APT, refer to the following sections of the Filebeat Reference:
  - **The APT section of Repositories for APT and YUM:** **https://www.elastic.co/guide/en/beats/filebeat/current/setup-repositories.html**
  - **Installing Logstash: https://www.elastic.co/guide/en/logstash/current/installing-logstash.html**
- To install Filebeat and Logstash for Red Hat-based Linux (YUM), see the YUM section of Repositories for APT and YUM: https://www.elastic.co/guide/en/beats/filebeat/current/setup-repositories.html#_yum

1. **Install Filebeat and Logstash**

- Download and install the public signing key. Run the following command anywhere in the VM:
  - **sudo rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch**



```
[root@localhost /]# sudo rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch
```

- Add the following in your **/etc/yum.repos.d/** directory in a file with a .repo suffix, for example, logstash.repo:
  - **[elastic-8.x]**

    name=Elastic repository for 8.x packages

    baseurl=https://artifacts.elastic.co/packages/8.x/yum

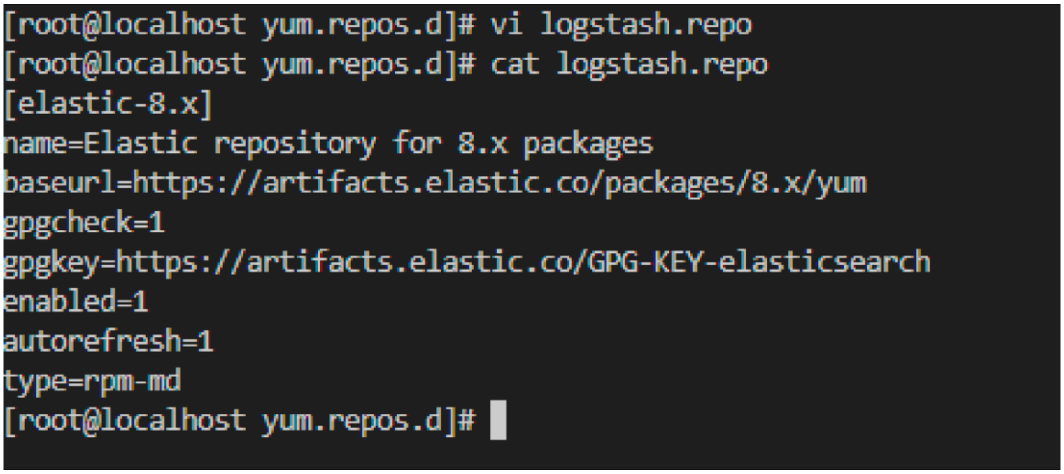
    gpgcheck=1

    gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

    enabled=1

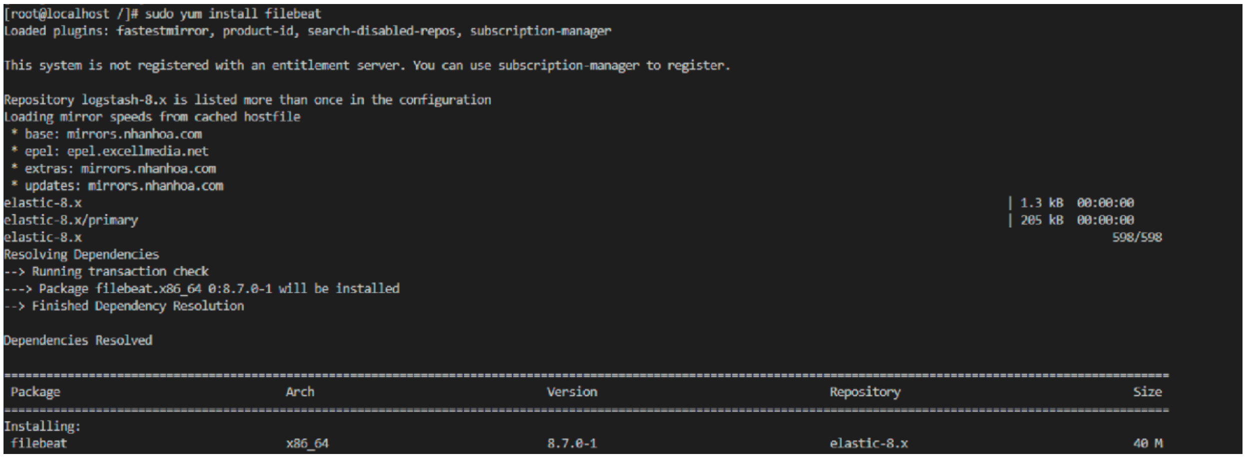
    autorefresh=1

    type=rpm-md



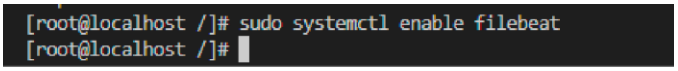
```
[root@localhost yum.repos.d]# vi logstash.repo
[root@localhost yum.repos.d]# cat logstash.repo
[elastic-8.x]
name=Elastic repository for 8.x packages
baseurl=https://artifacts.elastic.co/packages/8.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
[root@localhost yum.repos.d]# 
```

- Install and enable Filebeat:
  - **sudo yum install filebeat**



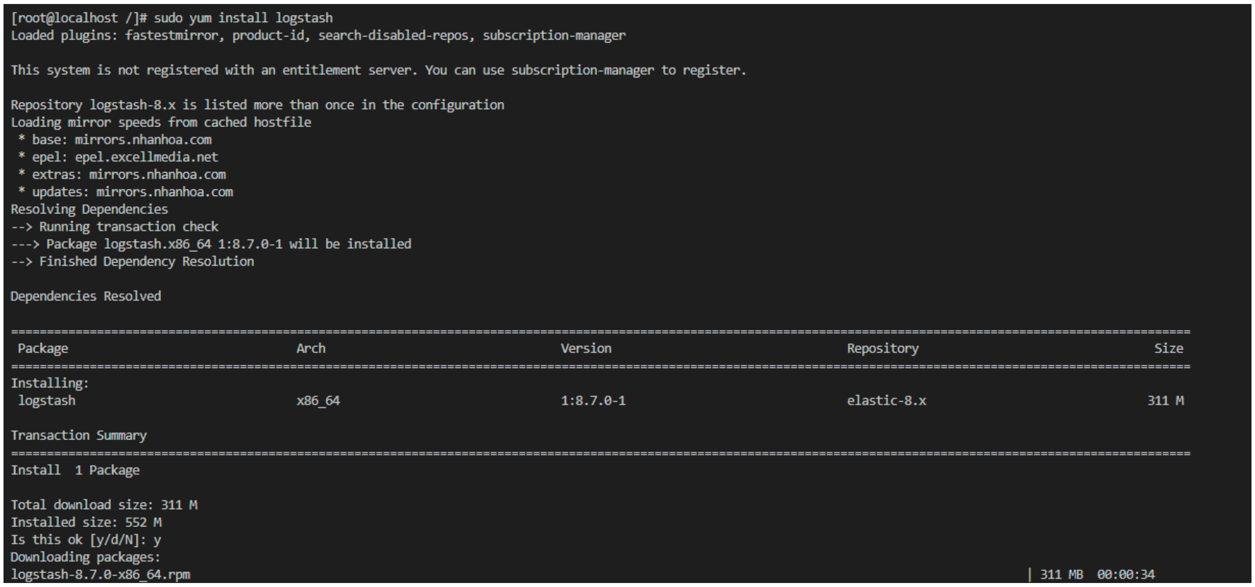
```
[root@localhost /]# sudo yum install filebeat
Loaded plugins: fastestmirror, product-id, search-disabled-repos, subscription-manager

This system is not registered with an entitlement server. You can use subscription-manager to register.

Repository logstash-8.x is listed more than once in the configuration
Loading mirror speeds from cached hostfile
 * base: mirrors.nhanhoa.com
 * epel: epel.excellmedia.net
 * extras: mirrors.nhanhoa.com
 * updates: mirrors.nhanhoa.com
elastic-8.x                                                                                    | 1.3 kB  00:00:00
elastic-8.x/primary                                                                            | 205 kB  00:00:00
elastic-8.x                                                                                                598/598
Resolving Dependencies
--> Running transaction check
---> Package filebeat.x86_64 0:8.7.0-1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

==================================================================================================================
 Package                     Arch                     Version                    Repository                  Size
==================================================================================================================
Installing:
 filebeat                    x86_64                   8.7.0-1                    elastic-8.x                 40 M
```

  - **sudo systemctl enable filebeat**



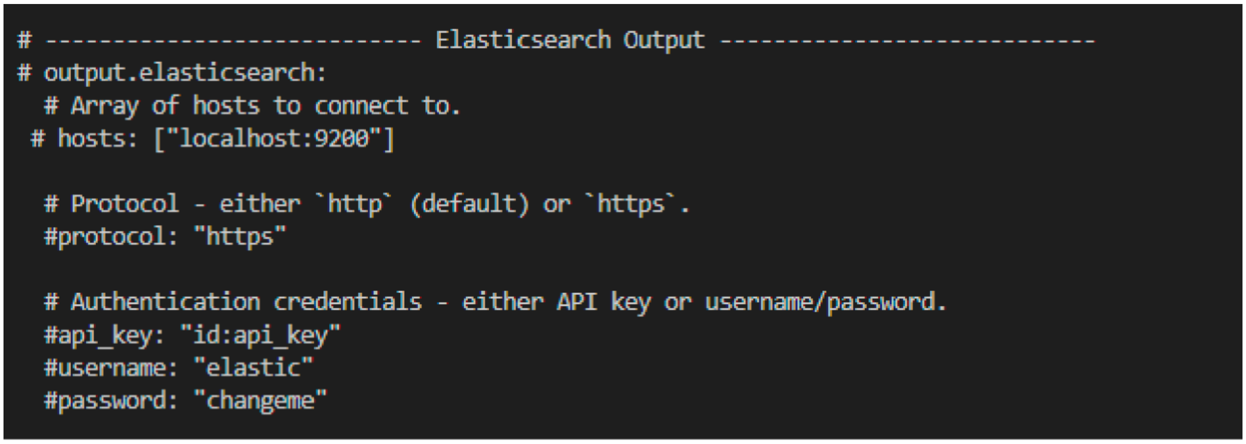
```
[root@localhost /]# sudo systemctl enable filebeat
[root@localhost /]#
```

- **Note:** If your system does not use systemd, run sudo chkconfig --add filebeat
- Install Logstash:
  - **sudo yum install logstash**



```
[root@localhost /]# sudo yum install logstash
Loaded plugins: fastestmirror, product-id, search-disabled-repos, subscription-manager

This system is not registered with an entitlement server. You can use subscription-manager to register.

Repository logstash-8.x is listed more than once in the configuration
Loading mirror speeds from cached hostfile
 * base: mirrors.nhanhoa.com
 * epel: epel.excellmedia.net
 * extras: mirrors.nhanhoa.com
 * updates: mirrors.nhanhoa.com
Resolving Dependencies
--> Running transaction check
---> Package logstash.x86_64 1:8.7.0-1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

==================================================================================================================
 Package                     Arch                     Version                    Repository                  Size
==================================================================================================================
Installing:
 logstash                    x86_64                   1:8.7.0-1                  elastic-8.x                311 M

Transaction Summary
==================================================================================================================
Install  1 Package

Total download size: 311 M
Installed size: 552 M
Is this ok [y/d/N]: y
Downloading packages:
logstash-8.7.0-x86_64.rpm                                                                  | 311 MB  00:00:34
```

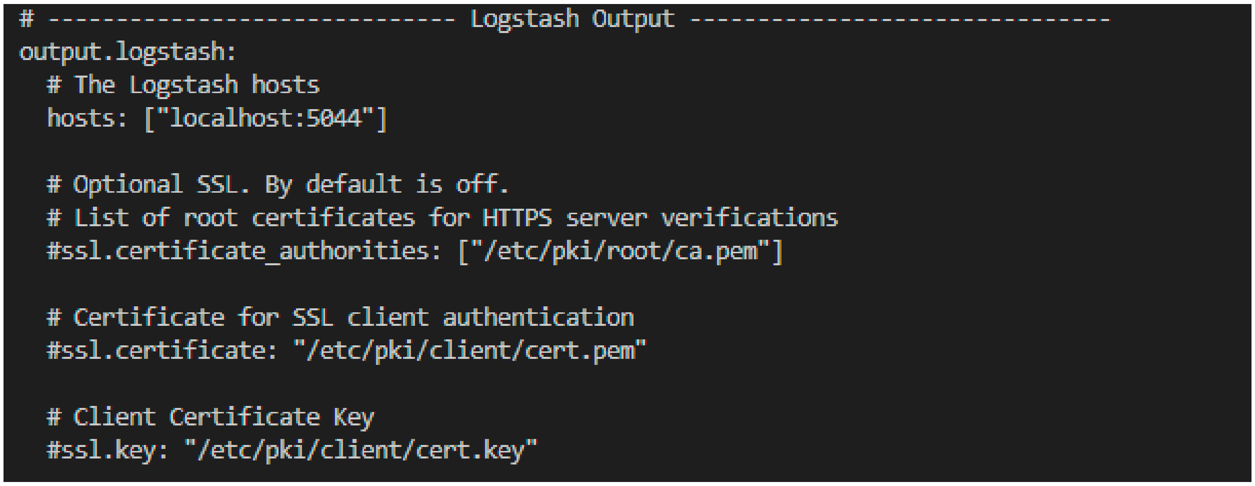
2. **Configure Filebeat to send events to Logstash**
   - Edit the filebeat.yml file:
     - **vi /etc/filebeat/filebeat.yml**
   - Comment out the Elasticsearch Output section.



```
# ---------------------------- Elasticsearch Output ----------------------------
# output.elasticsearch:
  # Array of hosts to connect to.
 # hosts: ["localhost:9200"]

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  #username: "elastic"
  #password: "changeme"
```

- Uncomment the Logstash Output section (uncomment only these two lines):
  - **output.logstash**

    hosts: [“localhost:5044”]



```
# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["localhost:5044"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"
```

- In the Logstash Output section, if you want to send data to a port other than the default port, that is, **port 5044**, replace the port number in the **hosts** field. (**Note:** When configuring Logstash, make sure to add this port to the configuration file.)

- In the Filebeat inputs section, comment out the existing configuration and add the following configuration:
  - **- type: netflow**

    max_message_size: 10KiB

    host: "0.0.0.0:2055"

    protocols: [v5, v9, ipfix]

    expiration_timeout: 30m

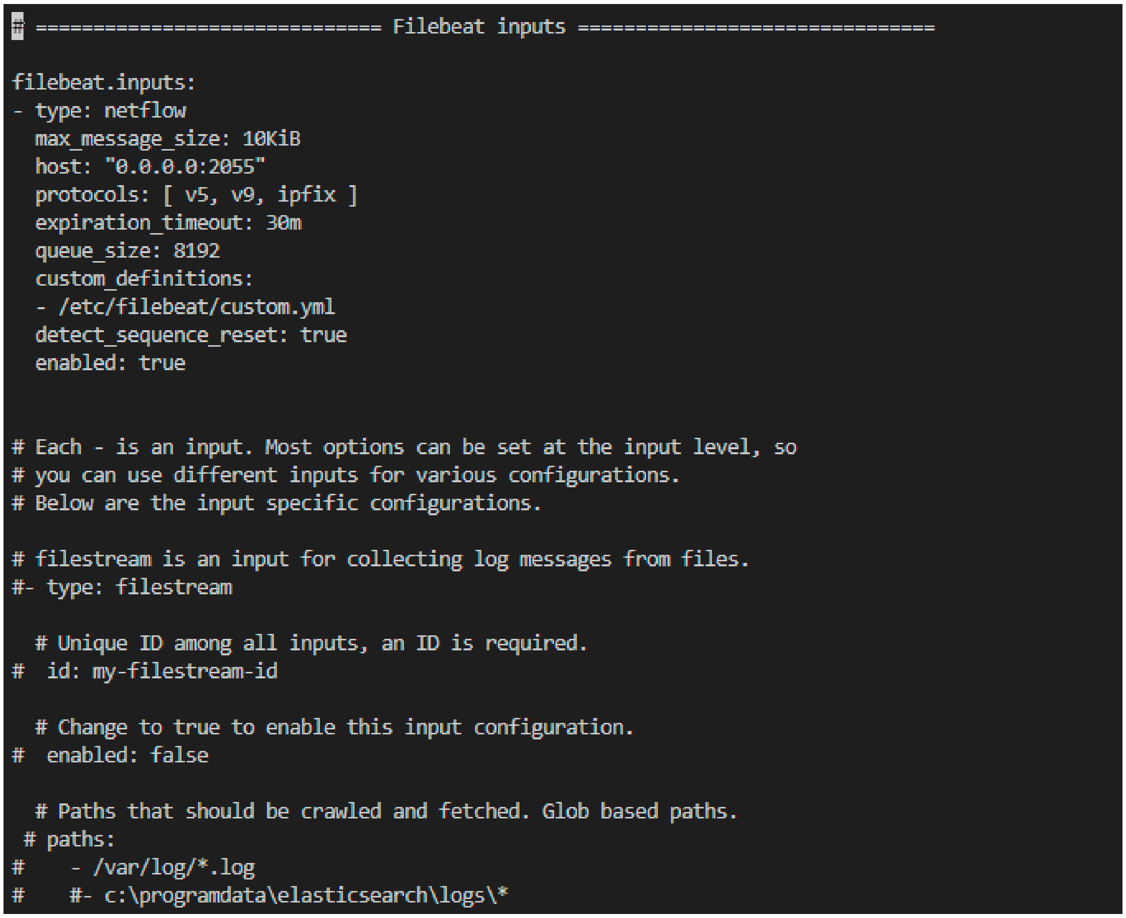
    queue_size: 8192

    custom_definitions:

    - /etc/filebeat/custom.yml

    detect_sequence_reset: true

    enabled: true



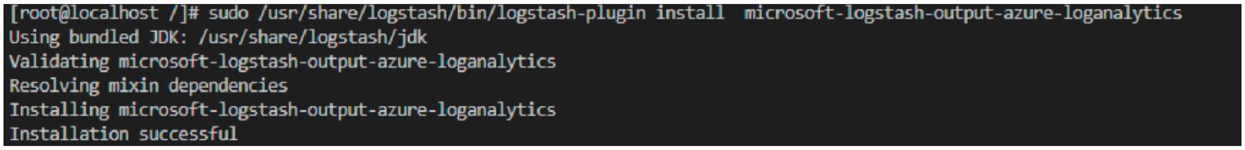
```
# ============================== Filebeat inputs ===============================

filebeat.inputs:
- type: netflow
  max_message_size: 10KiB
  host: "0.0.0.0:2055"
  protocols: [ v5, v9, ipfix ]
  expiration_timeout: 30m
  queue_size: 8192
  custom_definitions:
  - /etc/filebeat/custom.yml
  detect_sequence_reset: true
  enabled: true


# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

# filestream is an input for collecting log messages from files.
#- type: filestream

  # Unique ID among all inputs, an ID is required.
#  id: my-filestream-id

  # Change to true to enable this input configuration.
#  enabled: false

  # Paths that should be crawled and fetched. Glob based paths.
 # paths:
#    - /var/log/*.log
#    #- c:\programdata\elasticsearch\logs\*
```

- In the Filebeat inputs section, if you want to receive data from a port other than the default port, that is, **port 2055**, replace the port number in the **host** field.
- Add the provided custom.yml file inside the /etc/filebeat/ directory.

- Open the Filebeat input and output ports in the firewall:
  - **firewall-cmd --zone=public --permanent --add-port=2055/udp**
  - **firewall-cmd --zone=public --permanent --add-port=5044/udp**
- **Note:** If a custom port is added for Filebeat input or output, open that port in the firewall.

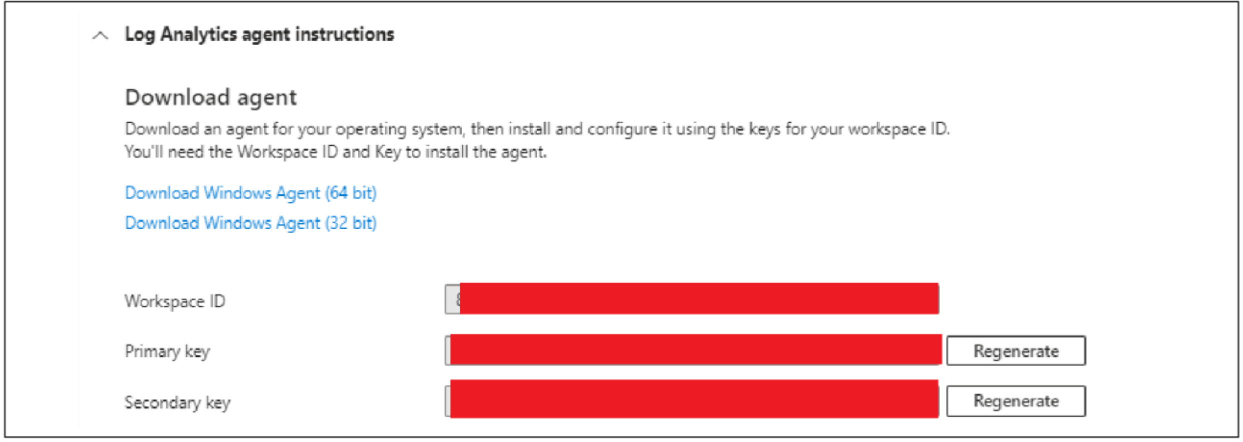
3. **Configure Logstash to send events to Microsoft Sentinel**

- Install the Azure Log Analytics plug-in:
  - **sudo /usr/share/logstash/bin/logstash-plugin install microsoft-logstash-output-azure-loganalytics**



```
[root@localhost /]# sudo /usr/share/logstash/bin/logstash-plugin install  microsoft-logstash-output-azure-loganalytics
Using bundled JDK: /usr/share/logstash/jdk
Validating microsoft-logstash-output-azure-loganalytics
Resolving mixin dependencies
Installing microsoft-logstash-output-azure-loganalytics
Installation successful
```

- Store the Log Analytics workspace key in the Logstash key store. The workspace key can be found in Azure portal under Log Analytics workspace > Select workspace. Under **Settings**, select Agent > Log Analytics agent instructions.



Log Analytics agent instructions

Download agent

Download an agent for your operating system, then install and configure it using the keys for your workspace ID.
You'll need the Workspace ID and Key to install the agent.

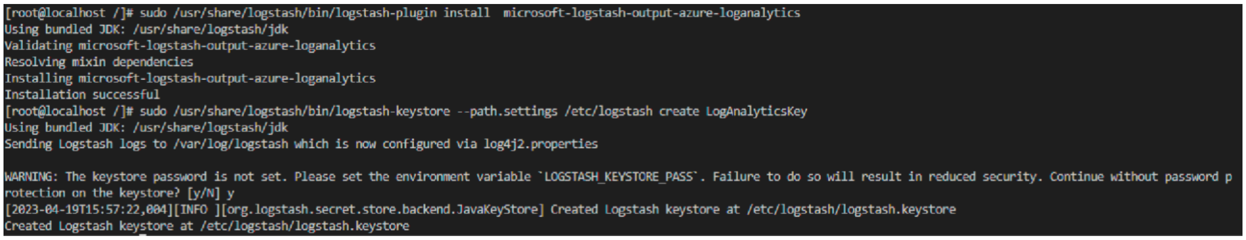
Download Windows Agent (64 bit)
Download Windows Agent (32 bit)

Workspace ID [redacted]

Primary key [redacted] Regenerate

Secondary key [redacted] Regenerate

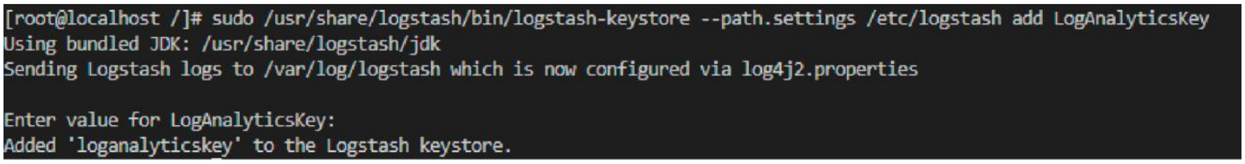
- Copy the primary key and run the following commands:
  - **sudo /usr/share/logstash/bin/logstash-keystore --path.settings /etc/logstash create LogAnalyticsKey**



```
[root@localhost /]# sudo /usr/share/logstash/bin/logstash-plugin install  microsoft-logstash-output-azure-loganalytics
Using bundled JDK: /usr/share/logstash/jdk
Validating microsoft-logstash-output-azure-loganalytics
Resolving mixin dependencies
Installing microsoft-logstash-output-azure-loganalytics
Installation successful
[root@localhost /]# sudo /usr/share/logstash/bin/logstash-keystore --path.settings /etc/logstash create LogAnalyticsKey
Using bundled JDK: /usr/share/logstash/jdk
Sending Logstash logs to /var/log/logstash which is now configured via log4j2.properties

WARNING: The keystore password is not set. Please set the environment variable `LOGSTASH_KEYSTORE_PASS`. Failure to do so will result in reduced security. Continue without password p
rotection on the keystore? [y/N] y
[2023-04-19T15:57:22,004][INFO ][org.logstash.secret.store.backend.JavaKeyStore] Created Logstash keystore at /etc/logstash/logstash.keystore
Created Logstash keystore at /etc/logstash/logstash.keystore
```

  - **sudo /usr/share/logstash/bin/logstash-keystore --path.settings /etc/logstash add LogAnalyticsKey**

- The above command will prompt you for the key. Paste the copied primary key into the prompt.

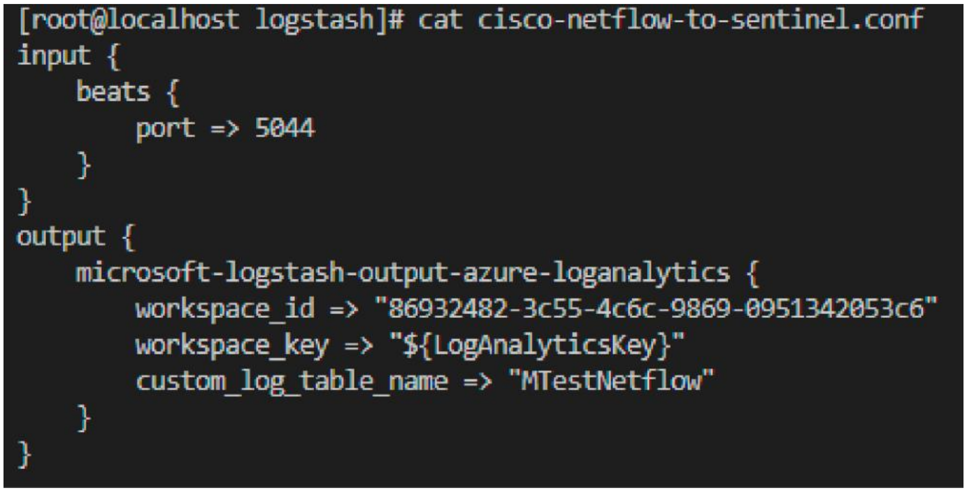


```
[root@localhost /]# sudo /usr/share/logstash/bin/logstash-keystore --path.settings /etc/logstash add LogAnalyticsKey
Using bundled JDK: /usr/share/logstash/jdk
Sending Logstash logs to /var/log/logstash which is now configured via log4j2.properties

Enter value for LogAnalyticsKey:
Added 'loganalyticskey' to the Logstash keystore.
```

- Create the configuration file /etc/logstash/cisco-netflow-to-sentinel.conf:

```
input {
    beats {
        port => <port_number> (Enter the output port number that was configured
during Filebeat configuration, for example, filebeat.yml.)
    }
}
output {
    microsoft-logstash-output-azure-loganalytics {
        workspace_id => "<workspace_id>"
        workspace_key => "${LogAnalyticsKey}"
        custom_log_table_name => "CiscoSDWANNetflow"
    }
}
```

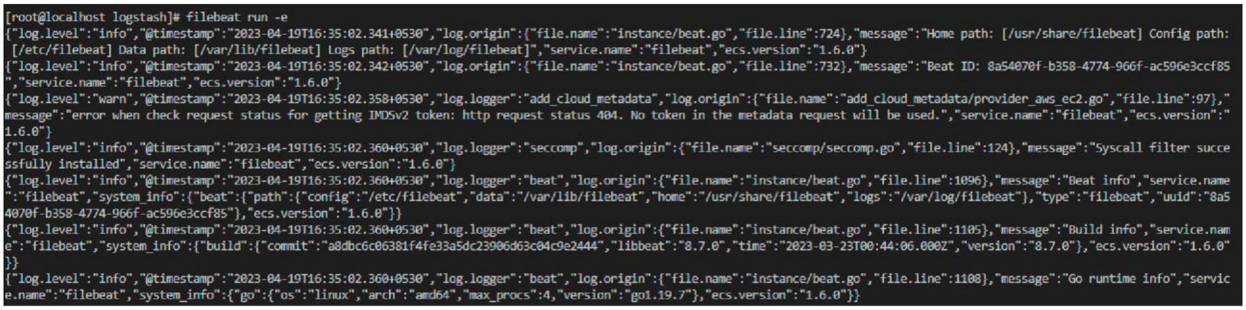
  - **Note: If the table is not present in Sentinel, it will create a new table.**



```
[root@localhost logstash]# cat cisco-netflow-to-sentinel.conf
input {
    beats {
        port => 5044
    }
}
output {
    microsoft-logstash-output-azure-loganalytics {
        workspace_id => "86932482-3c55-4c6c-9869-0951342053c6"
        workspace_key => "${LogAnalyticsKey}"
        custom_log_table_name => "MTestNetflow"
    }
}
```

4. **Run Filebeat**

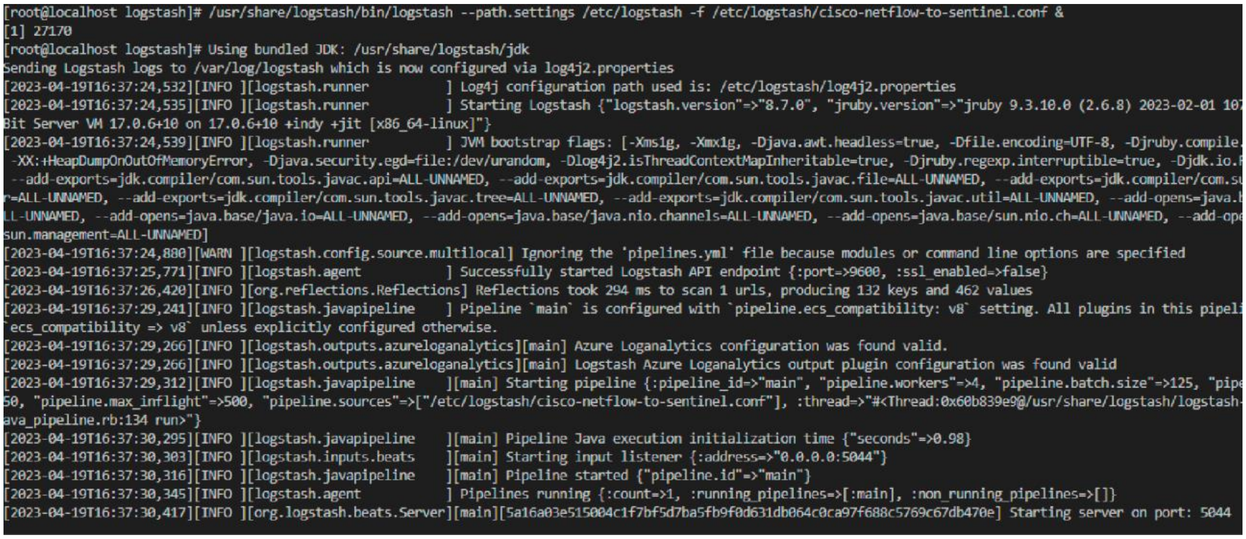
- Open a terminal and run the following command:
  - **systemctl start filebeat.**
- This command will run Filebeat in the background. To view the logs, stop Filebeat (**systemctl stop filebeat**) and then run the following command:
  - **filebeat run -e**



```
[root@localhost logstash]# filebeat run -e
{"log.level":"info","@timestamp":"2023-04-19T16:35:02.341+0530","log.origin":{"file.name":"instance/beat.go","file.line":724},"message":"Home path: [/usr/share/filebeat] Config path:
 [/etc/filebeat] Data path: [/var/lib/filebeat] Logs path: [/var/log/filebeat]","service.name":"filebeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2023-04-19T16:35:02.342+0530","log.origin":{"file.name":"instance/beat.go","file.line":732},"message":"Beat ID: 8a54070f-b358-4774-966f-ac596e3ccf85
","service.name":"filebeat","ecs.version":"1.6.0"}
{"log.level":"warn","@timestamp":"2023-04-19T16:35:02.358+0530","log.logger":"add_cloud_metadata","log.origin":{"file.name":"add_cloud_metadata/provider_aws_ec2.go","file.line":97},"
message":"error when check request status for getting IMDSv2 token: http request status 404. No token in the metadata request will be used.","service.name":"filebeat","ecs.version":"
1.6.0"}
{"log.level":"info","@timestamp":"2023-04-19T16:35:02.360+0530","log.logger":"seccomp","log.origin":{"file.name":"seccomp/seccomp.go","file.line":124},"message":"Syscall filter succe
ssfully installed","service.name":"filebeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2023-04-19T16:35:02.360+0530","log.logger":"beat","log.origin":{"file.name":"instance/beat.go","file.line":1096},"message":"Beat info","service.name
":"filebeat","system_info":{"beat":{"path":{"config":"/etc/filebeat","data":"/var/lib/filebeat","home":"/usr/share/filebeat","logs":"/var/log/filebeat"},"type":"filebeat","uuid":"8a5
4070f-b358-4774-966f-ac596e3ccf85"},"ecs.version":"1.6.0"}}
{"log.level":"info","@timestamp":"2023-04-19T16:35:02.360+0530","log.logger":"beat","log.origin":{"file.name":"instance/beat.go","file.line":1105},"message":"Build info","service.nam
e":"filebeat","system_info":{"build":{"commit":"a8dbc6c06381f4fe33a5dc23906d63c04c9e2444","libbeat":"8.7.0","time":"2023-03-23T00:44:06.000Z","version":"8.7.0"},"ecs.version":"1.6.0"
}}
{"log.level":"info","@timestamp":"2023-04-19T16:35:02.360+0530","log.logger":"beat","log.origin":{"file.name":"instance/beat.go","file.line":1108},"message":"Go runtime info","servic
e.name":"filebeat","system_info":{"go":{"os":"linux","arch":"amd64","max_procs":4,"version":"go1.19.7"},"ecs.version":"1.6.0"}}
```

5. **Run Logstash:**

- In another terminal window, run the following command:
  - **/usr/share/logstash/bin/logstash --path.settings /etc/logstash -f /etc/logstash/cisco-netflow-to-sentinel.conf &**
- This command will run Logstash in the background. To view the Logstash logs, terminate the above process and run the following command:
  - **/usr/share/logstash/bin/logstash --path.settings /etc/logstash -f /etc/logstash/cisco-netflow-to-sentinel.conf**



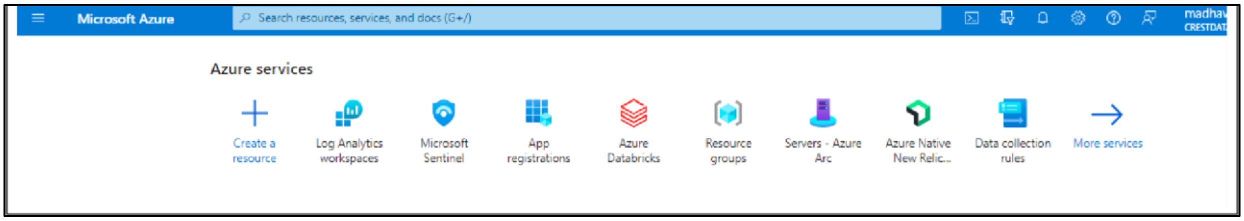
```
[root@localhost logstash]# /usr/share/logstash/bin/logstash --path.settings /etc/logstash -f /etc/logstash/cisco-netflow-to-sentinel.conf &
[1] 27170
[root@localhost logstash]# Using bundled JDK: /usr/share/logstash/jdk
Sending Logstash logs to /var/log/logstash which is now configured via log4j2.properties
[2023-04-19T16:37:24,532][INFO ][logstash.runner          ] Log4j configuration path used is: /etc/logstash/log4j2.properties
[2023-04-19T16:37:24,535][INFO ][logstash.runner          ] Starting Logstash {"logstash.version"=>"8.7.0", "jruby.version"=>"jruby 9.3.10.0 (2.6.8) 2023-02-01 107
Bit Server VM 17.0.6+10 on 17.0.6+10 +indy +jit [x86_64-linux]"}
[2023-04-19T16:37:24,539][INFO ][logstash.runner          ] JVM bootstrap flags: [-Xms1g, -Xmx1g, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djruby.compile.
 -XX:+HeapDumpOnOutOfMemoryError, -Djava.security.egd=file:/dev/urandom, -Dlog4j2.isThreadContextMapInheritable=true, -Djruby.regexp.interruptible=true, -Djdk.io.F
 --add-exports=jdk.compiler/com.sun.tools.javac.api=ALL-UNNAMED, --add-exports=jdk.compiler/com.sun.tools.javac.file=ALL-UNNAMED, --add-exports=jdk.compiler/com.su
r=ALL-UNNAMED, --add-exports=jdk.compiler/com.sun.tools.javac.tree=ALL-UNNAMED, --add-exports=jdk.compiler/com.sun.tools.javac.util=ALL-UNNAMED, --add-opens=java.b
LL-UNNAMED, --add-opens=java.base/java.io=ALL-UNNAMED, --add-opens=java.base/java.nio.channels=ALL-UNNAMED, --add-opens=java.base/sun.nio.ch=ALL-UNNAMED, --add-ope
sun.management=ALL-UNNAMED]
[2023-04-19T16:37:24,880][WARN ][logstash.config.source.multilocal] Ignoring the 'pipelines.yml' file because modules or command line options are specified
[2023-04-19T16:37:25,771][INFO ][logstash.agent           ] Successfully started Logstash API endpoint {:port=>9600, :ssl_enabled=>false}
[2023-04-19T16:37:26,420][INFO ][org.reflections.Reflections] Reflections took 294 ms to scan 1 urls, producing 132 keys and 462 values
[2023-04-19T16:37:29,241][INFO ][logstash.javapipeline    ] Pipeline `main` is configured with `pipeline.ecs_compatibility: v8` setting. All plugins in this pipeli
`ecs_compatibility => v8` unless explicitly configured otherwise.
[2023-04-19T16:37:29,266][INFO ][logstash.outputs.azureloganalytics][main] Azure Loganalytics configuration was found valid.
[2023-04-19T16:37:29,266][INFO ][logstash.outputs.azureloganalytics][main] Logstash Azure Loganalytics output plugin configuration was found valid
[2023-04-19T16:37:29,312][INFO ][logstash.javapipeline    ][main] Starting pipeline {:pipeline_id=>"main", "pipeline.workers"=>4, "pipeline.batch.size"=>125, "pipe
50, "pipeline.max_inflight"=>500, "pipeline.sources"=>["/etc/logstash/cisco-netflow-to-sentinel.conf"], :thread=>"#<Thread:0x60b839e9@/usr/share/logstash/logstash-
ava_pipeline.rb:134 run>"}
[2023-04-19T16:37:30,295][INFO ][logstash.javapipeline    ][main] Pipeline Java execution initialization time {"seconds"=>0.98}
[2023-04-19T16:37:30,303][INFO ][logstash.inputs.beats    ][main] Starting input listener {:address=>"0.0.0.0:5044"}
[2023-04-19T16:37:30,316][INFO ][logstash.javapipeline    ][main] Pipeline started {"pipeline.id"=>"main"}
[2023-04-19T16:37:30,345][INFO ][logstash.agent           ] Pipelines running {:count=>1, :running_pipelines=>[:main], :non_running_pipelines=>[]}
[2023-04-19T16:37:30,417][INFO ][org.logstash.beats.Server][main][5a16a03e515004c1f7bf5d7ba5fb9f0d631db064c0ca97f688c5769c67db470e] Starting server on port: 5044
```

Steps to ingest syslog data into Microsoft Sentinel

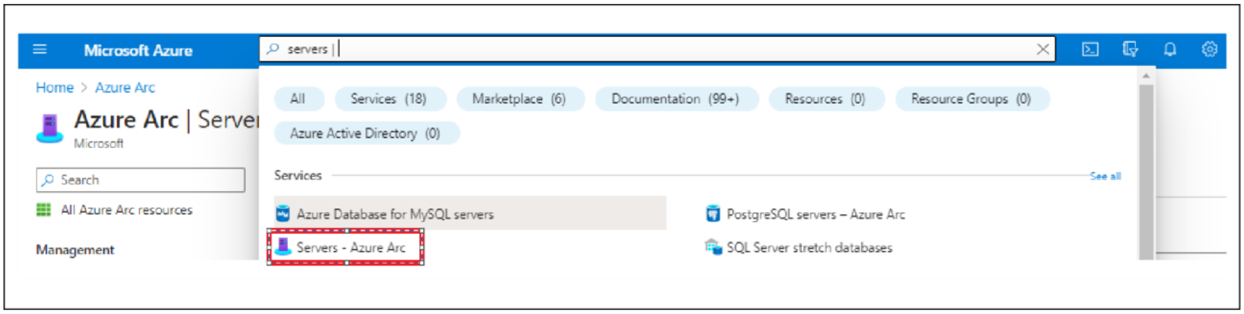
Azure Monitor Agent will be used to collect the syslog data into Sentinel. To enable this, you first need to create an Azure Arc server for the VM from which the syslog data will be sent.

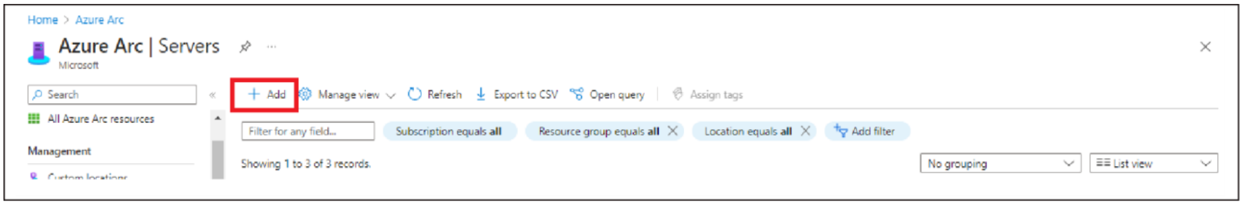
Add an Azure Arc server

- Log in to the Azure portal.

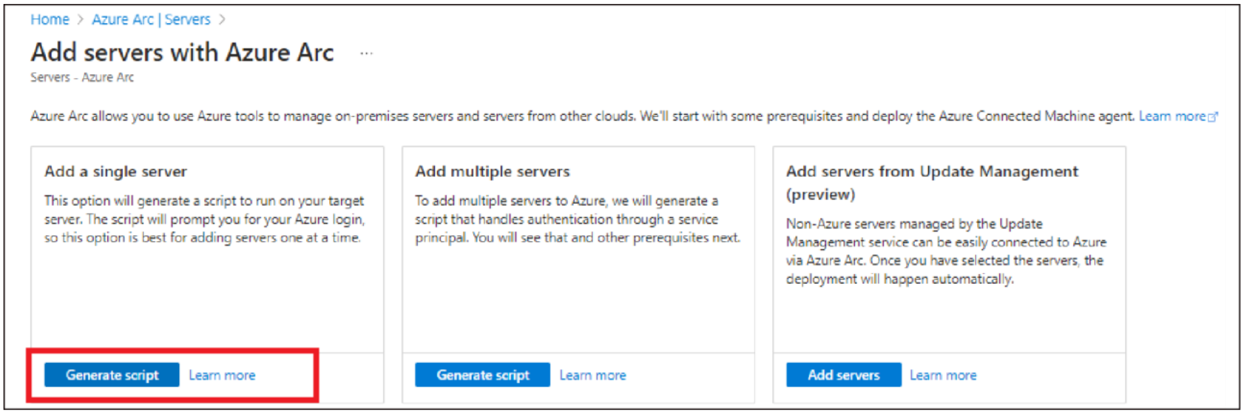


- Go to **Servers – Azure Arc** and click **Add**.





- Under "Add a single server," select **Generate Script**. Users can also generate scripts for multiple servers.



Add servers with Azure Arc

Servers - Azure Arc

Azure Arc allows you to use Azure tools to manage on-premises servers and servers from other clouds. We'll start with some prerequisites and deploy the Azure Connected Machine agent. Learn more

Add a single server

This option will generate a script to run on your target server. The script will prompt you for your Azure login, so this option is best for adding servers one at a time.

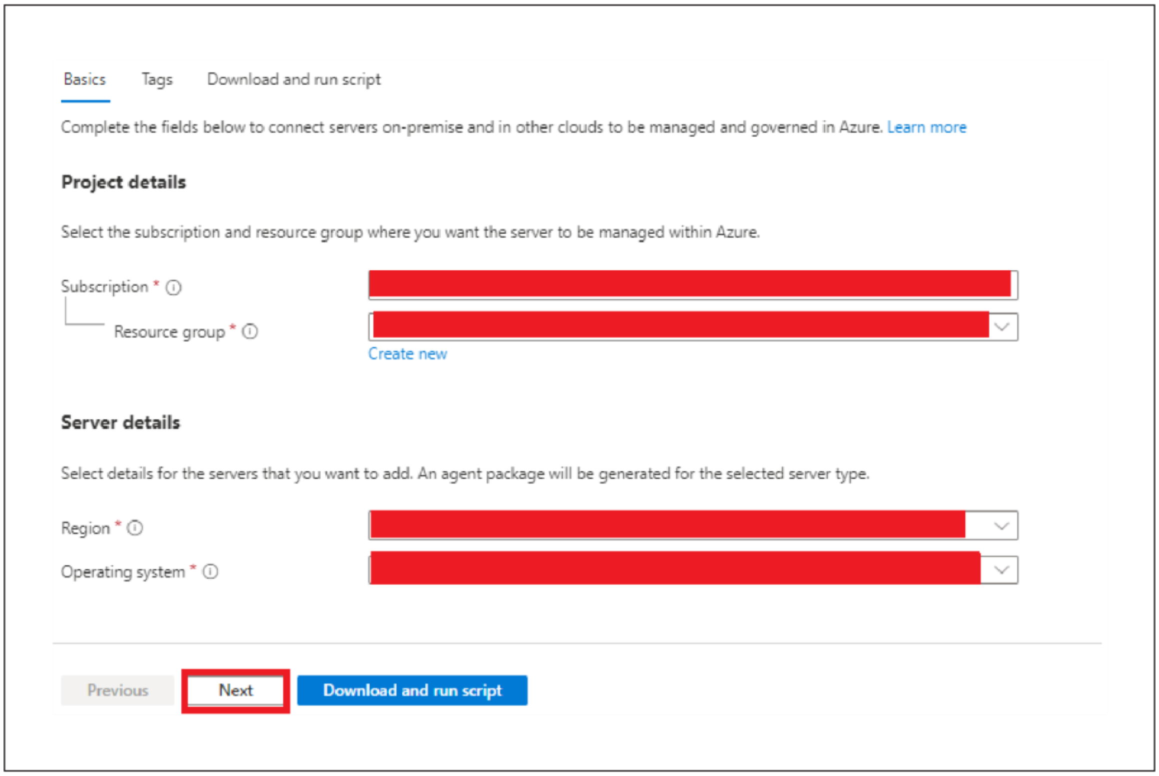
Add multiple servers

To add multiple servers to Azure, we will generate a script that handles authentication through a service principal. You will see that and other prerequisites next.

Add servers from Update Management (preview)

Non-Azure servers managed by the Update Management service can be easily connected to Azure via Azure Arc. Once you have selected the servers, the deployment will happen automatically.

- Review the information on the Prerequisites page, then select **Next**.
- On the Resource details page, provide the following information:
  - Select the subscription and resource group where you want the machine to be managed within Azure.
  - For **Region,** choose the Azure region in which the server's metadata will be stored.
  - For **Operating system**, select the operating system of the server you want to connect.
  - Choose the connectivity method for the Azure Connected Machine agent to connect to the internet. If you select **Proxy server**, enter the proxy server IP address or the name and port number that the machine will use in the specified format: http://<proxyURL>:<proxyport>.
  - Select **Next**.



Complete the fields below to connect servers on-premise and in other clouds to be managed and governed in Azure. Learn more

Project details

Select the subscription and resource group where you want the server to be managed within Azure.

Subscription * ⓘ [redacted]

Resource group * ⓘ [redacted]

Create new

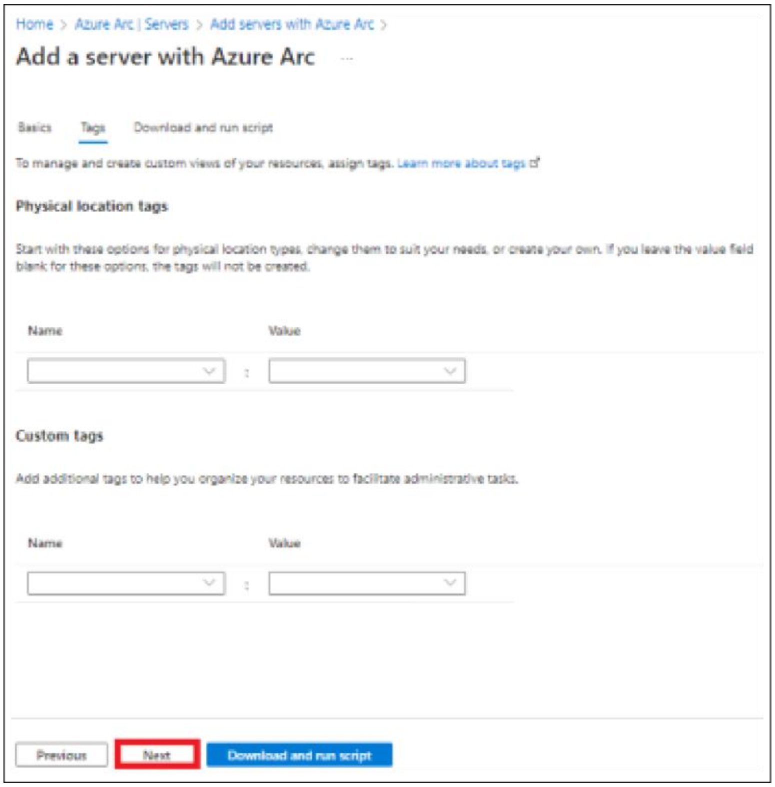
Server details

Select details for the servers that you want to add. An agent package will be generated for the selected server type.

Region * ⓘ [redacted]

Operating system * ⓘ [redacted]

- On the Tags page, review the suggested default physical location tags and enter a value, or specify one or more custom tags to support your standards. Then select **Next.**



Home > Azure Arc | Servers > Add servers with Azure Arc >

Add a server with Azure Arc

To manage and create custom views of your resources, assign tags. Learn more about tags

Physical location tags

Start with these options for physical location types, change them to suit your needs, or create your own. If you leave the value field blank for these options, the tags will not be created.

Custom tags

Add additional tags to help you organize your resources to facilitate administrative tasks.

- In the “Download or copy the following script” section, review the script. If you want to make any changes, use the **Previous** button to go back and update your selections. Otherwise, select **Download** to save the script file.

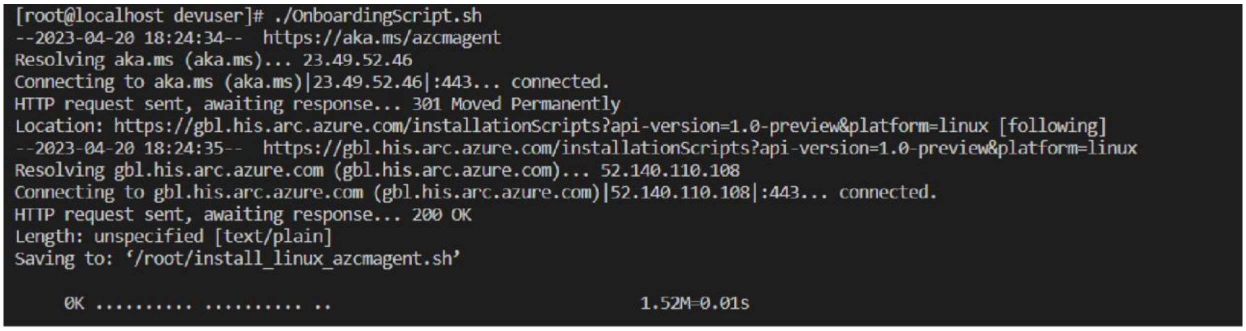
- Now that you've generated the script, the next step is to run it on the server that you want to onboard to Azure Arc.

- **For Azure VM**, follow the steps described in “Evaluate Azure Arc-enabled servers on an Azure virtual machine” (link below) before running the script:

    - **https://learn.microsoft.com/en-us/azure/azure-arc/servers/plan-evaluate-on-azure-virtual-machine**

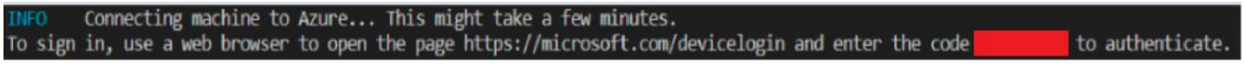
- Run the script using the following command:

    - **/<ScriptName>.sh**



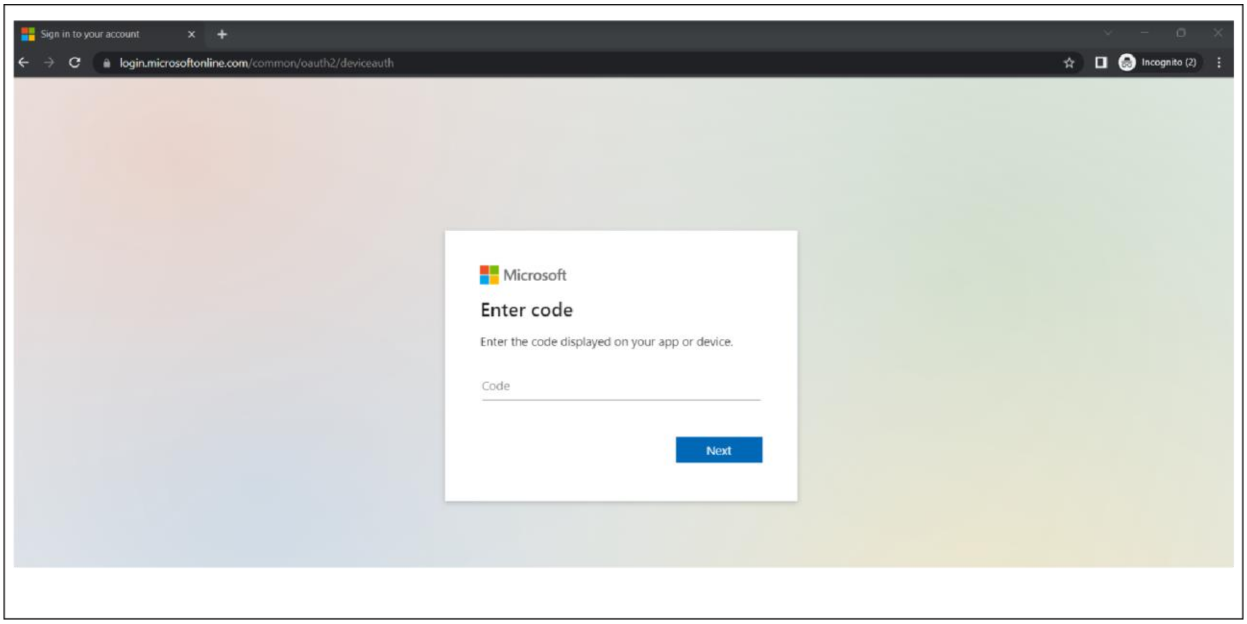
```
[root@localhost devuser]# ./OnboardingScript.sh
--2023-04-20 18:24:34--  https://aka.ms/azcmagent
Resolving aka.ms (aka.ms)... 23.49.52.46
Connecting to aka.ms (aka.ms)|23.49.52.46|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://gbl.his.arc.azure.com/installationScripts?api-version=1.0-preview&platform=linux [following]
--2023-04-20 18:24:35--  https://gbl.his.arc.azure.com/installationScripts?api-version=1.0-preview&platform=linux
Resolving gbl.his.arc.azure.com (gbl.his.arc.azure.com)... 52.140.110.108
Connecting to gbl.his.arc.azure.com (gbl.his.arc.azure.com)|52.140.110.108|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]
Saving to: ‘/root/install_linux_azcmagent.sh’

     0K .......... .......... ..                              1.52M=0.01s
```

- After the successful installation of the package, you will get the following “INFO” message:



```
INFO    Connecting machine to Azure... This might take a few minutes.
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code [redacted] to authenticate.
```

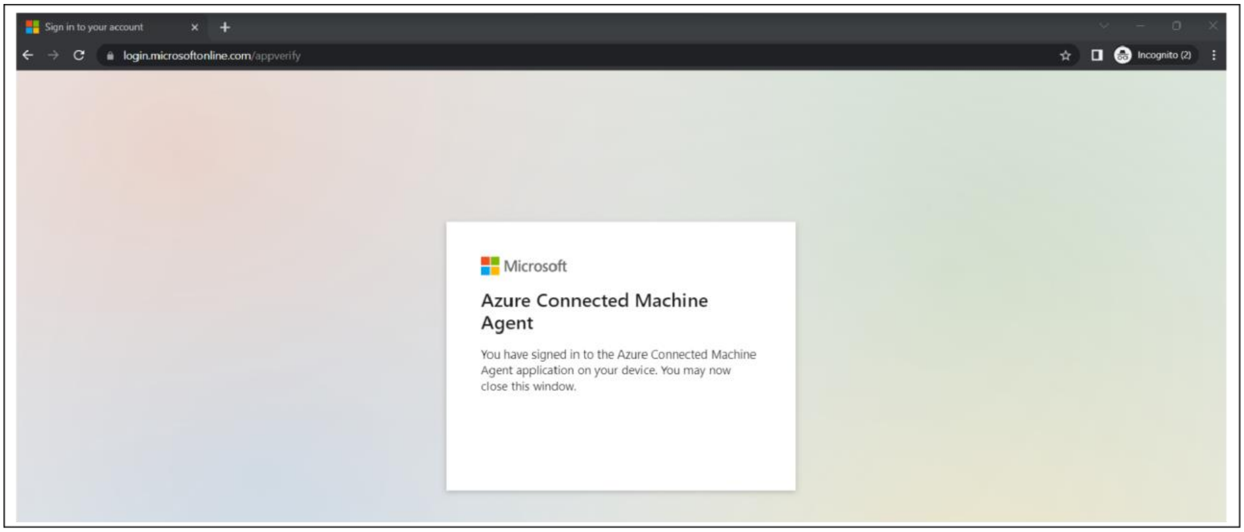
- Open the page https://microsoft.com/devicelogin and enter the code to authenticate.



Enter code

Enter the code displayed on your app or device.

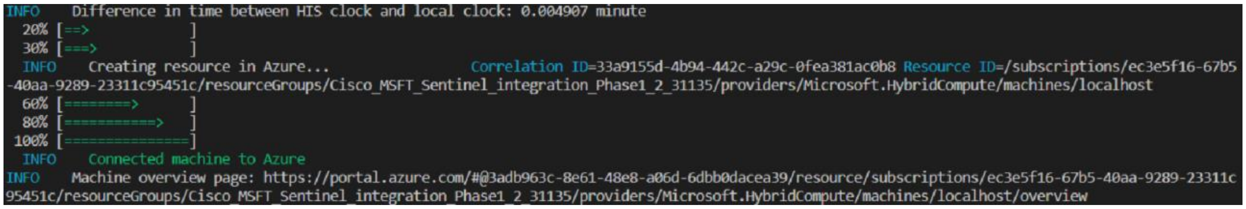
- After entering the code, you will see a confirmation message like the following:



Azure Connected Machine Agent

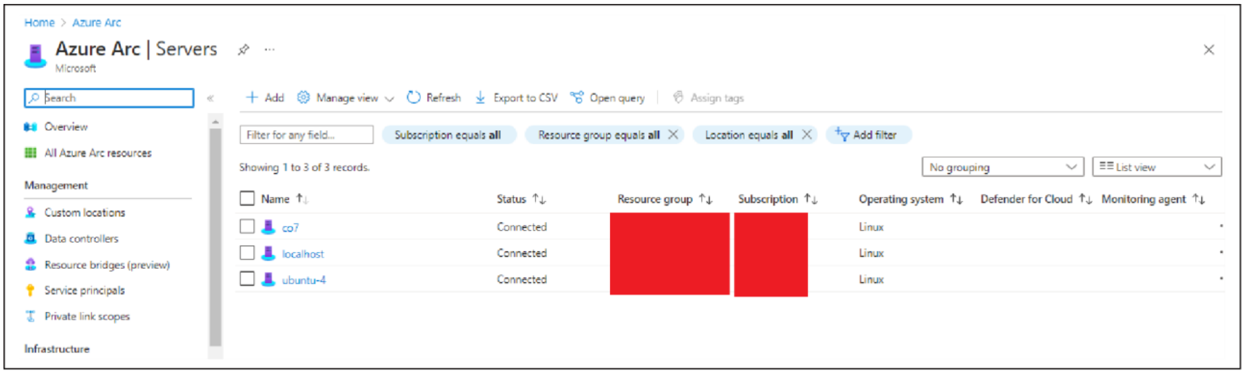
You have signed in to the Azure Connected Machine Agent application on your device. You may now close this window.

- Your machine will be connected to Azure.



```
INFO    Difference in time between HIS clock and local clock: 0.004907 minute
  20% [==>            ]
  30% [===>           ]
  INFO    Creating resource in Azure...                 Correlation ID=33a9155d-4b94-442c-a29c-0fea381ac0b8 Resource ID=/subscriptions/ec3e5f16-67b5
-40aa-9289-23311c95451c/resourceGroups/Cisco_MSFT_Sentinel_integration_Phase1_2_31135/providers/Microsoft.HybridCompute/machines/localhost
  60% [========>      ]
  80% [===========>   ]
 100% [===============]
  INFO    Connected machine to Azure
INFO    Machine overview page: https://portal.azure.com/#@3adb963c-8e61-48e8-a06d-6dbb0dacea39/resource/subscriptions/ec3e5f16-67b5-40aa-9289-23311c
95451c/resourceGroups/Cisco_MSFT_Sentinel_integration_Phase1_2_31135/providers/Microsoft.HybridCompute/machines/localhost/overview
```

- The script will download the Connected Machine agent from the Microsoft Download Center, install the agent on the server, create the Azure Arc-enabled server resource, and associate it with the agent.
- After you install the agent and configure it to connect to Azure Arc-enabled servers, go to the Azure portal to verify that the server has successfully connected. View your machine in the Azure portal.



Showing 1 to 3 of 3 records.

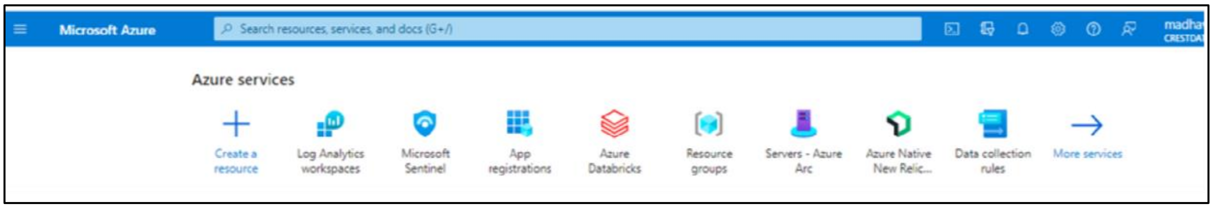
Name	Status	Resource group	Subscription	Operating system	Defender for Cloud	Monitoring agent
co7	Connected	[redacted]	[redacted]	Linux		
localhost	Connected	[redacted]	[redacted]	Linux		
ubuntu-4	Connected	[redacted]	[redacted]	Linux		

Reference: Quickstart: Connect hybrid machines with Azure Arc-enabled servers (https://learn.microsoft.com/en-us/azure/azure-arc/servers/learn/quick-enable-hybrid-vm)

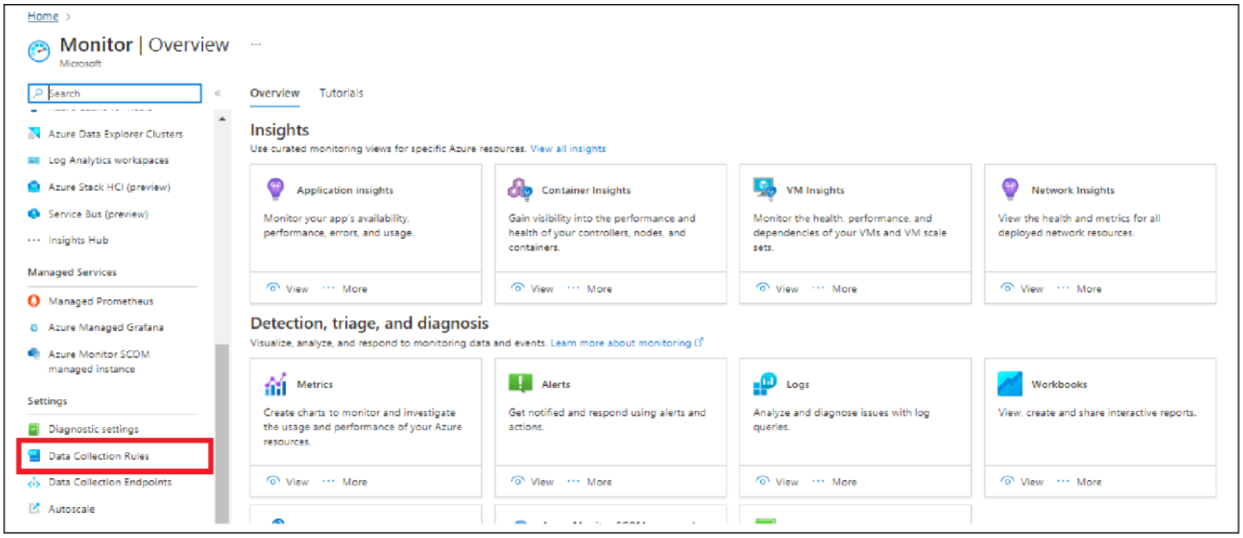
Now that you've enabled your Linux or Windows hybrid machine and successfully connected to the service, you need to create a Data Collection Rule to collect syslog data.

Create a Data Collection Rule

- Go to the Azure portal.



- Search for Monitor. Under **Settings**, select **Data Collection Rules** and then select **Create**.



Insights

Use curated monitoring views for specific Azure resources. View all insights

Application insights: Monitor your app's availability, performance, errors, and usage.

Container Insights: Gain visibility into the performance and health of your controllers, nodes, and containers.

VM Insights: Monitor the health, performance, and dependencies of your VMs and VM scale sets.

Network Insights: View the health and metrics for all deployed network resources.

Detection, triage, and diagnosis

Visualize, analyze, and respond to monitoring data and events. Learn more about monitoring

Metrics: Create charts to monitor and investigate the usage and performance of your Azure resources.

Alerts: Get notified and respond using alerts and actions.

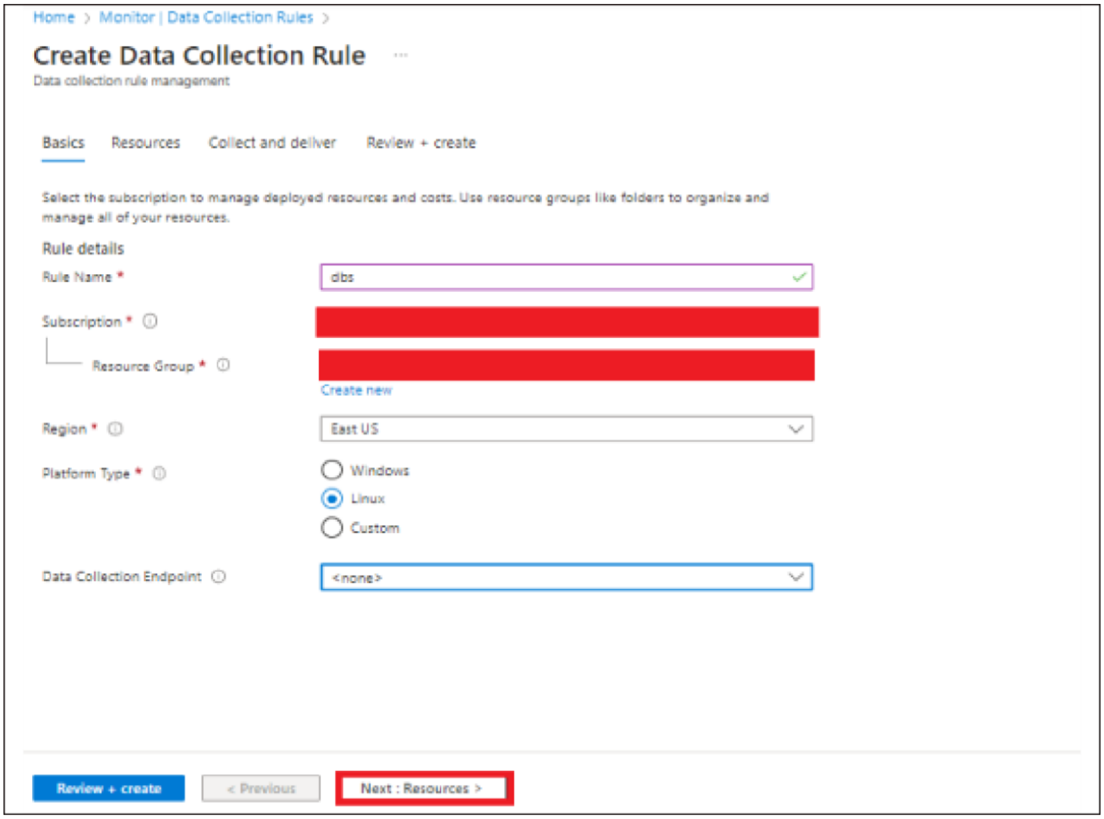
Logs: Analyze and diagnose issues with log queries.

Workbooks: View, create and share interactive reports.

- On the Basics panel, enter the following information:

Table 1. Mandatory fields for ‘Basics’ panel

Field	Value
Rule Name	Enter a name like dcr-syslog
Subscription	Select the appropriate subscription
Resource group	Select the appropriate resource group
Region	Select the region where your Microsoft Sentinel workspace is located
Platform Type	Linux


Home > Monitor | Data Collection Rules >
Create Data Collection Rule ...
Data collection rule management
Basics
Resources
Collect and deliver
Review + create
Create new
Review + create
< Previous
Next : Resources >

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources.

Rule details

Rule Name *: dbs ✓

Subscription *: [redacted]

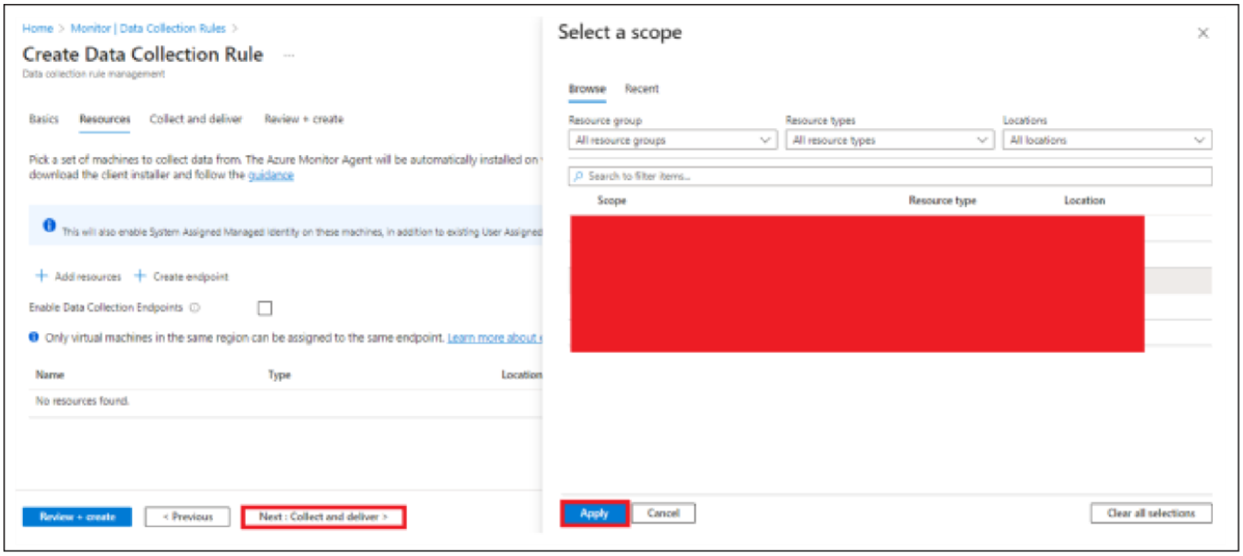
Resource Group *: [redacted]

Region *: East US

Platform Type *: ○ Windows ● Linux ○ Custom

Data Collection Endpoint: <none>

- Select **Next: Resources**.
- Select **Add resources**. Use the filters to find the virtual machine you'll use to collect logs.
- Select the virtual machine. Select **Apply**.
- Select **Next: Collect and deliver**.



Pick a set of machines to collect data from. The Azure Monitor Agent will be automatically installed on download the client installer and follow the guidance

This will also enable System Assigned Managed Identity on these machines, in addition to existing User Assigned

Enable Data Collection Endpoints ☐

Only virtual machines in the same region can be assigned to the same endpoint. Learn more about

Name	Type	Location
No resources found.		

Resource group: All resource groups

Resource types: All resource types

Locations: All locations

Search to filter items...

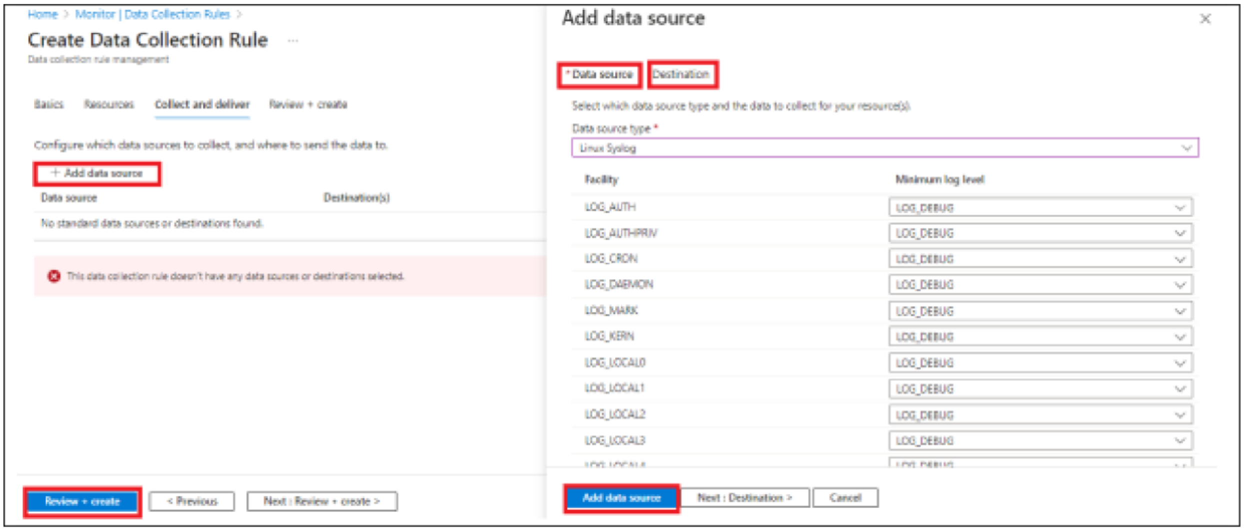
Scope	Resource type	Location
[redacted]		

- Select **Add data source**. For Data source type, select **Linux syslog**.
- For Minimum log level, leave the default value, LOG_DEBUG.
- Select **Next: Destination**.
- Select **Add destination**. Enter the following values:

Table 2. Mandatory fields for the Destination settings

Field	Value
Destination type	Azure Monitor Logs
Subscription	Select the appropriate subscription
Account or namespace	Select the appropriate Log Analytics workspace

- Select **Add data source**. Select: **Review + create**.



Configure which data sources to collect, and where to send the data to.

Data source	Destination(s)
No standard data sources or destinations found.	

This data collection rule doesn't have any data sources or destinations selected.

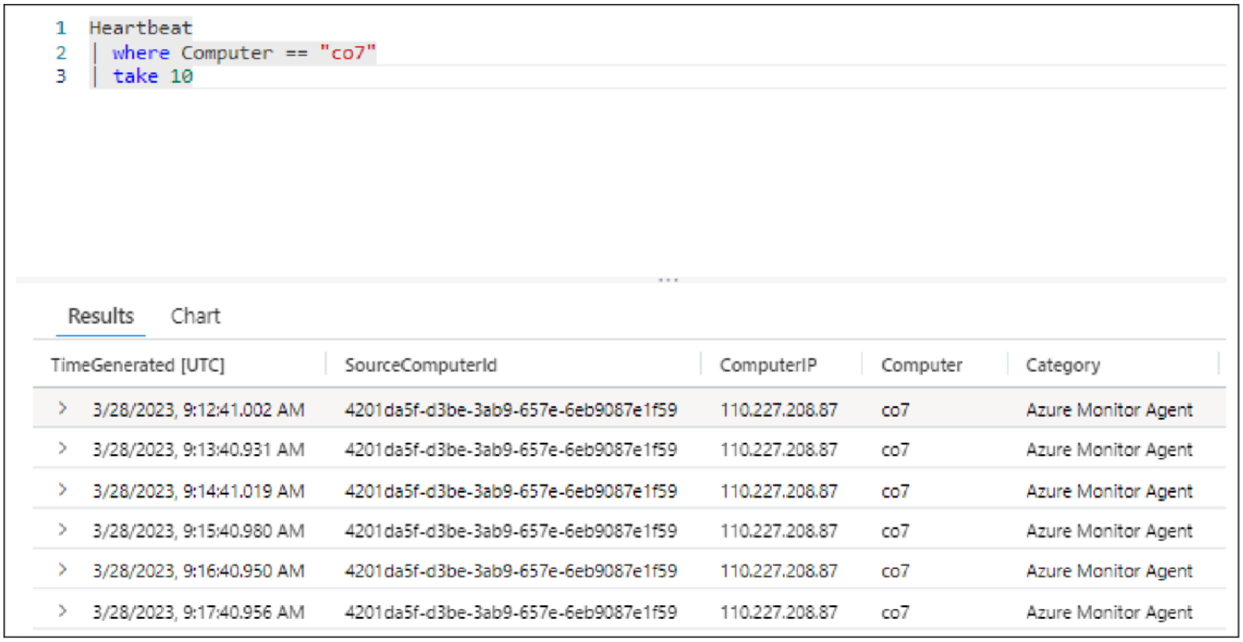
Select which data source type and the data to collect for your resource(s).

Data source type *: Linux Syslog

Facility	Minimum log level
LOG_AUTH	LOG_DEBUG
LOG_AUTHPRIV	LOG_DEBUG
LOG_CRON	LOG_DEBUG
LOG_DAEMON	LOG_DEBUG
LOG_MARK	LOG_DEBUG
LOG_KERN	LOG_DEBUG
LOG_LOCAL0	LOG_DEBUG
LOG_LOCAL1	LOG_DEBUG
LOG_LOCAL2	LOG_DEBUG
LOG_LOCAL3	LOG_DEBUG
LOG_LOCAL4	LOG_DEBUG

- Select **Create**. Wait for 20 minutes.
- In Microsoft Sentinel or Azure Monitor, verify that the Azure Monitor agent is running on your VM.
- In the Azure portal, search for and open Microsoft Sentinel or Monitor. If you're using Microsoft Sentinel, select the appropriate workspace. Under General, select **Logs**. Close the Queries page so that the New Query tab is displayed.
- Run the following query, replacing the Computer value with the name of your Linux virtual machine.

```
Heartbeat
| where Computer == "vm-ubuntu"
| take 10
```



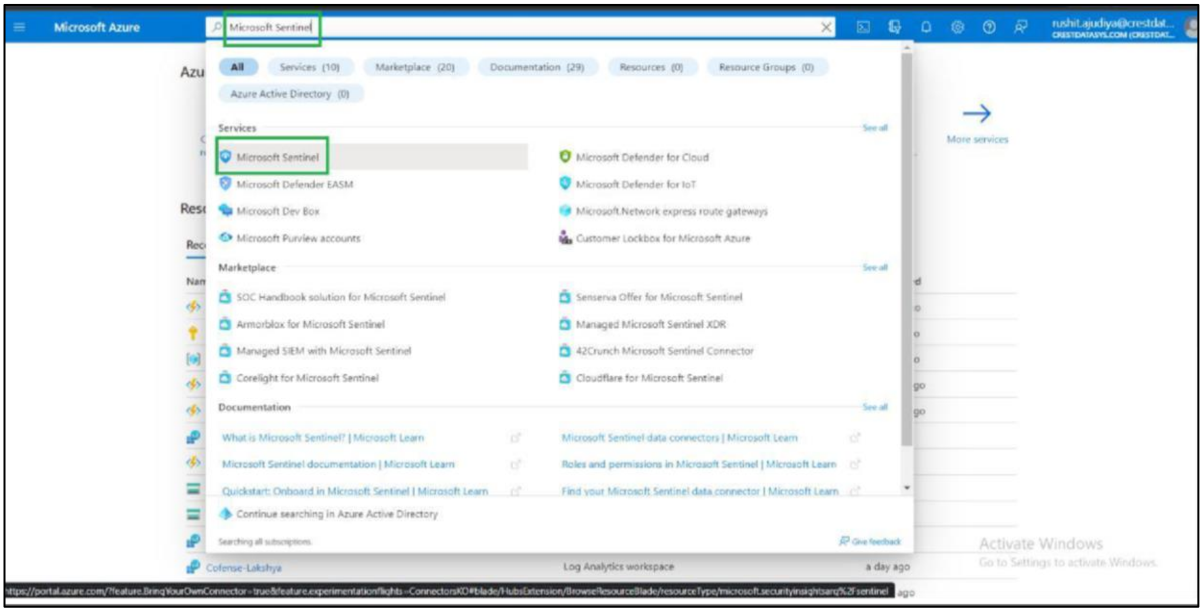
```
Heartbeat
| where Computer == "co7"
| take 10
```

	TimeGenerated [UTC]	SourceComputerId	ComputerIP	Computer	Category
>	3/28/2023, 9:12:41.002 AM	4201da5f-d3be-3ab9-657e-6eb9087e1f59	110.227.208.87	co7	Azure Monitor Agent
>	3/28/2023, 9:13:40.931 AM	4201da5f-d3be-3ab9-657e-6eb9087e1f59	110.227.208.87	co7	Azure Monitor Agent
>	3/28/2023, 9:14:41.019 AM	4201da5f-d3be-3ab9-657e-6eb9087e1f59	110.227.208.87	co7	Azure Monitor Agent
>	3/28/2023, 9:15:40.980 AM	4201da5f-d3be-3ab9-657e-6eb9087e1f59	110.227.208.87	co7	Azure Monitor Agent
>	3/28/2023, 9:16:40.950 AM	4201da5f-d3be-3ab9-657e-6eb9087e1f59	110.227.208.87	co7	Azure Monitor Agent
>	3/28/2023, 9:17:40.956 AM	4201da5f-d3be-3ab9-657e-6eb9087e1f59	110.227.208.87	co7	Azure Monitor Agent

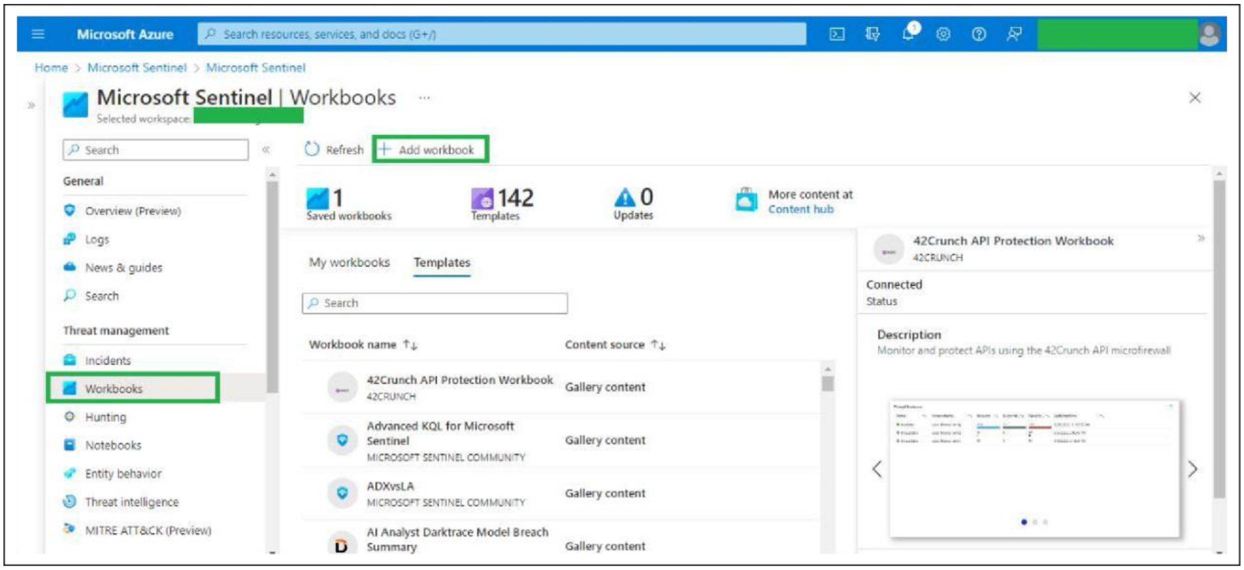
Reference: Tutorial: Forward Syslog data to a Log Analytics workspace with Microsoft Sentinel by using Azure Monitor Agent (https://learn.microsoft.com/en-us/azure/sentinel/forward-syslog-monitor-agent)

Deploy a Cisco Catalyst SD-WAN Sentinel Workbook

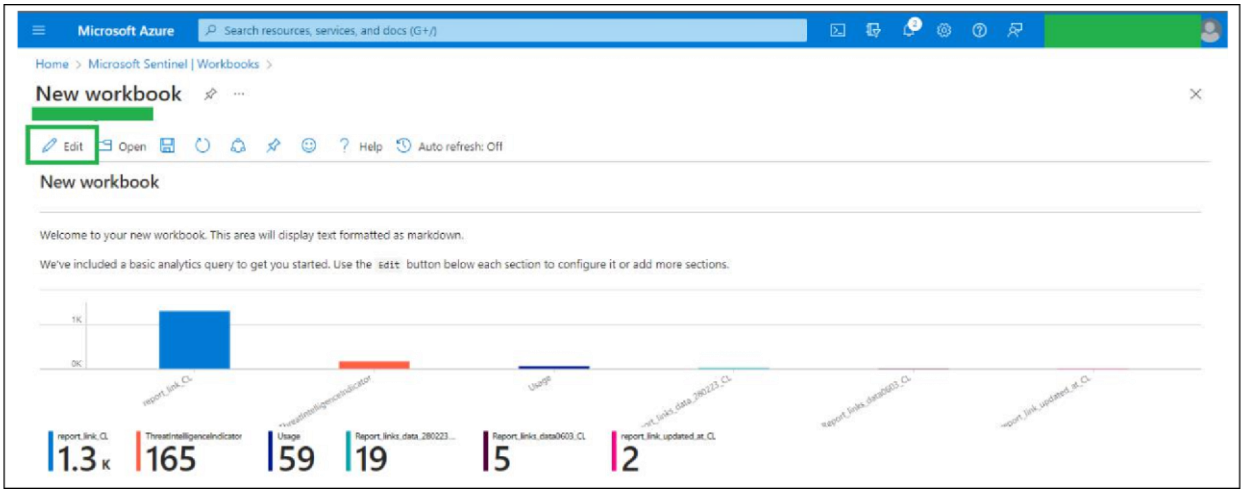
- Sign in to the Azure portal (https://portal.azure.com/#home).
- Search for the **Microsoft Sentinel** service in the Azure portal search bar, and select it.


Microsoft Azure
Microsoft Sentinel
All
Services (10)
Marketplace (20)
Documentation (29)
Resources (0)
Resource Groups (0)
Azure Active Directory (0)
Services
See all
Microsoft Sentinel
Microsoft Defender EASM
Microsoft Dev Box
Microsoft Purview accounts
Microsoft Defender for Cloud
Microsoft Defender for IoT
Microsoft.Network express route gateways
Customer Lockbox for Microsoft Azure
Marketplace
SOC Handbook solution for Microsoft Sentinel
Armorblox for Microsoft Sentinel
Managed SIEM with Microsoft Sentinel
Corelight for Microsoft Sentinel
Senserva Offer for Microsoft Sentinel
Managed Microsoft Sentinel XDR
42Crunch Microsoft Sentinel Connector
Cloudflare for Microsoft Sentinel
Documentation
What is Microsoft Sentinel? | Microsoft Learn
Microsoft Sentinel documentation | Microsoft Learn
Quickstart: Onboard in Microsoft Sentinel | Microsoft Learn
Microsoft Sentinel data connectors | Microsoft Learn
Roles and permissions in Microsoft Sentinel | Microsoft Learn
Find your Microsoft Sentinel data connector | Microsoft Learn
Continue searching in Azure Active Directory
Searching all subscriptions.
Give feedback
More services
Cofense-Lakshya
Log Analytics workspace
a day ago
Activate Windows
Go to Settings to activate Windows.

- Select the Microsoft Sentinel workspace in which you want to deploy the workbook.
- In the left panel, select **Workbooks.**
- Click **Add Workbook.**


Microsoft Azure
Search resources, services, and docs (G+/)
[redacted]
Home > Microsoft Sentinel > Microsoft Sentinel
Microsoft Sentinel | Workbooks
Selected workspace: [redacted]
Search
Refresh
Add workbook
General
Overview (Preview)
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
1 Saved workbooks
142 Templates
0 Updates
More content at Content hub
My workbooks
Templates
Search
Workbook name
Content source
42Crunch API Protection Workbook
42CRUNCH
Gallery content
Advanced KQL for Microsoft Sentinel
MICROSOFT SENTINEL COMMUNITY
Gallery content
ADXvsLA
MICROSOFT SENTINEL COMMUNITY
Gallery content
AI Analyst Darktrace Model Breach Summary
Gallery content
42Crunch API Protection Workbook
42CRUNCH
Connected
Status
Description
Monitor and protect APIs using the 42Crunch API microfirewall

- Click **Edit.**



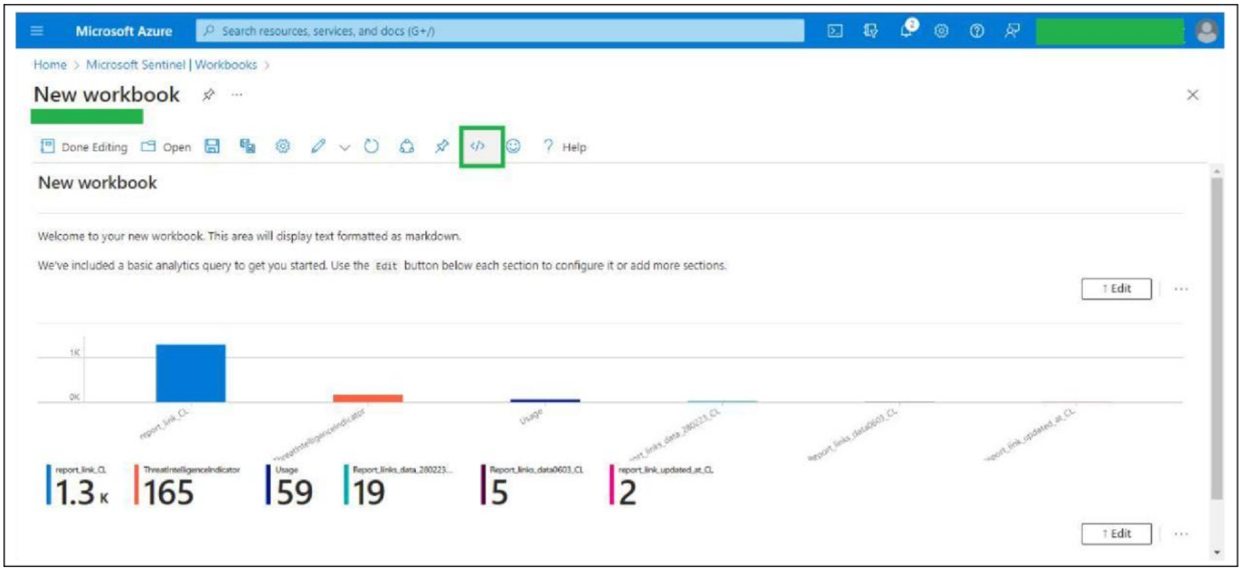
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel | Workbooks >
New workbook
Edit
Open
Help
Auto refresh: Off
1K
0K
report_link_CL
ThreatIntelligenceIndicator
Usage
report_links_data_280223_CL
Report_links_data0603_CL
report_link_updated_at_CL
report_link_CL
1.3 K
ThreatIntelligenceIndicator
165
Usage
59
Report_links_data_280223...
19
Report_links_data0603_CL
5
report_link_updated_at_CL
2

New workbook

Welcome to your new workbook. This area will display text formatted as markdown.

We've included a basic analytics query to get you started. Use the `Edit` button below each section to configure it or add more sections.

- Click the Advanced Editor button, as shown in the image below.



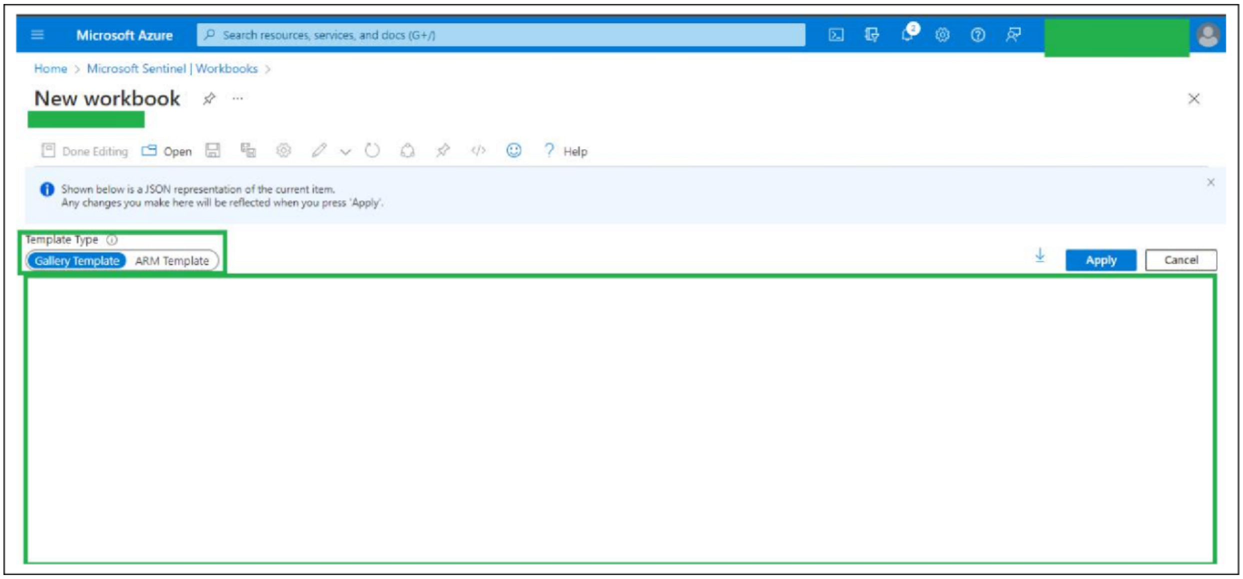
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Sentinel | Workbooks >
New workbook
Done Editing
Open
Help
Edit
1K
0K
report_link_CL
ThreatIntelligenceIndicator
Usage
report_links_data_280223_CL
Report_links_data0603_CL
report_link_updated_at_CL
report_link_CL
1.3 K
ThreatIntelligenceIndicator
165
Usage
59
Report_links_data_280223...
19
Report_links_data0603_CL
5
report_link_updated_at_CL
2
Edit

New workbook

Welcome to your new workbook. This area will display text formatted as markdown.

We've included a basic analytics query to get you started. Use the `Edit` button below each section to configure it or add more sections.

- For Template Type, choose **Gallery Template** and remove all the code within the code editor. Then paste the contents of the CiscoSDWAN.json file (provided by us and located in the workbooks directory) into the code editor.

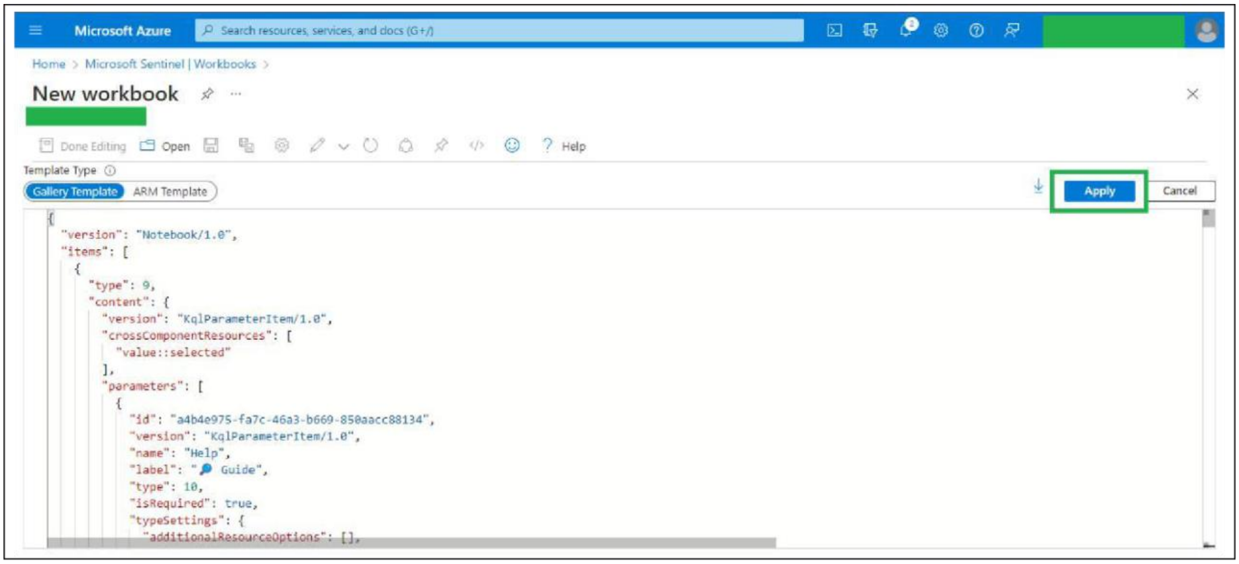


[redacted]

[redacted]

Shown below is a JSON representation of the current item.
Any changes you make here will be reflected when you press 'Apply'.

- Click **Apply**.

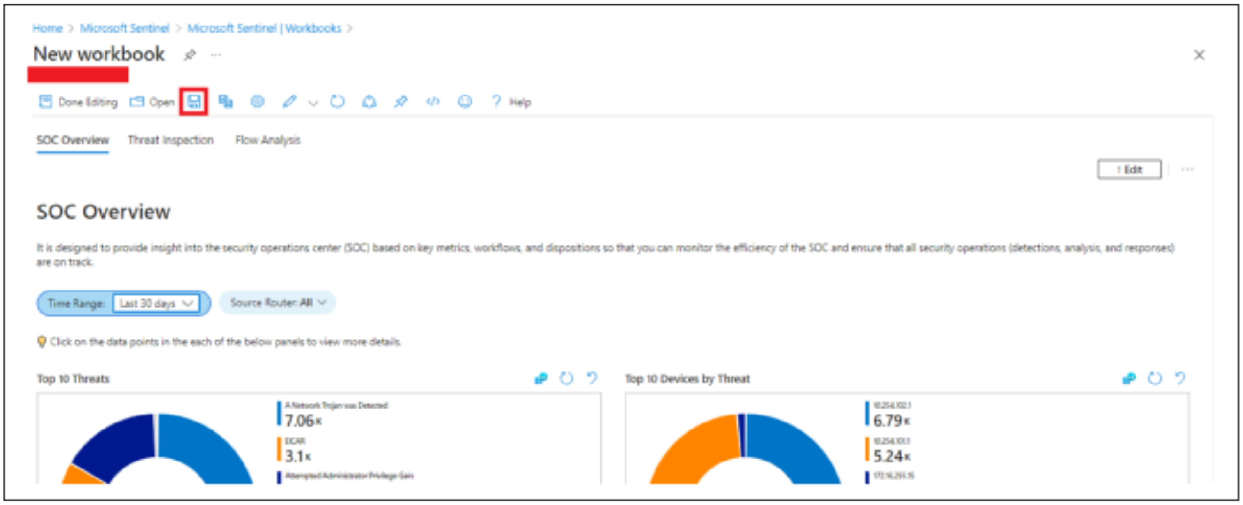


[redacted]

[redacted]

```
{
  "version": "Notebook/1.0",
  "items": [
    {
      "type": 9,
      "content": {
        "version": "KqlParameterItem/1.0",
        "crossComponentResources": [
          "value::selected"
        ],
        "parameters": [
          {
            "id": "a4b4e975-fa7c-46a3-b669-850aacc88134",
            "version": "KqlParameterItem/1.0",
            "name": "Help",
            "label": "🔎 Guide",
            "type": 10,
            "isRequired": true,
            "typeSettings": {
              "additionalResourceOptions": [],
```

- Click the **Save** button, as shown in the image below.



[redacted]

SOC Overview

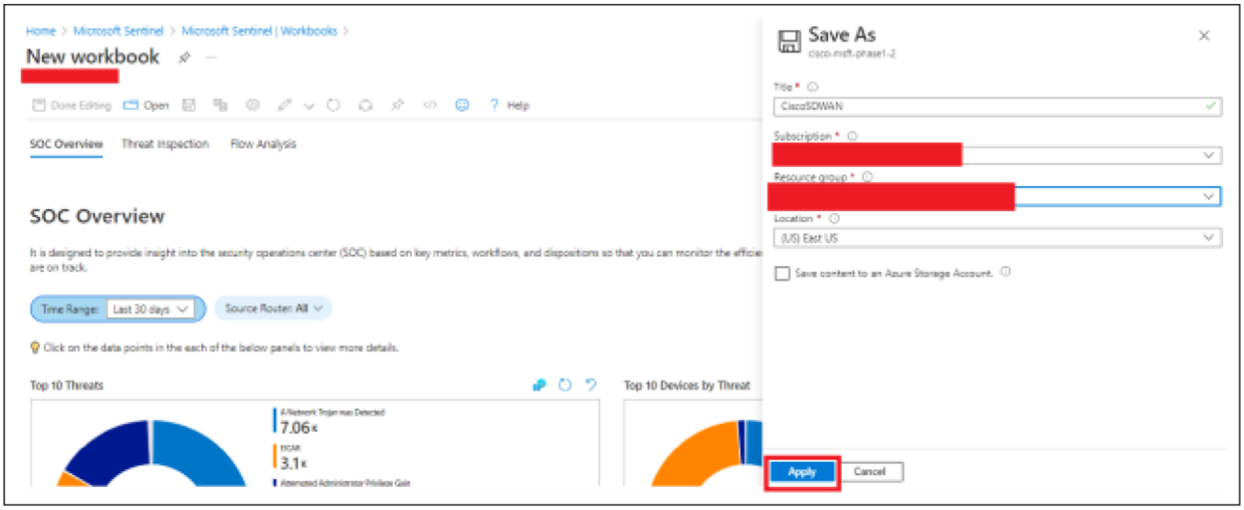
It is designed to provide insight into the security operations center (SOC) based on key metrics, workflows, and dispositions so that you can monitor the efficiency of the SOC and ensure that all security operations (detections, analysis, and responses) are on track.

Time Range: Last 30 days

Source Router: All

Click on the data points in the each of the below panels to view more details.

- Add the required data in the fields as shown in the image below (for example, Title: Cisco SD-WAN). Then click **Apply**.


Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >
New workbook
Done Editing
Open
? Help
SOC Overview
Threat Inspection
Flow Analysis
SOC Overview
It is designed to provide insight into the security operations center (SOC) based on key metrics, workflows, and dispositions so that you can monitor the efficie... are on track.
Time Range: Last 30 days
Source Router: All
Click on the data points in the each of the below panels to view more details.
Top 10 Threats
A Network Trojan was Detected
7.06K
EICAR
3.1K
Attempted Administrator Privilege Gain
Top 10 Devices by Threat
Apply
Cancel

[redacted]

Save As
cisco-msft-phase1-2

Title * CiscoSDWAN

Subscription * [redacted]

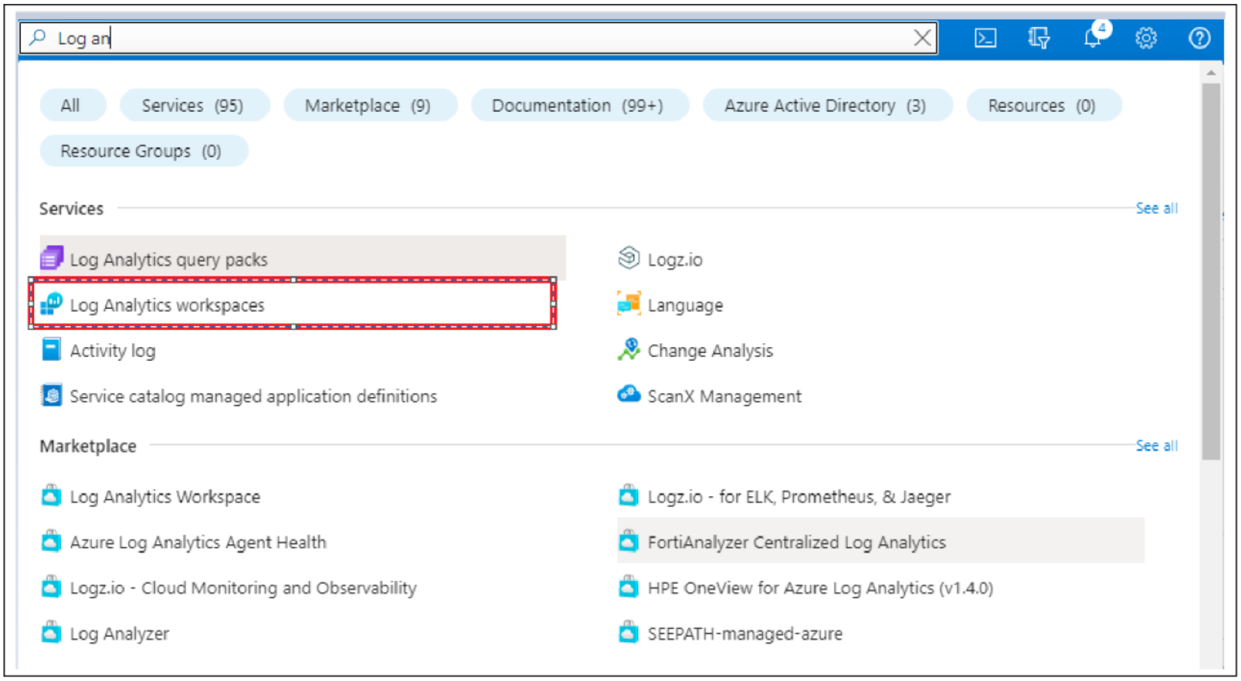
Resource group * [redacted]

Location * (US) East US

□ Save content to an Azure Storage Account.

Steps to deploy the Cisco Catalyst SD-WAN Sentinel parser functions

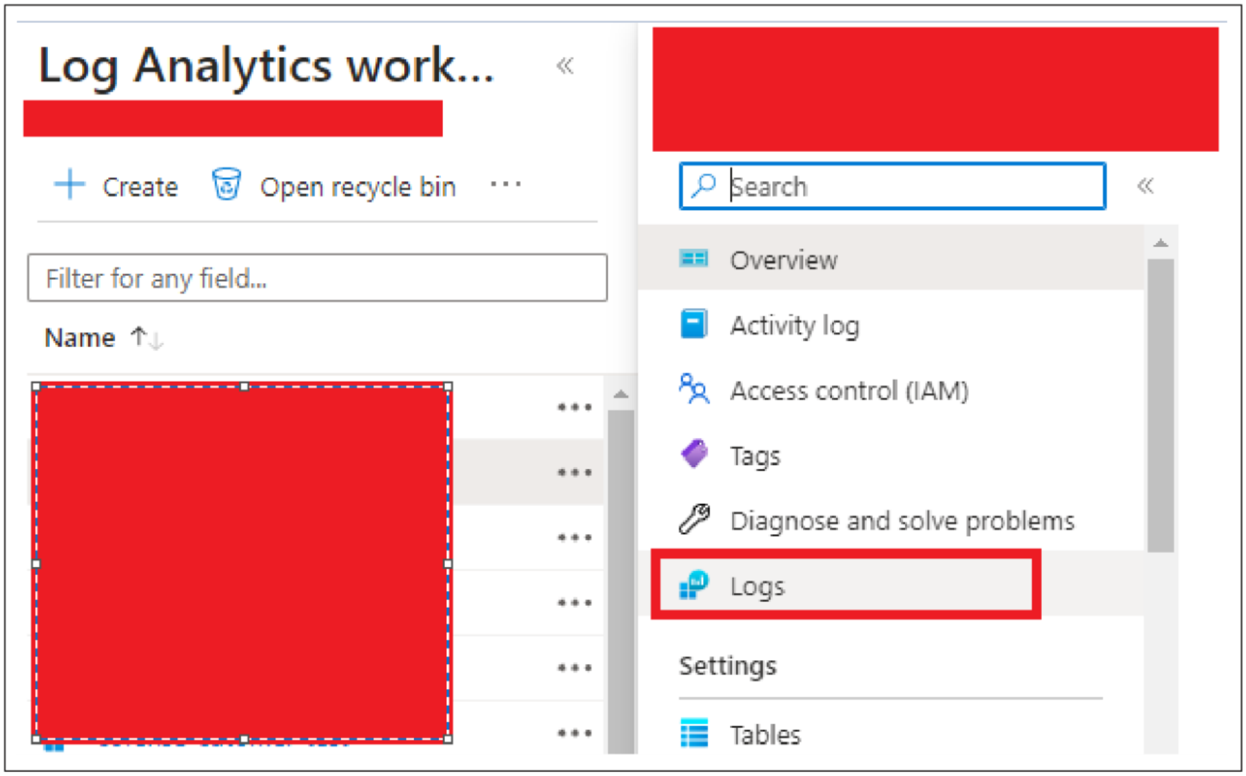
- Sign in to the Azure portal (https://portal.azure.com/#home).
- Search for the **Log Analytics workspaces** service in the Azure portal search bar, and select it.



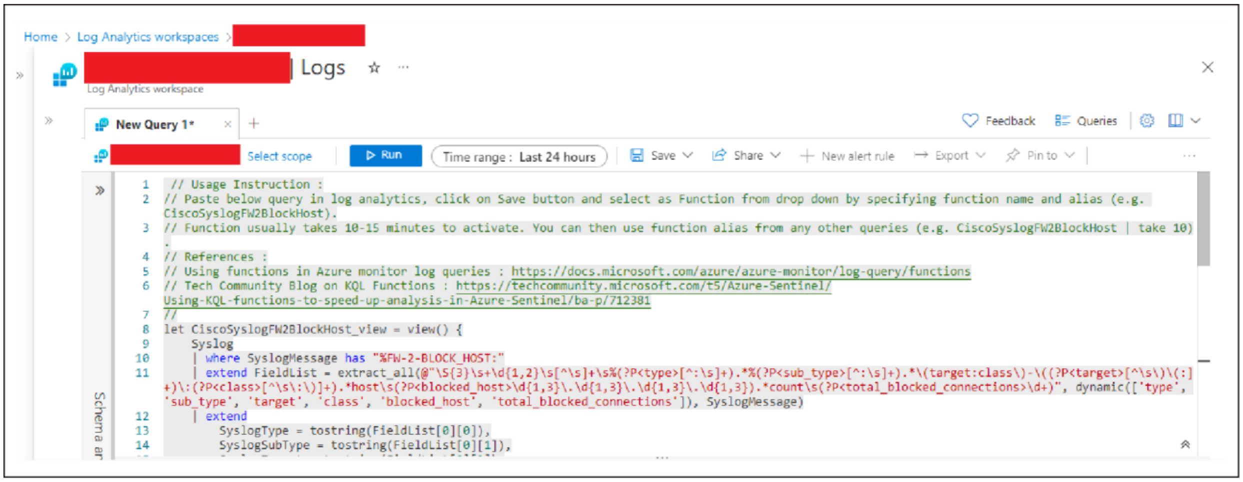
Log an

All
Services (95)
Marketplace (9)
Documentation (99+)
Azure Active Directory (3)
Resources (0)
Resource Groups (0)
Services
See all
Log Analytics query packs
Log Analytics workspaces
Activity log
Service catalog managed application definitions
Logz.io
Language
Change Analysis
ScanX Management
Marketplace
See all
Log Analytics Workspace
Azure Log Analytics Agent Health
Logz.io - Cloud Monitoring and Observability
Log Analyzer
Logz.io - for ELK, Prometheus, & Jaeger
FortiAnalyzer Centralized Log Analytics
HPE OneView for Azure Log Analytics (v1.4.0)
SEEPATH-managed-azure

- Select the workspace where the NetFlow or syslog data is collected.
- Select the **Logs** option.

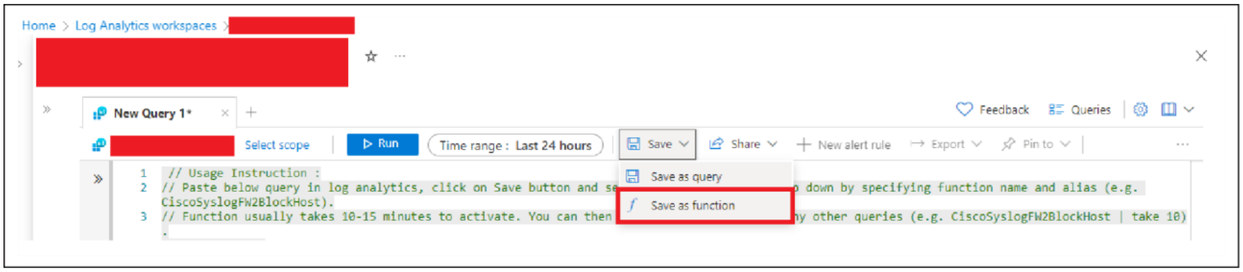


- Copy and paste the parser functions provided by us (in the Parsers directory).



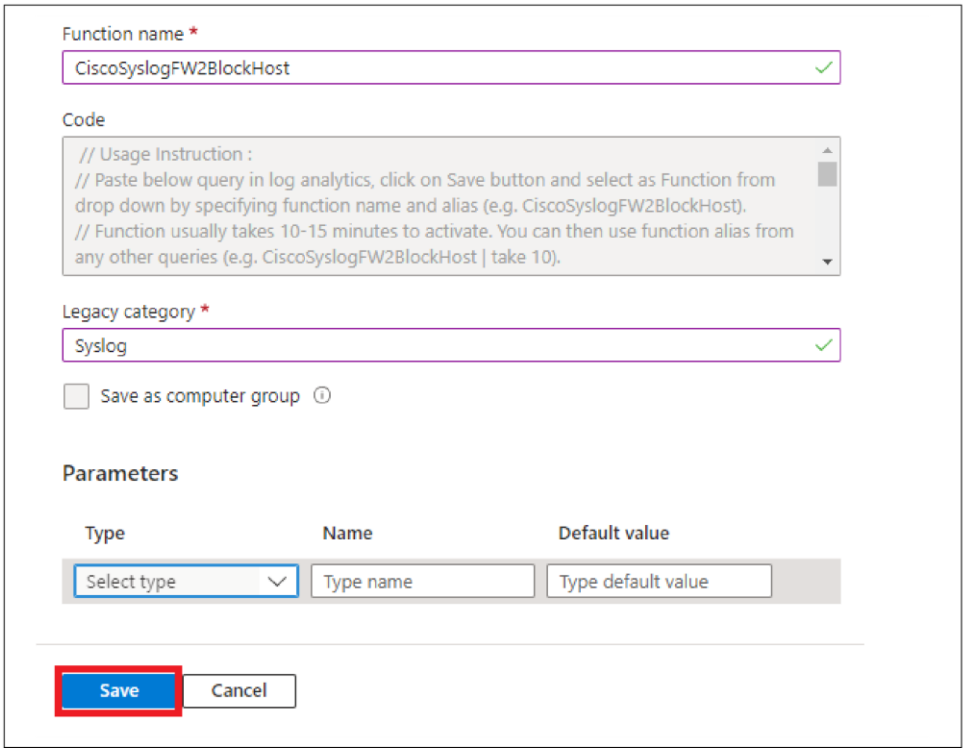
```
// Usage Instruction :
// Paste below query in log analytics, click on Save button and select as Function from drop down by specifying function name and alias (e.g. CiscoSyslogFW2BlockHost).
// Function usually takes 10-15 minutes to activate. You can then use function alias from any other queries (e.g. CiscoSyslogFW2BlockHost | take 10).
// References :
// Using functions in Azure monitor log queries : https://docs.microsoft.com/azure/azure-monitor/log-query/functions
// Tech Community Blog on KQL Functions : https://techcommunity.microsoft.com/t5/Azure-Sentinel/Using-KQL-functions-to-speed-up-analysis-in-Azure-Sentinel/ba-p/712381
//
let CiscoSyslogFW2BlockHost_view = view() {
    Syslog
    | where SyslogMessage has "%FW-2-BLOCK_HOST:"
    | extend FieldList = extract_all(@"\S{3}\s+\d{1,2}\s[^\s]+\s%(?P<type>[^:\s]+).*%(?P<sub_type>[^:\s]+).*\(target:class\)-\((?P<target>[^\s\)\(:]+)\:(?P<class>[^\s\:\)]+).*host\s(?P<blocked_host>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}).*count\s(?P<total_blocked_connections>\d+)", dynamic(['type', 'sub_type', 'target', 'class', 'blocked_host', 'total_blocked_connections']), SyslogMessage)
    | extend
        SyslogType = tostring(FieldList[0][0]),
        SyslogSubType = tostring(FieldList[0][1]),
```

- Click **Save as function**.



```
// Usage Instruction :
// Paste below query in log analytics, click on Save button and se    p down by specifying function name and alias (e.g.
CiscoSyslogFW2BlockHost).
// Function usually takes 10-15 minutes to activate. You can then    y other queries (e.g. CiscoSyslogFW2BlockHost | take 10)
.
```

- Enter the function name exactly as provided in the query's function name. Provide any other necessary details and click **Save.**



Function name *

CiscoSyslogFW2BlockHost

Code

```
// Usage Instruction :
// Paste below query in log analytics, click on Save button and select as Function from drop down by specifying function name and alias (e.g. CiscoSyslogFW2BlockHost).
// Function usually takes 10-15 minutes to activate. You can then use function alias from any other queries (e.g. CiscoSyslogFW2BlockHost | take 10).
```

Legacy category *

Syslog

□ Save as computer group

Parameters

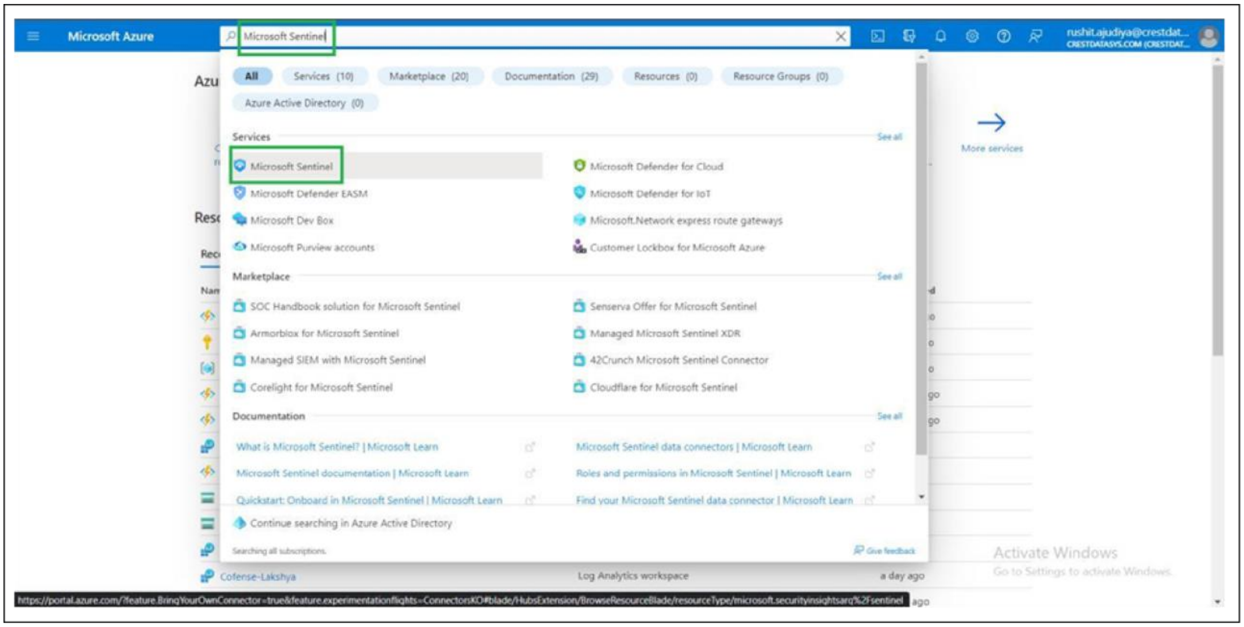
Type	Name	Default value
Select type	Type name	Type default value

Note:

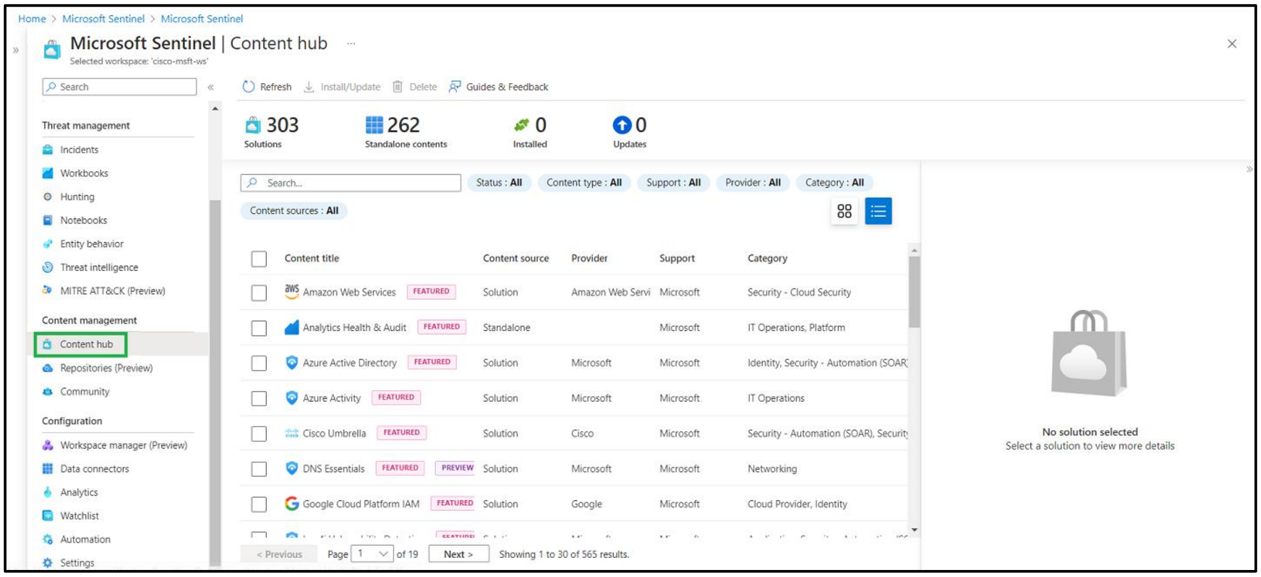
- To add other parsers that are in the Parsers directory, follow the above steps as needed.

Steps to deploy a Cisco Catalyst SD-WAN Sentinel analytic rule

- Log in to the Azure portal (https://portal.azure.com/#home) using the MS Azure credentials.
- Search for the **Microsoft Sentinel** service in the Azure portal search bar and select it.

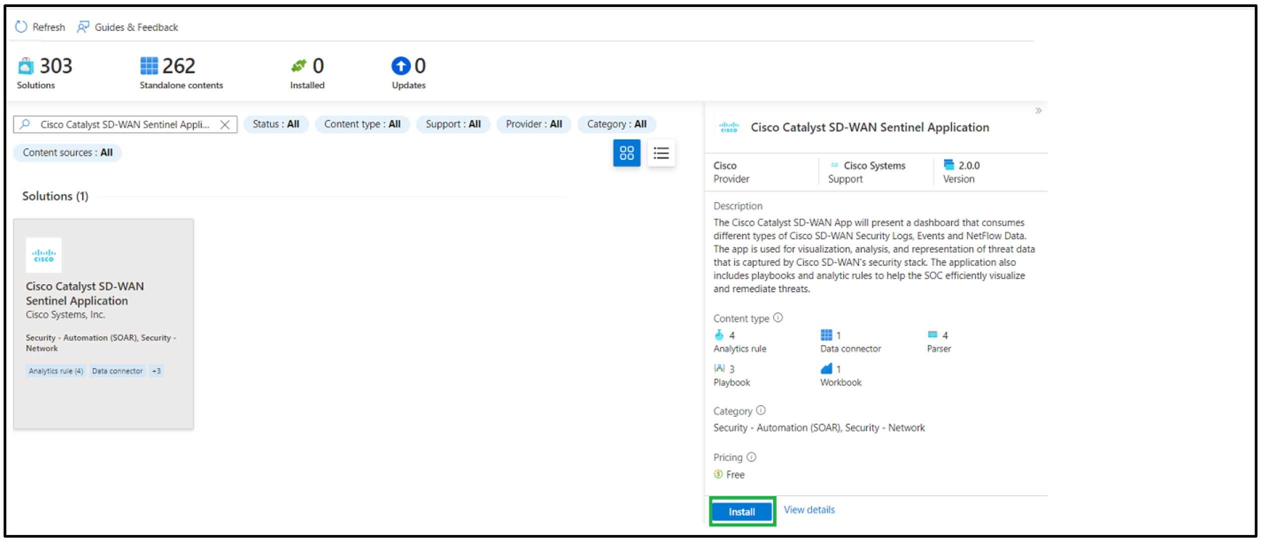

Microsoft Azure
Microsoft Sentinel
All
Services (10)
Marketplace (20)
Documentation (29)
Resources (0)
Resource Groups (0)
Azure Active Directory (0)
Services
See all
Microsoft Sentinel
Microsoft Defender for Cloud
Microsoft Defender EASM
Microsoft Defender for IoT
Microsoft Dev Box
Microsoft.Network express route gateways
Microsoft Purview accounts
Customer Lockbox for Microsoft Azure
Marketplace
See all
SOC Handbook solution for Microsoft Sentinel
Senserva Offer for Microsoft Sentinel
Armorblox for Microsoft Sentinel
Managed Microsoft Sentinel XDR
Managed SIEM with Microsoft Sentinel
42Crunch Microsoft Sentinel Connector
Corelight for Microsoft Sentinel
Cloudflare for Microsoft Sentinel
Documentation
See all
What is Microsoft Sentinel? | Microsoft Learn
Microsoft Sentinel data connectors | Microsoft Learn
Microsoft Sentinel documentation | Microsoft Learn
Roles and permissions in Microsoft Sentinel | Microsoft Learn
Quickstart: Onboard in Microsoft Sentinel | Microsoft Learn
Find your Microsoft Sentinel data connector | Microsoft Learn
Continue searching in Azure Active Directory
Searching all subscriptions.
Give feedback
More services
Cofense-Lakshya
Log Analytics workspace
a day ago
Activate Windows
Go to Settings to activate Windows.
https://portal.azure.com/?feature.BringYourOwnConnector=true&feature.experimentationflights=ConnectorsKO#blade/HubsExtension/BrowseResourceBlade/resourceType/microsoft.securityinsightsarg%2Fsentinel

- Select the Microsoft Sentinel workspace in which you want to deploy the solution.
- In the left panel, scroll down and select **Content Hub**.
- Use the search bar in Content Hub to look for the solution. Once the solution is certified in GitHub, it will become available in the Content Hub.



Content title	Content source	Provider	Support	Category
Amazon Web Services FEATURED	Solution	Amazon Web Servi	Microsoft	Security - Cloud Security
Analytics Health & Audit FEATURED	Standalone		Microsoft	IT Operations, Platform
Azure Active Directory FEATURED	Solution	Microsoft	Microsoft	Identity, Security - Automation (SOAR
Azure Activity FEATURED	Solution	Microsoft	Microsoft	IT Operations
Cisco Umbrella FEATURED	Solution	Cisco	Microsoft	Security - Automation (SOAR), Securit
DNS Essentials FEATURED PREVIEW	Solution	Microsoft	Microsoft	Networking
Google Cloud Platform IAM FEATURED	Solution	Google	Microsoft	Cloud Provider, Identity

- Click on your solution and from the right panel click **Install**.



303 Solutions | 262 Standalone contents | 0 Installed | 0 Updates

Cisco Catalyst SD-WAN Sentinel Appli... | Status : All | Content type : All | Support : All | Provider : All | Category : All | Content sources : All

Solutions (1)

Cisco Catalyst SD-WAN Sentinel Application
Cisco Systems, Inc.
Security - Automation (SOAR), Security - Network
Analytics rule (4) | Data connector | +3

Cisco Catalyst SD-WAN Sentinel Application

Cisco Provider | Cisco Systems Support | 2.0.0 Version

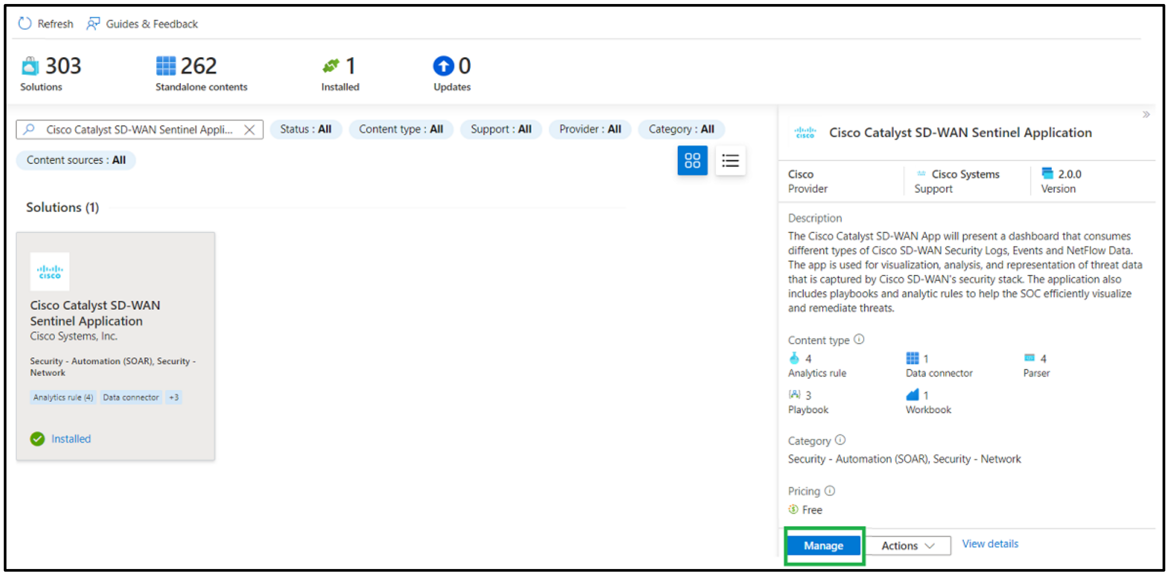
Description
The Cisco Catalyst SD-WAN App will present a dashboard that consumes different types of Cisco SD-WAN Security Logs, Events and NetFlow Data. The app is used for visualization, analysis, and representation of threat data that is captured by Cisco SD-WAN's security stack. The application also includes playbooks and analytic rules to help the SOC efficiently visualize and remediate threats.

Content type
4 Analytics rule | 1 Data connector | 4 Parser
3 Playbook | 1 Workbook

Category
Security - Automation (SOAR), Security - Network

Pricing
Free

- Now go to Content Hub from the Microsoft Sentinel workspace and search for the solution you have installed. It will show the status as installed; click **Manage** in the right panel.



303 Solutions | 262 Standalone contents | 1 Installed | 0 Updates

Cisco Catalyst SD-WAN Sentinel Appli... | Status : All | Content type : All | Support : All | Provider : All | Category : All | Content sources : All

Solutions (1)

Cisco Catalyst SD-WAN Sentinel Application
Cisco Systems, Inc.
Security - Automation (SOAR), Security - Network
Analytics rule (4) | Data connector | +3
Installed

Cisco Catalyst SD-WAN Sentinel Application

Cisco Provider | Cisco Systems Support | 2.0.0 Version

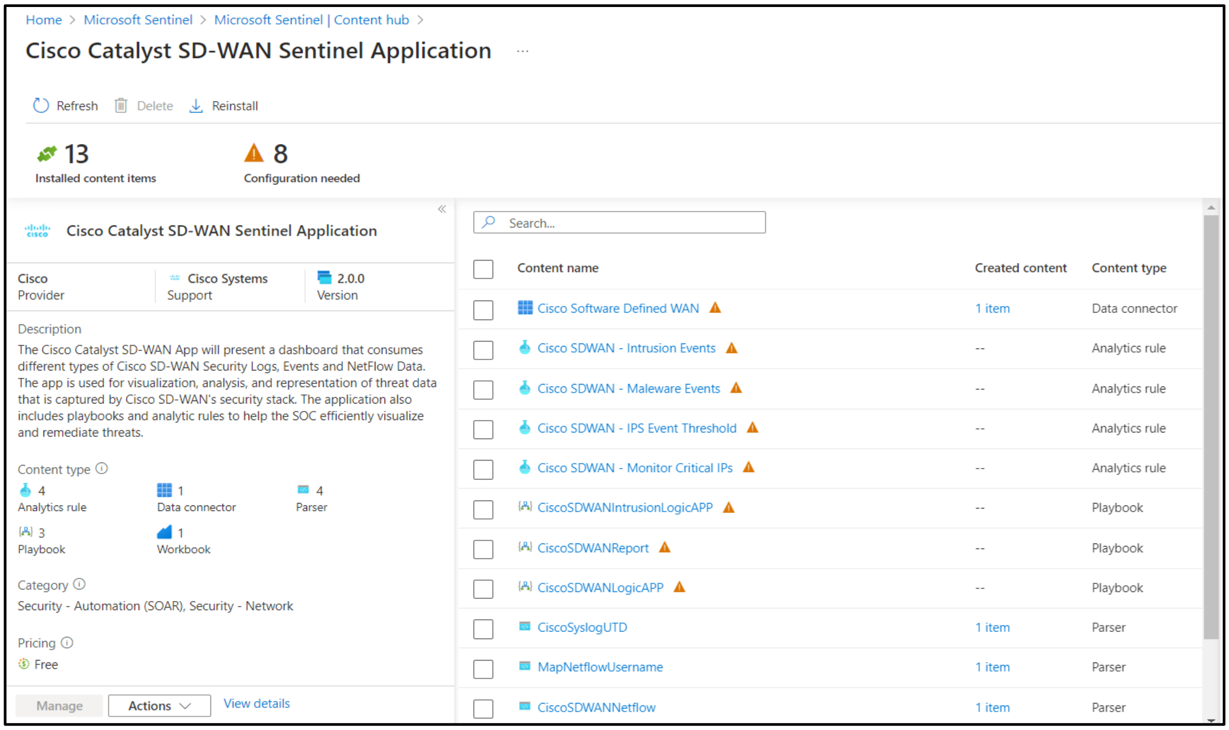
Description
The Cisco Catalyst SD-WAN App will present a dashboard that consumes different types of Cisco SD-WAN Security Logs, Events and NetFlow Data. The app is used for visualization, analysis, and representation of threat data that is captured by Cisco SD-WAN's security stack. The application also includes playbooks and analytic rules to help the SOC efficiently visualize and remediate threats.

Content type
4 Analytics rule | 1 Data connector | 4 Parser
3 Playbook | 1 Workbook

Category
Security - Automation (SOAR), Security - Network

Pricing
Free

- In the Cisco Catalyst SD-WAN solution, four parsers, one workbook, four analytic rules, and three playbooks will be available.



Home > Microsoft Sentinel > Microsoft Sentinel | Content hub >

Cisco Catalyst SD-WAN Sentinel Application ···

Refresh | Delete | Reinstall

13 Installed content items | 8 Configuration needed

Cisco Catalyst SD-WAN Sentinel Application

Cisco Provider	Cisco Systems Support	2.0.0 Version

Description

The Cisco Catalyst SD-WAN App will present a dashboard that consumes different types of Cisco SD-WAN Security Logs, Events and NetFlow Data. The app is used for visualization, analysis, and representation of threat data that is captured by Cisco SD-WAN's security stack. The application also includes playbooks and analytic rules to help the SOC efficiently visualize and remediate threats.

Content type

4 Analytics rule	1 Data connector	4 Parser
3 Playbook	1 Workbook	

Category

Security - Automation (SOAR), Security - Network

Pricing

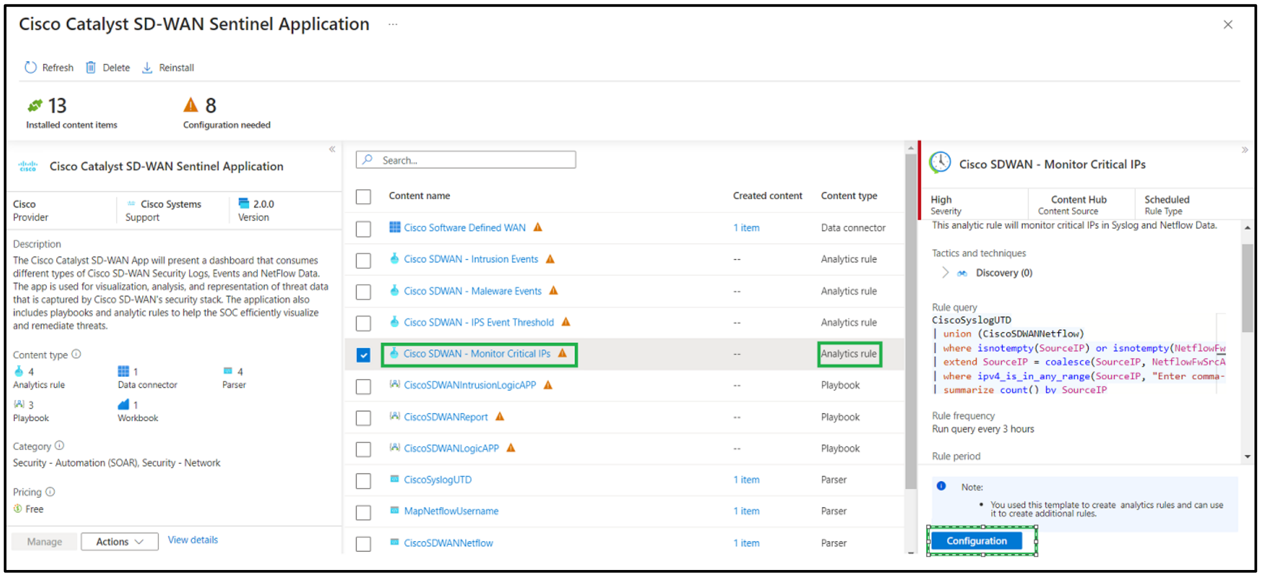
Free

Manage | Actions | View details

Search...

□	Content name	Created content	Content type
□	Cisco Software Defined WAN ⚠	1 item	Data connector
□	Cisco SDWAN - Intrusion Events ⚠	--	Analytics rule
□	Cisco SDWAN - Maleware Events ⚠	--	Analytics rule
□	Cisco SDWAN - IPS Event Threshold ⚠	--	Analytics rule
□	Cisco SDWAN - Monitor Critical IPs ⚠	--	Analytics rule
□	CiscoSDWANIntrusionLogicAPP ⚠	--	Playbook
□	CiscoSDWANReport ⚠	--	Playbook
□	CiscoSDWANLogicAPP ⚠	--	Playbook
□	CiscoSyslogUTD	1 item	Parser
□	MapNetflowUsername	1 item	Parser
□	CiscoSDWANNetflow	1 item	Parser

- Click the analytic rule you want to deploy and then click **Configure**.



Cisco Catalyst SD-WAN Sentinel Application ···

Refresh | Delete | Reinstall

13 Installed content items | 8 Configuration needed

Cisco Catalyst SD-WAN Sentinel Application

Cisco Provider	Cisco Systems Support	2.0.0 Version

Description

The Cisco Catalyst SD-WAN App will present a dashboard that consumes different types of Cisco SD-WAN Security Logs, Events and NetFlow Data. The app is used for visualization, analysis, and representation of threat data that is captured by Cisco SD-WAN's security stack. The application also includes playbooks and analytic rules to help the SOC efficiently visualize and remediate threats.

Content type

4 Analytics rule	1 Data connector	4 Parser
3 Playbook	1 Workbook	

Category

Security - Automation (SOAR), Security - Network

Pricing

Free

Manage | Actions | View details

Search...

□	Content name	Created content	Content type
□	Cisco Software Defined WAN ⚠	1 item	Data connector
□	Cisco SDWAN - Intrusion Events ⚠	--	Analytics rule
□	Cisco SDWAN - Maleware Events ⚠	--	Analytics rule
□	Cisco SDWAN - IPS Event Threshold ⚠	--	Analytics rule
☑	Cisco SDWAN - Monitor Critical IPs ⚠	--	Analytics rule
□	CiscoSDWANIntrusionLogicAPP ⚠	--	Playbook
□	CiscoSDWANReport ⚠	--	Playbook
□	CiscoSDWANLogicAPP ⚠	--	Playbook
□	CiscoSyslogUTD	1 item	Parser
□	MapNetflowUsername	1 item	Parser
□	CiscoSDWANNetflow	1 item	Parser

Cisco SDWAN - Monitor Critical IPs

High Severity	Content Hub Content Source	Scheduled Rule Type

This analytic rule will monitor critical IPs in Syslog and Netflow Data.

Tactics and techniques

Discovery (0)

Rule query

```
CiscoSyslogUTD
| union (CiscoSDWANNetflow)
| where isnotempty(SourceIP) or isnotempty(NetflowFw
| extend SourceIP = coalesce(SourceIP, NetflowFwSrcA
| where ipv4_is_in_any_range(SourceIP, "Enter comma-
| summarize count() by SourceIP
```

Rule frequency

Run query every 3 hours

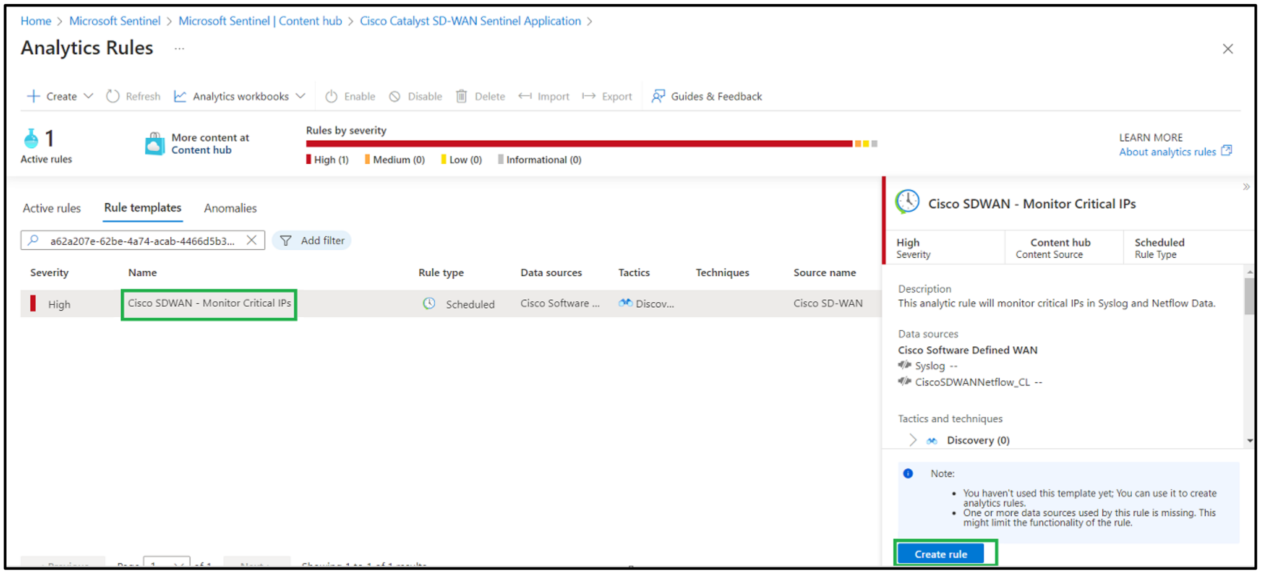
Rule period

Note:

- You used this template to create analytics rules and can use it to create additional rules.

Configuration

- Click the rule you want to deploy, then click **Create rule**.



Severity	Name	Rule type	Data sources	Tactics	Techniques	Source name
High	Cisco SDWAN - Monitor Critical IPs	Scheduled	Cisco Software ...	Discov...		Cisco SD-WAN

Cisco SDWAN - Monitor Critical IPs

High
Severity | Content hub
Content Source | Scheduled
Rule Type

Description
This analytic rule will monitor critical IPs in Syslog and Netflow Data.

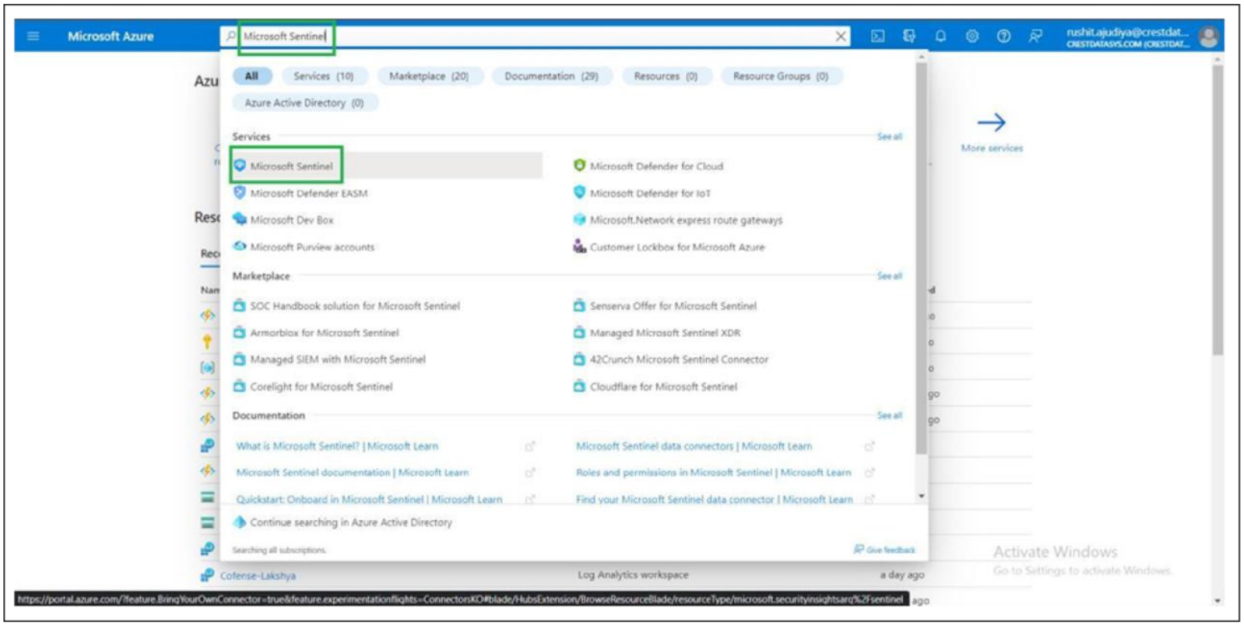
Data sources
Cisco Software Defined WAN
Syslog --
CiscoSDWANNetflow_CL --

Tactics and techniques
Discovery (0)

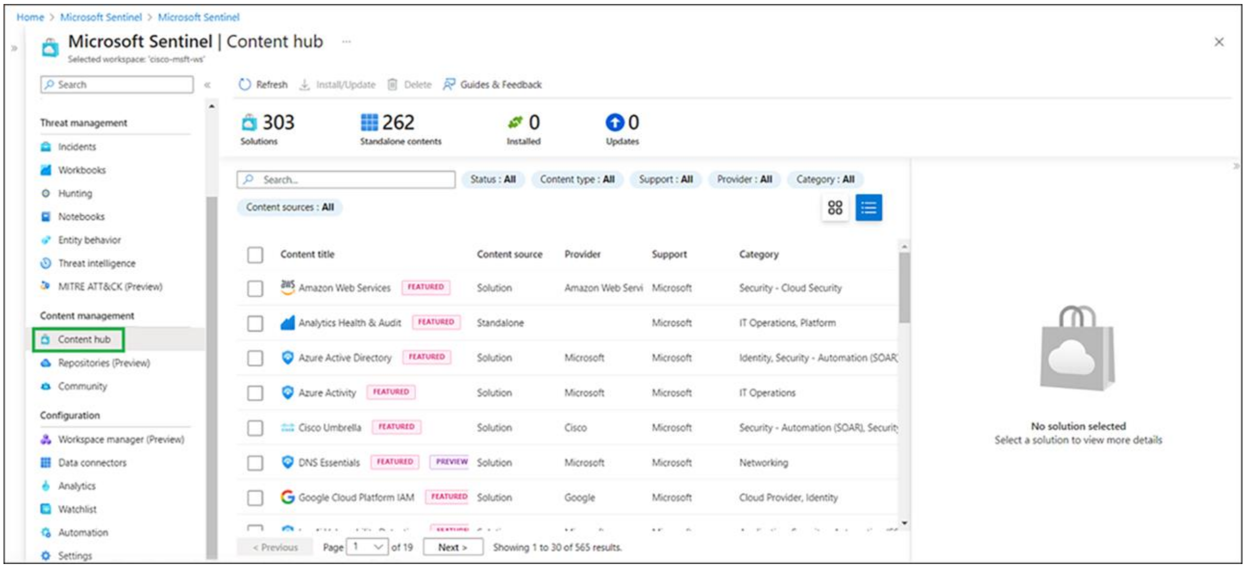
Note:
- You haven't used this template yet; You can use it to create analytics rules.
- One or more data sources used by this rule is missing. This might limit the functionality of the rule.

Steps to deploy a Cisco Catalyst SD-WAN Sentinel playbook

- Log in to the Azure portal (https://portal.azure.com/#home) using the MS Azure credentials.
- Search for the **Microsoft Sentinel** service in the Azure portal search bar and select it .


Microsoft Azure
Microsoft Sentinel
All
Services (10)
Marketplace (20)
Documentation (29)
Resources (0)
Resource Groups (0)
Azure Active Directory (0)
Services
See all
Microsoft Sentinel
Microsoft Defender EASM
Microsoft Dev Box
Microsoft Purview accounts
Microsoft Defender for Cloud
Microsoft Defender for IoT
Microsoft.Network express route gateways
Customer Lockbox for Microsoft Azure
Marketplace
SOC Handbook solution for Microsoft Sentinel
Armorblox for Microsoft Sentinel
Managed SIEM with Microsoft Sentinel
Corelight for Microsoft Sentinel
Senserva Offer for Microsoft Sentinel
Managed Microsoft Sentinel XDR
42Crunch Microsoft Sentinel Connector
Cloudflare for Microsoft Sentinel
Documentation
What is Microsoft Sentinel? | Microsoft Learn
Microsoft Sentinel documentation | Microsoft Learn
Quickstart: Onboard in Microsoft Sentinel | Microsoft Learn
Microsoft Sentinel data connectors | Microsoft Learn
Roles and permissions in Microsoft Sentinel | Microsoft Learn
Find your Microsoft Sentinel data connector | Microsoft Learn
Continue searching in Azure Active Directory
Searching all subscriptions.
Give feedback
More services
Cofense-Lakshya
Log Analytics workspace
a day ago
Activate Windows
Go to Settings to activate Windows.

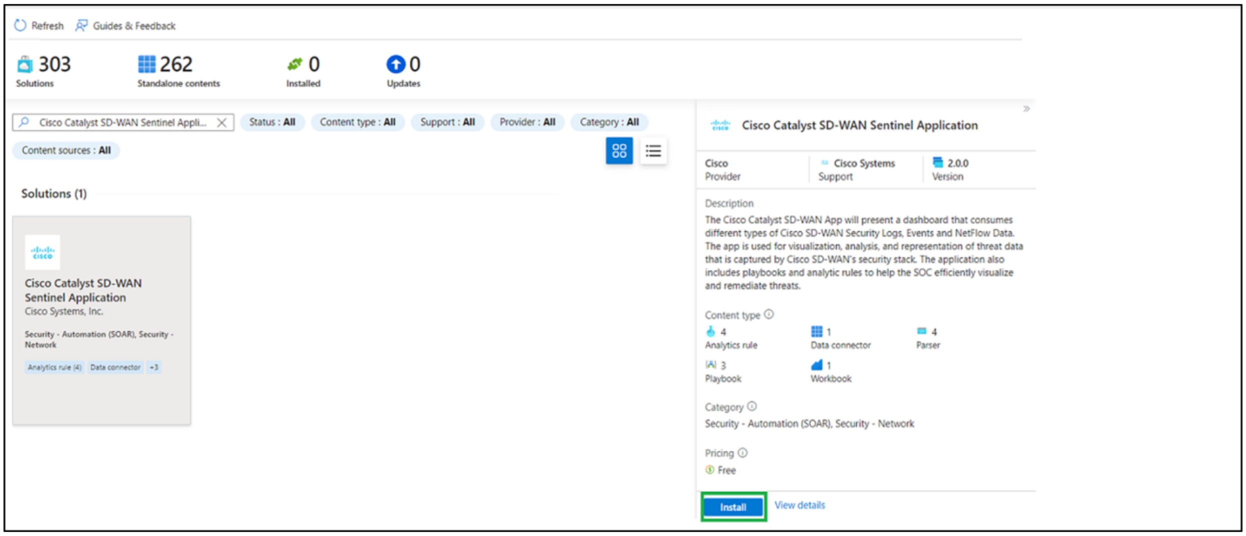
- Select the Microsoft Sentinel workspace in which you want to deploy the solution.
- In the left panel, scroll down and select **Content Hub**.
- Use the search bar in Content Hub to look for the solution. Once the solution is certified in GitHub, it will become available in Content Hub.



Content title	Content source	Provider	Support	Category
Amazon Web Services FEATURED	Solution	Amazon Web Servi	Microsoft	Security - Cloud Security
Analytics Health & Audit FEATURED	Standalone		Microsoft	IT Operations, Platform
Azure Active Directory FEATURED	Solution	Microsoft	Microsoft	Identity, Security - Automation (SOAR
Azure Activity FEATURED	Solution	Microsoft	Microsoft	IT Operations
Cisco Umbrella FEATURED	Solution	Cisco	Microsoft	Security - Automation (SOAR), Security
DNS Essentials FEATURED PREVIEW	Solution	Microsoft	Microsoft	Networking
Google Cloud Platform IAM FEATURED	Solution	Google	Microsoft	Cloud Provider, Identity

< Previous Page 1 of 19 Next > Showing 1 to 30 of 565 results.

- Click the solution, and from the right panel click **Install**.



Cisco Catalyst SD-WAN Sentinel Application

Provider: Cisco
Support: Cisco Systems
Version: 2.0.0

Description

The Cisco Catalyst SD-WAN App will present a dashboard that consumes different types of Cisco SD-WAN Security Logs, Events and NetFlow Data. The app is used for visualization, analysis, and representation of threat data that is captured by Cisco SD-WAN's security stack. The application also includes playbooks and analytic rules to help the SOC efficiently visualize and remediate threats.

Content type

4 Analytics rule
1 Data connector
4 Parser
3 Playbook
1 Workbook

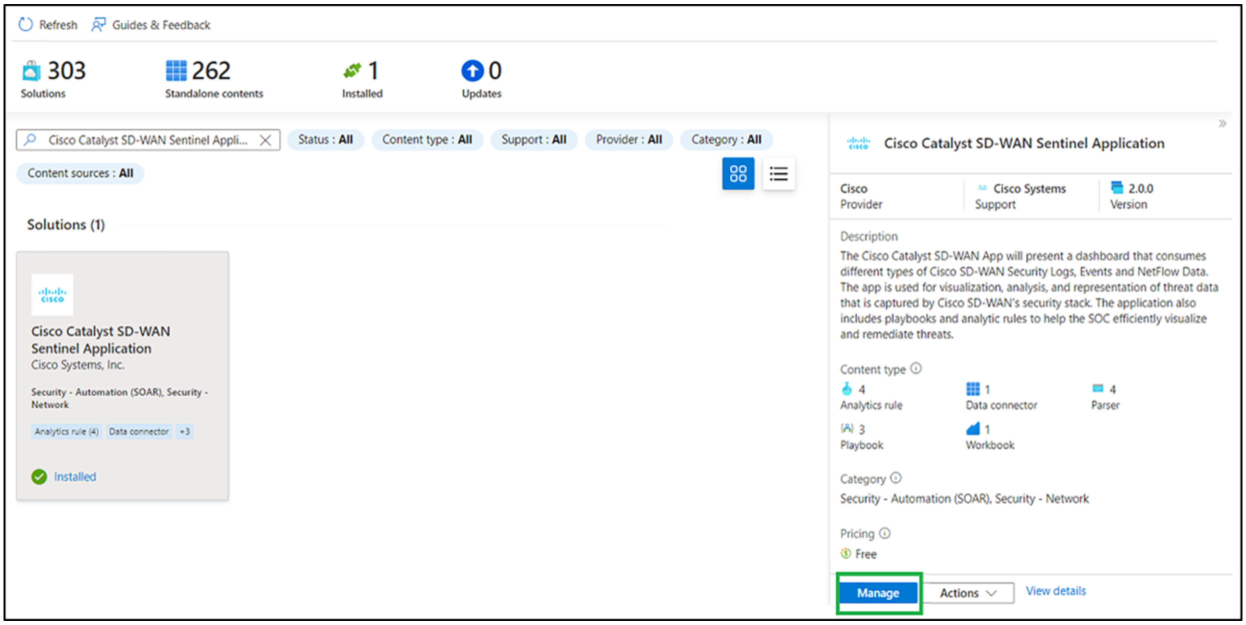
Category

Security - Automation (SOAR), Security - Network

Pricing

Free

- Now go to **Content Hub** from the Microsoft Sentinel workspace and search for the solution that you have installed. It will show the status as installed. Click **Manage** on the right panel.



303 Solutions | 262 Standalone contents | 1 Installed | 0 Updates

Solutions (1)

Cisco Catalyst SD-WAN Sentinel Application
Cisco Systems, Inc.
Security - Automation (SOAR), Security - Network
Installed

Cisco Catalyst SD-WAN Sentinel Application

Cisco Provider | Cisco Systems Support | 2.0.0 Version

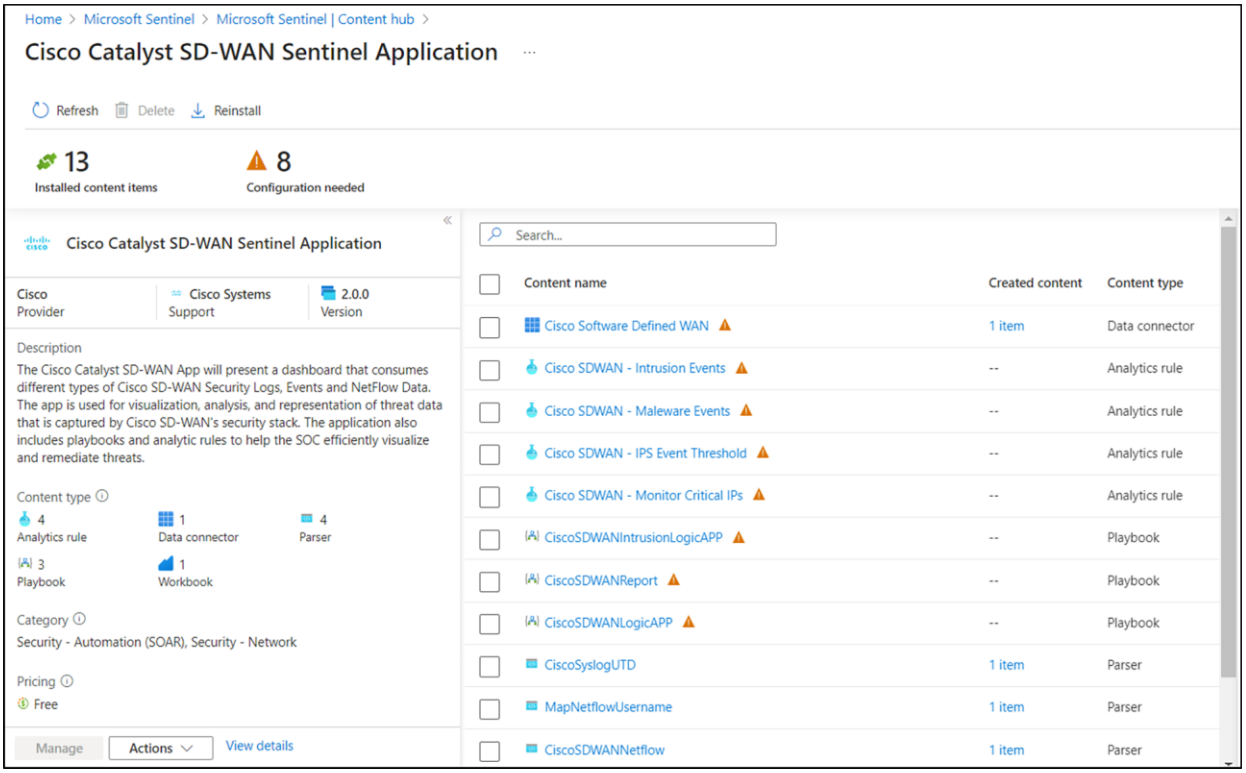
Description
The Cisco Catalyst SD-WAN App will present a dashboard that consumes different types of Cisco SD-WAN Security Logs, Events and NetFlow Data. The app is used for visualization, analysis, and representation of threat data that is captured by Cisco SD-WAN's security stack. The application also includes playbooks and analytic rules to help the SOC efficiently visualize and remediate threats.

Content type
4 Analytics rule | 1 Data connector | 4 Parser
3 Playbook | 1 Workbook

Category
Security - Automation (SOAR), Security - Network

Pricing
Free

- In the Cisco Catalyst SD-WAN solution, four parsers, one workbook, four analytic rules, and three playbooks will be available.


Home > Microsoft Sentinel > Microsoft Sentinel | Content hub >
Refresh
Delete
Reinstall
Search...
Manage
Actions
View details

Cisco Catalyst SD-WAN Sentinel Application

13 Installed content items | 8 Configuration needed

Cisco Catalyst SD-WAN Sentinel Application

Cisco Provider | Cisco Systems Support | 2.0.0 Version

Description
The Cisco Catalyst SD-WAN App will present a dashboard that consumes different types of Cisco SD-WAN Security Logs, Events and NetFlow Data. The app is used for visualization, analysis, and representation of threat data that is captured by Cisco SD-WAN's security stack. The application also includes playbooks and analytic rules to help the SOC efficiently visualize and remediate threats.

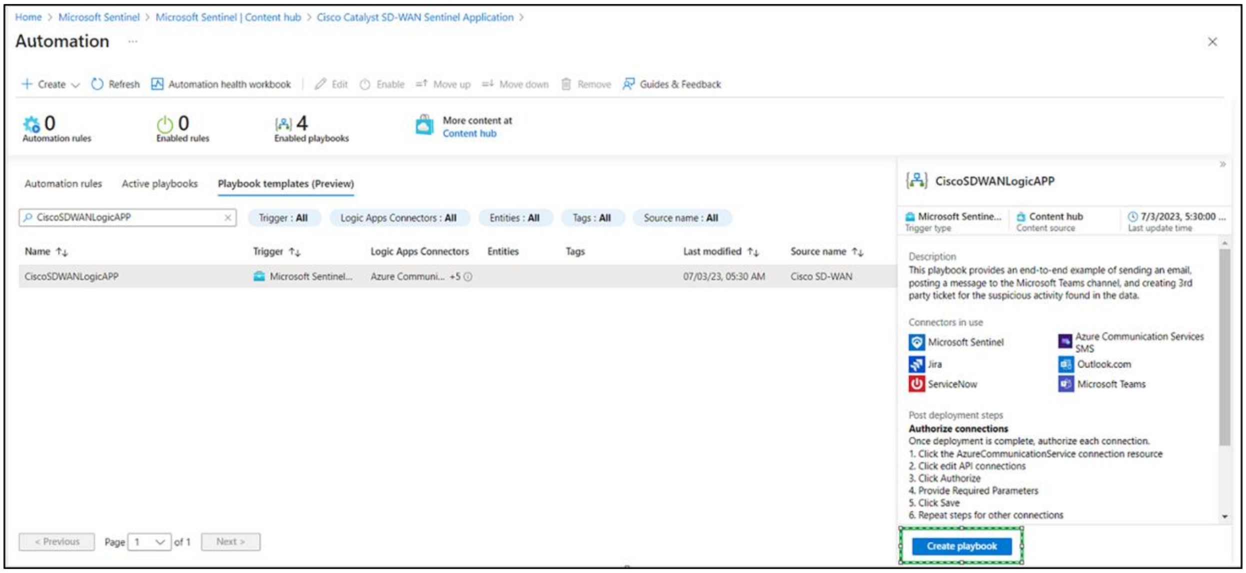
Content type
4 Analytics rule | 1 Data connector | 4 Parser
3 Playbook | 1 Workbook

Category
Security - Automation (SOAR), Security - Network

Pricing
Free

Content name	Created content	Content type
Cisco Software Defined WAN ⚠	1 item	Data connector
Cisco SDWAN - Intrusion Events ⚠	--	Analytics rule
Cisco SDWAN - Maleware Events ⚠	--	Analytics rule
Cisco SDWAN - IPS Event Threshold ⚠	--	Analytics rule
Cisco SDWAN - Monitor Critical IPs ⚠	--	Analytics rule
CiscoSDWANIntrusionLogicAPP ⚠	--	Playbook
CiscoSDWANReport ⚠	--	Playbook
CiscoSDWANLogicAPP ⚠	--	Playbook
CiscoSyslogUTD	1 item	Parser
MapNetflowUsername	1 item	Parser
CiscoSDWANNetflow	1 item	Parser

- On the next screen, go to the playbook template (preview) tab, search for the playbook name, select the playbook template, and click **Create playbook**.



Home > Microsoft Sentinel > Microsoft Sentinel | Content hub > Cisco Catalyst SD-WAN Sentinel Application >

Automation

0 Automation rules

0 Enabled rules

4 Enabled playbooks

More content at Content hub

Search: CiscoSDWANLogicAPP

Trigger : All | Logic Apps Connectors : All | Entities : All | Tags : All | Source name : All

Name	Trigger	Logic Apps Connectors	Entities	Tags	Last modified	Source name
CiscoSDWANLogicAPP	Microsoft Sentinel...	Azure Communi... +5			07/03/23, 05:30 AM	Cisco SD-WAN

CiscoSDWANLogicAPP

Microsoft Sentine... Trigger type | Content hub Content source | 7/3/2023, 5:30:00 ... Last update time

Description

This playbook provides an end-to-end example of sending an email, posting a message to the Microsoft Teams channel, and creating 3rd party ticket for the suspicious activity found in the data.

Connectors in use

Microsoft Sentinel, Azure Communication Services SMS, Jira, Outlook.com, ServiceNow, Microsoft Teams

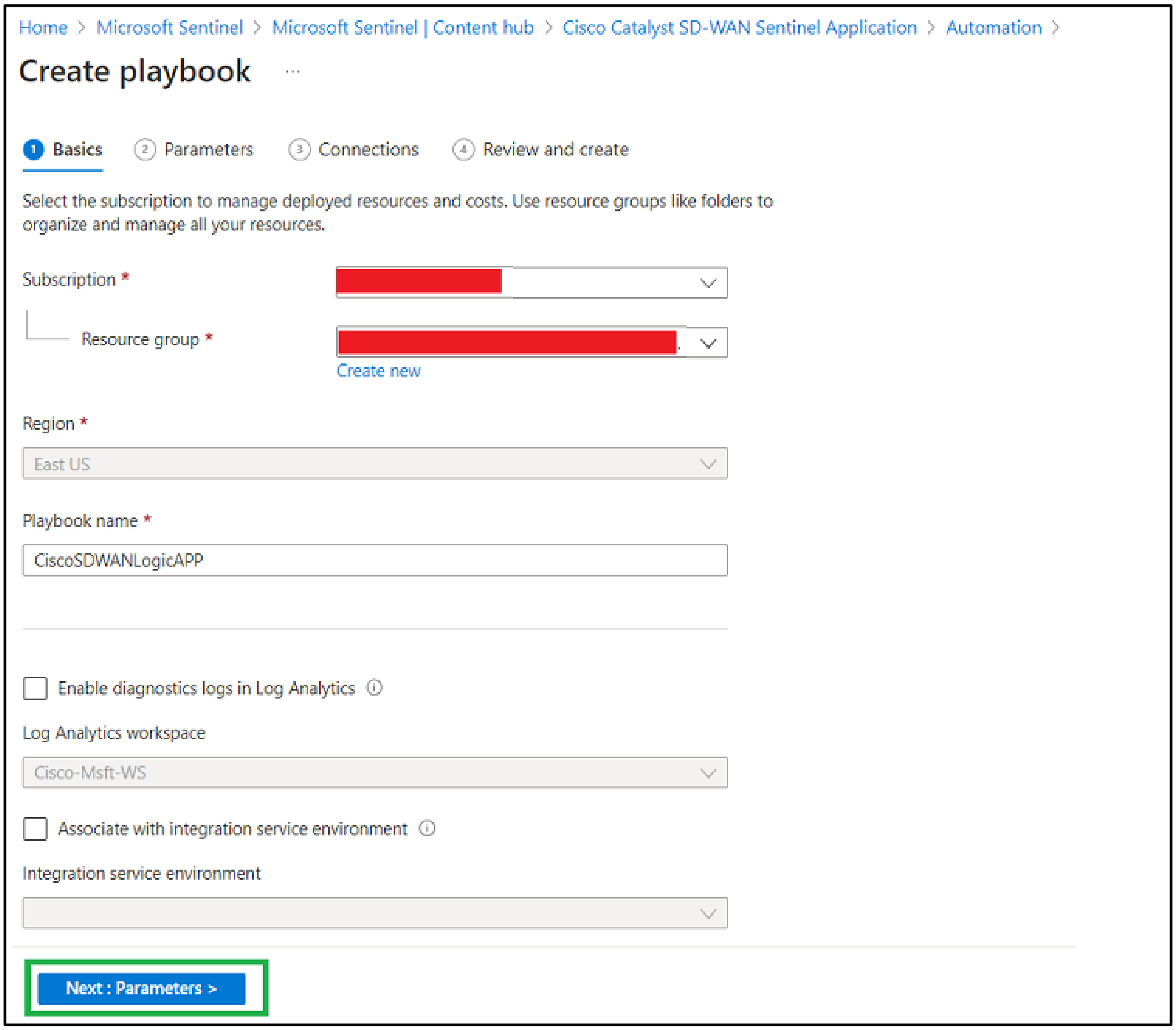
Post deployment steps

Authorize connections

Once deployment is complete, authorize each connection.

1. Click the AzureCommunicationService connection resource
2. Click edit API connections
3. Click Authorize
4. Provide Required Parameters
5. Click Save
6. Repeat steps for other connections

- Select the Subscription and Resource group and click **Next: Parameters**.



Home > Microsoft Sentinel > Microsoft Sentinel | Content hub > Cisco Catalyst SD-WAN Sentinel Application > Automation >

Create playbook

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * [redacted]

Resource group * [redacted]

Create new

Region * East US

Playbook name * CiscoSDWANLogicAPP

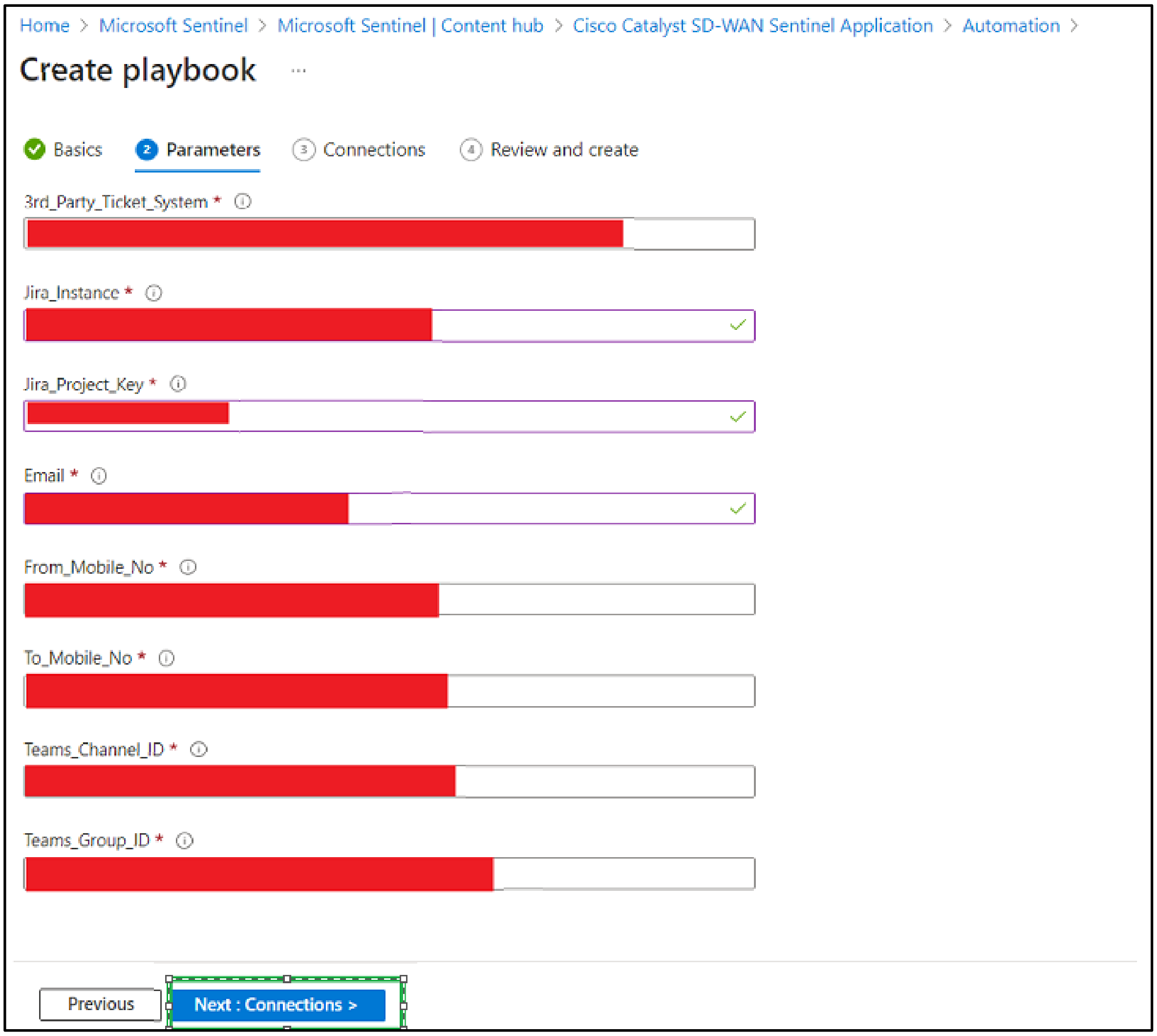
☐ Enable diagnostics logs in Log Analytics

Log Analytics workspace Cisco-Msft-WS

☐ Associate with integration service environment

Integration service environment

- Click **Next: Connections.**


Home > Microsoft Sentinel > Microsoft Sentinel | Content hub > Cisco Catalyst SD-WAN Sentinel Application > Automation >
Create playbook ...
Basics
2 Parameters
3 Connections
4 Review and create
Previous
Next : Connections >

3rd_Party_Ticket_System * ⓘ
[redacted]

Jira_Instance * ⓘ
[redacted] ✓

Jira_Project_Key * ⓘ
[redacted] ✓

Email * ⓘ
[redacted] ✓

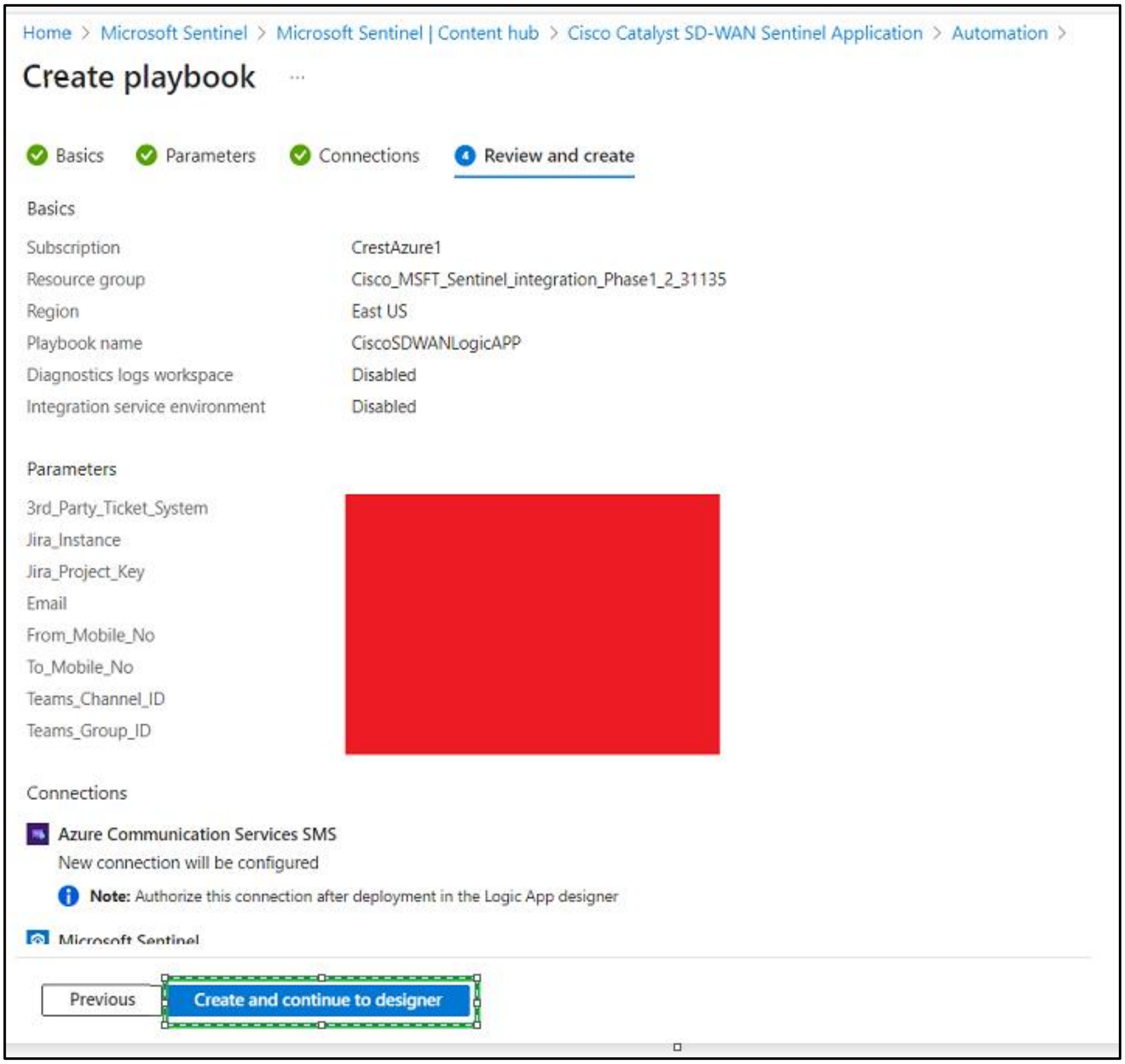
From_Mobile_No * ⓘ
[redacted]

To_Mobile_No * ⓘ
[redacted]

Teams_Channel_ID * ⓘ
[redacted]

Teams_Group_ID * ⓘ
[redacted]

- Keep the Connections tab as is. Click **Next: Review**.
- Click **Create and new to designer**.


Home > Microsoft Sentinel > Microsoft Sentinel | Content hub > Cisco Catalyst SD-WAN Sentinel Application > Automation >

Create playbook

Basics
Parameters
Connections
4 Review and create

Basics

Subscription	CrestAzure1
Resource group	Cisco_MSFT_Sentinel_integration_Phase1_2_31135
Region	East US
Playbook name	CiscoSDWANLogicAPP
Diagnostics logs workspace	Disabled
Integration service environment	Disabled

Parameters

3rd_Party_Ticket_System
Jira_Instance
Jira_Project_Key
Email
From_Mobile_No
To_Mobile_No
Teams_Channel_ID
Teams_Group_ID

[redacted]

Connections

Azure Communication Services SMS
New connection will be configured

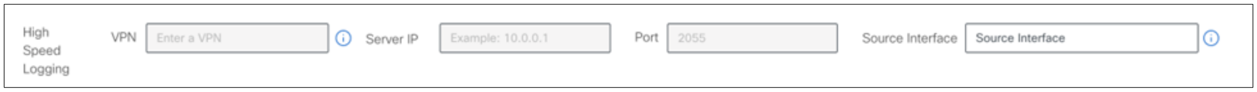
Note: Authorize this connection after deployment in the Logic App designer

Microsoft Sentinel

- Once deployment is complete, authorize each connection:
    - **Click the AzureCommunicationService connection resource.**
    - **Click Edit API connections.**
    - **Click Authorize.**
    - **Provide the required parameters.**
    - **Click Save.**
    - **Repeat these steps for other connections.**

Cisco Catalyst SD-WAN High Speed Logging (HSL) Records

The Sentinel application consumes HSL records (Netflow based) to populate the Zone Based Firewall (ZBFW) charts in the SOC Overview dashboard. To enable HSL, please follow the steps in the following link (step 5 of the link provided) https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/m-firewall-17.html#Cisco_Concept.dita_f1b319e6-ec37-49e7-b9ec-9720fa161fa6.



High Speed Logging

VPN: Enter a VPN

Server IP: Example: 10.0.0.1

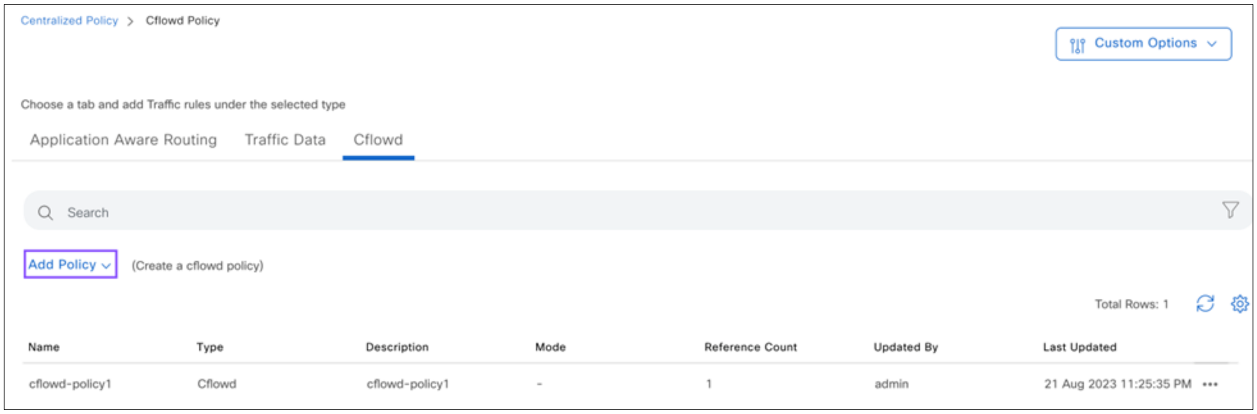
Port: 2055

Source Interface: Source Interface

Unified Security Logging

Unified Security Logs (Netflow based) are used to provide Username information and populate the ‘Top Policy Hits’ chart. To activate Unified Security Logging, enable the ‘Log’ flag under the Unified Security Policy summary page (step 7 of the below link) https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/m-firewall-17.html#Cisco_Concept.dita_f1b319e6-ec37-49e7-b9ec-9720fa161fa6.

After completing the aforementioned step, proceed to create a Cflowd Monitoring Policy using the below steps https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/ios-xe-17/policies-book-xe/traffic-flow-monitor.html#id_114091



Choose a tab and add Traffic rules under the selected type

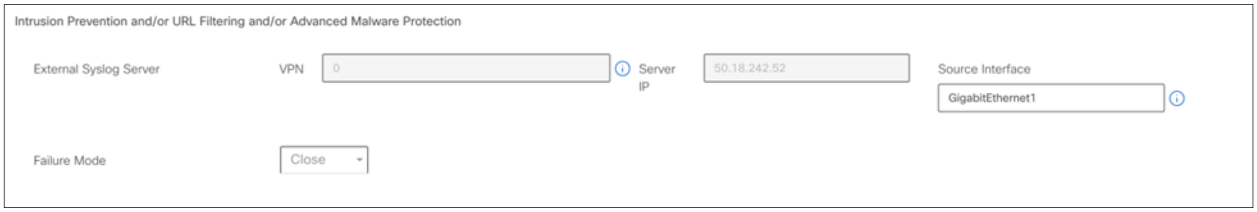
(Create a cflowd policy)

Total Rows: 1

Name	Type	Description	Mode	Reference Count	Updated By	Last Updated
cflowd-policy1	Cflowd	cflowd-policy1	-	1	admin	21 Aug 2023 11:25:35 PM

Syslog Configuration

The ‘Threat Inspection’ uses Syslog records to populate the dashboard charts. To configure syslog, follow step 12 of the following link https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/m-irewall-17.html#Cisco_Concept.dita_f1b319e6-ec37-49e7-b9ec-9720fa161fa6.



Intrusion Prevention and/or URL Filtering and/or Advanced Malware Protection

External Syslog Server

VPN: 0

Server IP: 50.18.242.52

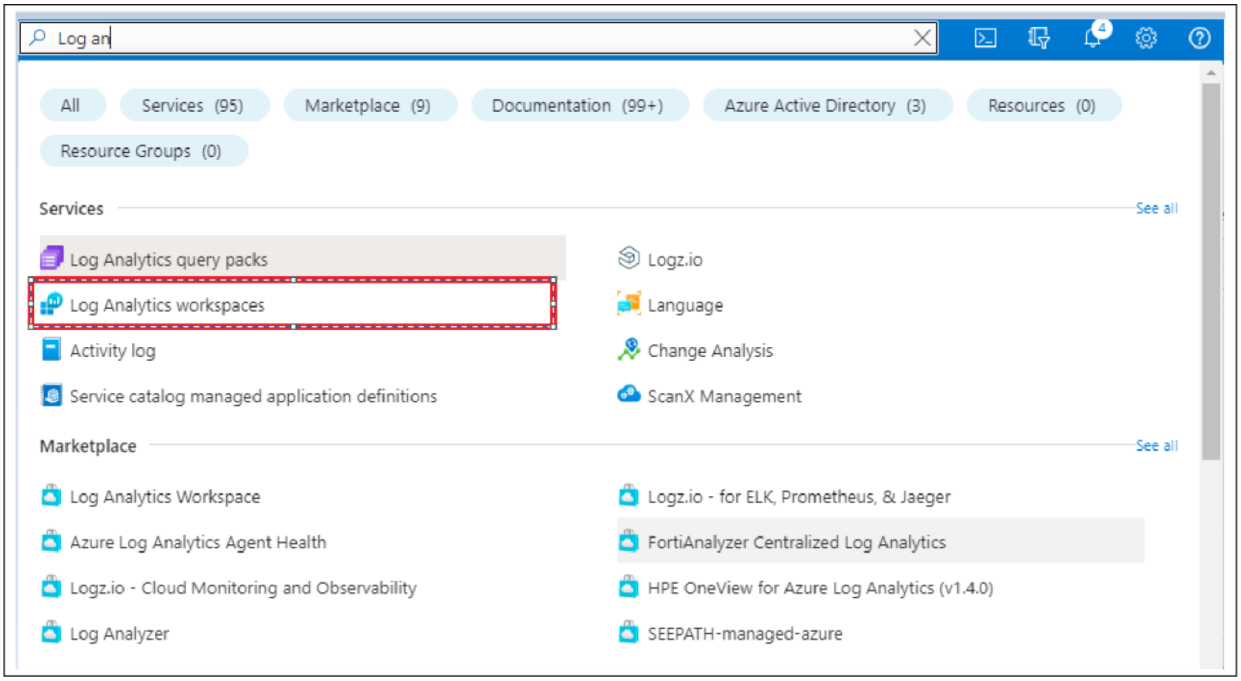
Source Interface: GigabitEthernet1

Failure Mode: Close

Usage

Locate the workspace

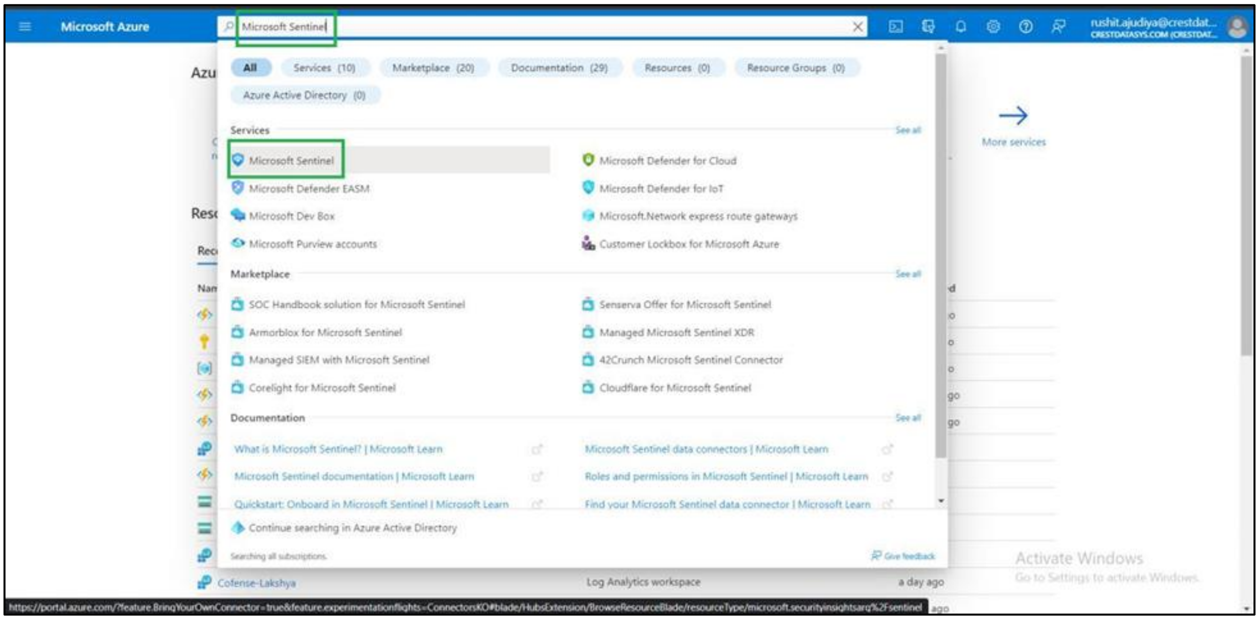
- Sign in to the Azure portal (https://portal.azure.com/#home).
- Search for the **Log Analytics workspaces** service in the Azure portal search bar and select it.


Log an
All
Services (95)
Marketplace (9)
Documentation (99+)
Azure Active Directory (3)
Resources (0)
Resource Groups (0)
Services
See all
Log Analytics query packs
Log Analytics workspaces
Activity log
Service catalog managed application definitions
Logz.io
Language
Change Analysis
ScanX Management
Marketplace
See all
Log Analytics Workspace
Azure Log Analytics Agent Health
Logz.io - Cloud Monitoring and Observability
Log Analyzer
Logz.io - for ELK, Prometheus, & Jaeger
FortiAnalyzer Centralized Log Analytics
HPE OneView for Azure Log Analytics (v1.4.0)
SEEPATH-managed-azure

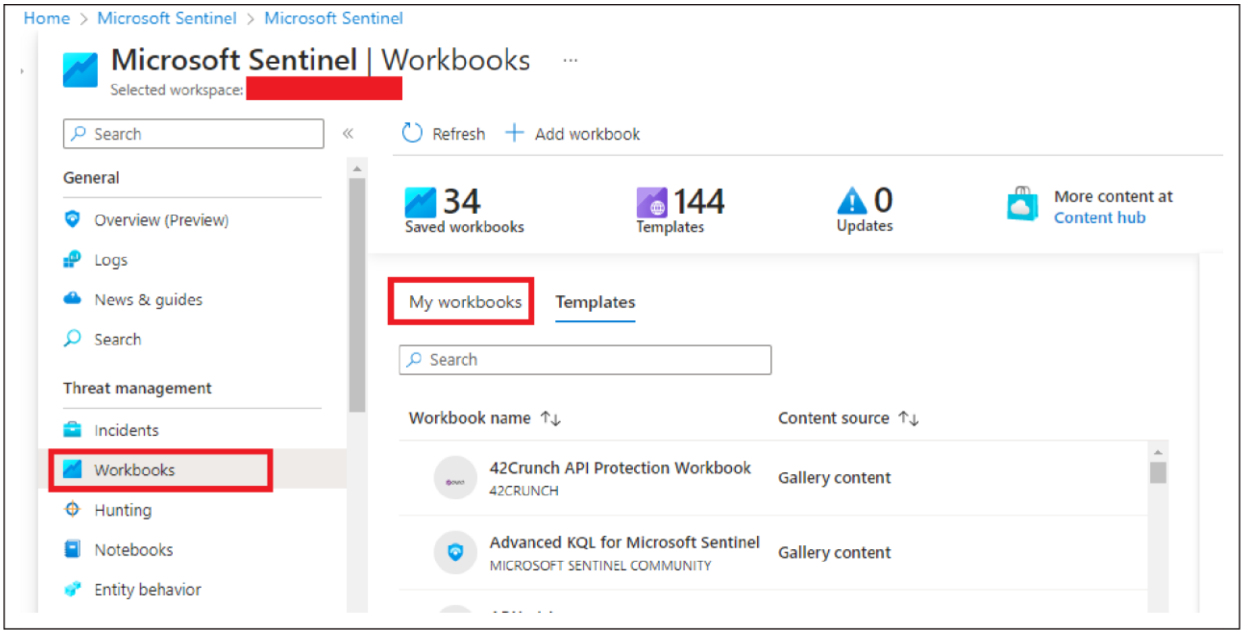
- Select the workspace where the NetFlow or syslog data is collected.

Locate the workbook

- Sign in to the Azure portal (https://portal.azure.com/#home).
- Search for the **Microsoft Sentinel** service in the Azure portal search bar and select it.


Microsoft Azure
Microsoft Sentinel
rushit.ajudiya@crestdat...
CRESTDATASYS.COM (CRESTDAT...
All
Services (10)
Marketplace (20)
Documentation (29)
Resources (0)
Resource Groups (0)
Azure Active Directory (0)
Services
See all
Microsoft Sentinel
Microsoft Defender EASM
Microsoft Dev Box
Microsoft Purview accounts
Microsoft Defender for Cloud
Microsoft Defender for IoT
Microsoft.Network express route gateways
Customer Lockbox for Microsoft Azure
Marketplace
See all
SOC Handbook solution for Microsoft Sentinel
Armorblox for Microsoft Sentinel
Managed SIEM with Microsoft Sentinel
Corelight for Microsoft Sentinel
Senserva Offer for Microsoft Sentinel
Managed Microsoft Sentinel XDR
42Crunch Microsoft Sentinel Connector
Cloudflare for Microsoft Sentinel
Documentation
See all
What is Microsoft Sentinel? | Microsoft Learn
Microsoft Sentinel documentation | Microsoft Learn
Quickstart: Onboard in Microsoft Sentinel | Microsoft Learn
Microsoft Sentinel data connectors | Microsoft Learn
Roles and permissions in Microsoft Sentinel | Microsoft Learn
Find your Microsoft Sentinel data connector | Microsoft Learn
Continue searching in Azure Active Directory
Searching all subscriptions.
Give feedback
More services
Cofense-Lakshya
Log Analytics workspace
a day ago
Activate Windows
Go to Settings to activate Windows.
https://portal.azure.com/?feature.BringYourOwnConnector=true&feature.experimentationflights=ConnectorsKO#blade/HubsExtension/BrowseResourceBlade/resourceType/microsoft.securityinsightsarg%2Fsentinel

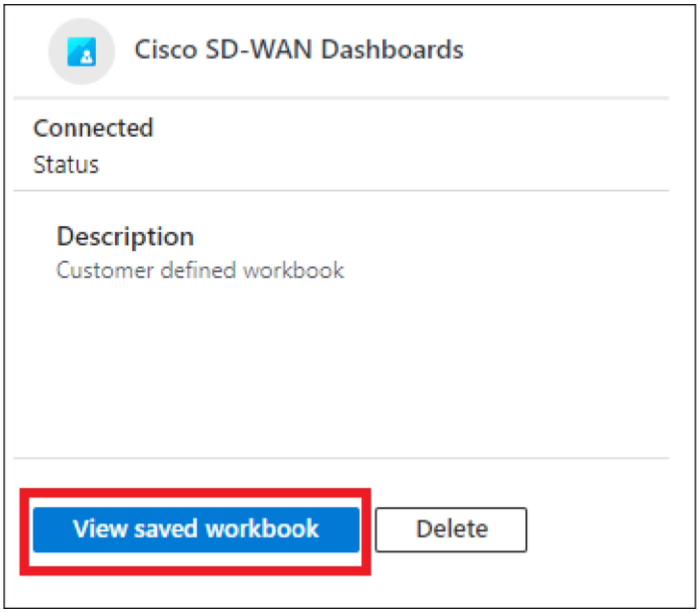
- Select the Microsoft Sentinel workspace in which you want to deploy the workbook.
- In the left panel, select **Workbooks** and then the **My Workbooks** tab.



Workbook name ↑↓	Content source ↑↓
42Crunch API Protection Workbook 42CRUNCH	Gallery content
Advanced KQL for Microsoft Sentinel MICROSOFT SENTINEL COMMUNITY	Gallery content

- Select the created workbook and click on the saved workbook.

[SR] > This does make sense as 'workbooks' here is located in multiple locations on the app

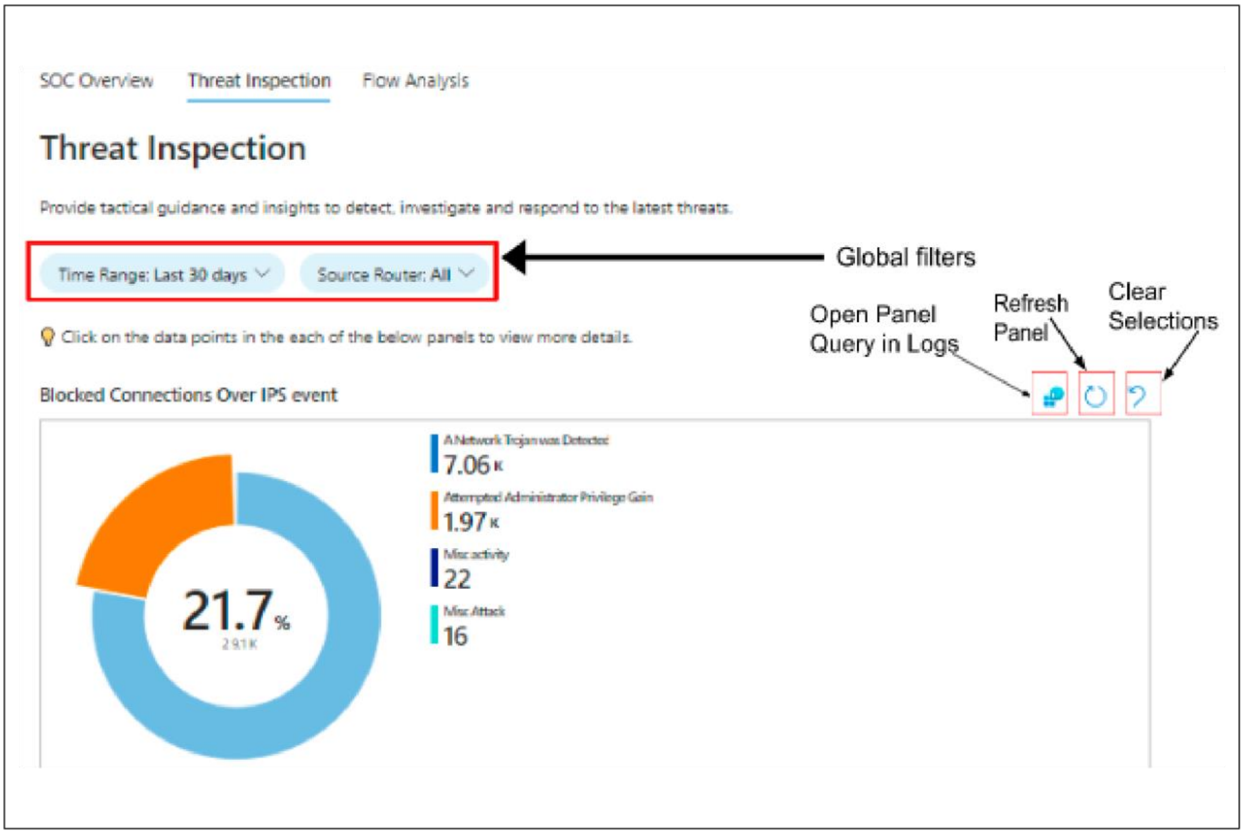


Cisco SD-WAN Dashboards

Connected
Status

Description
Customer defined workbook

Use the workbook



SOC Overview | Threat Inspection | Flow Analysis

Threat Inspection

Provide tactical guidance and insights to detect, investigate and respond to the latest threats.

Time Range: Last 30 days ˅ Source Router: All ˅

💡 Click on the data points in the each of the below panels to view more details.

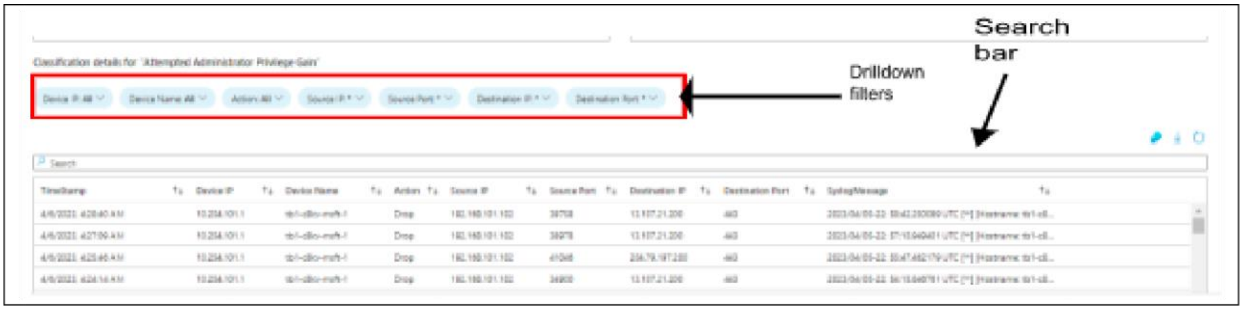
Blocked Connections Over IPS event

A Network Trojan was Detected 7.06 K

Attempted Administrator Privilege Gain 1.97 K

Misc activity 22

Misc Attack 16



Classification details for 'Attempted Administrator Privilege Gain'

Device IP: All ˅ Device Name: All ˅ Action: All ˅ Source IP: * ˅ Source Port: * ˅ Destination IP: * ˅ Destination Port: * ˅

Search

TimeStamp	Device IP	Device Name	Action	Source IP	Source Port	Destination IP	Destination Port	SyslogMessage
4/6/2023, 4:28:40 AM	10.234.101.1	sb1-dlo-mrft-l	Drop	192.168.101.102	39758	13.107.21.200	443	2023/04/05-22: 58:42.230080 UTC [**] [Hostname: sb1-c8...
4/6/2023, 4:27:09 AM	10.234.101.1	sb1-dlo-mrft-l	Drop	192.168.101.102	38978	13.107.21.200	443	2023/04/05-22: 57:10.949401 UTC [**] [Hostname: sb1-c8...
4/6/2023, 4:25:46 AM	10.234.101.1	sb1-dlo-mrft-l	Drop	192.168.101.102	41048	204.79.197.200	443	2023/04/05-22: 55:47.462179 UTC [**] [Hostname: sb1-c8...
4/6/2023, 4:24:14 AM	10.234.101.1	sb1-dlo-mrft-l	Drop	192.168.101.102	34900	13.107.21.200	443	2023/04/05-22: 54:15.840791 UTC [**] [Hostname: sb1-c8...

Limitations

Workbook

Table 3. Workbook Limitations

Visualization/parameter	Limits
Grid	Grids can display a maximum of 10,000 rows. Any further items are ignored, and a warning appears.
Charts	Charts are limited to 100 series. Charts are limited to 10,000 data points.
Maps	Maps are limited to displaying 100 points. Any further items are ignored, and a warning appears.
Drop-down	Drop-down-based parameters are limited to 1000 items. Any items returned by a query after that are ignored.
Drop-down	Drop-down is reset if no results are found in a particular time range, even though the default value is set.
Pie chart	In pie charts, whichever portion has the highest coverage is overridden. If the selected value has the highest coverage, it does not get overridden.

References

- Tutorial: Forward Syslog Data to a Log Analytics Workspace with Microsoft Sentinel by Using Azure Monitor Agent: https://learn.microsoft.com/en-us/azure/sentinel/forward-syslog-monitor-agent
- Quickstart: Connect Hybrid Machines with Azure Arc-Enabled Servers: https://learn.microsoft.com/en-us/azure/azure-arc/servers/learn/quick-enable-hybrid-vm
- Workbooks Result Limits: https://learn.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-limits

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C07-3773515-00 11/23