Vectra Detect (NDR) for Azure Sentinel AMA Configuration Guide

Version: April 2024

Table of Contents

Introduction

Vectra AI Detect for Microsoft Azure Sentinel v1.0 utilizes Microsoft OMS (Log Analytics) agent to collect event data from Vectra and send it to log analytics workspace. This agent is schedule for end-of-life August 31, 2024, and is replaced with the Azure Monitor Agent (AMA). This document explains how to configure Microsoft AMA to ingest Vectra event data into Microsoft Azure Sentinel Log Analytics.

Applicability

This document applies to environments where pre-existing deployments must migrate from OMS to AMA as well as for new deployments starting with AMA.

Architecture Summary

A data connector is deployed and configured to send Vectra data to log analytics. Once ingested into log analytics, Vectra data is stored in CEF format in the CommonSecurityLog. A workbook is included with the Vectra integration on the Content Hub and that workbook retrieves data from the CommonSecurityLog to provide the dashboards.

Existing deployments will enable and configure AMA and data will be ingested into the existing CommonSecurityLog. When operational, this will allow the OMS agent to be deprovisioned and while there may be some duplicate records during the time both OMS and AMA are running there should be no impact on any saved queries.

New deployments will need to enable and configure AMA and will need to install Vectra AI Detect from the content hub to obtain the Analytics Rules and Workbook but can simply ignore the OMS agent deployment instructions.

Pre-requisites

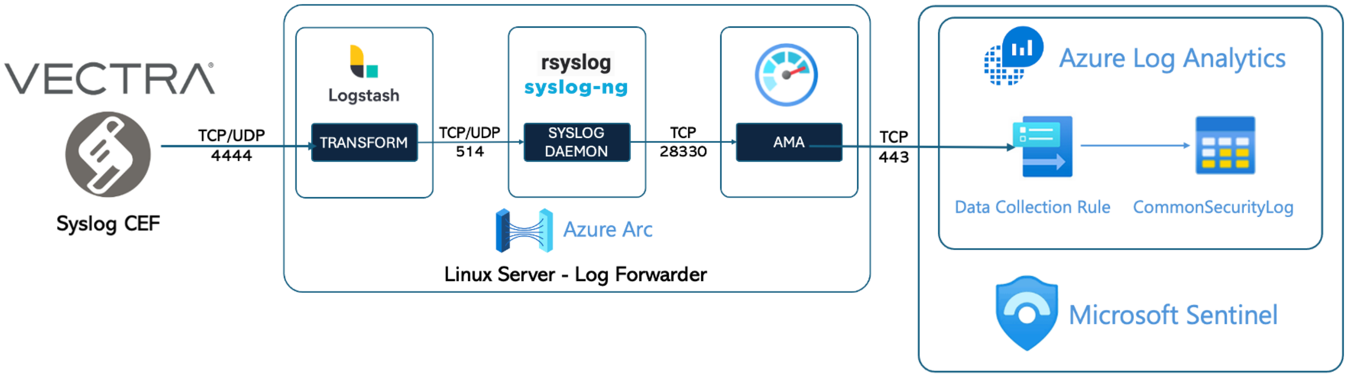
Microsoft Azure Monitor Agent (AMA) operates on an Azure Arc enabled Linux server. Vectra sends data in syslog CEF, so AMA requires rsyslog or syslog-ng on the Linux server.

Vectra provides syslog CEF data in a format that allows for backward compatibility with older syslog collectors (including OMS) but AMA doesn't support this format. To provide Vectra data in a compatible format for AMA, Logstash must be installed on the Linux server to perform the necessary transformation before handing off to rsyslog or syslog-ng.

In both scenarios, the following instructions require the log analytics workspace and associated resource groups are all configured and known.

Configuration Method: Logstash Transform

Using Logstash to transform the Vectra syslog messages is the preferred approach as it by provides the most flexibility. This method allows the operator to use their preferred syslog receiver (rsyslog or syslog-ng) and enables the Vectra data to be directed to a dedicated port so there is no possibility of conflict (erroneous transforms) when the Linux server is responsible for multiple data collectors.

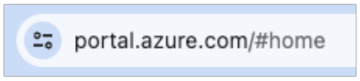


Install Arc Agent

The Linux log server that will be used to run AMA must be connected to Azure via the Arc machine agent.
If the machine is already connected to Azure using Azure Arc, this section can be skipped.

Start with an operable Linux server that has rsyslog installed and running.

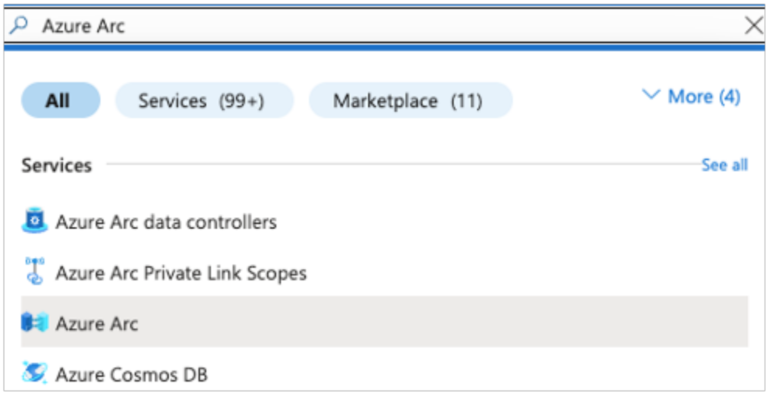
Access the Azure Portal



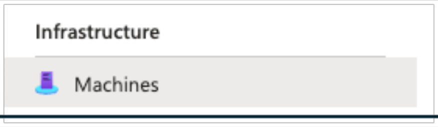
portal.azure.com/#home

Search resources for Azure Arc

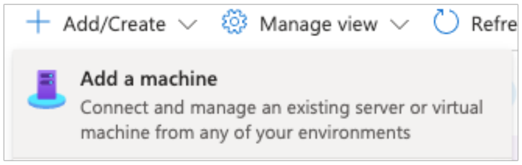
Select Azure Arc from the list



Select Machines from left-hand window

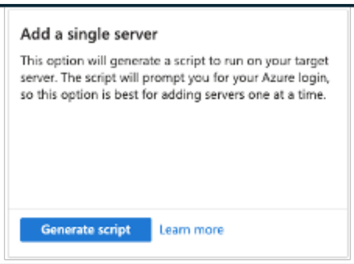


From Add/Create drop-down menu select Add a machine



Connect and manage an existing server or virtual machine from any of your environments

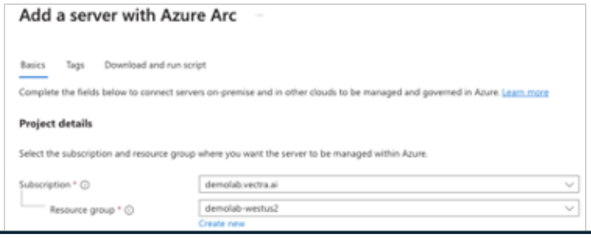
Select Generate script from Add a single server



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.

Enter appropriate Project details



Add a server with Azure Arc

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

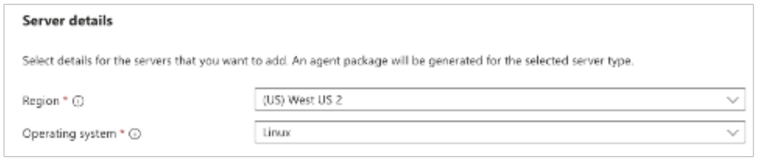
Project details

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

Subscription * : demolab.vectra.ai

Resource group * : demolab-westus2

Enter Server details



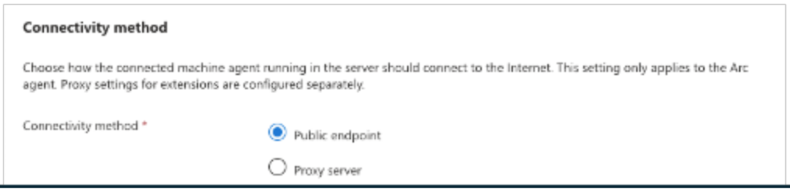
Server details

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

Region * : (US) West US 2

Operating system * : Linux

Select Connectivity method



Connectivity method

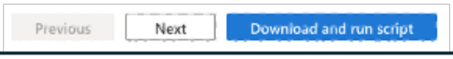
Choose how the connected machine agent running in the server should connect to the Internet. This setting only applies to the Arc agent. Proxy settings for extensions are configured separately.

Connectivity method *

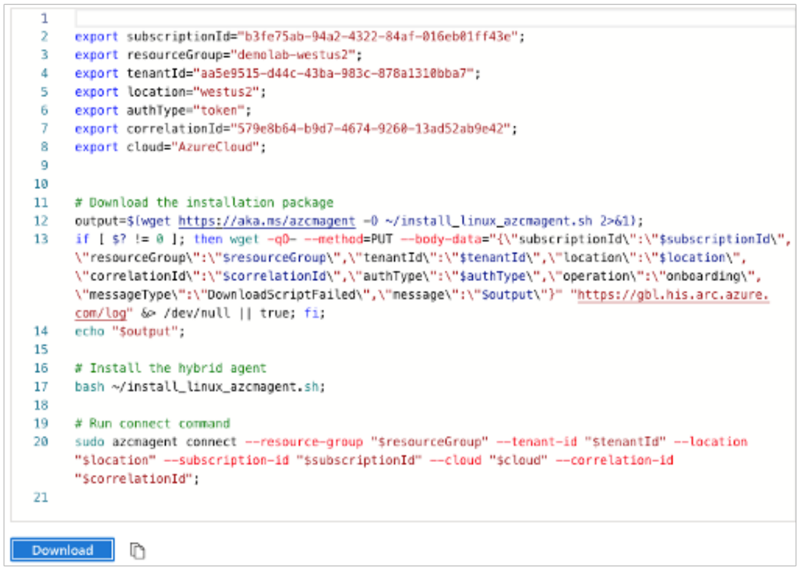
● Public endpoint

○ Proxy server

Select Download and run script

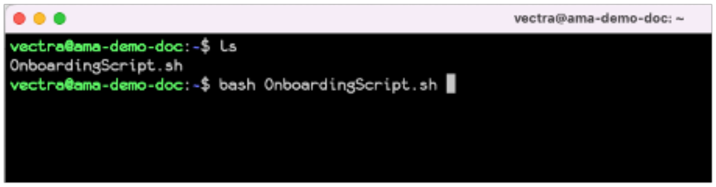


Download or copy the script code



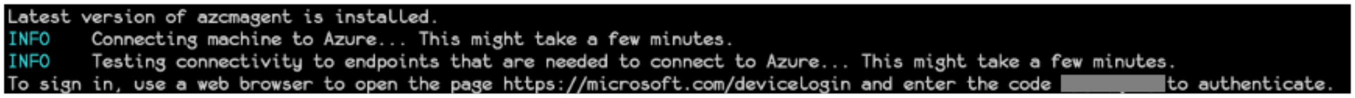
```

export subscriptionId="b3fe75ab-94a2-4322-84af-016eb01ff43e";
export resourceGroup="demolab-westus2";
export tenantId="aa5e9515-d44c-43ba-983c-878a1310bba7";
export location="westus2";
export authType="token";
export correlationId="579e8b64-b9d7-4674-9260-13ad52ab9e42";
export cloud="AzureCloud";


# Download the installation package
output=$(wget https://aka.ms/azcmagent -O ~/install_linux_azcmagent.sh 2>&1);
if [ $? != 0 ]; then wget -qO- --method=PUT --body-data="{\"subscriptionId\":\"$subscriptionId\",
\"resourceGroup\":\"$resourceGroup\",\"tenantId\":\"$tenantId\",\"location\":\"$location\",
\"correlationId\":\"$correlationId\",\"authType\":\"$authType\",\"operation\":\"onboarding\",
\"messageType\":\"DownloadScriptFailed\",\"message\":\"$output\"}" "https://gbl.his.arc.azure.
com/log" &> /dev/null || true; fi;
echo "$output";

# Install the hybrid agent
bash ~/install_linux_azcmagent.sh;

# Run connect command
sudo azcmagent connect --resource-group "$resourceGroup" --tenant-id "$tenantId" --location
"$location" --subscription-id "$subscriptionId" --cloud "$cloud" --correlation-id
"$correlationId";

```

Connect to your Linux server and upload the script and then run it



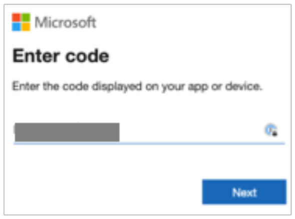
```
vectra@ama-demo-doc: ~
vectra@ama-demo-doc:~$ ls
OnboardingScript.sh
vectra@ama-demo-doc:~$ bash OnboardingScript.sh
```

When prompted, navigate to the URL provided and enter the code to authenticate



```
Latest version of azcmagent is installed.
INFO    Connecting machine to Azure... This might take a few minutes.
INFO    Testing connectivity to endpoints that are needed to connect 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.
```

Enter the code



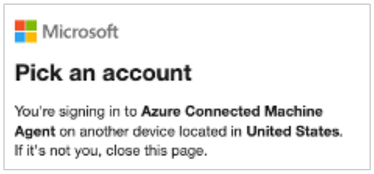
Microsoft

Enter code

Enter the code displayed on your app or device.

[redacted]

Select the account to authorize the agent with

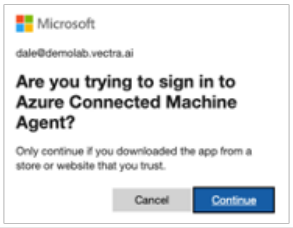


Microsoft

Pick an account

You're signing in to **Azure Connected Machine Agent** on another device located in **United States**. If it's not you, close this page.

Authorize the agent

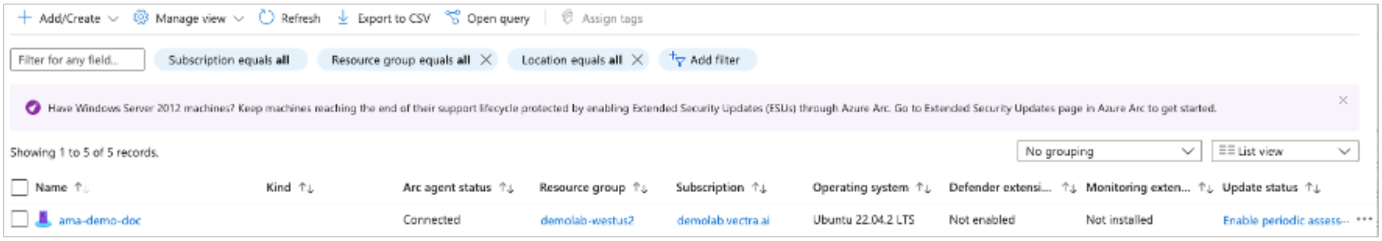


dale@demolab.vectra.ai

Are you trying to sign in to Azure Connected Machine Agent?

Only continue if you downloaded the app from a store or website that you trust.

Refresh the machines list and verify machine is present

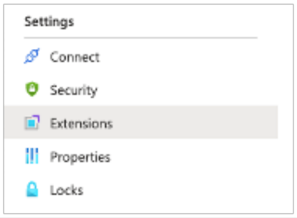


Have Windows Server 2012 machines? Keep machines reaching the end of their support lifecycle protected by enabling Extended Security Updates (ESUs) through Azure Arc. Go to Extended Security Updates page in Azure Arc to get started.

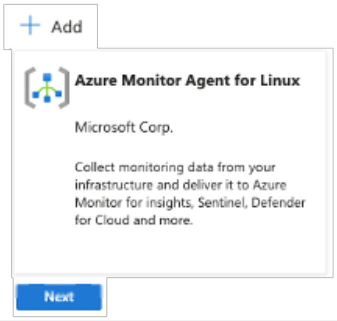
Showing 1 to 5 of 5 records.

Name	Kind	Arc agent status	Resource group	Subscription	Operating system	Defender extensi...	Monitoring exten...	Update status
ama-demo-doc		Connected	demolab-westus2	demolab.vectra.ai	Ubuntu 22.04.2 LTS	Not enabled	Not installed	Enable periodic assess...

Select the machine and then select Extensions from the left-hand menu



Select Add then select Azure Monitor Agent for Linux and click Next

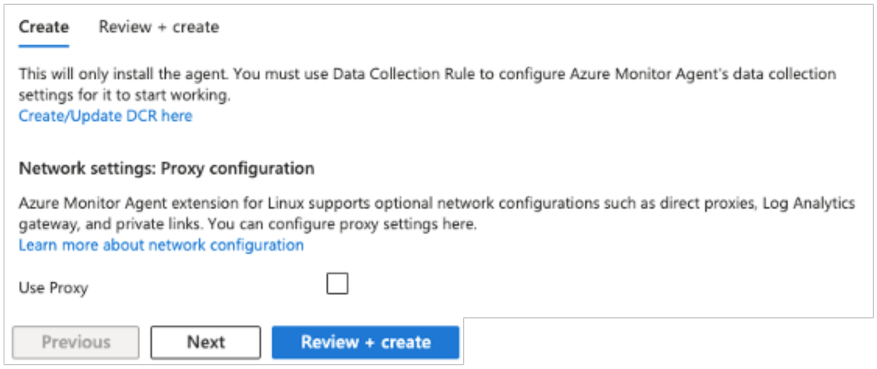


Azure Monitor Agent for Linux

Microsoft Corp.

Collect monitoring data from your infrastructure and deliver it to Azure Monitor for insights, Sentinel, Defender for Cloud and more.

Select Review + create
And then Create



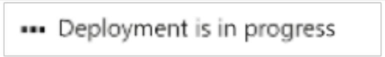
This will only install the agent. You must use Data Collection Rule to configure Azure Monitor Agent's data collection settings for it to start working.
Create/Update DCR here

Network settings: Proxy configuration

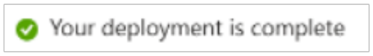
Azure Monitor Agent extension for Linux supports optional network configurations such as direct proxies, Log Analytics gateway, and private links. You can configure proxy settings here.
Learn more about network configuration

Use Proxy □

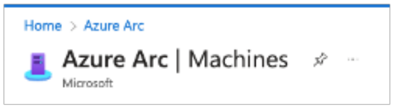
Deployment will start


Deployment is in progress

Wait several minutes for deployment to complete


Your deployment is complete

Navigate back to Azure Arc - Machines

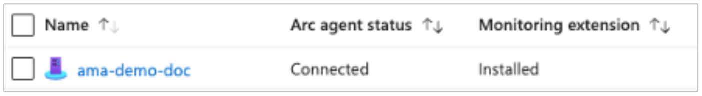


Home > Azure Arc

Azure Arc | Machines

Microsoft

Verify Arc agent status is Connected, and the Monitoring Extension is installed



Name	Arc agent status	Monitoring extension
ama-demo-doc	Connected	Installed

Install Logstash

Logstash must be installed on the Linux server to transform incoming data from Vectra. The following instructions may vary depending on Linux distribution being used. The following link provides detailed instructions on installing Logstash: https://www.elastic.co/guide/en/logstash/current/installing-logstash.html.

These instructions are for installing Logstash on Ubuntu Linux 22.04.

- Download and install the Public Signing Key.

  ```
  wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o
  /usr/share/keyrings/elastic-keyring.gpg
  ```

- Install transport package and agree to reboot Azure Arc services if prompted.

  ```
  sudo apt-get install apt-transport-https
  ```

- Save the repository definition.

  ```
  echo "deb [signed-by=/usr/share/keyrings/elastic-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt
  stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-8.x.list
  ```

- Install Logstash and agree to reboot the server after complete

  ```
  sudo apt-get update && sudo apt-get install logstash
  ```

- Create the Logstash manipulation template to transform the incoming data into a format that AMA can process.

  ```
  vi /etc/logstash/conf.d/detect-cf.conf
  ```

- Add this code to the template and save the file. NOTE: this example is listening on TCP port 4444 for incoming messages from Vectra, if you would like to use a different port then reflect that change in the input block.

  ```
  input {
    tcp {
      port => 4444
      type => detect
    }
  }

  filter {
    if [type] == "detect" {
      mutate { gsub => [ "[message]", " -:", "" ] }
        mutate {
          gsub => [ "message", "\\n", "" ]
      }
    }
  }

  output {
    tcp {
      host => "127.0.0.1"
      port => 514
      codec =>
        line {
          format => "%{message}"
  ```

```
            }
        }
    }
```

- Enable Logstash to start on reboot and restart the service.

```
systemctl enable logstash && systemctl restart logstash
```

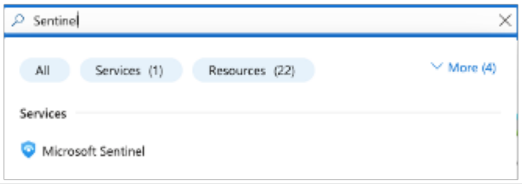
Install Data Connector

The data connector is responsible for controlling how data is shipped from AMA to the Log Analytics Workspace. Vectra data is provided in syslog CEF format and is stored in the CommonSecurityLog so that means a Common Event Format data connector is required.

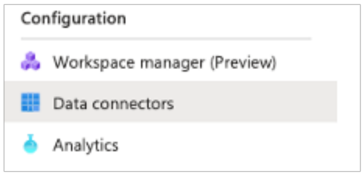
Access the Azure Portal

Search resources for Sentinel

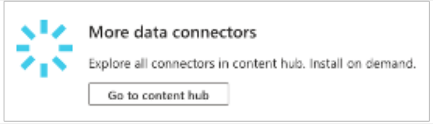
Select Microsoft Sentinel from the list then enter your workspace



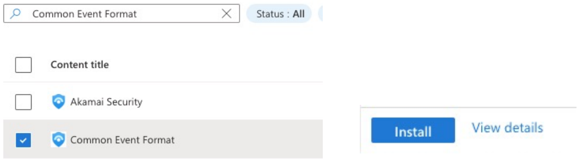
Select Data connectors from under the Configuration menu



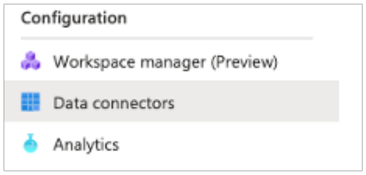
Go to content hub to install a connector on demand



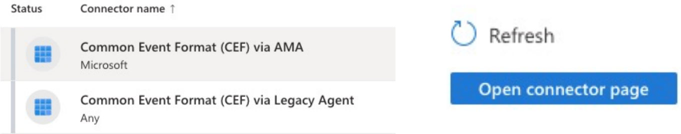
Search for Common Event Format and select it and then Install



Return to the Data connectors page

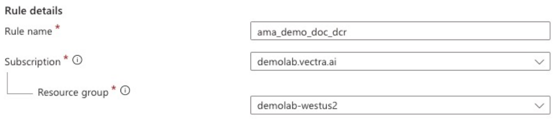


Refresh the page and select Common Event Format (CEF) via AMA and then Open connector page


Status
Connector name ↑
Common Event Format (CEF) via AMA
Microsoft
Common Event Format (CEF) via Legacy Agent
Any
Refresh
Open connector page

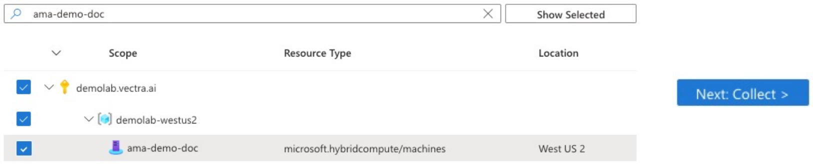
Create a new data collection rule

Create a new data collection rule using appropriate name and resource group



Rule details
Rule name * ama_demo_doc_dcr
Subscription * demolab.vectra.ai
Resource group * demolab-westus2

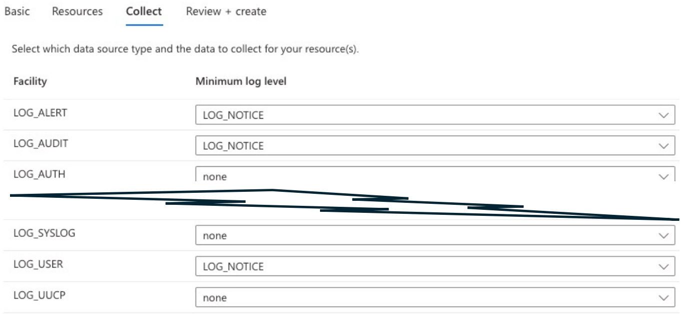
Search for your Arc connect AMA machine, select it and hit Next



ama-demo-doc | Show Selected

	Scope	Resource Type	Location
☑	demolab.vectra.ai		
☑	demolab-westus2		
☑	ama-demo-doc	microsoft.hybridcompute/machines	West US 2

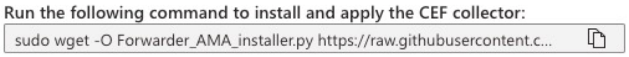
Configure the Collect portion of the DCR exactly as shown here



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

Facility	Minimum log level
LOG_ALERT	LOG_NOTICE
LOG_AUDIT	LOG_NOTICE
LOG_AUTH	none
LOG_SYSLOG	none
LOG_USER	LOG_NOTICE
LOG_UUCP	none

Copy the command and run it on your Linux server to attach the DCR



Run the following command to install and apply the CEF collector:

```
sudo wget -O Forwarder_AMA_installer.py https://raw.githubusercontent.c...
```

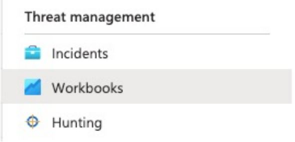
Note: if python is not linked to python3 then update the command to reference python3

Install Vectra Workbook

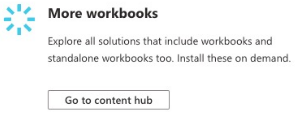
The Vectra workbook is available in the content hub, and it's used to visualize the data by providing several dashboards. The content pack also includes the analytics rules templates to generate incidents.

If this is a migration from OMS to AMA and the Workbook is already installed, then this section can be skipped.

Within Sentinel, navigate to the Workbooks page



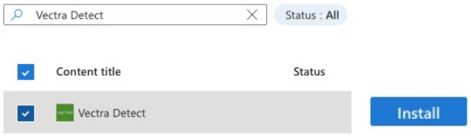
Go to content hub to install the Vectra workbook



More workbooks

Explore all solutions that include workbooks and standalone workbooks too. Install these on demand.

Search for Vectra Detect, select the workbook and install



Vectra Detect | Status : All

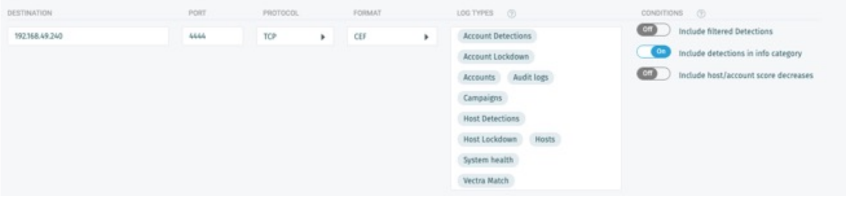
☑	Content title	Status
☑	Vectra Detect	

Configure Vectra

The Vectra platform must be configured to send syslog data to the AMA Linux server. Connect to your Vectra user interface to complete this configuration.

If this is an existing OMS deployment, then the configuration must be updated to point to the AMA Linux server configured above.

Configure Vectra > Settings – Notifications Syslog to send desired log types to the configured Logstash port on your AMA machine



DESTINATION: 192.168.49.240
PORT: 4444
PROTOCOL: TCP
FORMAT: CEF
LOG TYPES: Account Detections, Account Lockdown, Accounts, Audit logs, Campaigns, Host Detections, Host Lockdown, Hosts, System health, Vectra Match
CONDITIONS:
Off Include filtered Detections
On Include detections in info category
Off Include host/account score decreases

Validation

Everything should be configured at this point and should be validated to ensure data is being ingested properly.

- Connect to your AMA Linux server over ssh and then tail your syslog file.

```
tail -f /var/log/syslog
```

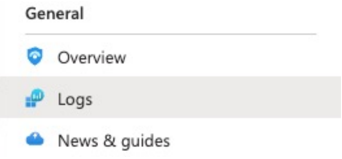
- The easiest way to force data (providing your Vectra configuration includes syslog of audit data) is to log on/off the Vectra user interface as this will trigger an audit log. If you are receiving syslog with entries that include vectra_cef_ then syslog data is making it from Vectra to the AMA server.

```
vectra_cef_
```

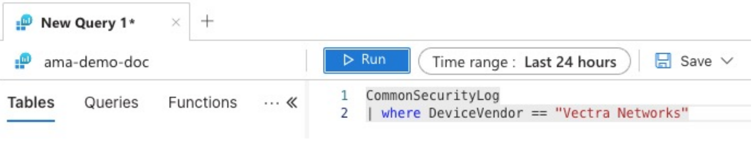
IMPORTANT: It can take 20 minutes for the initial data to make it into the CommonSecurityLog and then approximately every five minutes afterwards so please be patient.

- Navigate back to your Sentinel instance to continue validation.

Within Sentinel, navigate to the Logs page

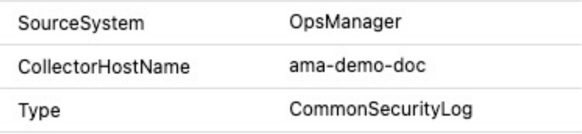


Construct KQL to query the CommonSecurityLog and verify that Vectra data is being ingested



```
CommonSecurityLog
| where DeviceVendor == "Vectra Networks"
```

Expand the results or add | project CollectorHostName to the KQL and verify your AMA server is the collector displayed



SourceSystem	OpsManager
CollectorHostName	ama-demo-doc
Type	CommonSecurityLog

Congratulations! Vectra data is now being ingested into Microsoft Sentinel using the Azure Monitoring Agent.

Disable OMS Agent

For existing deployments, the OMS agent should be disabled to prevent duplicate data from being ingested into the CommonSecurityLog.

- Connect to your OMS Linux server using ssh and disable the agent.

  ```
  sudo /opt/microsoft/omsagent/bin/service_control disable
  ```

- Refer to Microsoft documentation for complete instructions for removing the OMS agent. The following link includes a section on removing the agent.

  https://learn.microsoft.com/en-us/troubleshoot/azure/automation/reinstall-oms-agent-linux

- While it is safe to delete the existing Vectra AI Detect data connector if you do so you will need to reinstall the Vectra workbook. Please refer to the instructions earlier in this document.