VMware ESXi

Last updated: Jul. 14, 2025

Overview

Enable detections with data from VMware ESXi.

Requirements

Subscription: Falcon Next-Gen SIEM or Falcon Next-Gen SIEM 10GB

CrowdStrike clouds: Available in US-1, US-2, EU-1, US-GOV-1, and US-GOV-2.

Other requirements:

- Your environment must include a functioning deployment of VMware ESXi version 7 or later.
- Access to VMware ESXi with an Administrator account.
- An on-premises syslog server with a data shipper installed and configured to send the data to Falcon Next-Gen SIEM. For more info, see Configuring syslog port (514) on ESXi [https://kb.vmware.com/s/article/2003322].

Setup

> **Important:** Some of these steps are performed in third-party products. The CrowdStrike Falcon platform integrates the relevant settings as you configure them. However, CrowdStrike does not validate any third-party configurations. Perform the following steps with care, and validate your settings and values before finalizing configurations in Falcon.

Step 1: Configure and activate the VMware ESXi Data Connector

1. In the Falcon console, go to **Data connectors > Data connectors > Data connections [/data-connectors]**.
2. Click **+ Add connection**.
3. In the **Data Connectors** page, filter or sort by **Connector name**, **Vendor**, **Product**, **Connector Type**, **Author**, or **Subscription** to find and select the connector you want to configure.

   > **Tip:** This data connector's name is located in the header. For example, **Step 1: Configure and activate `<the_data_connector_name>`**.

4. In **New connection**, review connector metadata, version, and description. Click **Configure**.

   > **Note:** For connectors that are in a **Pre-production** state, a warning appears. Click **Accept** to continue configuration.

5. In the **Add new connector** page, enter a name and optional description to identify the connector.
6. Click the **Terms and Conditions** box, then click **Save**.
7. A banner message appears in the Falcon console when your API key and API URL are ready to be generated. To generate the API key, go to **Data connectors > Data connectors > Data connections [/data-connectors]**, click **Open menu** ⋮ for the data connector, and click **Generate API key**.
8. Copy and safely store the API key and API URL to use during connector configuration.

   > **Important:** Record your API key somewhere safe as it displays only once during connector setup. For more information about vendor-specific connector setup, see the Third-party data source integration guides [/documentation/page/a76b8289/data-connectors#c42a73ec].

Step 2: Configure your data shipper

You can use any data shipper that supports the HEC API [https://library.humio.com/logscale-api/log-shippers-hec.html] to complete this step. We recommend using the **Falcon LogScale Collector**.

1. In the Falcon console, navigate to **Support and resources > Resources and tools > Tool downloads [/support/tool-downloads]**.
2. Install the LogScale Collector based on your operating system. For example, `LogScale Collector for Windows - X64 vx.x.x`.
3. Open the LogScale Collector configuration file in a text editor. For file location, see Create a configuration - Local [https://library.humio.com/falcon-logscale-collector/log-collector-config.html#log-collector-config-editing-local].
4. Edit the `config.yaml` file. Examples of configuration files for syslog servers:

   - Linux

```
dataDirectory: /var/lib/humio-log-collector
sources:
  syslog_udp_514:
    type: syslog
    mode: udp
    port: 514
    sink: humio
sinks:
```

```
sinks:
  humio:
    type: hec
    proxy: none
    token: <generated_during_data_connector_setup>
    url: <generated_during_data_connector_setup>
```

- Windows

  ```
  dataDirectory: C:\ProgramData\LogScale Collector\
  sources:
    syslog_port_514:
      type: syslog
      mode: udp
      port: 514
      sink: humio
  sinks:
    humio:
      type: hec
      proxy: none
      token: <generated_during_data_connector_setup>
      url: <generated_during_data_connector_setup>
  ```

- Mac

  ```
  dataDirectory: /var/local/logscale-collector
  sources:
    syslog_port_514:
      type: syslog
      mode: udp
      port: 514
      sink: humio

  sinks:
    humio:
      type: hec
      proxy: none
      token: <generated_during_data_connector_setup>
      url: <generated_during_data_connector_setup>
  ```

5. Verify the `sources` and `sinks` sections are correct.

   - Check that no other services are listening on port 514. For example, this command is commonly used to check for listening ports on Linux:

     ```
     sudo netstat -lpn
     ```

     - If port 514 is not available, select a different port and confirm it is not in use. Update the `port` number.

     - If you're configuring multiple sources in the same configuration file, each sink must have a distinct port. For example, you cannot have two Humio sinks listening on port 514.

   - Check the local firewall and confirm that the configured port is not being blocked.

     Important: For Windows Firewall, add the LogScale Collector to your traffic allowlist.

   - Add the `token` and `url` generated during data connector setup. Remove `/services/collector` from the end of the `url`.

6. Save and exit the `config.yaml` file.

7. Restart the Falcon LogScale Collector.

   - For Linux, run this command in your terminal:

     ```
     sudo systemctl start humio-log-collector
     ```

   - For Windows, look for **Services** from the search bar, open **Services**, find **Humio Log Collector** and right-click **Restart**.

   - For Mac, run this command in your terminal:

     ```
     sudo launchctl kickstart -k system/com.crowdstrike.logscale-collector
     ```

Step 3: Configure the VMware ESXi Syslog service

When you configure the VMware ESXi Syslog service, logs are sent to hosts with the Falcon LogScale Collector installed and running as a syslog receiver. There are multiple methods available for configuring the ESXi syslog service. For more information on which configuration method is most appropriate for your environment, see Configuring syslog port (514) on ESXi [https://kb.vmware.com/s/article/2003322].

As an example, here are the steps to configure a remote syslog server using the ESXi vSphere web client. These steps are performed in the VMware ESXi administration interface.

1. From the VMware ESXi landing page, go to **Manage > System > Advanced Settings**.

2. In the **Key** column, search for and select the `Syslog.global.LogHost` key. This option enables exporting logs to a central logging server.

3. In the **Value** column, enter the IP or FQDN protocol, and port of your log forwarder. For example: `udp://192.0.2.1:514`.

For more syslog configuration settings on ESXi hosts, refer to VMware's documentation.

Note: We highly recommend configuring ESXi with an NTP server to help make logs consistent across the environment.

Step 4: Verify successful data ingestion

Verify that VMware ESXi data is being ingested and appearing in Next-Gen SIEM search results.

> **Important:** Search results aren't generated until an applicable event occurs. Before verifying successful data ingestion, wait until data connector status is **Active** and an event has occurred. Note that if an event timestamp is greater than the retention period, the data is not visible in search.

Verify that data is being ingested and appears in Next-Gen SIEM search results:

1. In the Falcon console, go to **Data connectors > Data connectors > Data connections [/data-connectors]**.
2. In the **Status** column, verify data connection status is **Active**.
3. In the **Actions** column, click **Open** menu ⋮ and select **Show events** to see all events related to this data connection in **Advanced Event Search**.
4. Confirm that at least one match is generated.

If you need to run a manual search, use this query in Advanced Event Search:

```
Vendor = VMware | Product = ESXi
```

To verify data ingestion in your ESXi server:

1. Connect to the ESXi server over SSH.
2. List all virtual machines and search for critical virtual machine files with this command.
   ```
   vim-cmd vmsvc/getallvms
   ```
   ```
   find / -type f | grep -E '\.vmx|\.vmdk'
   ```
3. To power off a virtual machine, enter this command.
   ```
   vim-cmd vmsvc/power.off 1
   ```

Data reference

Next-Gen SIEM events

Next-Gen SIEM events that can be generated by this data connector:

- Process:Start:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#b1nwxnx3]
- Session:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#x0113sk8]
- Session:Start:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#n0esexy6]
- Session:End:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#p03v6mbn]
- Network:Start:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#j2mj0bj0]
- Network:Connection:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#i0veu97i]
- Network:End:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#j0vgvx1w]
- Authentication:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#d6asyl12]
- Authentication:Start:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#v3639xkr]
- Configuration:Change:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#t8jh2vkl]
- Configuration:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#e1mjpydj]
- Iam:Change:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#w2o4xy4u]
- Host:End:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#m0caqh4x]

For more information about Next-Gen SIEM events, see Next-Gen SIEM Data Reference [/documentation/page/q1f14b54/next-gen-siem-data] .

‹ VersaONE Universal SASE Platform[/documentation/page/tcb88d3e/versaone-uni VMware vCenter › [/documentation/page/ODCPRn7E/vmware-vcenter]