VMware vCenter

Last updated: Jul. 3, 2025

Overview

VMware vCenter Server is a centralized management platform that enables organizations to manage virtual infrastructure, including ESXi hosts, virtual machines, storage, and networking from a single console. It provides comprehensive virtualization management, resource allocation, monitoring, and automation capabilities for VMware environments.

Use this connector to ingest the following log types:

- **Task Logs:** Records all operations performed on virtual objects, including creation, modification, and deletion of VMs and resources.
- **System Event Logs:** Captures system-level events, hardware status changes, and infrastructure alerts across the virtual environment.
- **Performance Logs:** Documents resource utilization, performance metrics, and capacity-related information for hosts and VMs.
- **Authentication Logs:** Tracks user login attempts, session management, and access control changes within vCenter.
- **Alarm Logs:** Records triggered alarms, warnings, and critical events related to virtual infrastructure components.
- **Configuration Logs:** Monitors changes to vCenter settings, host configurations, and virtual infrastructure modifications.
- **Security Event Logs:** Captures security-related events including permission changes, certificate management, and security policy updates.

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.

CrowdStrike access and permissions: Administrator or Connector Manager access to the Falcon console for the respective CID.

Vendor requirements

- VMware vCenter Server credentials with administrative privileges.
- Network connectivity between the CrowdStrike Falcon platform and vCenter Server.
- vCenter version 6.7 or later is recommended.

Parser: The default parser for this data connector requires logs in **syslog** format. For more info, see Parser [/documentation/page/ODCPRn7E/vmware-vcenter#Zb8DsMaH].

System requirements:

- For the Falcon LogScale Collector, see the list of supported operating system versions [https://library.humio.com/falcon-logscale-collector/log-collector-install.html#log-collector-install-compatibility].
- The size of your Falcon LogScale Collector instance depends on workload. See the LogScale Collector sizing guide [https://library.humio.com/falcon-logscale-collector/log-collector-install-sizing.html].

Setup

> **Important:** Some of these steps are performed in third-party products. CrowdStrike does not validate any third-party configurations in customer environments. Perform the following steps with care, and validate your settings and values before finalizing configurations in the Falcon console.

Step 1: Configure and activate the VMware vCenter 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

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:
  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 VMware vCenter

1. Log in to **VMware vCenter** as an administrator.

2. In **Appliance Management** menu, select **Syslog**.

3. In the **Forwarding Configuration** section, click **Configure**. The **Create Forwarding Configuration** window appears.

4. Enter the forwarding configuration details:

   a. **Server address:** Enter the server address of the Falcon LogScale Collector.

   b. **Protocol:** In the dropdown menu, select **UDP**.

   c. **Port:** Enter the listening port of the Falcon LogScale Collector. The default port is **514**.

5. Click **Save.**

Step 4: Verify successful data ingestion

> **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" | #repo = "3pi_vmware_vcenter" | #event.module = vcenter
```

Data reference

Parser

The default parser recommended to parse incoming data for this data connector is **vmware-vcenter**. This parser requires logs in **syslog** format.

Supported timestamp format: `yyyy-MM-dd'T'HH:mm:ss[.SSSSSS]XXX`

Example: `2025-02-11T21:23:11.354620+00:00`

Structure

An example of task logs. Task logs record tasks executed by the system, such as backups, updates, or other maintenance activities.

```
<134>1 2024-10-07T18:51:55.641952+00:00 localhost vpxd-main - - - 2024-10-07T18:51:55.160Z info vpxd[07615]
[Originator@6876 sub=vpxLro opID=169814ba-b3] [VpxLRO] -- FINISH lro-1886331
```

An example of system event logs. System event logs record system-level events, such as service startups, shutdowns, or hardware issues.

```
<134>1 2024-10-07T18:51:58.102282+00:00 localhost sps - - - 2024-10-07T18:51:58.102Z
      [pool-36-thread-2] INFO  opId=5d3daec1-2601-48cd-8ab5-b292e9c2e321
com.vmware.vim.sms.StorageManagerImpl
      - Starting Timer: queryProvider.
```

An example of performance logs. These logs record performance-related data, such as resource utilization, latency, or throughput.

```
<134>1 2024-11-21T17:58:55.909225+00:00 vcenter-example vpxd-profiler - - - sign/Class=
```

An example of authentication logs. These logs record authentication attempts, successes, and failures.

```
<86>1 2024-11-08T17:32:50.496661+00:00 vcenter-example sshd 19123 - -  Accepted keyboard-interactive/pam
for root from 10.102.9.80 port 53561 ssh2
```

An example of alarm logs. These logs record alarm events, such as triggered alarms or alarm state changes.

```
<86>1 2024-11-08T17:32:50.496661+00:00 vcenter-example sshd 19123 - -  Accepted keyboard-interactive/pam
for root from 10.102.9.80 port 53561 ssh2
```

An example of configuration logs. These logs record configuration changes, updates, or modifications.

```
<134>1 2025-01-09T15:59:27.343420+00:00 vcenter-example vpxd-main - - - 2025-01-09T15:59:27.296Z info
vpxd[06405] [Originator@6876 sub=VmProv opID=m2z4gqu7-158597-auto-3edi-h5:70022584-9b-02] Creating VM with
spec (vim.vm.ConfigSpec) {...}
```

An example of security event logs. These logs record security-related events, such as access control changes, permission updates, or security breaches.

```
<134>1 2024-11-01T19:52:48.785661+00:00 vcsa8 vum-vmacore - - - 2024-11-01T19:52:48.785Z info vmware-vum-
server[11743] [Originator@6876 sub=SessionAuthData] [vciSessionAuthData 76] Trying to get current VC
connection for session [523fbddd-22b6-dde5-735e-f213475ea843]; user: com.vmware.vim.eam
```

Next-Gen SIEM events

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

- Authentication:Start:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#v3639xkr]
- Authentication:End:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#v9a3adya]
- Authentication:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#d6asyl12]
- Database:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#s4okeeji]
- File:Creation:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#g2in7h52]
- Host:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#w5nxhce9]
- Iam:Change:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#w2o4xy4u]
- Network:Connection:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#i0veu97i]
- Network:Protocol:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#h6gvlrpt]
- Network:Start:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#j2mj0bj0]
- Process:End:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#m7os2kgj]
- Process:Info:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#p5eme1kf]
- 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]
- Web:Access:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#p9vhn5jb]

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

‹ VMware ESXi[/documentation/page/x38607f0/vmware-e VMware Workspace One UEM › [/documentation/page/Svmnel6V/vmware-workspace-one-uem]