Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Set up an Adaptive Response relay from a Splunk Cloud Platform Enterprise Security search head to an on-premises device

Generated: 6/13/2022 9:54 am

Set up an Adaptive Response relay from a Splunk Cloud Platform Enterprise Security search head to an on-premises device

Splunk Cloud Platform customers can utilize Adaptive Response actions in Splunk Enterprise Security (ES) without exposing infrastructure controls and administration to the open internet. Adaptive response relay allows adaptive response actions to queue on the Splunk Cloud Platform ES search head. These queued actions store metadata and search results that allow a separate proxy component to execute those adaptive response actions from within the on-premises environment.

> You must install Splunk Enterprise Security on the heavy forwarder prior to configuring it for Adaptive Response actions.

You need to perform the following steps to set up Adaptive Response actions:

1. Install the technology add-on for Adaptive Response on your heavy forwarder.
2. Configure your Splunk Cloud Platform ES search head with an API key.
3. Configure your on-premises heavy forwarder with an API key.
4. Configure your on-premises heavy forwarder with a modular action relay.
5. Configure your Splunk Cloud Platform ES search head with a modular action worker.
6. Configure adaptive response actions for your Splunk Cloud Platform ES search head.

Install the technology add-on for Adaptive Response on your heavy forwarder

For an on-premises heavy forwarder to perform Adaptive Response actions, you must install the actions on both the Splunk Cloud Platform ES search head and the heavy forwarder. These actions are installed by default with ES in `$SPLUNK_HOME/etc/apps/SA-ThreatIntelligence`, but you need to install them manually on your heavy forwarder.

1. From the Splunk ES menu bar of the Splunk Cloud Platform ES search head, select **Configure > General > General Settings.**
2. Locate the **Distributed Configuration Management** item.
3. Click **Splunk_TA_AROnPrem** to download the app.
4. Install the app on the heavy forwarder.

Configure your Splunk Cloud Platform ES search head with an API key

The API key allows you to authenticate from the KV Store collection and Common Action Model (CAM) queue. You must create and manage your own API key. The API key follows a specific format, and it does not support two-factor authentication. For a Splunk Cloud Platform environment that requires two-factor authentication, turn off this feature by not setting an API key.

1. Retrieve the heavy forwarder's `serverName` value by running the following search on the heavy forwarder:

   ```
   | rest /services/server/info | table serverName
   ```

   Take note of this name because you will need it when you set up your heavy forwarder. In this example the `serverName` value is `hf1`.
2. Install the Common Information Model version 4.12 or higher on the Splunk Cloud Platform ES search head, if you haven't done so already.

3. Generate an API key on the Splunk Cloud Platform ES search head.
    1. From the Splunk ES menu bar, select **Configure > CIM Setup**, and then click the **Adaptive Response** tab.
    2. Under **Manage API Keys** do the following steps:
        1. In the **Key Name** field, type the `serverName` value that you retrieved: in this case, `hf1`.
        2. To generate the API key value, type the following URI into a browser window of your Splunk Cloud Platform ES search head:
           `https://<yoursplunkserver>/en-US/splunkd/__raw/alerts/modaction_queue/key`
           This will return a random 128-character string in the valid format.
        3. Copy and paste the string into the **API Key** field.
           Take note of this string because you will use it when you configure your heavy forwarder.

Configure your on-premises heavy forwarder with an API key

An API key allows the heavy forwarder to authenticate against the Splunk Cloud Platform ES search head. The API key on the heavy forwarder must match the API key on the Splunk Cloud Platform ES search head.

1. Install the Common Information Model version 4.12 or higher on the heavy forwarder, if you haven't done so already.
2. From the Splunk ES menu bar, select **Configure > CIM Setup**, and then click the **Adaptive Response** tab.
3. Under **Manage API Keys** do the following steps:
    1. On the key management page, in the **Key Name** field, type the `serverName` value that you took note of in the Configure your Splunk Cloud Platform ES search head with an API key section.
    2. On the key management page, in the **API Key** field, paste the string that you took note of in the Configure your Splunk Cloud Platform ES search head with an API key section.

Configure your on-premises heavy forwarder with a modular action relay

The modular action relay is where you set the heavy forwarder to retrieve queued search results from a Splunk Cloud Platform correlation search so that it can execute adaptive response actions on premises.

1. From the Splunk ES menu bar, select **Settings > Data inputs**.
2. Scroll down to Modular Action Relay and click **+ Add new**.
    1. Type a **Name** for the relay, such as `relay1`.
    2. Type the **Remote Search Head URI** in the format of `protocol://servername:port`, such as: `https://10.224.62.249:8089`.
       8089 is the default port for Splunk Cloud Platform. However, port 8089 is not open for communication from the designated heavy forwarder. You must create a Splunk Cloud Platform Operations request to open the 8089 port from an approved IP list so that the heavy forwarder can communicate with the Splunk Enterprise Security search head.
    3. Type a **Description** for the relay, such as `remote search head`.
    4. Type the **Api Key Name** (the `serverName` value that you took note of in the Configure your Splunk Cloud Platform ES search head with an API key section), such as `hf1`.
    5. Type `True` in the **Verify** field to verify the certificates between the worker and the Splunk Cloud Platform ES search head.
    6. (Optional) If your ES search head is using a privately signed SSL certificate, add your root CA certificate chain file to the `Splunk_SA_CIM/auth` directory on the heavy forwarder and provide its file name to this input in the **Client Certificate** field. If your search head is in Splunk Cloud Platform, this is not an issue.

Configure your Splunk Cloud Platform ES search head with a modular action worker

The modular action worker is where you specify the `serverName` value of the heavy forwarder that the Splunk Cloud Platform ES search head will queue search results for.

1. From the Splunk ES menu bar of the Splunk Cloud Platform ES search head, select **Configure > Content > Content Management**.
2. Type `Modular Action Workers` in the search filter.
3. Click the name of the **Modular Action Workers** lookup.
4. Add a worker set and the name of the worker. The `worker_set` value is used when running Adaptive Response actions from ES. The `cam_worker` is the actual name of the heavy forwarder that will execute the actions.
    1. Leave the row with **local** as-is because it allows for local execution of actions on the Splunk Cloud Platform ES search head.
    2. In the **worker_set** column, type a descriptive name for the heavy forwarder: `onprem`.
    3. In the **cam_workers** column, type the `serverName` value that you took note of in the Configure your Splunk Cloud Platform ES search head with an API key section, such as `"["hf1"]"`.
    The format requires array-style notation of `"["nameofworker"]"` with each worker name in quotes and separated with commas in CSV encoded JSON. An example of multiple workers is `"[""hf1"",""hf2""]"`.

Configure Adaptive Response actions for your Splunk Cloud Platform ES search head

See Configure Adaptive Response actions for a correlation search in Splunk Enterprise Security for information about configuring Adaptive Response actions in general.

The Worker Set drop-down menu is specific to Adaptive Response actions on a Splunk Cloud Platform ES search head. After completing the in the Configure your Splunk Cloud Platform ES search head with a modular action worker section, when you create or edit a correlation search to add an Adaptive Response action, the drop-down menu includes the `worker_set` that you created.

Select the `worker_set` to use for executing those Adaptive Response actions from within the on-premises environment.

The results of Adaptive Response actions, ping for example, are found in `"index=main source=ping"`.

Troubleshoot Adaptive Response relay from Splunk Cloud Platform ES search head to an on-premises device

The Adaptive Response modular input runs at a default interval of 2 minutes. To avoid exposing critical infrastructure controls, adaptive response actions are queued on the Splunk Cloud Platform search head. To avoid performance problems with the Common Action Model (CAM) queue, adjust the interval to run less frequently, and do not set it below 10 seconds. The queued actions store metadata and search results that enables a proxy to run adaptive response actions from your on-premise environment.

You can adjust the CAM queue interval based on your needs. A more frequent execution time will place additional load on the Splunk Cloud Platform ES search head.

Ensure that your heavy forwarder is configured to forward its data to your indexers. This includes forwarding data from the relayed modular actions. You can run a search similar to the following search on your ES search head to verify that data is forwarding, where `hf1` is the name of your heavy forwarder:

```
index="cim_modactions" host=hf1
```

If this search never returns results, then your heavy forwarder is experiencing issues connecting to the ES search head.

Related information about distributed Adaptive Response actions

See the following related information about distributed Adaptive Response actions.

- See Adaptive Response framework in Splunk ES on the Splunk Developer Portal.
- See Create an Adaptive Response action on the Splunk Developer Portal.
- See Example distributed Adaptive Response action on the Splunk Developer Portal.
- See Create an Adaptive Response action for Enterprise Security in the *Splunk Add-on Builder User Guide*.