Install the Cisco Security Cloud App in Distributed Environment

Components of Distributed Splunk Deployment

In a distributed Splunk deployment, the architecture includes several core components, each with a distinct role:

1. **Indexers (IH)**

   Store indexed data and handle search requests from search heads.

2. **Indexer Manager** (formerly **Cluster Master**)

   Coordinates the configuration, replication, and management of clustered indexers.

3. **Search Heads (SH)**

   Execute searches and provide the search interface for users.

4. **Heavy Forwarders (HF)**

   Ingest, process, parse, and forward data to indexers. Heavy forwarders are typically used for inputs that require parsing, filtering, or enrichment before indexing.

5. **Deployment Server** (optional)

   Manages configuration files and application deployment to forwarders and other Splunk components.

6. **Search Head Deployer (SHD)**

   Manages and deploys configuration updates to the search head cluster.

Important In a distributed Splunk architecture, configure and run modular inputs only on the Heavy Forwarder (HF). Do not configure modular inputs on search heads or indexers.

Install Splunk in Distributed Environment

This procedure describes how to install the Cisco Security Cloud App in a distributed Splunk deployment.

Before you begin

Ensure the following:

- All Splunk instances are running compatible Splunk versions.
- You have obtained the Splunk add-on package.
- Network connectivity between all instances is verified, including required ports and firewall rules.

Procedure

Step 1 **Install the app on Heavy Forwarders (HF)**

a) Log in to the Heavy Forwarder.
b) Copy the installtion package to the following directory:

```
$SPLUNK_HOME/etc/apps
```

c) Restart the Splunk service.

Note
You can install the TA using the Splunk UI from Splunkbase or by uploading the TA archive.

Step 2 **Install the app on Search Heads (SH)**

a) Log in to the Search Head Deployer.
b) Copy the installation package to the following directory:

```
$SPLUNK_HOME/etc/shcluster/apps/
```

c) Extract the package.
d) Apply the configuration bundle to all search heads by running the following command:

```
$SPLUNK_HOME/bin/splunk apply shcluster-bundle -target https://<shc_captain>:<mgmt_port>
--answer-yes
```

Where `<shc_captain>` is the IP address of the Search Head Cluster captain.

To define the IP, run the following command on a search head:

```
/opt/splunk/bin/splunk show shcluster-status
```

e) Restart the Splunk service on each search head, or perform a rolling restart from the captain:

```
/opt/splunk/bin/splunk rolling-restart shcluster-members
```

f) Verify that the app appears in the list of apps and add-ons.

We recommend that you disable the visibility of the app on search heads to prevent inputs from being created on search heads. This is to avoid any conflict from the data collection components on the search heads with user search activity. To ensure the app is not visible, select **Edit properties** and change it to **No**.

Step 3 **Install the TA on Indexers (IH)**

a) Log in to the Indexer Manager.

b) Copy the TA package to the following directory:

```
$SPLUNK_HOME/etc/manager-apps/
```

c) Apply the cluster bundle by running the following command:

```
$SPLUNK_HOME/bin/splunk apply cluster-bundle
```

d) Restart the Splunk service on each indexer, or perform a rolling restart from the Indexer Manager:

```
/bin/splunk rolling-restart cluster-peers
```

Configure Inputs in Distributed Environment

This section describes how to configure inputs on the **Heavy Forwarder (HF)** and how to define indexes on the **Indexer Manager**.

Before you begin

Procedure

Step 1 **Configuration on Heavy Forwarders (HF)**

a) Modify the `outputs.conf` file to store the `_internal` index locally

```
$SPLUNK_HOME/etc/system/local/outputs.conf
```

```
[forwardedindex.filter]
whitelist = .*
blacklist = _internal
```

b) Create inputs using either the Splunk UI or the CLI. To create inputs from the UI, refer to the Splunk user guide. To create inputs using the CLI, edit the `inputs.conf` file located at `$SPLUNK_HOME/etc/apps/CiscoSecurityCloud/local/inputs.conf`. Define the source paths, polling intervals, ports, and other input parameters. For example,

```
[sbg_multicloud_defense_input://MCD_input_name]
index = cisco_multicloud_defense
interval = 300
port = 8088
sourcetype = cisco:multicloud:defense
```

c) Restart the Splunk service on the Heavy Forwarder if you make any changes using the CLI.

Step 2 **Configuration on the Indexer Manager**

a) Define indexes for the TA data in the `indexes.conf` file located at `$SPLUNK_HOME/etc/manager-apps/_cluster/local/indexes.conf` on the Indexer Manager. For example,

```
[cisco_duo]
coldPath = $SPLUNK_DB/cisco_duo/colddb
homePath = $SPLUNK_DB/cisco_duo/db
thawedPath = $SPLUNK_DB/cisco_duo/thaweddb
```

b) Place the app package in `$SPLUNK_HOME/etc/manager-apps/`directory.

c) Propagate the configuration to all indexers by running:

```
$SPLUNK_HOME/bin/splunk apply cluster-bundle
```

Known Limitations in Distributed Environment

REST API Limitations for Heavy Forwarder Inputs

In a Search Head Cluster, search head peers do not have access to the `inputs.conf` file on the Heavy Forwarder.

The REST endpoint, `/services/data/inputs/all` is designed to list data inputs that are **local to the Search Head only**. Inputs configured on a Heavy Forwarder are not returned by this endpoint because the Heavy Forwarder is a separate Splunk instance.

Impact

The following command does not return Heavy Forwarder inputs when executed on a Search Head, the following dashboards are affected:

```
| rest
        /services/data/inputs/all
```

- **Data Integrity**: Status and Connectivity panels
- **Resource Utilization**:
  - Cisco API Throughput
  - Process Health
  - Error Handling
  - Health Monitoring by Input Connection

Troubleshoot App Installation in Distributed Environment

Use this section to diagnose common issues related to data ingestion, parsing, permissions, and performance.

App Data Not Appearing on Search Heads (SH)

- **Verify input configuration**
  - Ensure `inputs.conf` is correctly configured on the Heavy Forwarders (HF):

```
$SPLUNK_HOME/etc/apps/CiscoSecurityCloud/local/inputs.conf
```

- **Check data forwarding**
  - Confirm that Heavy Forwarders are forwarding data to the correct indexers.
- **Verify index configuration**
  - Ensure data is being written to the correct index.
  - Confirm that Search Heads have permission to search the index.
- **Check logs on the Heavy Forwarder**
  - Review the following log for errors:

    ```
    $SPLUNK_HOME/var/log/splunk/splunkd.log
    ```
- **Validate data from the Search Head**
  - Run the following SPL query on the Search Head:

    ```
    index=<index> | stats count by host, source
    ```

Data Parsing Issues

- **Verify props and transforms**
  - Confirm that `props.conf` and `transforms.conf` are configured correctly.
  - Ensure the configurations are applied on the correct tier (Heavy Forwarder or Indexer), as required.
- **Validate configuration using btool**
  - Run the following command to confirm active configurations:

    ```
    splunk btool props list --debug
    ```
- **Check file permissions**
  - Ensure all app files have appropriate file permissions.
  - Restrictive permissions may prevent Splunk from accessing required files.
- **Verify role permissions**
  - Confirm that Search Head roles have access to:
    - app-related indexes
    - Associated knowledge objects
- **Data Latency**
  - If data ingestion is delayed, run the following command on Heavy Forwarders and Indexers to identify bottlenecks:

    ```
    splunk show queues
    ```

- **Verify load balancing**
  - If multiple indexers are used, ensure data is properly load-balanced across them.

Useful Troubleshooting Commands

- **splunkd.log**

  Check the following log on Heavy Forwarders and Indexers for errors related to data forwarding or parsing:

  ```
  $SPLUNK_HOME/var/log/splunk/splunkd.log
  ```

- **btool configuration check**

  Verify configuration syntax:

  ```
  splunk btool check
  ```

- **Indexer data validation**

  Run the following search on Indexers to confirm data indexing:

  ```
  index=<your_index> | stats count by host, source
  ```