Splunk® Enterprise
Distributed Search 8.0.4

Add a cluster member

Generated: 6/09/2020 2:14 am
Add a cluster member

There are several categories of members that you might need to add to a cluster:

- **A new member.** In this case, you want to expand the cluster by adding a new member.
- **A member that was previously removed from the cluster.** In this case, you removed the member with the `splunk remove` command and now want to add it back.
- **A member that left the cluster without being removed from it.** This can happen if, for example, the instance shut down unexpectedly.

This topic treats each of these categories separately through a set of high-level procedures, each of which references one or more detailed steps.

**Add a new member**

Install a new Splunk Enterprise instance and add it to the cluster:

1. Install a new instance of Splunk Enterprise on its own machine or virtual machine. See Hardware and operating system requirements.
2. Initialize the instance. See Initialize the instance.
3. Add the instance to the cluster. See Add the instance.

**Add a member that was previously removed from the cluster**

These procedures are for Splunk Enterprise instances that were previously members of this cluster but were removed from it with the `splunk remove shcluster-member` command. See "Remove a cluster member."

**Add a removed member**

To add a removed member:

1. Clean the instance to remove any existing configurations that could interfere with the cluster. See "Clean the instance."
2. Add the instance to the cluster. "Add the instance."

**Add a member that was both removed and disabled**

To add a member that was both removed and disabled:

1. Clean the instance to remove any existing configurations that could interfere with the cluster. See "Clean the instance."
2. Initialize the instance. See "Initialize the instance."
3. Add the instance to the cluster. "Add the instance."

**Add a member that left the cluster without being removed from it**

A typical reason for a member falling into this category is a temporary failure of the cluster member.
For members that left the cluster without being explicitly removed from it:

1. Start the instance with the `splunk start` command.

2. Depending on how long the member has been down, you might need to run the `splunk resync shcluster-replicated-config` command to download the current set of configurations.

See "Handle failure of a cluster member" for information on the `splunk resync shcluster-replicated-config` command, along with a discussion of other issues related to dealing with a failed member.

**Detailed steps**

The high-level procedures for adding a cluster member use the detailed steps in this section. Depending on the particular situation that you are handling, you might need to use only a subset of these steps. See the high-level procedures, earlier in this topic, to determine which of these steps your situation requires.

**Clean the instance**

**Note:** This step is not necessary if you are adding a new instance that contains only the default set of configurations.

If you are adding an existing instance to the cluster, you must first stop the instance and run the `splunk clean all` command:

```
splunk stop
splunk clean all
splunk start
```

The `splunk clean all` command deletes configuration updates that could interfere with the goal of maintaining the necessary identical configurations and apps across all cluster members. It does not delete any existing settings under the `shclustering` stanza in `server.conf`.

**Caution:** This step deletes most previously configured settings on the instance.

For a discussion of configurations that must be shared by all members, see "How configuration changes propagate across the search head cluster."

For more information on the `splunk clean` command, access the online CLI help:

```
splunk help clean
```

**Initialize the instance**

If the member is new to the cluster, you must initialize it before adding it to the cluster:

```
splunk init shcluster-config -auth <username>:<password> -mgmt_uri <URI>:<management_port> -replication_port <replication_port> -replication_factor <n> -conf_deploy_fetch_url <URL>:<management_port> -secret <security_key> -shcluster_label <label>
splunk restart
```

**Note the following:**
• See "Deploy a search head cluster" for details on the `splunk init shcluster-config` command, including the meaning of the various parameters.
• The `conf_deploy_fetch_url` parameter specifies the URL and management port for the deployer instance. You must set it when adding a new member to an existing cluster, so that the member can immediately contact the deployer for the latest configuration bundle, if any. See "Use the deployer to distribute apps and configuration updates."

This step is for new members only. Do not run it on members rejoining the cluster.

**Add the instance**

The final step is to add the instance to the cluster. You can run the `splunk add shcluster-member` command either on the new member or from any current member of the cluster. The command requires different parameters depending on where you run it from.

**When running the splunk add command on the new member itself, use this version of the command:**

```
splunk add shcluster-member -current_member_uri <URI>:<management_port>
```

Note the following:

• `current_member_uri` is the management URI and port of any current member of the cluster that this node is joining. This parameter allows the new node to communicate with the cluster.

**When running the splunk add command from a current cluster member, use this version of the command:**

```
splunk add shcluster-member -new_member_uri <URI>:<management_port>
```

Note the following:

• `new_member_uri` is the management URI and port of the new member that you are adding to the cluster. This parameter must be identical to the `-mgmt_uri` value you specified when you initialized this member.

**Post-add activity**

After the member joins or rejoins the cluster, it applies all replicated and deployed configuration updates:

1. It contacts the deployer to get the configuration bundle.

2. It contacts the captain and downloads the replicated configuration tarball.

See "How configuration changes propagate across the search head cluster."