Splunk® DB Connect Deploy and Use
Splunk DB Connect 3.1.4

Install and configure Splunk DB Connect on a
distributed Splunk platform deployment

Generated: 6/07/2019 3:04 pm
Install and configure Splunk DB Connect on a distributed Splunk platform deployment

To use Splunk DB Connect in a distributed search environment, including search head clusters, you must install the app on search heads and heavy forwarders.

- DB Connect does not allow you to run scheduled inputs and outputs on a search head cluster from DB Connect 3.x.x. If you want to perform the scheduled tasks, you must run them on a heavy forwarder.
- In a distributed environment, the heavy forwarder will need to be able to search your deployment's indexers in order to output to the DB. See Deploy a distributed search environment in the Distributed Search manual to learn how to set up distributed search on your deployment's heavy forwarders.
- DB Connect 3.x.x does not support resource pooling. See migrate DB Connect 2.x.x to DB Connect 3.x.x on distributed deployment.
- DB Connect is incompatible with deployment server. Do not attempt to distribute DB Connect using deployment server.
- DB Connect is incompatible with search head pooling, which was deprecated with Splunk Enterprise 6.2.0.

Deployment topologies

Design your deployment based on architecture and performance considerations. The list below specifies the typical deployment topologies in which you can install Splunk DB Connect. In all cases, you should install DB Connect on a dedicated search head.

- Single search head, multiple indexers, load-balanced forwarders
- Multiple search heads, multiple indexers, load-balanced forwarders
- Indexer cluster, single search head
- Search head cluster, multiple independent indexers, load-balanced forwarders

For general information about configuring the topology components described in this section, see Distributed Splunk Enterprise overview, or any of the following topics:

- Single search head: Deploy a distributed search environment, Add search peers to the search head
- Search head clusters: About search head clustering, Search head clustering architecture
Deploy DB Connect on search head clusters

You can deploy Splunk DB Connect in a search head clustering environment. To install, use the deployer to distribute DB Connect to all of the search head cluster members. Be aware that you must use the cluster deployer, not Deployment Server, to distribute DB Connect to search head cluster members. For more information about configuring search head clusters, see Configure the search head cluster.

1. If you have not already done so, deploy and configure a search head cluster.
2. Install the database driver(s) for the database(s) you want to connect to with DB Connect. Access the instructions on the Install database drivers for details.
3. Install DB Connect on the deployer. Access the instructions on the Single server deployment for details.
4. Set up identities and connections for your database(s).
5. Copy the `splunk_app_db_connect` directory from
   
   `$SPLUNK_HOME/etc/apps/` to the
   
   `$SPLUNK_HOME/etc/shcluster/apps/` directory on the deployer. Note that this includes all custom configuration files as well as JDBC drivers. Note that `kerberos_client.conf`, `identity.dat` cannot be replicated to other SHC nodes after it's been modified. You need to copy the files manually to other SHC nodes.
6. Deploy the configuration bundle by running the `splunk apply shcluster-bundle` command on the deployer:
   
   `splunk apply shcluster-bundle -target <URI>:-management_port> -auth <username>:<password>`

   ◊ The `-target` parameter specifies the URI and management port for any member of the cluster, for example, `https://10.0.1.14:8089`. You specify only one cluster member but the deployer pushes to all members. This parameter is required.
   ◊ The `-auth` parameter specifies credentials for the deployer instance.
7. The deployer displays a message that asks you to acknowledge that the cluster members may restart. Click Y to acknowledge.

For more information about deploying a configuration bundle, see Deploy a configuration bundle.

For full instructions about how to use the deployer to distribute apps, add-ons, and their configuration bundles, see Use the deployer to distribute apps and configuration updates.

When you use DB Connect in a search head clustering (SHC) environment, use the deployer to push configuration changes to SHC members. If you prefer to use the DB Connect UI or modify .conf files and then replicate configuration to SHC members, restart Splunk Enterprise on SHC members after you have updated them with the new configuration. There are three reasons why you must restart SHC members after updating their configuration:

- When you make a configuration change on a search head, such as a change to the RPC server port, Splunk Enterprise replicates changes to the SHC members automatically. However, the SHC members may still use the old configuration until you restart them.
- Splunk Enterprise automatically replicates SHC for changes you make to most of the DB Connect-specific settings and objects through the REST API. Splunk Enterprise does not automatically replicate changes you make by editing .conf files on a search head. To ensure that Splunk Enterprise replicates all your changes, and to replicate any changes you made by editing .conf files, you must restart the search head on which you made the change.
- Splunk Enterprise does not automatically replicate changes you make by editing kerberos_client.conf and identity.dat files. You need to manually replicate the files to other SHC node.

A note about indexes

When you create a database input, you must select the index you want to index the data your database receives. When you choose an index, by default you must choose one of the indexes on that instance of Splunk Enterprise. This means that you cannot choose an index that you have configured on a search peer but not distributed to the rest of the deployment.

To select an index that you have not configured on, for instance, a forwarder or search head that is running DB Connect, you can create or edit an indexes.conf file, and then distribute it using Deployment Server. Although
you cannot distribute DB Connect configuration using a Deployment Server, you can distribute *indexes.conf* files.

To configure peer indexes in a distributed deployment, follow the instructions in Configure the peer indexes in an indexer cluster. First, you edit the *indexes.conf* file, and then you distribute it to peers. This practice ensures that you configure search heads and forwarders to send all logs to the indexer tier, which prevents this distribution of *indexes.conf* from causing Splunk Enterprise to create local indexes on search heads and forwarders.

Once you have distributed the configuration, applications like DB Connect know which indexes exist to validate configuration.