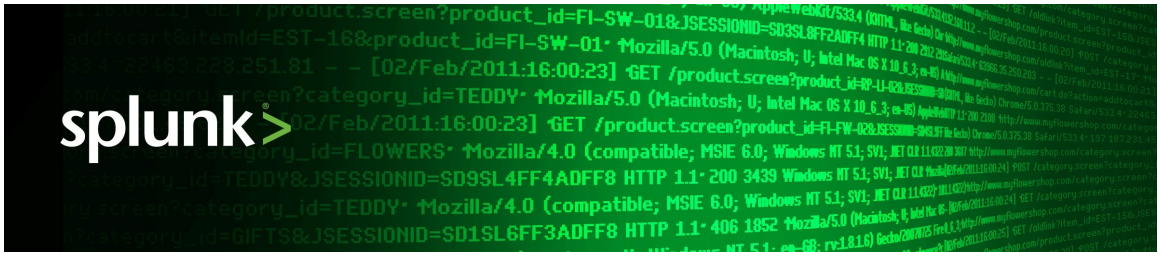

Splunk® Enterprise Installation Manual 7.1.0

How to upgrade a distributed Splunk Enterprise environment

Generated: 5/21/2018 4:50 pm

How to upgrade a distributed Splunk Enterprise environment

Distributed Splunk Enterprise environments vary widely. Some have multiple indexers or search heads, some have search head pools, and others have indexer- and search-head clusters. These types of environments present challenges over upgrading single-instance installations.

Determine the upgrade procedure to follow for your type of environment

Depending on the kind of distributed environment you have, you might have to follow separate instructions to complete the upgrade. This topic provides guidance on how to upgrade distributed environments that do not have any clustered elements like index- or search-head clusters. It also has information on how to upgrade environments that use the deprecated **search head pool** feature. Environments with clustered elements, such as indexer clusters and search head clusters, have different upgrade procedures in different topics.

- To upgrade a distributed environment that has a search head pool or does not have any clustered elements, follow the procedures in this topic.
- To upgrade an environment with index clusters, see Upgrade an indexer cluster in *Managing Indexers and Clusters of Indexers*.
- To upgrade an environment with search head clusters, see Upgrade a search head cluster in *Distributed Search*.
- If you have additional questions about upgrading your distributed Splunk Enterprise environment, log a case at the Splunk Support Portal.

Cross-version compatibility between distributed components

While there is some range in compatibility between various Splunk software components, they work best when they are all at a specific version. If you have to upgrade one or more components of a distributed deployment, you should confirm that the components you upgrade remain compatible with the components that you don't.

- For information on compatibility between differerent versions of **search heads** and **search peers** (indexers), see System requirements and other deployment considerations for distributed search in *Distributed Search*.
- For information on compatibility between indexers and forwarders, see Compatibility between forwarders and indexers in *Forwarding Data*.

Test apps prior to the upgrade

Before you upgrade a distributed environment, confirm that Splunk apps work on the version of Splunk Enterprise that you want to upgrade to. You must test apps if you want to upgrade a distributed environment with a search head pool, because search head pools use shared storage space for apps and configurations.

When you upgrade, the migration utility warns of apps that need to be copied to shared storage for pooled search heads when you upgrade them. It does not copy them for you. You must manually copy updated apps, including apps that ship with Splunk Enterprise (such as the Search app) - to shared storage during the upgrade process. Failure to do so can cause problems with the user interface after you complete the upgrade.

1. On a reference machine, install the full version of Splunk Enterprise that you currently run.
2. Install the apps on this instance.
3. Access the apps to confirm that they work as you expect.
4. Upgrade the instance.
5. Access the apps again to confirm that they still work.

If the apps work as you expect, move them to the appropriate location during the upgrade of your distributed environment:

- If you use non-pooled search heads, move the apps to `$SPLUNK_HOME/etc/apps` on each search head during the search head upgrade process.
- If you use pooled search heads, move the apps to the shared storage location where the pooled search heads expect to find the apps.

Upgrade a distributed environment with multiple indexers and non-pooled search heads

This procedure upgrades the search head tier, then the indexing tier, to maintain availability.

Prepare the upgrade

1. Confirm that any apps that the non-pooled search heads use will work on the upgraded version of Splunk, as described in "Test your apps prior to the upgrade" in this topic.

2. (Optional) If you use a **deployment server** in your environment, disable it temporarily. This prevents the server from distributing invalid configurations to your other components.
3. (Optional) Upgrade the deployment server, but do not restart it.

Upgrade the search heads

1. Disable one of the search heads.
2. Upgrade the search head. Do not let it restart.
3. After you upgrade the search head, place the confirmed working apps into the `$SPLUNK_HOME/etc/apps` directory of the search head.
4. Re-enable and restart the search head.
5. Test apps on the search head for operation and functionality.
6. If there are no problems with the search head, then disable and upgrade the remaining search heads, one by one. Repeat this step until you have reached the last search head in your environment.
7. (Optional) Test each search head for operation and functionality after you bring it up.
8. After you upgrade the last search head, test all of the search heads for operation and functionality.

Upgrade the indexers

1. Disable and upgrade the indexers, one by one. You can restart the indexers immediately after you upgrade them.
2. Test search heads to ensure that they find data across all indexers.
3. After you upgrade all indexers, restart your deployment server.

Upgrade a distributed environment with multiple indexers and pooled search heads

If your distributed environment has **pooled search heads**, the process to upgrade the environment becomes significantly more complex. If your organization has restrictions on downtime, use a maintenance window to perform this upgrade.

Following are the key concepts to upgrade this kind of environment.

- Pooled search heads must be enabled and disabled as a group.
- The version of Splunk Enterprise on all pooled search heads must be the same.
- You must test apps and configurations that the search heads use prior to upgrading the search head pool.

If you have additional concerns about this guidance here, you can log a case through the Splunk Support Portal.

To upgrade a distributed Splunk environment with multiple indexers and pooled search heads:

Prepare the upgrade

See "Configure search head pooling" in the *Distributed Search* manual for instructions on how to enable and disable search head pooling on each search head.

1. Confirm that any apps that the pooled search heads use will work on the upgraded version of Splunk Enterprise, as described in "Test your apps prior to the upgrade" in this topic.
2. If you use a **deployment server** in your environment, disable it temporarily. This prevents the server from distributing invalid configurations to your other components.
3. Upgrade your deployment server, but do not restart it.
4. Designate a search head in your search head pool to upgrade as a test for functionality and operation.
5. For the remainder of these instructions, refer to that search head as "Search Head #1."

Note: You must remove search heads from a search head pool temporarily before you upgrade them. This must be done for several reasons:

- To prevent changes to the apps and user objects hosted on the search head pool shared storage.
- To stop the inadvertent migration of local apps and system settings to shared storage during the upgrade.
- To ensure that you have a valid local configuration to use as a fallback, should a problem occur during the upgrade.

If problems occur as a result of the upgrade, search heads can be temporarily used in a non-pooled configuration as a backup.

Upgrade the search head pool

Caution: Remove each search head from the search head pool before you upgrade it, and add it back to the pool after you upgrade. While you don't need to confirm operation and functionality of each search head, only one search head at a time can be up during the upgrade phase.

1. Bring down all of the search heads in your environment. At this point, searching capability becomes unavailable, and remains unavailable until you restart all of the search heads after upgrading.
2. Place the confirmed working apps in the search head pool shared storage area.
3. Remove Search Head #1 from the search head pool.
4. Upgrade Search Head #1.
5. Restart Search Head #1.
6. Test the search head for operation and functionality. In this case, "operation and functionality" means that the instance starts and that you can log into it. It does not mean that you can use apps or objects hosted on shared storage. It also does not mean distributed searches will run correctly.
7. If the upgraded Search Head #1 functions as desired, bring it down.
8. Copy the apps and user preferences from the search head to the shared storage.
9. Add the search head back to the search head pool.
10. Restart the search head.
11. Upgrade the remaining search heads in the pool with this procedure, one by one.

Restart the search heads

1. After you have upgraded the last search head in the pool, restart all of them.
2. Test all search heads for operation and functionality across all of the apps and user objects that are hosted on the search head pool.
3. Test distributed search across all of your indexers.

Upgrade the indexers

For information on version compatibility between search heads and indexers, see System requirements and other deployment considerations for distributed search in *Distributed Search*.

1. (Optional if you do not have downtime concerns) Choose an indexer to keep the environment running, and designate it as "Indexer #1".
2. (Optional if you do not have downtime concerns) Choose a second indexer to upgrade, and designate it as "Indexer #2."
3. If you need to maintain uptime, bring down all of the indexers except Indexer #1. Otherwise, bring all indexers down and continue at Step 7.
4. Upgrade Indexer #2.
5. Bring up Indexer #2 and test for operation and functionality.

6. Once you have confirmed proper operation on Indexer #2, bring down Indexer #1.
7. Upgrade Indexer #1 and all of the remaining indexers, one by one. You can restart the indexers immediately after you upgrade them.
8. Confirm operation and functionality across all of the indexers.
9. Restart the deployment server, and confirm its operation and functionality.

Upgrade forwarders

When you upgrade your distributed environment, you can also upgrade any universal forwarders in that environment. This is not required, however, and you might want to consider whether or not you need to. Forwarders are always compatible with later versions of indexers.

To upgrade universal forwarders, see the following topics in the *Universal Forwarder* manual.

- Upgrade the Windows universal forwarder
- Upgrade the universal forwarder for *nix systems