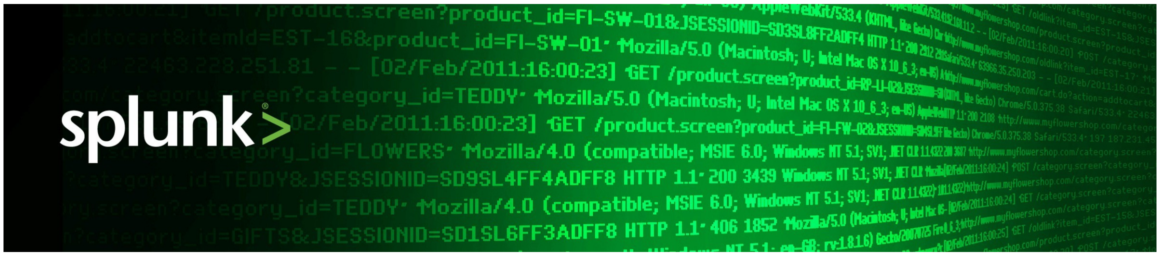

Splunk® Enterprise Installation Manual 7.1.0

Migrate a Splunk Enterprise instance from one physical machine to another

Generated: 5/21/2018 4:51 pm

Migrate a Splunk Enterprise instance from one physical machine to another

Important: These migration instructions are for on-premises Splunk Enterprise instances only.
If you are a Splunk Cloud customer or want to migrate your data from Splunk Enterprise to Splunk Cloud, do not use these instructions. Contact Professional Services for assistance.

You can migrate a Splunk Enterprise instance from one server, operating system, architecture, or filesystem to another, while maintaining the indexed data, configurations, and users. Migrating an instance of Splunk Enterprise different than upgrading one, which is merely installing a new version on top of an older one.

Do not attempt to migrate a Splunk Enterprise installation to Splunk Cloud using these instructions. Doing so could result in data loss. Speak with Professional Services or your Splunk Cloud representative for information and instructions.

When to migrate

There are a number of reasons to migrate a Splunk Enterprise install:

- Your Splunk Enterprise installation is on a host that you wish to retire or reuse for another purpose.
- Your Splunk Enterprise installation is on an operating system that either your organization or Splunk no longer supports, and you want to move it to an operating system that does have support.
- You want to switch operating systems (for example, from *nix to Windows or vice versa)
- You want to move your Splunk Enterprise installation to a different file system.
- Your Splunk Enterprise installation is on 32-bit architecture, and you want to move it to a 64-bit architecture for better performance.
- Your Splunk Enterprise installation is on a system architecture that you plan to stop supporting, and you want to move it to an architecture that you do support.

Considerations for migrating Splunk Enterprise

While migrating a Splunk Enterprise instance is simple in many cases, there are some important considerations to note when doing so. Depending on the type, version, and architecture of the systems involved in the migration, you might need to consider more than one of these items at a time.

When you migrate a Splunk Enterprise instance, note the following.

Differences in Windows and Unix path separators

The path separator (the character used to separate individual directory elements of a path) on *nix and Windows is different. When you move index files between these operating systems, you must confirm that the path separator you use is correct for the target operating system. You must also make sure that you update any Splunk configuration files (in particular, `indexes.conf`) to use the correct path separator.

For more information about how path separators can impact Splunk Enterprise installations, see Differences between *nix and Windows in Splunk operations in the *Admin* manual.

Windows permissions

When moving a Splunk Enterprise instance between Windows hosts, make sure that the destination host has the same rights assigned to it that the source host does. This includes but is not limited to the following:

- Ensure that the file system and share permissions on the target host are correct and allow access for the user that runs Splunk Enterprise.
- If Splunk Enterprise runs as an account other than the Local System user, that the user is a member of the local Administrators group and has the appropriate Local Security Policy or Domain Policy rights assigned to it by a Group Policy object

Architecture changes

If you downgrade the architecture that your Splunk Enterprise instance runs on (for example, 64-bit to 32-bit), you might experience degraded search performance on the new host due to the larger files that the 64-bit operating system and Splunk Enterprise instance created.

Distributed and clustered Splunk environments

When you want to migrate data on a distributed Splunk instance (that is, an indexer that is part of a group of search peers, or a search head that has been configured to search indexers for data), you should remove the instance from the distributed environment before attempting to migrate it.

Bucket IDs and potential bucket collision

If you migrate a Splunk Enterprise instance to another Splunk instance that already has existing indexes with identical names, you must make sure that the individual buckets within those indexes have bucket IDs that do not collide. Splunk Enterprise does not start if it encounters indexes with buckets that have colliding bucket IDs. When you copy index data, you might need to rename the copied bucket files to prevent this condition.

How to migrate

When you migrate on *nix systems, you can extract the tar file you downloaded directly over the copied files on the new system, or use your package manager to upgrade using the downloaded package. On Windows systems, the installer updates the Splunk files automatically.

1. Stop Splunk Enterprise on the host from which you want to migrate.
2. Copy the entire contents of the $SPLUNK_HOME directory from the old host to the new host.
3. Install the appropriate version of Splunk Enterprise for the target platform.
4. Confirm that index configuration files (indexes.conf) contain the correct location and path specification for any non-default indexes.
5. Start Splunk Enterprise on the new instance.
6. Log into Splunk Enterprise with your existing credentials.
7. After you log in, confirm that your data is intact by searching it.

How to move index buckets from one host to another

If you want to retire a Splunk Enterprise instance and immediately move the data to another instance, you can move individual buckets of an index between hosts, as long as:

When you copy individual bucket files, you must make sure that no bucket IDs conflict on the new system. Otherwise, Splunk Enterprise does not start. You might need to rename individual bucket directories after you move them from the source system to the target system.</code>

1. Roll any hot buckets on the source host from hot to warm.
2. Review indexes.conf on the old host to get a list of the indexes on that host.

3. On the target host, create indexes that are identical to the ones on the source system.
4. Copy the index buckets from the source host to the target host.
5. Restart Splunk Enterprise.