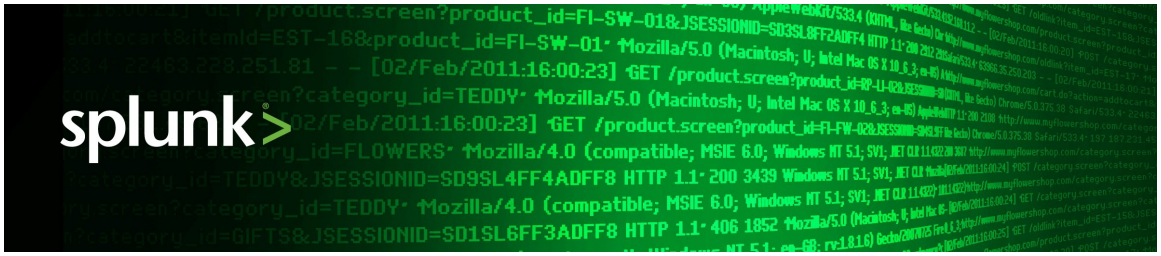

Splunk® Enterprise Installation Manual 7.1.0

Install on Linux

Generated: 5/18/2018 8:42 am

Install on Linux

You can install Splunk Enterprise on Linux using RPM or DEB packages or a tar file, depending on the version of Linux your host runs.

To install the Splunk **universal forwarder**, see Install a *nix universal forwarder in the *Universal Forwarder* manual. The universal forwarder is a separate executable, with a different installation package and its own set of installation procedures.

Upgrading Splunk Enterprise

If you are upgrading, see How to upgrade Splunk Enterprise for instructions and migration considerations before you upgrade.

Tar file installation

What to know before installing with a tar file

Knowing the following items helps ensure a successful installation with a tar file:

- Some non-GNU versions of `tar` might not have the `-C` argument available. In this case, to install in `/opt/splunk`, either `cd` to `/opt` or place the tar file in `/opt` before you run the `tar` command. This method works for any accessible directory on your host file system.
- Splunk Enterprise does not create the `splunk` user. If you want Splunk Enterprise to run as a specific user, you must create the user manually before you install.
- Confirm that the disk partition has enough space to hold the uncompressed volume of the data you plan to keep indexed.

Installation procedure

1. Expand the tar file into an appropriate directory using the `tar` command:

   ```
   tar xvzf splunk_package_name.tgz
   ```
   The default installation directory is `splunk` in the current working directory. To install into `/opt/splunk`, use the following command:

   ```
   tar xvzf splunk_package_name.tgz -C /opt
   ```

RedHat RPM installation

RPM packages are available for Red Hat, CentOS, and similar versions of Linux.

The `rpm` package does not provide any safeguards when you use it to upgrade. While you can use the `--prefix` flag to install it into a different directory, upgrade problems can occur If the directory that you specified with the flag does not match the directory where you initially installed the software.

After installation, software package validation commands (such as `rpm -Vp <rpm_file>` might fail because of intermediate files that get deleted during the installation process. To verify your Splunk installation package, use the `splunk validate files` CLI command instead.

1. Confirm that the RPM package you want is available locally on the target host.
2. Verify that the Splunk Enterprise user account that will run the Splunk services can read and access the file.
3. If needed, change permissions on the file.
   ```
   chmod 744 splunk_package_name.rpm
   ```
4. Invoke the following command to install the Splunk Enterprise RPM in the default directory `/opt/splunk`.

   ```
   rpm -i splunk_package_name.rpm
   ```
5. (Optional) To install Splunk in a different directory, use the `--prefix` flag.

   ```
   rpm -i --prefix=/opt/new_directory splunk_package_name.rpm
   ```

Replace an existing Splunk Enterprise installation with an RPM package

- Run `rpm` with the `--prefix` flag and reference the existing Splunk Enterprise directory.

  ```
  rpm -i --replacepkgs --prefix=/splunkdirectory/
  splunk_package_name.rpm
  ```

Automate RPM installation with Red Hat Linux Kickstart

- If you want to automate an RPM install with Kickstart, edit the kickstart file and add the following.

  ```
  ./splunk start --accept-license
  ./splunk enable boot-start
  ```
  The `enable boot-start` line is optional.

Debian .DEB installation

Prerequisites to installation

- You can install the Splunk Enterprise Debian package only into the default location, `/opt/splunk`.
- This location must be a regular directory, and cannot be a symbolic link.
- You must have access to the root user or have sudo permissions to install the package.
- The package does not create environment variables to access the Splunk Enterprise installation directory. You must set those variables on your own.

If you need to install Splunk Enterprise somewhere else, or if you use a symbolic link for `/opt/splunk`, then use a tar file to install the software.

Installation procedure

- Run the `dpkg` installer with the Splunk Enterprise Debian package name as an argument.

```
dpkg -i splunk_package_name.deb
```

Debian commands for showing installation status

Splunk package status:

```
dpkg --status splunk
```

List all packages:

```
dpkg --list
```

Information on expected default shell and caveats for Debian shells

Splunk Enterprise expects you to run commands from the `bash` shell. It expects `bash` to be available from `/bin/sh`.

On later versions of Debian Linux (for example, Debian Squeeze), the default shell is the `dash` shell.

Using the `dash` shell can result in zombie processes - processes that have completed execution, yet remain in the process table and cannot be killed or removed.

If you run Debian Linux, consider changing your default shell to be `bash`.

Next steps

Now that you have installed Splunk Enterprise:

- Start it and create administrator credentials. See Start Splunk Enterprise for the first time.
- Configure it to start at boot time. See Configure Splunk software to start at boot time.
- Learn what comes next. See what happens next?

Uninstall Splunk Enterprise

To learn how to uninstall Splunk Enterprise, see Uninstall Splunk Enterprise.