**Prerequisities:**

1. \*NIX or Windows Server Core installed on dedicated server (This can be virtual initially)
   1. If initially using virtual servers, create dedicated servers and add dedicated servers to cluster.
   2. Allow for replication of data
   3. And remove 1 virtual instance, then allow for replication, and then remove another virtual instance and allow for replication until all virtual instances have been replaced by dedicated servers
   4. You may need to set replication factor to N indexers – 1 (e.g. if you have 3 indexers, set replication factor to 2)
2. Each Indexer instance fully STIG compliant
3. Each indexer instance fully patched
4. Firewall rules to allow inbound port 9998 (indexing), 8089 (Management Port), 8191 (KV Store), 514 (syslog)
5. Firewall rules to allow other Indexers, Search Heads, Enterprise Security and Splunk Server Instances
6. 12 Cores per Indexer
7. Minimum 3 Indexers for a Cluster
8. 16 GB RAM per Indexer
9. 800+ IOPS Hard Drive
10. 2+ TB Hard Drive

**Note:**

(As per Splunk Documentation) If you run Splunk Enterprise in a virtual machine (VM) on any platform, performance decreases. This is because virtualization works by providing hardware abstraction on a machine into pools of resources. VMs that you define on the system draw from these resource pools. Splunk Enterprise needs sustained access to a number of resources, particularly disk I/O, for indexing operations. If you run Splunk Enterprise in a VM or alongside other VMs, indexing and search performance can degrade.

**Install Splunk on a Linux Instance:**

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.

**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
   1. . chmod 744 splunk\_package\_name.rpm
4. Invoke the following command to install the Splunk Enterprise RPM in the default directory /opt/splunk.
   1. rpm -i splunk\_package\_name.rpm
5. (Optional) To install Splunk in a different directory, use the --prefix flag.
   1. 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.