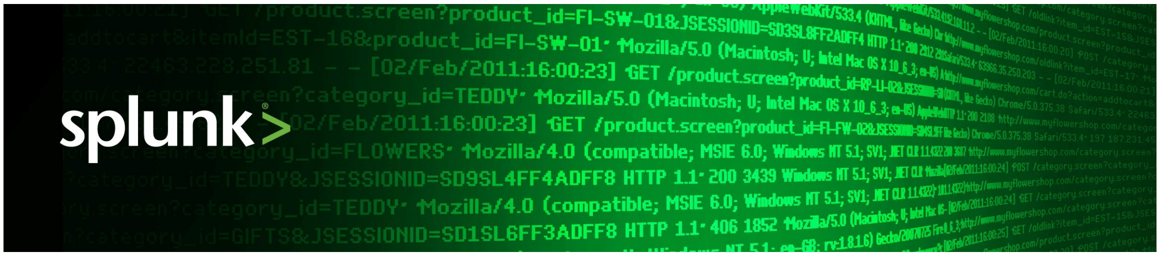

Splunk® Enterprise Updating Splunk Enterprise Instances 6.5.0

Plan a deployment

Generated: 11/11/2016 8:31 am

Plan a deployment

To set up a deployment server, you need to configure both the deployment server and the deployment clients, although most configuration occurs on the deployment server side. The main actions you need to perform are these:

- Configure the deployment clients to connect to a deployment server.
- Create directories on the deployment server to hold the deployment apps and populate them with content.
- Create mappings between deployment clients and app directories (the **server classes**).

The order in which you perform these actions is, to some degree, up to you, although a suggested procedure is described below, in "The basic steps".

After you set up the clients, the app directories, and the mappings, you can populate the app directories with content. At any time, you can tell the deployment server to distribute new or updated content from the app directories to the clients they're mapped to.

Important: Do not use deployment server or forwarder management to distribute updates to peer nodes (indexers) in an indexer cluster. Similarly, do not use deployment server to distribute apps or configuration files to search head cluster members. See "Deployment server and clusters".

Deployment server system requirements

Deployment server machine requirements

Because of high CPU and memory usage during app downloads, it is recommended that the deployment server instance reside on a dedicated machine.

Operating system compatibility

Unix deployment servers can update both Windows and Unix clients. Windows deployment servers, however, should be used only with Windows clients.

Use a Unix deployment server to update Unix deployment clients. Apps that employ scripted inputs, alerts, search commands, and so on, can run into permission problems when deployed from Windows to Unix. Specifically, scripts and other programs will not be set to executable upon delivery to the Unix clients.

Client version compatibility

6.x deployment servers are compatible with deployments clients running 5.0 and above.

Deployment server and other roles

For most deployments, the deployment server must run on a dedicated Splunk Enterprise instance that is not serving as an indexer or a search head. The exception is if the deployment server has only a small number of clients, 50 or less. Under those limited circumstances, it is possible for an indexer or search head to double as a deployment server.

Similarly, do not host a distributed management console, which is essentially a search head, on a deployment server with more than 50 clients.

You can, however, usually run a search head cluster **deployer** on the same instance as the deployment server. See "Deployer requirements" in the *Distributed Search* manual.

For more information about deployment server sizing, read "Estimate deployment server performance."

What to configure

You need to configure both the deployment server and the deployment clients:

- **On each deployment client,** you specify its deployment server by invoking a CLI command, by directly editing a configuration file, or (on Windows universal forwarders only) during installation.
- **On the deployment server,** you create directories in which the deployment apps will live. You can then use forwarder management to define server classes that encapsulate the client/app mappings.

The basic steps

To set up the deployment server, you need to perform several steps on both the deployment clients and the deployment server. Although the order of the steps is optional to some degree, here's a recommended order:

1. Determine your remote configuration needs. Questions to ask include:

◊ What types of Splunk Enterprise components do I want to configure remotely? For example: forwarders, indexers.
◊ Within each component type, what characteristics dictate the configuration needs? For example: machine type, geographic location, application.

2. Group your deployment clients by their configuration needs. You can group clients by application, machine type, or any other criteria that make sense for your deployment topology. A client can be a member of multiple groups. For example, forwarder-x might be a member of the linux-x86_64 machine type, the north-american geographic location, and the security application groups, and forwarder-y might be a member of the windows-intel machine type, the asian geographic location, and the security application groups.

These groups form the basis for your server classes. A server class maps a group of deployment clients to sets of content (in the form of deployment apps) that get deployed to them. A client can belong to mutiple server classes. For guidance on the ways that you can group deployment clients into server classes, see "About server classes."

3. Choose one of your Splunk Enterprise instances to be the deployment server. Deployment server capability is automatically enabled on Splunk Enterprise, so there is nothing you need to do in this step, beyond choosing the instance. This is the instance where you will place the downloadable content and define your server classes. The deployment server distributes content updates to its set of deployment clients.

In most cases, the deployment server requires a dedicated Splunk Enterprise instance. See "Deployment server system requirements."

Important: The deployment server cannot be a deployment client of itself. If it is, the following error will appear in `splunkd.log`: "This DC shares a Splunk instance with its DS: unsupported configuration".

4. On each deployment client, specify the deployment server chosen in step 3. Refer to "Configure deployment clients" for details. You can add more clients later.

5. On the deployment server's file system, create directories for the deployment apps that will hold the content you plan to distribute to clients. Put the app content into those directories, either now or later. Refer to "Create deployment apps" for details. You can add more deployment apps later.

6. On the deployment server, create the server classes that map deployment clients to deployment apps. Refer to "About server classes" for details on configuring server classes.

Note: In most cases, the forwarder management interface can handle the server class configuration. For some unusual situations, you might need to directly edit the underlying configuration file. No matter whether you use forwarder management or directly edit the configuration file, the basic steps are the same.

Once you've completed this configuration process, you can start distributing content to the clients. See "Deploy apps to clients" for information on how to deploy new content to clients.

SSL encryption

SSL encryption using default certificates is enabled out-of-the-box. If you change the SSL configuration on the deployment server, you must change it on its deployment clients as well. The deployment server and its clients must agree in the SSL settings for their `splunkd` management ports. *They must all have SSL enabled, or they must all have SSL disabled.*

To disable the SSL configuration on a Splunk Enterprise instance, set the `enableSplunkdSSL` attribute in server.conf to "false":

```
[sslConfig]
enableSplunkdSSL = false
```

For detailed information on using SSL with deployment server, see "Securing deployment server and clients" in the *Securing Splunk* manual.