Configure the universal forwarder

Before a forwarder can forward data, it must have a configuration. A configuration:

- Tells the forwarder what data to send.
- Tells it where to send the data.

Because the universal forwarder does not have Splunk Web, you must give the forwarder a configuration either during the installation (on Windows systems only) or later, as a separate step. To perform post-installation configuration, you can:

- Use the **CLI**. The CLI lets you do nearly all configuration in a small number of steps, but does not give you full access to the feature set of the forwarder.
- Create or modify configuration files on the forwarder directly.
- Use a deployment server. The deployment server can ease distribution of configurations, but does not make a forwarder forward data by itself. You must use the deployment server to deliver configurations to the forwarders so that they collect the data you want and send it to the place you want.

About configuring the universal forwarder with configuration files

Configuration files are text files that the universal forwarder reads when it starts up or when you reload a configuration. Forwarders must read configuration files to know where to get and send data. These files give you full access to the forwarder feature set, but editing configuration files can be difficult or mistake-prone at times. See "About configuration files" and "Configuration file precedence" in the Splunk Enterprise *Admin* manual, for details on how configuration files work.

Key configuration files are:

- inputs.conf controls how the forwarder collects data.
- outputs.conf controls how the forwarder sends data to an indexer or other forwarder.
- server.conf for connection and performance tuning.
- deploymentclient.conf for connecting to a deployment server.

You make changes to configuration files by editing them with a text editor. You can use any editor that you want as long as it can write files in ASCII/UTF-8 format.

The forwarder works with configurations for forwarding data in `outputs.conf` in `$SPLUNK_HOME/etc/system/local/`). See Configure forwarding with outputs.conf.

> The universal forwarder has a SplunkUniversalForwarder app, which includes preconfigured settings that let the forwarder run in a streamlined mode. Do not edit any configuration files within that app unless you receive specific instructions.

Best practices for deploying configuration updates across universal forwarders

You can use the following methods to deploy configuration updates across your set of universal forwarders:

- Edit or copy the configuration files for each universal forwarder manually (This is only useful for small deployments.)
- Use the Splunk **deployment server** to push configured apps to your set of universal forwarders.

- Use your own deployment tools (puppet or Chef on *nix or System Center Configuration Manager on Windows) to push configuration changes.

Configure the universal forwarder from the CLI

The CLI lets you configure most forwarding parameters without having to edit configuration files. It does not give you full access to all forwarding parameters, and you must edit configuration files in those cases.

When you make configuration changes with the CLI, the universal forwarder writes the configuration files. This prevents typos and other mistakes that can occur when you edit configuration files directly.

The forwarder writes configurations for forwarding data to `outputs.conf` in `$SPLUNK_HOME/etc/system/local/`). See Configure forwarding with outputs.conf, for information on `outputs.conf`.

Examples for using the CLI to configure a universal forwarder

Following are example procedures on how to configure a universal forwarder to connect to a receiving indexer.

Configure the universal forwarder to connect to a receiving indexer

From a shell or command prompt on the forwarder, run the command:

```
./splunk add forward-server <host name or ip address>:<listening port>
```

For example, to connect to the receiving indexer with the hostname `idx.mycompany.com` and that host listens on port 9997 for forwarders, type in:

```
./splunk add forward-server idx1.mycompany.com:9997
```

Configure the universal forwarder to connect to a deployment server

From a shell or command prompt on the forwarder, run the command:

```
./splunk set deploy-poll <host name or ip address>:<management port>
```

For example, if you want to connect to the deployment server with the hostname `ds1.mycompany.com` on the default management port of 8089, type in:

```
./splunk set deploy-poll ds1.mycompany.com:8089
```

Configure a data input on the forwarder

The Splunk Enterprise *Getting Data In* manual has information on what data a universal forwarder can collect.

1. Determine what data you want to collect.

2. From a shell or command prompt on the forwarder, run the command that enables that data input. For example, to monitor the `/var/log` directory on the host with the universal forwarder installed, type in:

```
./splunk add monitor /var/log
```

The forwarder asks you to authenticate and begins monitoring the specified directory immediately after you log in.

Restart the universal forwarder

Some configuration changes might require that you restart the forwarder.

To restart the universal forwarder, use the same CLI `restart` command that you use to restart a full Splunk Enterprise instance:

- **On Windows:** Go to `%SPLUNK_HOME%\bin` and run this command:

```
splunk restart
```

- **On *nix systems:** From a shell prompt on the host, go to `$SPLUNK_HOME/bin`, and run this command:

```
./splunk restart
```