Using the Universal Forwarder to gather data

Most IT environments today range from multiple servers in the closet of your office to hundreds of endpoint servers located in multiple geographically distributed data centers.

When the data we want to collect is not located directly on the server where Splunk is installed, the Splunk UF can be installed on your remote endpoint servers and used to forward data back to Splunk to be indexed.

The UF is similar to the Splunk server in that it has many of the same features, but it does not contain Splunk Web and doesn't come bundled with the Python executable and libraries. Additionally, the UF cannot process data in advance, such as performing line breaking and timestamp extraction.

This recipe will guide you through configuring the Splunk UF to forward data to a Splunk indexer and will show you how to set up the indexer to receive the data.

Getting ready

To step through this recipe, you will need a server with the Splunk UF installed but not configured. You will also need a running Splunk server. No other prerequisites are required.

TIP

To obtain the UF software, you need to go to http://www.splunk.com/en_us/download.html and register for an account if you do not already have one. Then, either download the software directly to your server or download it to your laptop or workstation and upload it to your server via a file-transfer process such as SFTP.

How to do it…

Follow the steps in the recipe to configure the Splunk Forwarder to forward data and the Splunk indexer to receive data:

1. On the server with the UF installed, open a command prompt if you are a Windows user or a terminal window if you are a Unix user.
2. Change to the `$SPLUNK_HOME/bin` directory, where `$SPLUNK_HOME` is the directory in which the Splunk Forwarder was installed.

   For Unix, the default installation directory will be `/opt/splunkforwarder/bin`. For Windows, it will be `C:\Program Files\SplunkUniversalForwarder\bin`.

   TIP

   If using Windows, `omit ./` in front of the Splunk command in the upcoming steps.

3. Start the Splunk Forwarder if not already started, using the following command:

   ```
   ./splunk start
   ```

4. Accept the license agreement.
5. Enable the UF to autostart, using the following command:

   ```
   ./splunk enable boot-start
   ```

6. Set the indexer that this UF will send its data to. Replace the host value with the value of the indexer as well as the username and password for the UF:

   ```
   ./splunk add forward-server <host>:9997 -auth
   <username>:<password>
   ```

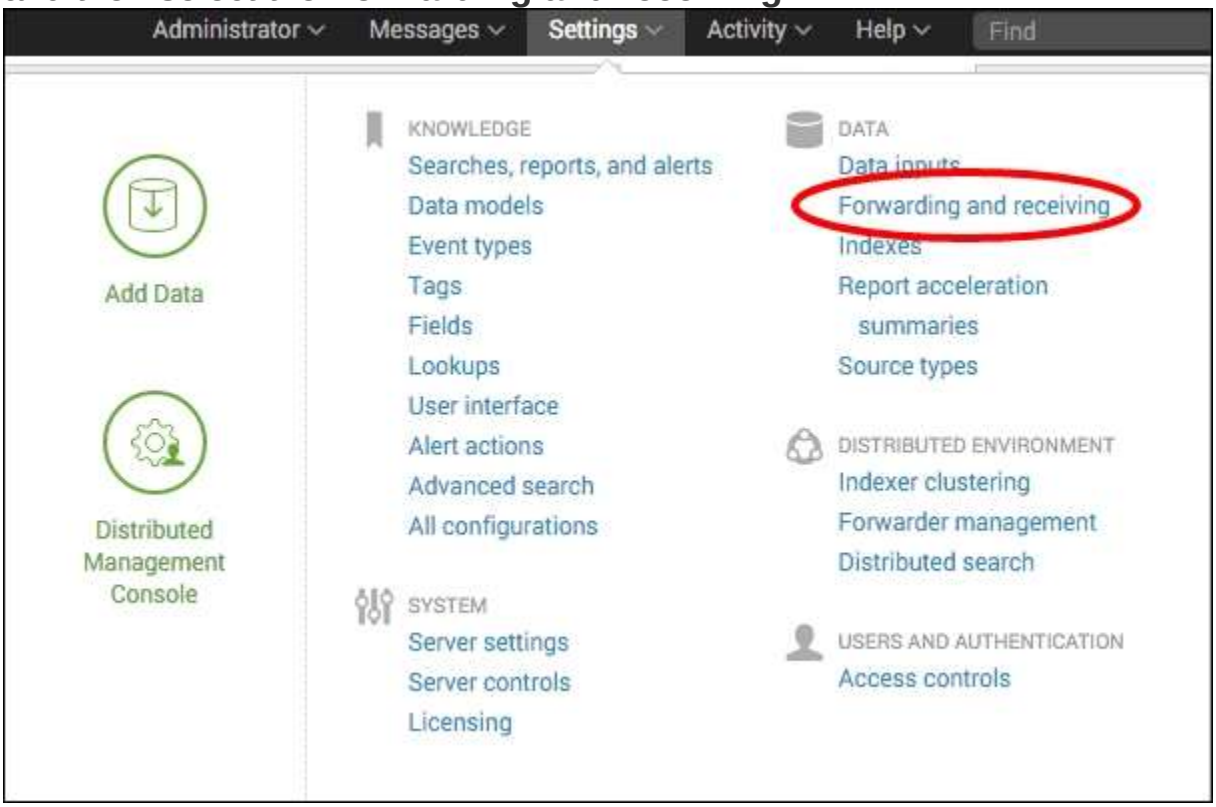
   The username and password to log in to the Forwarder (default is `admin:changeme`) is `<username>:<password>`.

   TIP

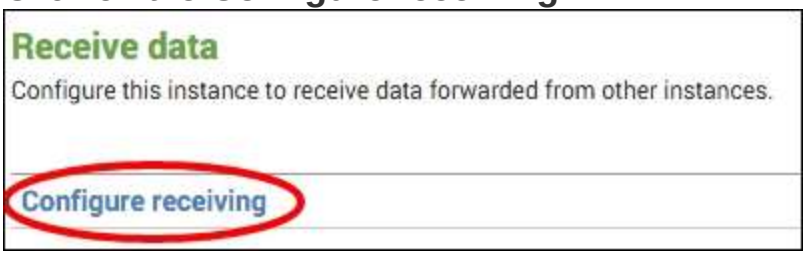
   Additional receiving indexers can be added in the same way by repeating the command in the previous step with a different indexer host or IP. Splunk will automatically load balance the forwarded data if more than one receiving indexer is specified in this manner. Port 9997 is the default Splunk TCP port and should only be changed if it cannot be used for some reason.

On the receiving Splunk indexer servers:

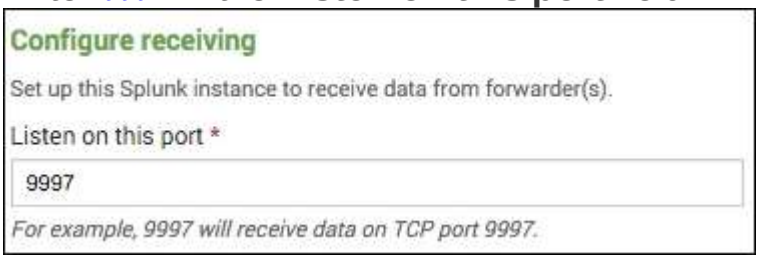
1. Log in to your receiving Splunk indexer server. From the home launcher, in the top right-hand corner click on the **Settings** menu item and then select the **Forwarding and receiving** link.



2. Click on the **Configure receiving** link.



3. Click on **New**.
4. Enter `9997` in the **Listen on this port** field.



5. Click on **Save** and restart Splunk. The UF is installed and configured to send data to your Splunk server, and the Splunk server is configured to receive data on the default Splunk TCP port 9997.

How it works…

When you tell the forwarder which server to send data to, you basically add a new configuration stanza into an `outputs.conf` file behind the scenes. On the Splunk server, an `inputs.conf` file will contain a `[splunktcp]` stanza to enable receiving. The `outputs.conf` file on the Splunk forwarder will be located in `$SPLUNK_HOME/etc/system/local`, and the `inputs.conf` file on the Splunk server will be located in the local directory of the app you were in (the launcher app in this case) when configuring receiving.

Using forwarders to collect and forward data has many advantages. The forwarders communicate with the indexers on TCP port 9997 by default, which makes for a very simple set of firewall rules that need to be opened. Forwarders can also be configured to load balance their data across multiple indexers, increasing search speeds and availability. Additionally, forwarders can be configured to queue the data they collect if communication with the indexers is lost. This can be extremely important when collecting data that is not read from logfiles, such as performance counters or syslog streams, as the data cannot be re-read.

There's more…

While configuring the settings of the UF can be performed via the command-line interface of Splunk, as outlined in this recipe, there are several other methods to update the settings quickly and allow for customization of the many configuration options that Splunk provides.

ADD THE RECEIVING INDEXER VIA OUTPUTS.CONF

The receiving indexers can be directly added to the `outputs.conf` configuration file on the UF.
Edit `$SPLUNK_HOME/etc/system/local/outputs.conf`, add your input, and then, restart the UF. The following example configuration is provided, where two receiving indexers are specified. The `[tcpout-server]` stanza can be

leveraged to add output configurations specific to an individual receiving indexer:

```
[tcpout]
defaultGroup = default-autolb-group

[tcpout:default-autolb-group]
disabled = false
server = mysplunkindexer1:9997,mysplunkindexer2:9997

[tcpout-server://mysplunkindexer1:9997]
[tcpout-server://mysplunkindexer2:9997]
```

TIP

If nothing has been configured in `inputs.conf` on the UF, but `outputs.conf` is configured with at least one valid receiving indexer, the Splunk forwarder will only send internal forwarder health-related data to the indexer. It is, therefore, possible to configure a forwarder correctly and be detected by the Splunk indexers, but not actually send any real data.