Splunk® Enterprise Getting Data In 9.0.0

Get data from TCP and UDP ports

Generated: 7/07/2022 8:01 pm

Get data from TCP and UDP ports

The Splunk platform lets you ingest data that comes in over a network port. It can accept data from both the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) network protocols.

Splunk Enterprise accepts this kind of data from **heavy forwarders** or **universal forwarders** that capture the data and send it to the Splunk Enterprise instance. For security, Splunk Enterprise accepts connections only from forwarders that have the correct Secure Sockets Layer (SSL) certificates to connect to the instance. If you want to send data from a TCP or UDP source such as the syslog service, use the universal forwarder to listen to the source and forward the data to your Splunk Enterprise deployment.

You can configure the forwarder to accept an input on any TCP or UDP port. The forwarder consumes any data that arrives on these ports. You can use this method to capture data from network services such as the syslog service. You can also set up the netcat service and bind it to a network port.

Network ports and Splunk Enterprise

TCP is the network protocol that underlies the Splunk Enterprise data distribution scheme. Use the TCP protocol to send data from any remote host to your Splunk Enterprise server. Splunk Enterprise can index remote data from any application that transmits over TCP.

Both Splunk Enterprise and the universal forwarder support monitoring over UDP. The best practice is to use TCP to send network data whenever possible. UDP is not desirable as a transport because, among other reasons, it does not guarantee the delivery of network packets.

For Syslog, the best practice is to use a syslog server, such as syslog-ng or Splunk Connect for Syslog.

When you monitor TCP network ports, the user that Splunk Enterprise or the universal forwarder runs as must have access to the port you want to monitor. On many UNIX operating systems, by default, you must run Splunk Enterprise as the root user to listen directly on a port below 1024.

Confirm how your network device handles external monitoring before you use the network monitoring input

Before you begin monitoring the output of a network device with the network monitor, confirm how the device interacts with external network monitors.

If you configure some network devices, such as a Cisco Adaptive Security Appliance (ASA), to log TCP network activity and the device can't connect to the monitor, it might reduce performance on the device or stop it from logging. By default, the Cisco ASA stops accepting incoming network connections when it encounters network congestion or connectivity problems.

Add a network input to a forwarder and send the data to Splunk Cloud Platform

Splunk Cloud Platform can accept network data that arrives only from either a universal or heavy forwarder. Before you can collect network data for Splunk Cloud Platform, you must have the following:

- An installed universal or heavy forwarder.

- The Splunk Cloud Platform universal forwarder credentials package. This package sets up the forwarding connection to your Splunk Cloud Platform instances and makes sure that data is transmitted securely between the forwarder and Splunk Cloud Platform.
- A text editor to edit the input and forwarding configurations.

Add a network input using a configuration file

On either a heavy forwarder or a universal forwarder, use a text editor to add a stanza for a network input to the inputs.conf configuration file in the $SPLUNK_HOME/etc/system/local/ directory, or %SPLUNK_HOME%\etc\system\local on Windows, or in your own custom application directory in $SPLUNK_HOME/etc/apps/. If you haven't worked with Splunk configuration files before, see About configuration files in the Splunk Enterprise *Admin Manual* before you start.

> While this procedure focuses on configuring forwarders to send network data to {Splunk Enterprise} instances, you can perform it without modifications on any Splunk Enterprise instance.

You can configure any number of settings and values for an input type. If you do not specify a value for a setting, the forwarder uses default values. These values are either defined in the Splunk platform code or exist in default configuration files within the $SPLUNK_HOME/etc/system/default/ directory on the instance, or %SPLUNK_HOME%\etc\system\default on Windows..

Following is the general procedure to configure a network input:

1. Use a text editor to open the inputs.conf configuration file in one of the directories described in this section.
2. Add an input stanza that represents the kind of network data that you want to collect.
3. (Optional) Provide additional settings to configure how the Spunk platform handles the data.
4. Save the file and exit the text editor.
5. Restart the forwarder or Splunk Enterprise instance.

Configure a TCP network input

When you configure a TCP network input, the forwarder listens on that input for incoming network data over the TCP protocol.

This stanza configures the forwarder to listen to the server specified by `<remote server>` on the specified `<port>`. If `<remote server>` is blank, the software listens to all connections on the specified port.

```
[tcp://<remote server>:<port>]
<attrbute1> = <val1>
<attrbute2> = <val2>
...
```

The following settings control how the data is stored on the Splunk platform:

Setting	Description	Default
`host = <string>`	Sets the host field to a static value for this stanza. Also sets the host key initial value. The Splunk platform uses the key during parsing and indexing, in particular to set the host field. It also uses the host field at search time. The platform prepends `<string>` with `host::`.	The IP address or fully-qualified domain name of the host where the data originates.

Setting	Description	Default
`index = <string>`	Sets the index where Splunk Enterprise stores the events from this input. The Splunk platform prepends `<string>` with `index::`. On Splunk Cloud Platform, confirm that this index is present before you configure this setting.	`main` or whatever you set the default index to
`sourcetype = <string>`	Sets the sourcetype field for events from this input. Also declares the source type for this data, instead of letting Splunk Enterprise determine it. This is important both for searchability and for applying the relevant formatting for this type of data during parsing and indexing. Sets the sourcetype key initial value. Splunk Enterprise uses the key during parsing and indexing, in particular to set the source type field during indexing. Splunk Enterprise uses the source type field that it used at search time. The Splunk platform prepends `<string>` with `sourcetype::`.	Splunk Enterprise chooses a source type based on various aspects of the data. There is no hard-coded default.
`source = <string>`	Sets the source field for events from this input. The Splunk platform prepends `<string>` with `source::`. Do not override the source key unless absolutely necessary. The input layer provides a more accurate string to aid in problem analysis and investigation by recording the file from which the data is retrieved. Consider using source types, tagging, and search wildcards before overriding this value.	

The input file pathindexQueue

Specifies where the input processor deposits the events that it reads.

Set it to `parsingQueue` to apply the props.conf file and other parsing rules to your data. Set it to `indexQueue` to send your data directly into the index.

parsingQueuedns | none

A value of `ip` sets the host to the IP address of the remote server.

`dns` sets the host to the DNS entry of the remote server.

`none` leaves the host as specified.

ip

Configure an encrypted TCP network input over SSL

Use this stanza type if you receive encrypted, unparsed network data from a forwarder or third-party system. Set `<port>` to the port on which the forwarder or third-party system sends unparsed, encrypted data.

`[tcp-ssl:<port>]`

Configure a UDP network input

This type of input stanza is similar to the TCP type, except that it listens on a UDP network port. If you provide `<remote server>`, the port that you specify only accepts data from that host. If you don't specify anything for `<remote server>`, the port accepts data that comes from any host.

```
[udp://<remote server>:<port>]
<attrbute1> = <val1>
<attrbute2> = <val2>
...
```

The following settings control how the Splunk platform stores the data:

Setting	Description	Default
`host = <string>`	Sets the host field to a static value for this stanza. Also sets the host key initial value. Splunk Enterprise uses this key during parsing and indexing, in particular to set the host field. It also uses the host field at search time. The `<string>` is prepended with `host::`.	The IP address or fully-qualified domain name of the host where the data originated.
`index = <string>`	Sets the index where Splunk Enterprise stores events from this input. The `<string>` is prepended with `index::`.	`main` or whatever you set the default index to
`sourcetype = <string>`	Sets the sourcetype field for events from this input. Also declares the source type for this data, as opposed to letting Splunk Enterprise determine it. This is important both for searchability and for applying the relevant formatting for this type of data during parsing and indexing. Sets the sourcetype key initial value. Splunk Enterprise uses the key during parsing and indexing, in particular to set the source type field during indexing. It also uses the source type field that it used at search time. The `<string>` is prepended with `sourcetype::`.	Splunk Enterprise picks a source type based on various aspects of the data. There is no hard-coded default.
`source = <string>`	Sets the source field for events from this input. The `<string>` is prepended with `source::`. Do not override the source key unless absolutely necessary. The input layer provides a more accurate string to aid in problem analysis and investigation by recording the file from which the data is retrieved. Consider use of source types, tagging, and search wildcards before overriding this value.	

The input file path.indexQueueSets where the input processor deposits the events that it reads. Set to `parsingQueue` to apply the props.conf file and other parsing rules to your data. Set to `indexQueue` to send your data directly into the index.parsingQueue`_rcvbuf = <integer>`Sets the receive buffer for the UDP port, in bytes. If the value is 0 or negative, Splunk Enterprise ignores the value.1,572,864 unless the value is too large for an OS. In this case, Splunk Enterprise halves the value from this default continuously until the buffer size is at an acceptable level.`no_priority_stripping = true | false`

Sets how Splunk Enterprise handles receiving syslog data.

If you set this setting to true, Splunk Enterprise does not strip the <priority> syslog field from received events.

Depending on how you set this setting, Splunk Enterprise also sets event timestamps differently. When set to true, Splunk Enterprise honors the timestamp as it comes from the source. When set to false, Splunk Enterprise assigns events the local time.

false (Splunk Enterprise strips <priority>.)`no_appending_timestamp = true | false`Sets how Splunk Enterprise applies timestamps and hosts to events.

If you set this setting to true, Splunk Enterprise does not append a timestamp and host to received events.

Do not configure this setting if you want to append timestamp and host to received events.

false (Splunk Enterprise appends timestamps and hosts to events)

Add a network input using Splunk Web

You can use Splunk Web to add network inputs on Splunk Enterprise or on a heavy forwarder that you want to configure to send data to Splunk Cloud Platform. Splunk Web is not available on universal forwarders, and Splunk Cloud Platform can't monitor network inputs directly using Splunk Web.

Go to the Add Data page

You can get to the Add data page in two ways.

To go to the Add Data page by Splunk Settings, follow these steps:

1. Click **Settings**.
2. Click **Data Inputs**.
3. Select **TCP** or **UDP**.
4. Click **New Local TCP** or **New Local UDP** to add an input.

To go to the Add Data page by Splunk Home, follow these steps:

1. Click the **Add Data** link in Splunk Home.
2. Click **Monitor** to monitor a network port on the local machine, or **Forward** to receive network data from another machine.

   Forwarding a file requires additional setup.
3. If you select **Forward**, choose or create the group of forwarders you want this input to apply to.
4. Click **Next**.

Specify the network input

1. Click **TCP** / **UDP** to add an input.
2. Click the **TCP** or **UDP** button to select a TCP or UDP input.
3. In the **Port** field, enter a port number.
4. In the **Source name override** field, enter a new source name to override the default source value, if necessary.

   Consult Splunk Support before changing the Source name override value.
5. If this is a TCP network input, decide whether you want this port to accept connections from all hosts or only one host in the **Only accept connection from** field. If you only want the input to accept connections from one host, enter the host name or IP address of the host. You can use wildcards to specify hosts.
6. Click **Next** to continue to the **Input Settings** page.

Specify input settings

The **Input Settings** page lets you configure source type, application context, default host value, and index. All of these parameters are optional.

1. Set the **Source type**. This is a default field that Splunk Enterprise adds to events and uses to determine processing characteristics, such as timestamps and event boundaries.
2. Set a value for **Host**. You have several choices:
   - Select **IP** to set the input processor to rewrite the host with the IP address of the remote server.
   - Select **DNS** to set the host to the DNS entry of the remote server.
   - Select **Custom** to set the host to a user-defined label.

   Learn more about setting the host value in About hosts.

   > The host value sets only the host field in the resulting events. Setting this value does not direct the Splunk platform to look on a specific host on your network.
3. For **Index**, set the index that you want Splunk Enterprise to send data to for this input. Leave the value as `default` unless you have defined multiple indexes to handle different types of events. In addition to indexes for user data, Splunk Enterprise has a number of utility indexes, which also appear in this dropdown box.
4. Click **Review**.

Review your choices

After entering all your input settings, review your selections. the Splunk platform lists the options you selected, including the type of monitor, the source, the source type, the application context, and the index.

1. Review the settings.
2. If they are not what you want, click the left angle bracket (**<**) to go back to the previous step in the wizard. Otherwise, click **Submit**.

A Success page appears and the Splunk platform begins indexing the specified network input.

Add a network input using the CLI

You can use the CLI on a universal or heavy forwarder to configure it to send data to Splunk Cloud Platform. You can also use the CLI on a Splunk Enterprise instance. To access the CLI, navigate to the `$SPLUNK_HOME/bin/` directory (%SPLUNK_HOME%\bin on Windows) and use the `./splunk` command.

If you get stuck, the CLI has help. Access the CLI help by typing `splunk help`. Individual commands have their own help pages as well and can be accessed by typing `splunk help <command>`.

The following CLI commands are available for network input configuration:

Command	Command syntax	Action
add	`add tcp|udp <port> [-parameter value] ...`	Add inputs from `<port>`.
edit	`edit tcp|udp <port> [-parameter value] ...`	Edit a previously added input for `<port>`.
remove	`remove tcp|udp <port>`	Remove a previously added data input.
list	`list tcp|udp [<port>]`	List the currently configured monitor.

The `<port>` is the port number on which to listen for data. The user you run the Splunk platform as must have access to this port.

You can modify the configuration of each input by setting any of these optional parameters:

Parameter	Description
`sourcetype`	Provide a sourcetype field value for events from the input source.
`index`	Provide the destination index for events from the input source.
`hostname`	Provide a host name to set as the host field value for events from the input source.
`remotehost`	Provide an IP address to exclusively accept data from.
`resolvehost`	Set to true or false (T | F). Default is false. Set to true to use DNS to set the host field value for events from the input source.
`restrictToHost`	Provide a host name or IP address to accept connections only from the specified host or IP address.

Examples

The following example shows how to configure a UDP input to watch port 514 and set the source type to `syslog` on a *nix system:

```
./splunk add udp 514 -sourcetype syslog
```

The following example shows how to set the UDP input host value using DNS name resolution on a *nix system. Use `auth` with your username and password:

```
./splunk edit udp 514 -resolvehost true -auth admin:ch@ng3d
```

Change restricted hosts on a TCP network input

If you decide to only accept connections from a specific host when you create a TCP input, after you save that input, you can't change or remove that host later, either from Splunk Web or the CLI.

To change or remove the restricted host of a port, you must first delete the input that contains the old restricted host. Then, you must add a new input that either contains the new restricted host or has no restriction.

UDP packets and line merging

The Splunk platform doesn't index each UDP packet as an independent event. Instead, it performs event merging on the data stream and merges events together if they don't have a clear timestamp.

You can avoid this problem by editing the underlying source type in the props.conf file and setting the `SHOULD_LINEMERGE` setting to `false`. This keeps the Splunk platform from merging packets together.