

Heavy Forwarders >

Why?

- Index and parse data locally
- Load balance
- Specific data routing rules



Heavy Forwarders >

- A complete installation of Splunk
 - The same installation you would use for an indexer or search head
- Apply a forwarding license
 - Settings > Licensing > Change license group >

Change license group

The type of license group determines what sorts of licenses can be used in the pools on this license server.
[Learn more](#)

☐ Enterprise license

This license adds support for multi-user and distributed deployments, alerting, role-based security, single sign-on, scheduled PDF delivery, and unlimited data volumes.

There are no valid Splunk *Enterprise licenses* installed. You will be prompted to install a license if you choose this option.

☒ Forwarder license

Use this group when configuring Splunk as a forwarder. [Learn more](#)

☐ Free license

Use this group when you are running Splunk Free. This license has a 500MB/day daily indexing volume.
[Learn more](#)

☐ Enterprise Trial license

This is your included download trial. IMPORTANT: If you switch to another license, you cannot return to the Trial. You must install an Enterprise license or switch to Splunk Free.

Heavy Forwarders >

Configuration

- Settings > Forwarding and Receiving > Add new (under Forward data)

Forwarding and receiving

Forward data

Set up forwarding between two or more Splunk instances.

[Forwarding defaults](#)

[Configure forwarding](#)

Actions

[Add new](#)

Receive data

Configure this instance to receive data forwarded from other instances.

[Configure receiving](#)

Actions

[Add new](#)

Heavy Forwarders >

Configuration

- Enter new hostname:port number, or IP:port number
- Separate multiples with commas

Add new

[Forwarding and receiving](#) » [Forward data](#) » Add new

Enter host:port to forward data to. Data will be auto load balanced to each host:port.

Host *

Set as host:port or IP:port.

You must also enable receiving on this host.

Cancel

Save

Heavy Forwarders >

Configuration

- To save a copy of the data locally, select Forwarding defaults

Forwarding and receiving

Forward data
Set up forwarding between two or more Splunk instances.

Forwarding defaults

Configure forwarding

Actions

Add new

Receive data
Configure this instance to receive data forwarded from other instances.

Configure receiving

Actions

Add new

Heavy Forwarders >

Forwarding defaults

[Forwarding and receiving](#) » Forwarding defaults

Store a local copy of forwarded events?

☐ Yes ☒ No

This saves a copy of all indexed data on this Splunk instance and forwards copies to other instances.

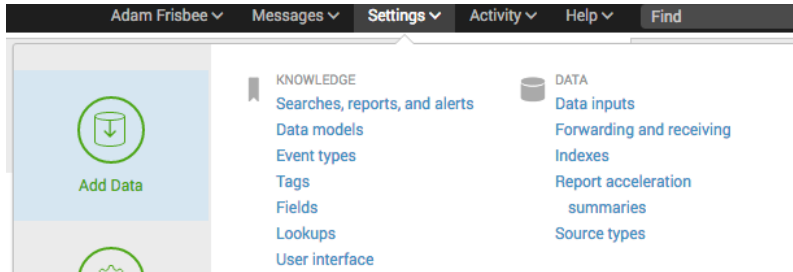
Cancel

Save

Heavy Forwarders >

| Universal | Heavy |
|---------------------------------------|---------------------------------|
| "Light" agent | Full Splunk Enterprise instance |
| Event parsing available in some cases | Event parsing available |
| No event routing | Event routing available |

Monitoring Files & Folders >



upload

files from my computer

Local log files
Local structured files (e.g. CSV)
[Tutorial for adding data](#)



monitor

files and ports on this Splunk indexer

Files - WMI - TCP/UDP - Scripts
Modular inputs for external data sources



forward

data from Splunk forwarder

Files - TCP/UDP - Scripts

Monitoring Files & Folders >

Add Data

Select Source

Set Source Type

Input Settings

Review

Done

<

Next >

Files & Directories

Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector

Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP

Configure Splunk to listen on a network port.

Scripts

Get data from any API, service, or database with a script.

Nest Thermostat Information

Collect usage data from your Nest thermostat by pulling data from Nest.com's webapp.

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. Splunk monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. [Learn More](#)

File or Directory?

Browse

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Continuously Monitor

Index Once

Whitelist?

Blacklist?

© Adam Frisbee, adamfrisbee.com

Monitoring Files & Folders >

Select source

☒ C:\

- > Info
- > Install
- > PerfLogs
- > Program Files
- > Program Files (x86)
- > Python27
- > Users
- > Windows

KBSERVICE.SHUTDOWN

SLC-P-SPLUNK_patchlog.csv

update.vbs

Windows

Select source

- > bin
- > boot
- > dev
- > etc
- > home
- > lib
- > lib64
- > lost+found
- > media
- > mnt
- > moodledata
- > opt
- > proc
- > root
- > run
- > sbin
- > srv
- > sys
- > tmp
- > usr
- > var

initrd.img

vmlinuz

Linux

Monitoring Files & Folders >

splunk> Apps

Add Data

Select Source

Input Settings

Review

Done

< Review >

Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Automatic

Select

New

web

App context

Application contexts are folders within a Splunk instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. [Learn More](#)

App Context

Search & Reporting

Host

When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Constant value

Regular expression on path

Segment in path

Host field value

website

Index

Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index

web

[Create a new index](#)

Thanks, Splunkers!

