

Splunk Server Setup

1. Set up **Receiving** on Splunk Server

Navigate to Settings->Forwarding and receiving

The screenshot shows the Splunk web interface. At the top, the navigation bar includes 'Administrator', '1 Messages', 'Settings', 'Activity', 'Help', and 'Find'. A red arrow points to the 'Settings' menu. Below the navigation bar, a sidebar on the left contains 'Add Data', 'Explore Data', and 'Monitoring Console'. The main content area displays a search bar and a list of settings categories: KNOWLEDGE, DATA, DISTRIBUTED ENVIRONMENT, SYSTEM, and USERS AND AUTHENTICATION. A red arrow points to 'Forwarding and receiving' under the DATA category. Below this, the 'Forward data' section is visible, followed by the 'Receive data' section. In the 'Receive data' section, a red arrow points to the 'Configure receiving' link.

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

Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

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

Type	Actions
Configure receiving	+ Add new

Click **New Receiving Port**, then enter default port 9997

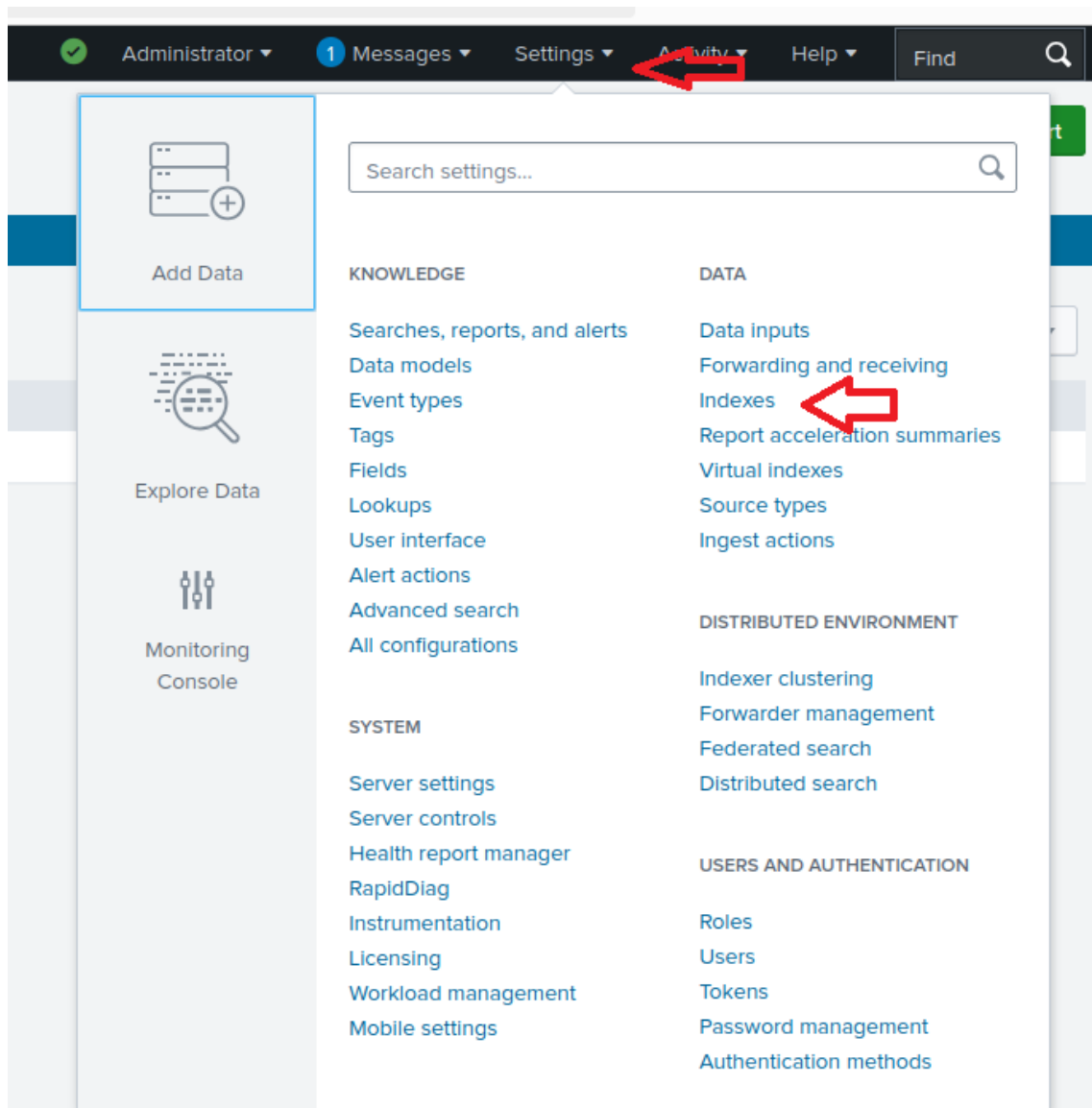
Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *

For example, 9997 will receive data on TCP port 9997.

2. Set up **Index** on Splunk server



Click **New Index**

Input **winsrvlogs** as Index Name and **Save**

Indexes

A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. [Learn more](#)

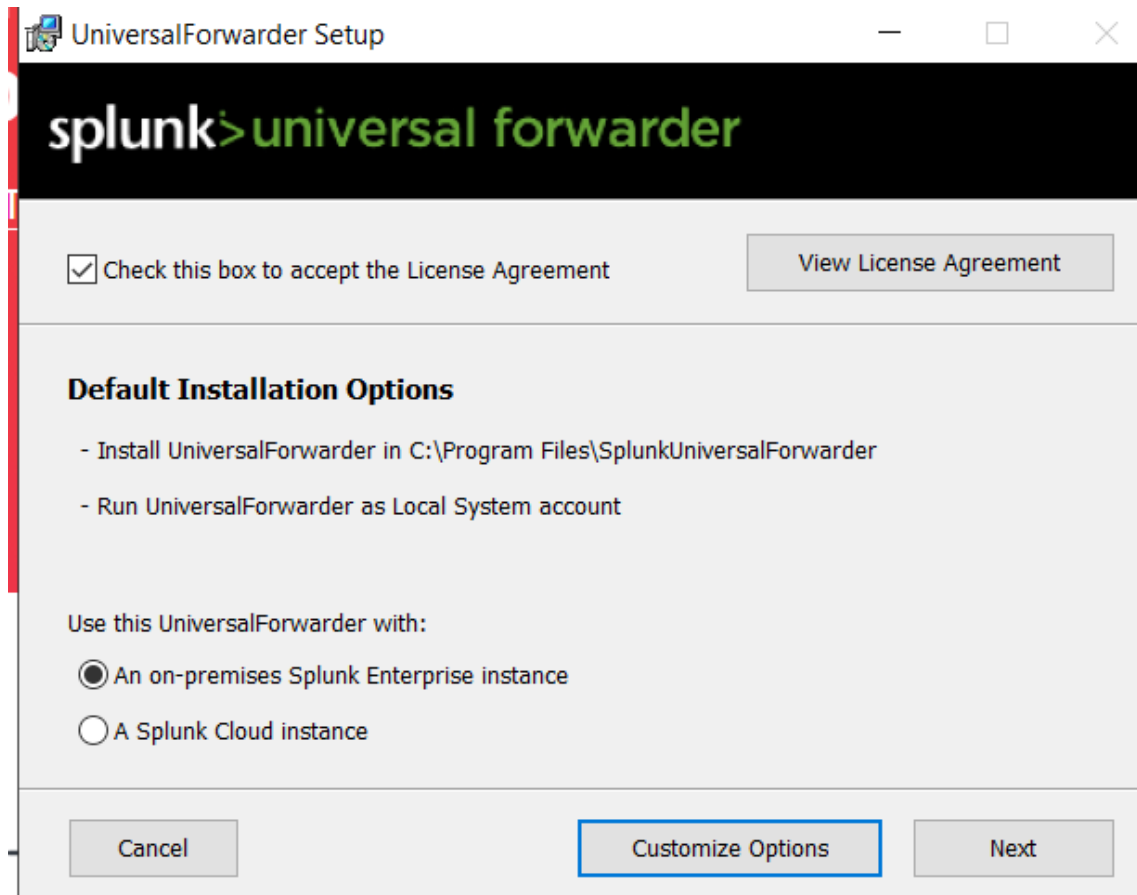
16 Indexes 20 per page

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path	Status
_audit	Edit Delete Disable	Events	system	2 MB	489.28 GB	118K	34 minutes ago	a few seconds ago	\$SPLUNK_DB/_auditdb	N/A	✓ Enabled
_configtracker	Edit Delete Disable	Events	system	2 MB	489.28 GB	199	34 minutes ago	a few seconds ago	\$SPLUNK_DB/_configtrackerdb	N/A	✓ Enabled
_disappevent	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	489.28 GB	0			\$SPLUNK_DB/_disappeventdb	N/A	✓ Enabled
_diskclient	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	489.28 GB	0			\$SPLUNK_DB/_diskclientdb	N/A	✓ Enabled
_stphomehome	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	489.28 GB	0			\$SPLUNK_DB/_stphomehome/db	N/A	✓ Enabled
_internal	Edit Delete Disable	Events	system	2 MB	489.28 GB	17K	34 minutes ago	a few seconds ago	\$SPLUNK_DB/_internaldb	N/A	✓ Enabled
_introspection	Edit Delete Disable	Events	system	4 MB	489.28 GB	2.6K	34 minutes ago	a few seconds ago	\$SPLUNK_DB/_introspectiondb	N/A	✓ Enabled
_metrics	Edit Delete Disable	Metrics	system	5 MB	489.28 GB	12K	34 minutes ago	a few seconds ago	\$SPLUNK_DB/_metricsdb	N/A	✓ Enabled
_metrics_rollup	Edit Delete Disable	Metrics	system	1 MB	489.28 GB	0			\$SPLUNK_DB/_metrics_rollupdb	N/A	✓ Enabled
_telemetry	Edit Delete Disable	Events	system	1 MB	489.28 GB	0			\$SPLUNK_DB/_telemetrydb	N/A	✓ Enabled
_thefakebucket	Edit Delete Disable	Events	system	1 MB	489.28 GB	0			\$SPLUNK_DB/_thefakebucketdb	N/A	✓ Enabled
history	Edit Delete Disable	Events	system	1 MB	489.28 GB	0			\$SPLUNK_DB/historydb	N/A	✓ Enabled
main	Edit Delete Disable	Events	system	1 MB	489.28 GB	0			\$SPLUNK_DB/maindb	N/A	✓ Enabled
splunklogger	Edit Delete Disable	Events	system	0 B	489.28 GB	0			\$SPLUNK_DB/splunkloggerdb	N/A	✗ Disabled
summary	Edit Delete Disable	Events	system	1 MB	489.28 GB	0			\$SPLUNK_DB/summarydb	N/A	✓ Enabled
winsrvlogs	Edit Delete Disable	Events	search	1 MB	500 GB	0			\$SPLUNK_DB/winsrvlogsdb	N/A	✓ Enabled

Install Splunk forwarder on Windows Server 2019

Go to link https://www.splunk.com/en_us/download/universal-forwarder.html to download universal forwarder for Windows server. The purpose of deploying splunk forwarder on windows server is to send logs and everything from Windows Server to Splunk for future investigation.

1. Install Splunk forwarder on Windows and just click **Next**



splunk>universal forwarder

Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

Username:

☐ Generate random password

Password:

Confirm password:

Cancel

Back

Next

Below is the reason to setup static ip on splunk server.

splunk>universal forwarder

If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Deployment Server

Hostname or IP

:

*Enter the hostname or IP of your deployment server, e.g.
ds.splunk.com*

default is 8089

Cancel

Back

Next

UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Receiving Indexer

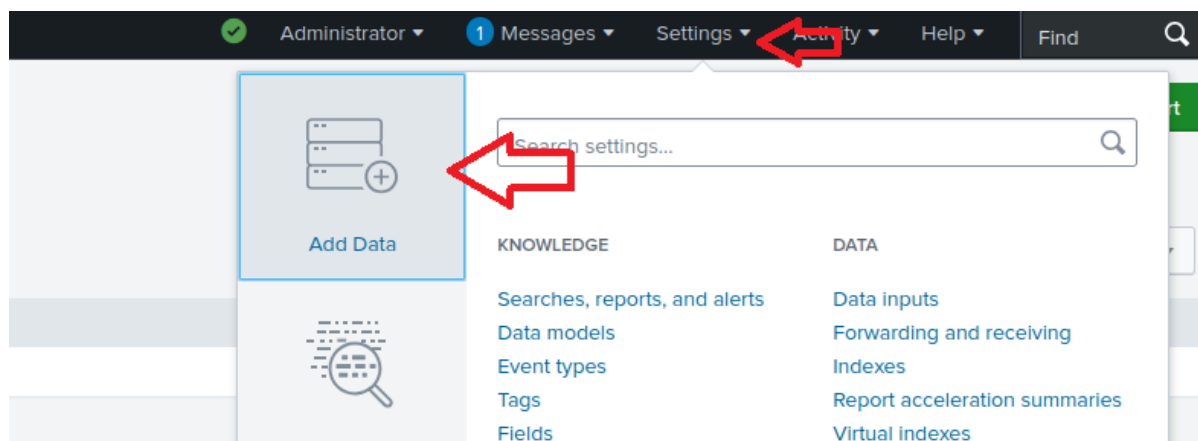
Hostname or IP

:

Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com *default is 9997*

Configure Forward on Splunk Server

1. Setting -> Add Data



2. Choose **Forward**

What data do you want to send to the Splunk platform?

Follow guides for onboarding popular data sources



Cloud computing

Get your cloud computing data in to the Splunk platform.

10 data sources



Networking

Get your networking data in to the Splunk platform.

2 data sources



Operating System

Get your operating system data in to the Splunk platform.

1 data source



Security

Get your security data in to the Splunk platform.

3 data sources

4 data sources in total

Or get data in with the following methods



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 platform instance

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



Forward

data from a Splunk forwarder

Files - TCP/UDP - Scripts

3. Select host **Windows SRV**, input **New Server Class Name** and Next

splunk>enterprise

Apps

Add Data

Select Forwarders

Select Source

Input Settings

Review

Done

< Back

Next >

Select Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. [Learn More](#)

Select Server Class

New

Existing

Available host(s)

add all

WINDOWS SRV

Selected host(s)

remove all

WINDOWS SRV

New Server Class Name

AD

4. Local Event Logs -> add all

Add Data

Select Forwarders Select Source Input Settings Review Done

< Back Next >

Local Event Logs
Collect event logs from this machine.

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

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

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

Splunk Assist Instance Identifier
Assigns a random identifier to every node

Systemd Journal Input for Splunk
This is the input that gets data from journald (systemd's logging component) into Splunk.

Logd Input for the Splunk platform
This input collects data from logd on macOS and sends it to the Splunk platform.

[Splunk Server Gateway](#)

Universal Forwarders to monitor local Windows event log channels, indexed by installed applications, services, and system processes. The for every event log input defined in the Splunk platform. [Learn More](#)

Available Item(s) [add all >](#)

Application
ForwardedEvents
Security
Setup
System

Select the Windows Event Logs you want to index from the list.

Selected Item(s) <

Application
ForwardedEvents
Security
Setup
System

Splunk platform instance have access to?

or monitoring event logs of remote Windows machines?

5. index -> winsrvlogs

Add Data

Select Forwarders Select Source Input Settings Review Done

< Back Review >

Input Settings

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

Index

The Splunk platform 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 [Create a new index](#)

FAQ

- > How do indexes work?
- > How do I know when to create or use multiple indexes?

Add Data

Select Forwarders Select Source Input Settings Review Done

< Back Submit >

Review

Server Class Name AD

List of Forwarders

Collection Name localhost

Input Type Windows Event Logs

Event Logs

Index winsrvlogs

6. Now Windows Server host has shown up in Splunk

New Search

source="WinEventLog:*" index="winsrvlogs"

✓ 8,963 events (before 9/18/24 7:21:27.000 PM) No Event Sampling ▾

Events (8,963) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

< Hide Fields

≡ All Fields

SELECTED FIELDS

a host 1

a source 4

a sourcetype 4

INTERESTING FIELDS

a Account_Domain 11

a Account_Name 53

a ComputerName 3

host

1 Value, 100% of events

Selected Yes No

Reports

Top values

Top values by time

Rare values

Events with this field

Values	Count	%
SRV	8,963	100%

EventLog:Application

System

← → ▾ ▴ Control Panel > System and Security > System

Control Panel Home

Device Manager

Remote settings

Advanced system settings

View basic information about your computer

Windows edition

Windows Server 2019 Standard

© 2018 Microsoft Corporation. All rights reserved.

Windows Server 2019

System

Processor:

AMD Ryzen 7 5800X 8-Core Processor

3.79 GHz (2 processors)

Installed memory (RAM):

4.00 GB

System type:

64-bit Operating System, x64-based processor

Pen and Touch:

No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name:

SRV

Full computer name:

SRV.test.local

Computer description:

SRV

Domain:

test.local

Windows activation

Windows is activated [Read the Microsoft Software License Terms](#)

Product ID: 00429-80456-02966-AA114

See also

Security and Maintenance

Also, Windows Server Local Event Logs has been forwarded to Splunk

source="WinEventLog:*" index="winsrvlogs"

✓ 8,963 events (before 9/18/24 7:21:27.000 PM) No Event Sampling ▼

Events (8,963) Patterns Statistics Visualization

Format Timeline ▼ – Zoom Out + Zoom to Selection × Deselect



< Hide Fields

≡ All Fields

SELECTED FIELDS

a host 1
a source 4
a sourcetype 4

INTERESTING FIELDS

a Account_Domain 11
a Account_Name 53
a ComputerName 3
EventCode 100+
EventType 5
a index 1
a Keywords 8
linecount 40

sourcetype

4 Values, 100% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Values	Count	%
WinEventLog:Security	5,730	63.929%
WinEventLog:System	2,540	28.339%
WinEventLog:Application	659	7.352%
WinEventLog:Setup	34	0.379%

ComputerName=SRV-test.local

Show all 12 lines

Event Viewer

File Action View Help

Event Viewer (Local)

Custom Views

Windows Logs

Application

Security

Setup

System

Forwarded Events

Applications and Services Logs

Subscriptions

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	9/18/2024 12:23:08 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	9/18/2024 12:23:08 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	9/18/2024 12:23:08 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	9/18/2024 12:22:36 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	9/18/2024 12:22:36 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	9/18/2024 12:22:08 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	9/18/2024 12:22:08 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	9/18/2024 12:22:08 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	9/18/2024 12:21:08 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	9/18/2024 12:21:08 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	9/18/2024 12:21:08 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	9/18/2024 12:20:36 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	9/18/2024 12:20:36 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	9/18/2024 12:20:08 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	9/18/2024 12:20:08 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	9/18/2024 12:20:08 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	9/18/2024 12:19:45 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	9/18/2024 12:19:34 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	9/18/2024 12:19:34 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	9/18/2024 12:19:34 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	9/18/2024 12:19:34 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	9/18/2024 12:19:34 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	9/18/2024 12:19:34 PM	Microsoft Windows security auditing.	4672	Special Logon

Event 4634, Microsoft Windows security auditing.

General Details

An account was logged off.

Actions

Security

Open Saved Lo

Create Custom

Import Custom

Clear Log...

Filter Current L

Properties

Find...

Save All Events

Attach a Task Tr

View

Refresh

Help

Event 4634, Microso

Event Propert

Attach Task To

Copy

Save Selected E

Refresh

Help