



yapılandır'a tıklayıp ardından new receiving portu yapılandırarak devam edeceğiz.

**Forwarding and receiving**

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

[Forwarding defaults](#)

[Configure forwarding](#)

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

[Configure receiving](#) [+ Add new](#)

[New Receiving Port](#)

25 per page

Varsayılan olarak, Splunk örneği verileri 9997 portundaki yönlendiriciden alır. Bu portu kullanmak veya değiştirmek bize kalmış. Şimdilik, Splunk'ımızı aşağıda gösterildiği gibi 9997 portunu dinlemeye başlayacak şekilde yapılandıracağız ve Kaydedeceğiz:

**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.

[Cancel](#) [Save](#)

Dinleme portumuz 9997 artık etkinleştirildi ve veriyi bekliyor. İstersek, Eylemler sütununun altındaki Sil seçeneğine tıklayarak bu girişi silebiliriz.

**Receive data** [New Receiving Port](#)

[Forwarding and receiving](#) » [Receive data](#)

Successfully saved "9997".

Showing 1-1 of 1 item

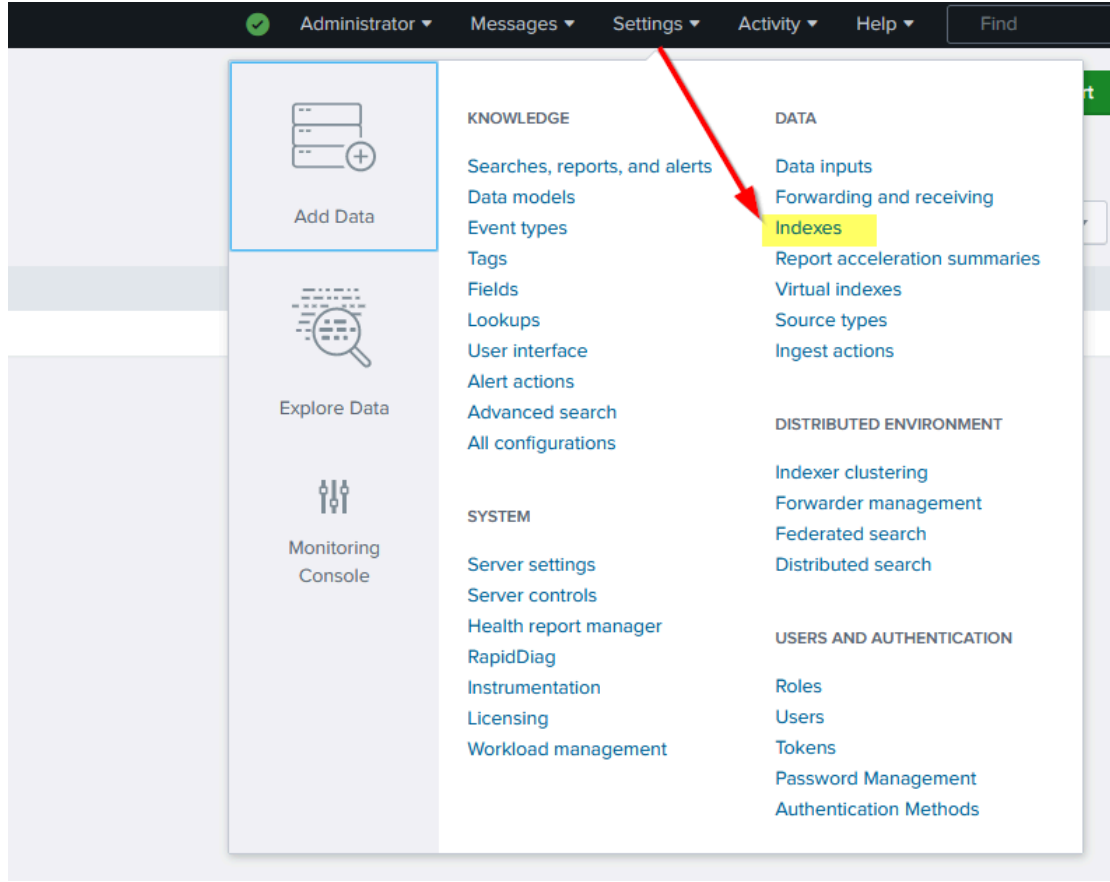
filter

25 per page

Listen on this port	Status	Actions
9997	Enabled   <a href="#">Disable</a>	<a href="#">Delete</a>

## Dizin Oluşturma

Artık bir dinleme portunu etkinleştirdiğimize göre, önemli bir sonraki adım, tüm alınan verileri depolayacak bir dizin oluşturmaktır. Bir dizin belirtmezsek, alınan verileri ana dizin adı verilen varsayılan dizinde depolamaya başlayacaktır.



Dizinler sekmesi kullanıcı tarafından veya varsayılan olarak oluşturulan tüm dizinleri içerir. Bu, Boyut, Olay Sayısı, Ana Yol, Durum vb. gibi dizinler hakkında bazı önemli meta verileri gösterir.

Indexes											
A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. <a href="#">Learn more</a>											
12 Indexes <input type="text" value="filter"/> <input type="button" value="Q"/>											
20 per page											
Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path	Status
__audit	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Disable</a>	Events	system	4 MB	488.28 GB	30.6K	3 days ago	a few seconds ago	\$SPLUNK_DB/audit/db	N/A	Enabled
__configtracker	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Disable</a>	Events	system	3 MB	488.28 GB	250	3 days ago	7 minutes ago	\$SPLUNK_DB/__configtracker/db	N/A	Enabled
__internal	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Disable</a>	Events	system	84 MB	488.28 GB	1.58M	3 days ago	a few seconds ago	\$SPLUNK_DB/__internaldb/db	N/A	Enabled
__introspection	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Disable</a>	Events	system	289 MB	488.28 GB	216K	3 days ago	a few seconds ago	\$SPLUNK_DB/__introspection/db	N/A	Enabled
__metrics	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Disable</a>	Metrics	system	48 MB	488.28 GB	1.39M	3 days ago	a few seconds ago	\$SPLUNK_DB/__metrics/db	N/A	Enabled
__metrics_rollup	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Disable</a>	Metrics	system	1 MB	488.28 GB	0			\$SPLUNK_DB/__metrics_rollup/db	N/A	Enabled
__telemetry	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Disable</a>	Events	system	1 MB	488.28 GB	26	2 days ago	6 hours ago	\$SPLUNK_DB/__telemetry/db	N/A	Enabled
__thefishbucket	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Disable</a>	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/thefishbucket/db	N/A	Enabled
history	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Disable</a>	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/historydb/db	N/A	Enabled
main	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Disable</a>	Events	system	7 MB	488.28 GB	69.4K	3 years ago	26 minutes ago	\$SPLUNK_DB/defaultdb/db	N/A	Enabled
splunklogger	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Enable</a>	Events	system	0 B	488.28 GB	0			\$SPLUNK_DB/splunklogger/db	N/A	Disabled
summary	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Disable</a>	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/summarydb/db	N/A	Enabled

**New Index** düğmesine tıklayın, formu doldurun ve dizini oluşturmak için **Save**'e tıklayın. Aşağıda gösterildiği gibi Linux\_host adında bir dizin oluşturduk:

**New Index**

**General Settings**

Index Name:

Index Data Type: ☒ Events ☐ Metrics

Home Path:

Cold Path:

Thawed Path:

Data Integrity Check: ☒ Enable ☐ Disable

Max Size of Entire Index:  GB

Max Size of Hot/Warm/Cold Bucket:  GB

**Save** **Cancel**

## Yönlendiriciyi Yapılandırma

Verileri doğru hedefe gönderdiğinden emin olmak için yönlendiriciyi yapılandırmanın zamanı geldi. Linux ana bilgisayar terminaline geri dönün, /opt/splunkforwarder/bin dizinine gidin: Bu komut, 9997 portunu dinleyen yönlendirici sunucuyu ekleyecektir.

```
root@coffely:/opt/splunkforwarder/bin# ./splunk add forward-server 10.10.183.89:9997
Added forwarding to: 10.10.183.89:9997.
root@coffely:/opt/splunkforwarder/bin#
```

## Linux Günlük Kaynakları

Linux tüm önemli günlüklerini aşağıda gösterildiği gibi /var/log dosyasına depolar. Burada syslog'u Splunk'a aktaracağız. Diğer tüm günlükler aynı yöntem kullanılarak aktarılabilir.

```

ubuntu@crackme: /var/log$ ls
Xorg.0.log          dmesg.1.gz          prime-offload.log
Xorg.0.log.old      dmesg.2.gz          prime-supported.log
alternatives.log    dmesg.3.gz          private
amazon              dmesg.4.gz          samba
appport.log         dpkg.log             speech-dispatcher
appport.log.1       fontconfig.log       syslog
apt                 gdm3                 syslog.1
audit               gpu-manager-switch.log
auth.log            gpu-manager.log      syslog.2.gz
auth.log.1          hp                   syslog.3.gz
btmp                journal              syslog.4.gz
cloud-init-output.log
cloud-init.log      kern.log              syslog.5.gz
cups                kern.log.1            syslog.6.gz
dist-upgrade        landscape             syslog.7.gz
dmesg               lastlog               unattended-upgrades
dmesg.0             lightdm               wtmp
openvpn

```

Sonra, Splunk forwarder'a hangi günlük dosyalarını izleyeceğini söyleyeceğiz. Burada, Splunk Forwarder'a /var/log/syslog dosyasını izlemesini söyleyeceğiz.

```

root@coffely:/opt/splunkforwarder/bin# ./splunk add monitor /var/log/syslog -index Linux_host
Added monitor of '/var/log/syslog'.

```

## Inputs.conf'u keşfetme

Yukarıda kullandığımız komutlardan sonra eklenen yapılandırmaya /opt/splunkforwarder/etc/apps/search/local dizininde bulunan inputs.conf dosyasını da açabiliriz.

```

root@coffely:/opt/splunkforwarder/etc/apps/search/local# ls
inputs.conf

```

input.conf dosyasının içeriğini cat komutunu kullanarak görebiliriz.

```

root@coffely:/opt/splunkforwarder/etc/apps/search/local# cat inputs.conf
[monitor:///var/log/syslog]
disabled = false
index = Linux_host

```

## Logger Utility'yi Kullanma


Logger, syslog dosyasına eklenen test günlüklerini oluşturmak için yerleşik bir komut satırı aracıdır. Syslog dosyasını zaten izlediğimiz ve tüm günlükleri Splunk'a gönderdiğimiz için, bir sonraki adımda oluşturduğumuz günlük Splunk günlükleriyle bulunabilir. Komutu çalıştırmak için aşağıdaki komutu kullanın.

```
root@coffely:/opt/splunkforwarder/bin# logger "coffely-has-the-best-coffee-in-town"
root@coffely:/opt/splunkforwarder/bin# tail -1 /var/log/syslog
Nov 26 20:37:18 coffely ubuntu: coffely-has-the-best-coffee-in-town
root@coffely:/opt/splunkforwarder/bin#
```

New Search

Save As ▾Create Table ViewClose

index=Linux\_host

All time ▾

✓ 813 events (before 9/7/23 11:06:37.000 AM)No Event Sampling ▾

Job ▾||▣→🖨️⬇️💡 Smart Mode ▾

Events (813)PatternsStatisticsVisualization

Format Timeline ▾Zoom Out+ Zoom to SelectionX Deselect

1 hour per column

ListFormat20 Per Page ▾< Prev12345678...Next >

< Hide Fields≡ All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

# date\_hour 5

# date\_mday 1

# date\_minute 36

a date\_month 1

i	Time	Event
>	9/7/23 11:06:33.000 AM	Sep 7 11:06:33 coffely ubuntu: coffely-has-the-best-coffee-in-town host = coffely   source = /var/log/syslog   sourcetype = syslog
>	9/7/23 11:02:22.000 AM	Sep 7 11:02:22 coffely systemd-timesyncd[370]: Timed out waiting for reply from 185.125.190.57:123 (ntp.ubuntu.com). host = coffely   source = /var/log/syslog   sourcetype = syslog
>	9/7/23 11:02:11.000 AM	Sep 7 11:02:11 coffely systemd-timesyncd[370]: Timed out waiting for reply from 185.125.190.56:123 (ntp.ubuntu.com). host = coffely   source = /var/log/syslog   sourcetype = syslog