

Veri alımını yapılandırmak Splunk'un önemli bir parçasıdır. Bu, verilerin analistler tarafından indekslenmesini ve aranabilir olmasını sağlar.

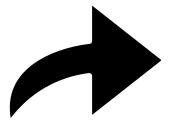
Splunk, İşletim Sistemi günlükleri, Web Uygulamaları, Saldırı Algılama günlükleri, Osquery günlükleri vb. gibi çeşitli günlük kaynaklarından veri kabul eder.

Splunk Forwarders

Splunk, farklı kullanım durumlarında kullanılabilen iki temel türde ileticiye sahiptir. Bunlar aşağıda açıklanmıştır:

Heavy Forwarders

Günlükleri hedefe iletmeden önce kaynakta bir filtre uygulamamız, analiz etmemiz veya değişiklik yapmamız gerektiğinde kullanılır.



Universal Forwarders

Hedef bilgisayara yüklenen hafif bir aracıdır ve temel amacı, herhangi bir filtre veya indeksleme uygulamadan günlükleri almak ve bunları Splunk örneğine veya başka bir yönlendiriciye göndermektir.

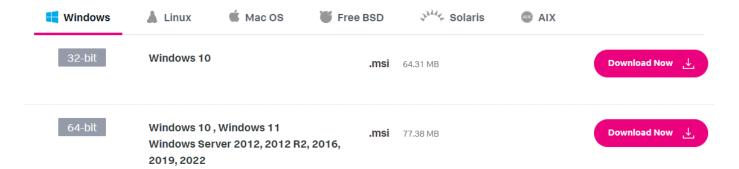
Ayrı olarak indirilmesi ve kullanımdan önce etkinleştirilmesi gerekir.

Evrensel yönlendiriciler resmi Splunk web sitesinden indirilebilir. Aşağıda gösterildiği gibi çeşitli işletim sistemlerini destekler:

Splunk Universal Forwarder 9.0.3

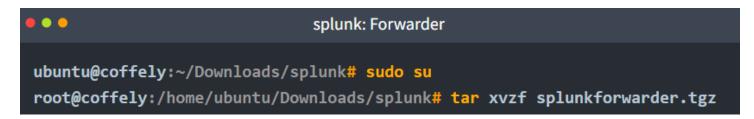
Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package



Yönlendiriciyi Yükleme

Kullanıcıyı sudo olarak değiştirin, aşağıdaki komutla yönlendiriciyi açın ve yükleyin.



Yukarıdaki komut, **splunkforwarder** klasöründeki tüm gerekli dosyaları yükleyecektir. Sonra, bu klasörü **mv splunkforwarder /opt/** komutuyla **/opt/** yoluna taşıyacağız.

```
root@coffely:/home/ubuntu/Downloads/splunk# mv splunkforwarder /opt/
root@coffely:/home/ubuntu/Downloads/splunk# cd /opt/splunkforwarder
root@coffely:/opt/splunkforwarder# ./bin/splunk start --accept-license

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.

Create credentials for the administrator account.

Characters do not appear on the screen when you type in credentials.

Please enter an administrator username:
```

Şimdi Splunk forwarder örneğini çalıştıracağız ve aşağıda gösterildiği gibi ona yeni kimlik bilgilerini sağlayacağız:

```
Please enter an administrator username: gozde
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Failed to auto-set default user.
Failed to create the unit file. Please do it manually later.
Splunk> Like an F-18, bro.
Checking prerequisites...
        Checking mgmt port [8089]: open
                Creating: /opt/splunkforwarder/var/lib/splunk
                Creating: /opt/splunkforwarder/var/run/splunk
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/
static/css
```

Varsayılan olarak, Splunk yönlendiricisi 8089 numaralı portta çalışır. Sistem portun kullanılamaz olduğunu tespit ederse, kullanıcıdan özel portu isteyecektir.