

```
d=EST-6&product_id=AV-5B-02" "Opera/9.01 (Windows NT 5.1; U; en)" 1
-01" "Opera/9.01 (Windows NT 5.1; U; en)" 695 130.253.37.97 [05/Mar
06 195.69.160.22 [05/Mar/2014 18:10:54:192] "GET /cart.do?action=r
ws NT 5.1; SV1)" 163 131.178.233.243 [05/Mar/2014 18:10:54:171] "G
; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 S
on=addtocart&itemId=EST-7&product_id=FI-SW-01" "Mozilla/4.0 (compa
ion=purchase&itemId=EST-27&product_id=EL-DH-01" "Mozilla/4.0 (comp
1 "http://buttercup-shopping.com/category.do?action=addtocart&item
1437 "http://buttercup-shopping.com/category.do?action=addtocart&item
screen?category_id=SURPRISE&JSESSIONID=5D75L3FF9ADFF10 HTTP 1.1" 24
SESSIONID=5D35L1FF7ADFF2 HTTP 1.1" 200 2567 "http://buttercup-shop
1.1" 200 1649 "http://buttercup-shopping.com/category.screen?category
p-shopping.com/category.screen?category_id=BOUQUET5" "Mozilla/5.0 (
FF3ADFF4 HTTP 1.1" 200 363 "http://buttercup-shopping.com/product.i
```

splunk>enterprise

Splunk ile terminalden ilerlemek için bilmemiz gereken en temel komutları bu yazıda paylaşacağım. Bu komutlar /opt/splunk/ dizininden çalıştırılır. Aynı komutları farklı platformlarda kullanabileceğimizi belirtmek önemlidir.

splunk start

Splunk start komutu Splunk sunucusunu başlatmak için kullanılır. Bu komut gerekli tüm Splunk işlemlerini başlatır ve sunucunun gelen verileri kabul etmesini sağlar. Sunucu zaten çalışıyorsa, bu komutun hiçbir etkisi olmayacaktır.

```
Splunk start

root@coffely:/opt/splunk#./bin/splunk start
Splunk> Finding your faults, just like mom.
....
Checking prerequisites...
  Checking http port [8000]: open
  Checking mgmt port [8089]: open
  Checking appserver port [127.0.0.1:8065]: open
  Checking kvstore port [8191]: open
  Checking configuration... Done.
....
....
The Splunk web interface is at http://coffely:8000
```

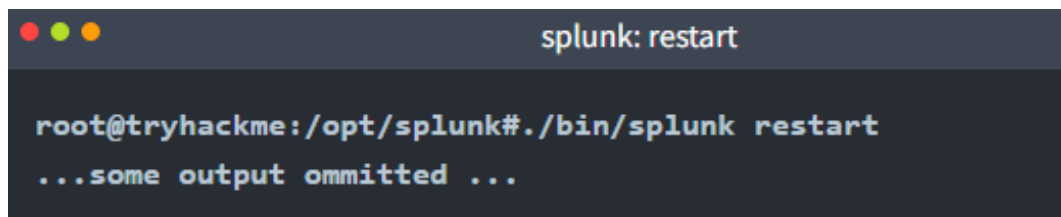
splunk stop

Splunk stop komutu Splunk sunucusunu durdurmak için kullanılır. Bu komut çalışan tüm Splunk işlemlerini durdurur ve sunucunun gelen verileri kabul etmesini devre dışı bırakır. Sunucu çalışmıyorsa, bu komutun hiçbir etkisi olmayacaktır.

```
ubuntu@coffely:/opt/splunk$ sudo su
root@coffely:/opt/splunk# ./bin/splunk stop
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.
.....
Stopping splunk helpers...
Done.
root@coffely:/opt/splunk#
```

splunk restart

Splunk yeniden başlatma komutu Splunk sunucusunu yeniden başlatmak için kullanılır. Bu komut tüm çalışan Splunk işlemlerini durdurur ve sonra tekrar başlatır. Bu, Splunk yapılandırma dosyalarında değişiklik yapıldığında veya sunucunun herhangi bir nedenle yeniden başlatılması gerektiğinde yararlıdır.



```
splunk: restart

root@tryhackme:/opt/splunk# ./bin/splunk restart
...some output ommitted ...
```

splunk status

Splunk status komutu, Splunk sunucusunun durumunu kontrol etmek için kullanılır. Bu komut, sunucunun mevcut durumu hakkında, çalışıp çalışmadığı ve oluşabilecek hatalar dahil olmak üzere bilgi görüntüler.

```
root@coffely:/opt/splunk# ./bin/splunk status
splunkd is running (PID: 4739).
splunk helpers are running (PIDs: 4740 4862 4923 4933 4950 4992 5537).
root@coffely:/opt/splunk#
```

splunk add oneshot

Splunk add oneshot komutu, Splunk dizinine tek bir olay eklemek için kullanılır. Bu, test amaçları veya daha büyük bir veri akışının parçası olmayabilecek bireysel olaylar eklemek için yararlıdır.

```
splunk: add oneshot

root@coffely:/opt/splunk# ./bin/splunk add oneshot
...some output ommitted ...
```

splunk search

Splunk arama komutu, Splunk dizininde veri aramak için kullanılır. Bu komut, belirli olayları aramak için kullanılabileceği gibi, Splunk'un arama dilini kullanarak daha karmaşık aramalar yapmak için de kullanılabilir.

```
root@coffely:/opt/splunk# ./bin/splunk search coffely
WARNING: Server Certificate Hostname Validation is disabled.
.conf/[sslConfig]/cliVerifyServerName for details.
Splunk username: gozde
Password:
root@coffely:/opt/splunk#
```

splunk help

En önemli komut, tüm yardım seçeneklerini sağlayan help komutudur.

```
Welcome to Splunk's Command Line Interface (CLI).

Type these commands for more help:

    help [command]           type a command name to access its help page
    help [object]           type an object name to access its help page
    help [topic]            type a topic keyword to get help on a topic
    help commands           display a full list of CLI commands
    help clustering         commands that can be used to configure the
clustering setup
    help shclustering       commands that can be used to configure the
Search Head Cluster setup
    help control, controls  tools to start, stop, manage Splunk process
```