srsenthi@LIN73000604 MINGW64 ~

$ cd D:

srsenthi@LIN73000604 MINGW64 /d

$ cd Users/srsenthi/splunk/boxes/

srsenthi@LIN73000604 MINGW64 /d/Users/srsenthi/splunk/boxes

$ vagrant box add ubuntu-xenial-base xenial-server-cloudimg-amd64-vagrant.box

==> box: Box file was not detected as metadata. Adding it directly...

==> box: Adding box 'ubuntu-xenial-base' (v0) for provider:

box: Unpacking necessary files from: file://D:/Users/srsenthi/splunk/boxes/x enial-server-cloudimg-amd64-vagrant.box

box:

The box you're attempting to add already exists. Remove it before

adding it again or add it with the `--force` flag.

Name: ubuntu-xenial-base

Provider: virtualbox

Version: 0

srsenthi@LIN73000604 MINGW64 /d/Users/srsenthi/splunk/boxes

$ ls

xenial-server-cloudimg-amd64-vagrant.box

srsenthi@LIN73000604 MINGW64 /d/Users/srsenthi/splunk/boxes

$ vagrant box list

ubuntu-xenial-base (virtualbox, 0)

srsenthi@LIN73000604 MINGW64 /d/Users/srsenthi/splunk/boxes

$

srsenthi@LIN73000604 MINGW64 ~

$ cd d:

srsenthi@LIN73000604 MINGW64 /d

$ cd Users/srsenthi/splunk/with-ubuntu-indexer/

srsenthi@LIN73000604 MINGW64 /d/Users/srsenthi/splunk/with-ubuntu-indexer

$ vagrant up

Bringing machine 'indexer' up with 'virtualbox' provider...

==> indexer: Clearing any previously set forwarded ports...

==> indexer: Clearing any previously set network interfaces...

==> indexer: Preparing network interfaces based on configuration...

indexer: Adapter 1: nat

indexer: Adapter 2: hostonly

==> indexer: Forwarding ports...

indexer: 22 (guest) => 2222 (host) (adapter 1)

==> indexer: Running 'pre-boot' VM customizations...

==> indexer: Booting VM...

==> indexer: Waiting for machine to boot. This may take a few minutes...

indexer: SSH address: 127.0.0.1:2222

indexer: SSH username: ubuntu

indexer: SSH auth method: password

indexer: Warning: Connection reset. Retrying...

==> indexer: Machine booted and ready!

==> indexer: Checking for guest additions in VM...

==> indexer: Setting hostname...

==> indexer: Mounting shared folders...

indexer: /vagrant => D:/Users/srsenthi/splunk/with-ubuntu-indexer

==> indexer: Machine already provisioned. Run `vagrant provision` or use the `--provision`

==> indexer: flag to force provisioning. Provisioners marked to run always will still run.

srsenthi@LIN73000604 MINGW64 /d/Users/srsenthi/splunk/with-ubuntu-indexer

$ vagrant ssh

Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-79-generic x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:

http://www.ubuntu.com/business/services/cloud

1 package can be updated.

0 updates are security updates.

Last login: Fri Jun 16 06:18:58 2017 from 10.0.2.2

ubuntu@indexer:~$ sudo su

root@indexer:/home/ubuntu# cd /va

vagrant/ var/

root@indexer:/home/ubuntu# cd /vagrant/

root@indexer:/vagrant# ls

splunk-6.6.0-1c4f3bbe1aea-linux-2.6-amd64.deb Vagrantfile

ubuntu-xenial-16.04-cloudimg-console.log

root@indexer:/vagrant# cd /opt/splunk/bin/

root@indexer:/opt/splunk/bin# ./splunk start

splunkd 17530 was not running.

Stopping splunk helpers...

Done.

Stopped helpers.

Removing stale pid file... done.

Splunk> Like an F-18, bro.

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.

Checking critical directories... Done

Checking indexes...

Validated: \_audit \_internal \_introspection \_telemetry \_thefishbucket history main summary

Done

Checking filesystem compatibility... Done

Checking conf files for problems...

Done

Checking default conf files for edits...

Validating installed files against hashes from '/opt/splunk/splunk-6.6.0-1c4f3bbe1aea-linux-2.6-x86\_64-manifest'

All installed files intact.

Done

All preliminary checks passed.

Starting splunk server daemon (splunkd)...

Done

Waiting for web server at http://127.0.0.1:8000 to be available............ Done

If you get stuck, we're here to help.

Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://indexer:8000

root@indexer:/opt/splunk/bin# ipconfig

No command 'ipconfig' found, did you mean:

Command 'iconfig' from package 'ipmiutil' (universe)

Command 'iwconfig' from package 'wireless-tools' (main)

Command 'ifconfig' from package 'net-tools' (main)

ipconfig: command not found

root@indexer:/opt/splunk/bin# ip addr

1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

inet 127.0.0.1/8 scope host lo

valid\_lft forever preferred\_lft forever

inet6 ::1/128 scope host

valid\_lft forever preferred\_lft forever

2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state UP group default qlen 1000

link/ether 02:1f:97:0f:e2:73 brd ff:ff:ff:ff:ff:ff

inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3

valid\_lft forever preferred\_lft forever

inet6 fe80::1f:97ff:fe0f:e273/64 scope link

valid\_lft forever preferred\_lft forever

3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state UP group default qlen 1000

link/ether 08:00:27:b9:4f:af brd ff:ff:ff:ff:ff:ff

inet 172.31.0.201/24 brd 172.31.0.255 scope global enp0s8

valid\_lft forever preferred\_lft forever

inet6 fe80::a00:27ff:feb9:4faf/64 scope link

valid\_lft forever preferred\_lft forever

root@indexer:/opt/splunk/bin#

srsenthi@LIN73000604 MINGW64 ~

$ cd d:

c

srsenthi@LIN73000604 MINGW64 /d

$ cd Users/srsenthi/splunk/with-ubuntu-forwarder/

srsenthi@LIN73000604 MINGW64 /d/Users/srsenthi/splunk/with-ubuntu-forwarder

$ ls

splunkforwarder-6.6.1-aeae3fe0c5af-linux-2.6-amd64.deb Vagrantfile

ubuntu-xenial-16.04-cloudimg-console.log

srsenthi@LIN73000604 MINGW64 /d/Users/srsenthi/splunk/with-ubuntu-forwarder

$ vagrant up

Bringing machine 'forwarder' up with 'virtualbox' provider...

==> forwarder: Clearing any previously set forwarded ports...

==> forwarder: Fixed port collision for 22 => 2222. Now on port 2200.

==> forwarder: Clearing any previously set network interfaces...

==> forwarder: Preparing network interfaces based on configuration...

forwarder: Adapter 1: nat

forwarder: Adapter 2: hostonly

==> forwarder: Forwarding ports...

forwarder: 22 (guest) => 2200 (host) (adapter 1)

==> forwarder: Running 'pre-boot' VM customizations...

==> forwarder: Booting VM...

==> forwarder: Waiting for machine to boot. This may take a few minutes...

forwarder: SSH address: 127.0.0.1:2200

forwarder: SSH username: ubuntu

forwarder: SSH auth method: password

==> forwarder: Machine booted and ready!

==> forwarder: Checking for guest additions in VM...

==> forwarder: Setting hostname...

==> forwarder: Configuring and enabling network interfaces...

==> forwarder: Mounting shared folders...

forwarder: /vagrant => D:/Users/srsenthi/splunk/with-ubuntu-forwarder

==> forwarder: Machine already provisioned. Run `vagrant provision` or use the `--provision`

==> forwarder: flag to force provisioning. Provisioners marked to run always will still run.

srsenthi@LIN73000604 MINGW64 /d/Users/srsenthi/splunk/with-ubuntu-forwarder

$

srsenthi@LIN73000604 MINGW64 /d/Users/srsenthi/splunk/with-ubuntu-forwarder

$ vagrant ssh

Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-79-generic x86\_64)

\* Documentation: https://help.ubuntu.com

\* Management: https://landscape.canonical.com

\* Support: https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:

http://www.ubuntu.com/business/services/cloud

1 package can be updated.

0 updates are security updates.

Last login: Fri Jun 16 06:31:23 2017 from 10.0.2.2

ubuntu@forwarder1:~$

ubuntu@forwarder1:~$ sudo su

root@forwarder1:/home/ubuntu# cd /vagrant/

root@forwarder1:/vagrant# cd /opt/splunkforwarder/bin/

root@forwarder1:/opt/splunkforwarder/bin# ./splunk list forwarder-server

splunkd 4560 was not running.

Stopping splunk helpers...

Done.

Stopped helpers.

Removing stale pid file... done.

Command error: The subcommand 'forwarder-server' is not valid for command 'list'.

Data forwarding configuration management tools.

Commands:

enable local-index [-parameter <value>] ...

disable local-index [-parameter <value>] ...

display local-index

add forward-server server

remove forward-server server

list forward-server

Objects:

forward-server a Splunk forwarder to forward data to be indexed

local-index a local search index on the Splunk server

root@forwarder1:/opt/splunkforwarder/bin# ./splunk add forwarder-server 172.31.0.201:9997

Command error: The subcommand 'forwarder-server' is not valid for command 'add'.

Data forwarding configuration management tools.

Commands:

enable local-index [-parameter <value>] ...

disable local-index [-parameter <value>] ...

display local-index

add forward-server server

remove forward-server server

list forward-server

Objects:

forward-server a Splunk forwarder to forward data to be indexed

local-index a local search index on the Splunk server

root@forwarder1:/opt/splunkforwarder/bin# ./splunk add forward-server 172.31.0.201:9997

172.31.0.201:9997 forwarded-server already present

root@forwarder1:/opt/splunkforwarder/bin# ./splunk start

Splunk> Like an F-18, bro.

Checking prerequisites...

Checking mgmt port [8089]: open

Checking conf files for problems...

Done

Checking default conf files for edits...

Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-6.6.1-aeae3fe0c5af-linux-2.6-x86\_64-manifest'

All installed files intact.

Done

All preliminary checks passed.

Starting splunk server daemon (splunkd)...

Done

root@forwarder1:/opt/splunkforwarder/bin# ./splunk list monitor

Your session is invalid. Please login.

Splunk username: admin

Password:

Monitored Directories:

$SPLUNK\_HOME/var/log/splunk

/opt/splunkforwarder/var/log/splunk/audit.log

/opt/splunkforwarder/var/log/splunk/btool.log

/opt/splunkforwarder/var/log/splunk/conf.log

/opt/splunkforwarder/var/log/splunk/first\_install.log

/opt/splunkforwarder/var/log/splunk/license\_usage.log

/opt/splunkforwarder/var/log/splunk/metrics.log.1

/opt/splunkforwarder/var/log/splunk/migration.log.2017-06-13.10-35-11

/opt/splunkforwarder/var/log/splunk/migration.log.2017-06-13.10-36-09

/opt/splunkforwarder/var/log/splunk/migration.log.2017-06-13.10-37-08

/opt/splunkforwarder/var/log/splunk/migration.log.2017-06-16.06-33-42

/opt/splunkforwarder/var/log/splunk/mongod.log

/opt/splunkforwarder/var/log/splunk/remote\_searches.log

/opt/splunkforwarder/var/log/splunk/scheduler.log

/opt/splunkforwarder/var/log/splunk/searchhistory.log

/opt/splunkforwarder/var/log/splunk/splunkd-utility.log

/opt/splunkforwarder/var/log/splunk/splunkd\_access.log

/opt/splunkforwarder/var/log/splunk/splunkd\_stderr.log

/opt/splunkforwarder/var/log/splunk/splunkd\_stdout.log

/opt/splunkforwarder/var/log/splunk/splunkd\_ui\_access.log

$SPLUNK\_HOME/var/log/splunk/license\_usage\_summary.log

/opt/splunkforwarder/var/log/splunk/license\_usage\_summary.log

$SPLUNK\_HOME/var/log/splunk/metrics.log

/opt/splunkforwarder/var/log/splunk/metrics.log

$SPLUNK\_HOME/var/log/splunk/splunkd.log

/opt/splunkforwarder/var/log/splunk/splunkd.log

$SPLUNK\_HOME/var/spool/splunk/...stash\_new

/var/log

/var/log/apt

/var/log/apt/history.log

/var/log/apt/term.log

/var/log/auth.log

/var/log/btmp

/var/log/cloud-init-output.log

/var/log/cloud-init.log

/var/log/dist-upgrade

/var/log/dpkg.log

/var/log/fsck

/var/log/fsck/checkfs

/var/log/fsck/checkroot

/var/log/kern.log

/var/log/lastlog

/var/log/lxd

/var/log/syslog

/var/log/syslog.1

/var/log/syslog.2.gz

/var/log/syslog.3.gz

/var/log/syslog.4.gz

/var/log/unattended-upgrades

/var/log/unattended-upgrades/unattended-upgrades-dpkg.log

/var/log/unattended-upgrades/unattended-upgrades.log

/var/log/wtmp

Monitored Files:

$SPLUNK\_HOME/etc/splunk.version

root@forwarder1:/opt/splunkforwarder/bin# ./splunk list monitor

Monitored Directories:

$SPLUNK\_HOME/var/log/splunk

/opt/splunkforwarder/var/log/splunk/audit.log

/opt/splunkforwarder/var/log/splunk/btool.log

/opt/splunkforwarder/var/log/splunk/conf.log

/opt/splunkforwarder/var/log/splunk/first\_install.log

/opt/splunkforwarder/var/log/splunk/license\_usage.log

/opt/splunkforwarder/var/log/splunk/metrics.log.1

/opt/splunkforwarder/var/log/splunk/migration.log.2017-06-13.10-35-11

/opt/splunkforwarder/var/log/splunk/migration.log.2017-06-13.10-36-09

/opt/splunkforwarder/var/log/splunk/migration.log.2017-06-13.10-37-08

/opt/splunkforwarder/var/log/splunk/migration.log.2017-06-16.06-33-42

/opt/splunkforwarder/var/log/splunk/mongod.log

/opt/splunkforwarder/var/log/splunk/remote\_searches.log

/opt/splunkforwarder/var/log/splunk/scheduler.log

/opt/splunkforwarder/var/log/splunk/searchhistory.log

/opt/splunkforwarder/var/log/splunk/splunkd-utility.log

/opt/splunkforwarder/var/log/splunk/splunkd\_access.log

/opt/splunkforwarder/var/log/splunk/splunkd\_stderr.log

/opt/splunkforwarder/var/log/splunk/splunkd\_stdout.log

/opt/splunkforwarder/var/log/splunk/splunkd\_ui\_access.log

$SPLUNK\_HOME/var/log/splunk/license\_usage\_summary.log

/opt/splunkforwarder/var/log/splunk/license\_usage\_summary.log

$SPLUNK\_HOME/var/log/splunk/metrics.log

/opt/splunkforwarder/var/log/splunk/metrics.log

$SPLUNK\_HOME/var/log/splunk/splunkd.log

/opt/splunkforwarder/var/log/splunk/splunkd.log

$SPLUNK\_HOME/var/spool/splunk/...stash\_new

/var/log

/var/log/apt

/var/log/apt/history.log

/var/log/apt/term.log

/var/log/auth.log

/var/log/btmp

/var/log/cloud-init-output.log

/var/log/cloud-init.log

/var/log/dist-upgrade

/var/log/dpkg.log

/var/log/fsck

/var/log/fsck/checkfs

/var/log/fsck/checkroot

/var/log/kern.log

/var/log/lastlog

/var/log/lxd

/var/log/syslog

/var/log/syslog.1

/var/log/syslog.2.gz

/var/log/syslog.3.gz

/var/log/syslog.4.gz

/var/log/unattended-upgrades

/var/log/unattended-upgrades/unattended-upgrades-dpkg.log

/var/log/unattended-upgrades/unattended-upgrades.log

/var/log/wtmp

Monitored Files:

$SPLUNK\_HOME/etc/splunk.version

root@forwarder1:/opt/splunkforwarder/bin# ./splunk list monitor

Monitored Directories:

$SPLUNK\_HOME/var/log/splunk

/opt/splunkforwarder/var/log/splunk/audit.log

/opt/splunkforwarder/var/log/splunk/btool.log

/opt/splunkforwarder/var/log/splunk/conf.log

/opt/splunkforwarder/var/log/splunk/first\_install.log

/opt/splunkforwarder/var/log/splunk/license\_usage.log

/opt/splunkforwarder/var/log/splunk/metrics.log.1

/opt/splunkforwarder/var/log/splunk/migration.log.2017-06-13.10-35-11

/opt/splunkforwarder/var/log/splunk/migration.log.2017-06-13.10-36-09

/opt/splunkforwarder/var/log/splunk/migration.log.2017-06-13.10-37-08

/opt/splunkforwarder/var/log/splunk/migration.log.2017-06-16.06-33-42

/opt/splunkforwarder/var/log/splunk/mongod.log

/opt/splunkforwarder/var/log/splunk/remote\_searches.log

/opt/splunkforwarder/var/log/splunk/scheduler.log

/opt/splunkforwarder/var/log/splunk/searchhistory.log

/opt/splunkforwarder/var/log/splunk/splunkd-utility.log

/opt/splunkforwarder/var/log/splunk/splunkd\_access.log

/opt/splunkforwarder/var/log/splunk/splunkd\_stderr.log

/opt/splunkforwarder/var/log/splunk/splunkd\_stdout.log

/opt/splunkforwarder/var/log/splunk/splunkd\_ui\_access.log

$SPLUNK\_HOME/var/log/splunk/license\_usage\_summary.log

/opt/splunkforwarder/var/log/splunk/license\_usage\_summary.log

$SPLUNK\_HOME/var/log/splunk/metrics.log

/opt/splunkforwarder/var/log/splunk/metrics.log

$SPLUNK\_HOME/var/log/splunk/splunkd.log

/opt/splunkforwarder/var/log/splunk/splunkd.log

$SPLUNK\_HOME/var/spool/splunk/...stash\_new

/var/log

/var/log/apt

/var/log/apt/history.log

/var/log/apt/term.log

/var/log/auth.log

/var/log/btmp

/var/log/cloud-init-output.log

/var/log/cloud-init.log

/var/log/dist-upgrade

/var/log/dpkg.log

/var/log/fsck

/var/log/fsck/checkfs

/var/log/fsck/checkroot

/var/log/kern.log

/var/log/lastlog

/var/log/lxd

/var/log/syslog

/var/log/syslog.1

/var/log/syslog.2.gz

/var/log/syslog.3.gz

/var/log/syslog.4.gz

/var/log/unattended-upgrades

/var/log/unattended-upgrades/unattended-upgrades-dpkg.log

/var/log/unattended-upgrades/unattended-upgrades.log

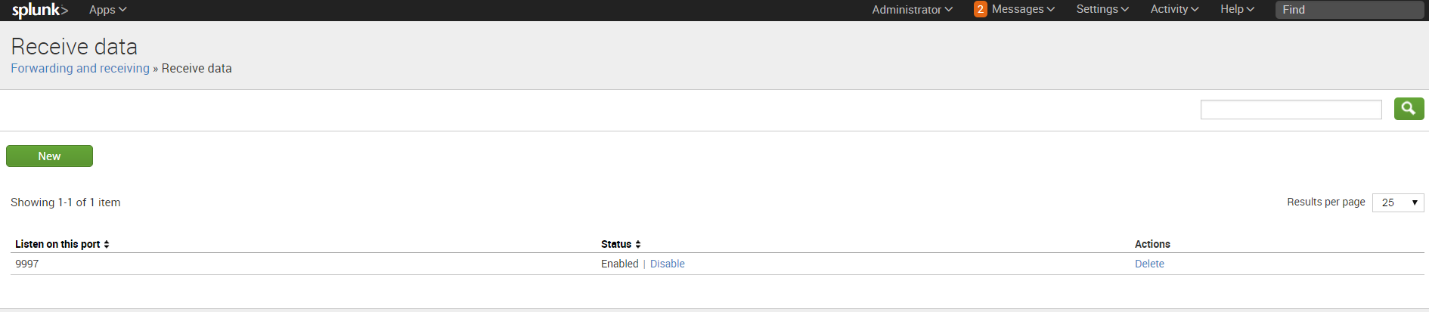
/var/log/wtmp

Monitored Files:

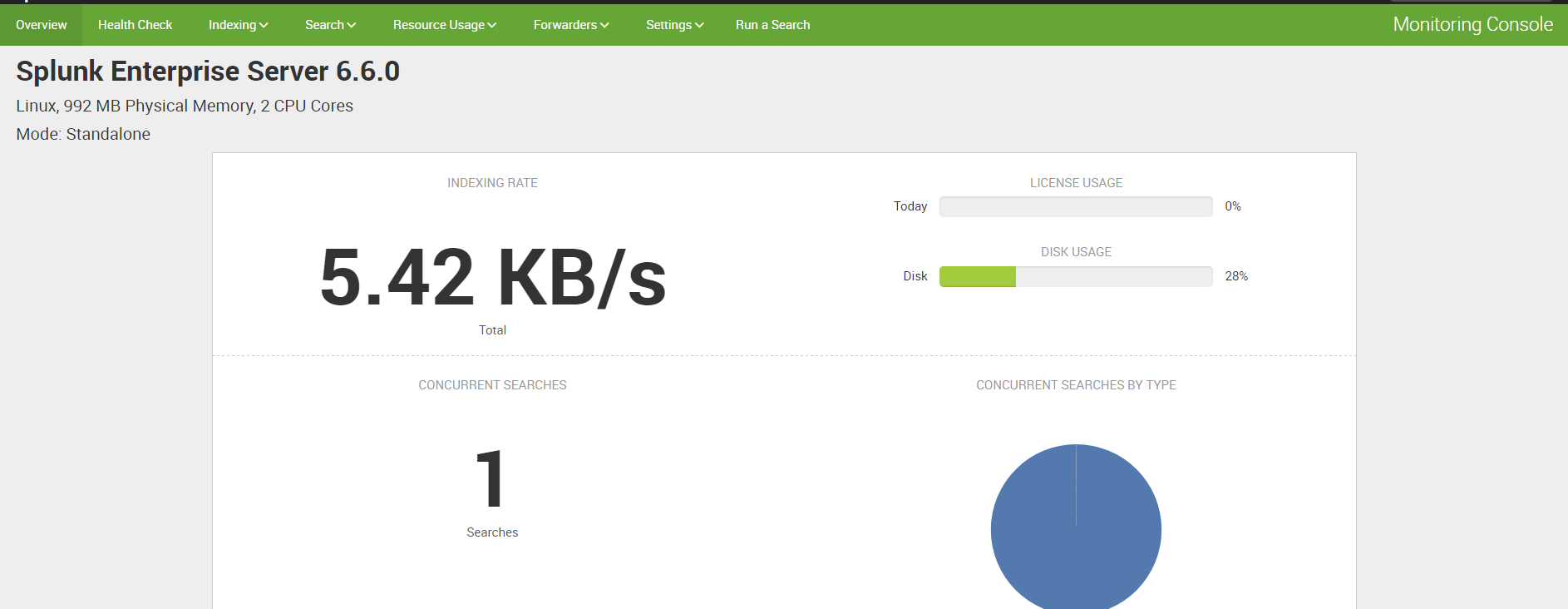
$SPLUNK\_HOME/etc/splunk.version

root@forwarder1:/opt/splunkforwarder/bin#

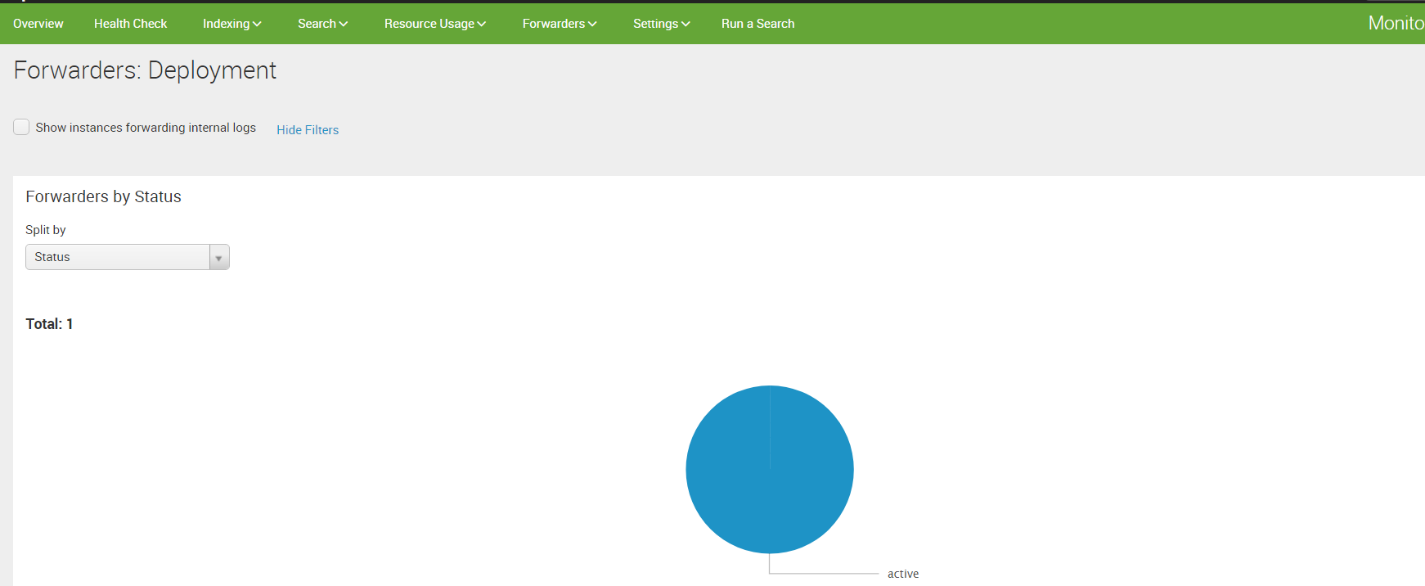
Go to Settings 🡪 forwarding and Receiving 🡪 click configure Receiving 🡪

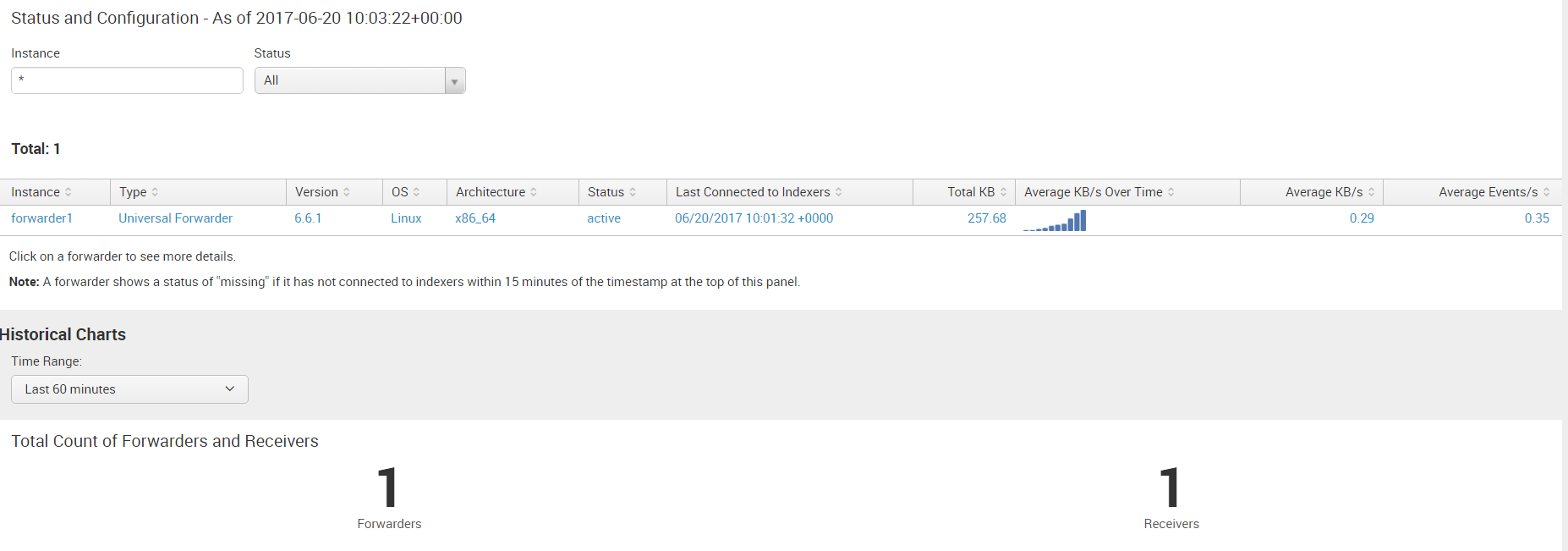


Click on Settings 🡪Monitoring Console 🡪

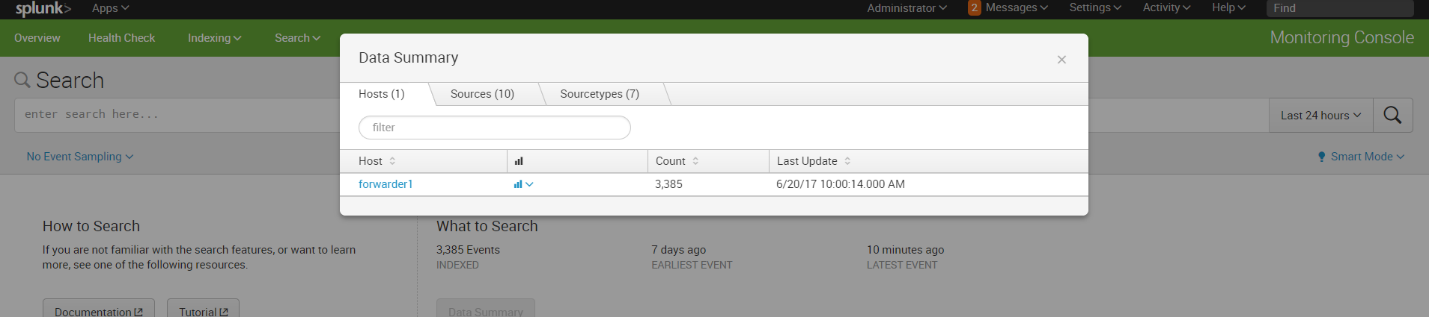


Click on forwarders 🡪forwarders Deployment





Click on Run a Search 🡪 data summary



Click on forwarder

