Splunk Lab

SERVER CREDENTIALS

password	Public IP	Private IP	HostName
Anumeh@15plunkMaster	216.121.71.2	10.102.110.2	master.example.com
Anumeh@15plunkSearch	216.121.71.3	10.102.110.3	search.example.com
Anumeh@15plunkIndexer1	216.121.71.4	10.102.110.4	indexer1.example.com
Anumeh@15plunkIndexer2	216.121.71.5	10.102.110.5	indexer2.example.com
Anumeh@15plunkIndexer3	216.121.71.6	10.102.110.6	indexer3.example.com
Anumeh@15plunkForwarder1	216.121.71.7	10.102.110.7	forwarder1.example.com
Anumeh@15plunkForwarder2	216.121.71.8	10.102.110.8	forwarder2.example.com
Anumeh@15plunkForwarder3	216.121.71.9	10.102.110.9	forwarder3.example.com

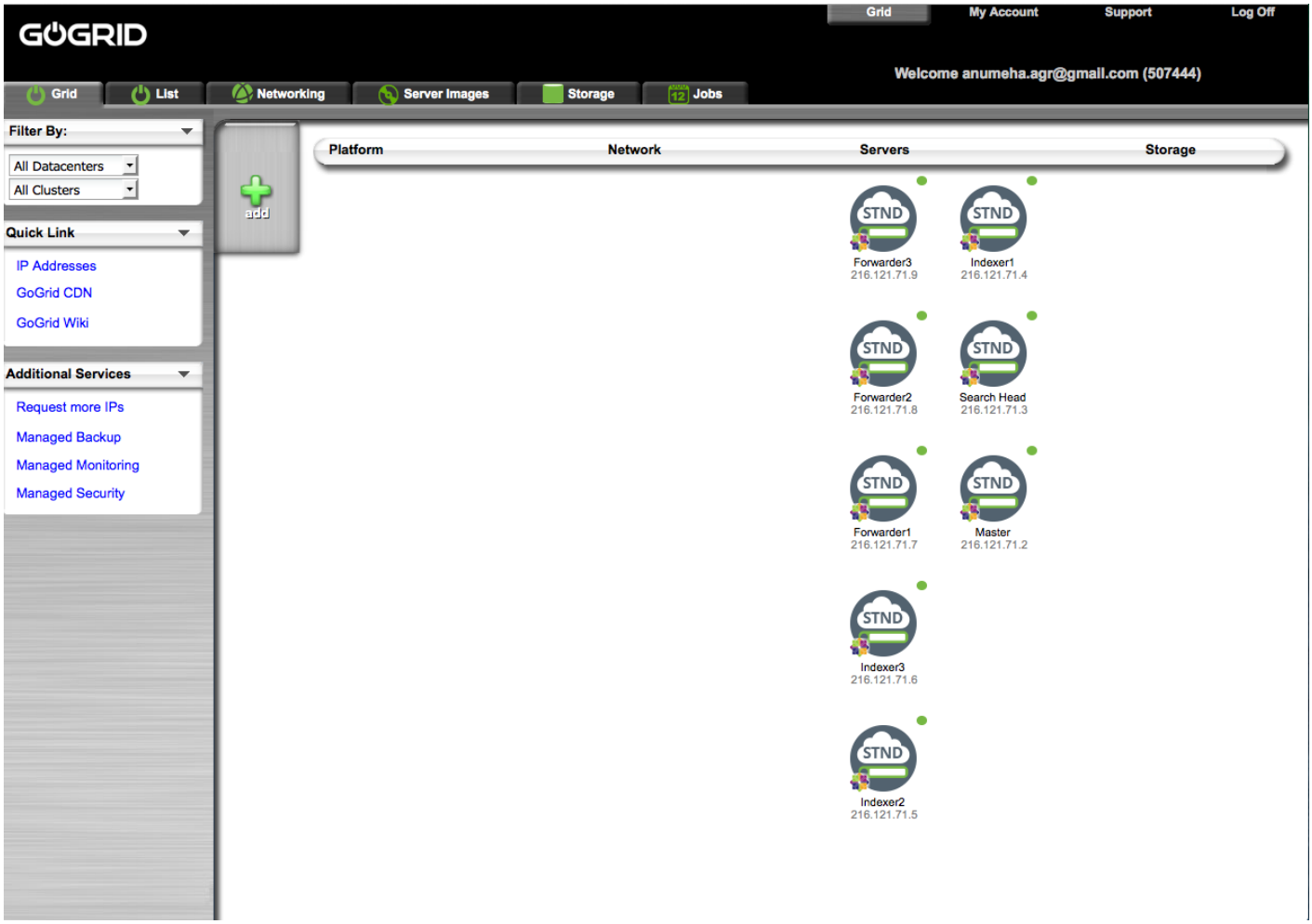
WEB INTERFACE CREDENTIALS FOR MASTER, SERACH_HEAD AND INDEXERS.

	URL	username	Password
master	http://216.121.71.2:8000	admin	Anumeh@15plunkMaster
search	http://216.121.71.3:8000	admin	Anumeh@15plunkSearch
indexer1	http://216.121.71.4:8000	admin	Anumeh@15plunkIndexer1
indexer2	http://216.121.71.5:8000	admin	Anumeh@15plunkIndexer2
indexer3	http://216.121.71.6:8000	admin	Anumeh@15plunkIndexer3

1. STEPS FOR CLUSTER SETUP

Created following servers on GoGrid

1 master, 1 Search, 3 Indexer server. And all of these servers are Standard, Medium servers of 2GB RAM and 2 cores.



STEPS FOR SETTING UP HOSTNAME CONFIGURATION

Step 1: Changed the hostname for each server using hostname <hostname>,
ex. hostname master.example.com

Step 2: Change the value of HOSTNAME in /etc/sysconfig/network to the <hostname>
ex. HOSTNAME=master.example.com

Step 3: Restart the service network using the command

service network restart.

Step 4: Open/etc/sysconfig/network-scripts/ifcfg-eth1 and make following changes.

DEVICE=eth1
BOOTPROTO=static
ONBOOT=yes
IPADDR=10.102.110.3
NETMASK=255.255.255.0

Step 5: Edit etc/hosts file and add the hostnames of all the servers. Delete the second line and add the below lines. here IP address is the private ip of the hosts.

10.102.110.2 master.example.com master
10.102.110.3 search.example.com search
10.102.110.4 indexer1.example.com indexer1
10.102.110.5 indexer2.example.com indexer2
10.102.110.6 indexer3.example.com indexer3
10.102.110.7 forwarder1.example.com forwarder1
10.102.110.8 forwarder2.example.com forwarder2
10.102.110.9 forwarder3.example.com forwarder3

Step 6: Now run the below commands

ifup eth1
service iptables stop
chkconfig iptables off

STEPS FOR OPENING PORTS ON ALL THE SERVERS

Step 1: Add following lines to /etc/sysconfig/iptables below port 22

-A INPUT -m state --state NEW -m tcp -p tcp --dport 8000 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 8089 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 9997 -j ACCEPT

Step 2: Restart iptables service

service iptables restart

1.1 STEPS FOR INSTALLING SPLUNK

Step 1: Downloaded the latest splunk package **splunk-6.2.0-237341-Linux-x86_64.tgz** to local machine

Step 2: scp this splunk package to following servers

216.121.71.2	master
216.121.71.3	search
216.121.71.4	indexer1
216.121.71.5	indexer2
216.121.71.6	indexer3

Step 3: Tar File Install.
Following command extracts and install the splunk in /opt directory

```
tar xvzf splunk_package_name.tgz -C /opt

Ex: tar xvzf splunk-6.2.0-237341-Linux-x86_64.tgz -C /opt
```

Step 4: To start splunk change directory from root to /opt/splunk/bin

```
cd /opt/splunk/bin/

./splunk start --accept-license
./splunk enable boot-start   //to enable boot start splunk.
```

1.3 MONITOR /var/log

Run the below command from /opt/splunk/bin for all the indexers.

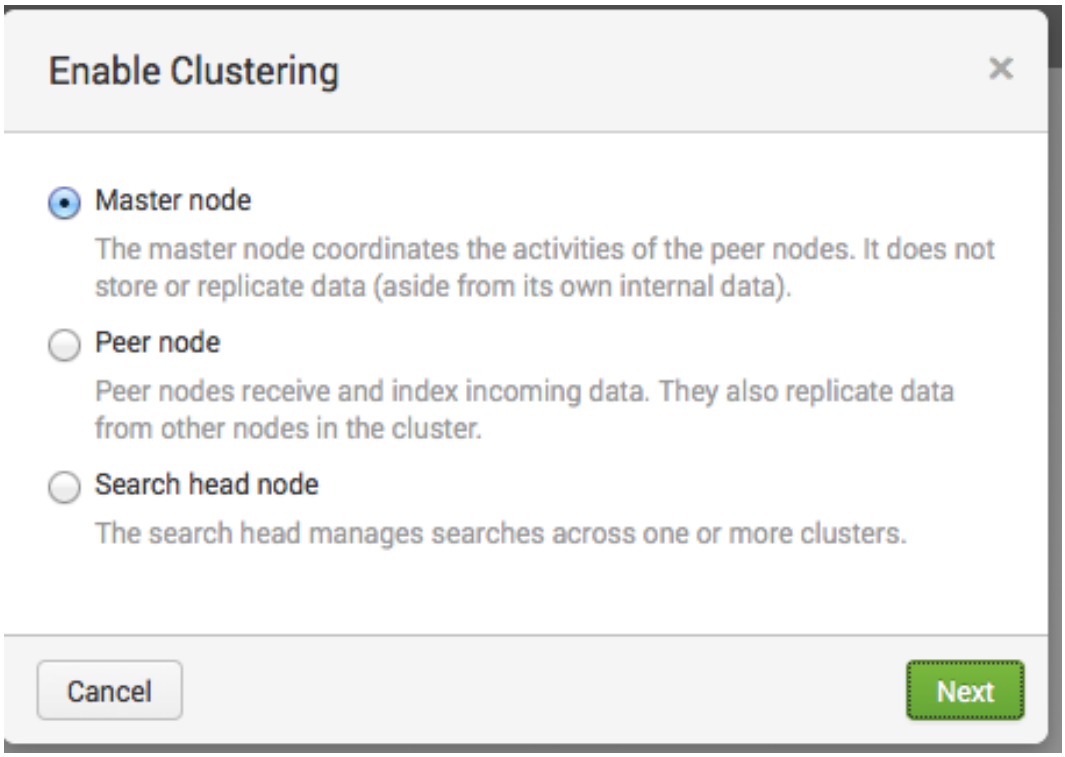
```
./splunk add monitor /var/log
```

1.3.1 STEPS FOR MASTER SERVER CONFIGURATION

Step 1: Log in to master server (http://216.121.71.2:8000) and change password.
Log in again

Step 2: Click on Setting tab from the top right menu

Step 3: In the DISTRIBUTED ENVIRONMENT OPTION, select indexer clustering



Step 5: Select Master Node and Click Next

Step 6: Select following configurations
Replication Factor = 3
Search Factor = 1
Security Key = Optional

Step 7: Now Click Enable Indexer Clustering

1.3.2 STEPS FOR SEARCH HEAD CONFIGURATION

Step 1: Log in to search head (http://216.121.71.3:8000)

Step 2: Click on Setting tab from the top right menu

Step 3: In the DISTRIBUTED ENVIRONMENT OPTION, select indexer clustering

Step 4: select Search head node and click Next

Step 5: Enter master server details including master ip, master port and keep Security Key value as Optional.

Step 6: Click on Enable Indexer Clustering

1.3.3 STEPS FOR PEER NODE CONFIGURATION

Step 1: Log in to indexer1 (http://216.121.71.4:8000)

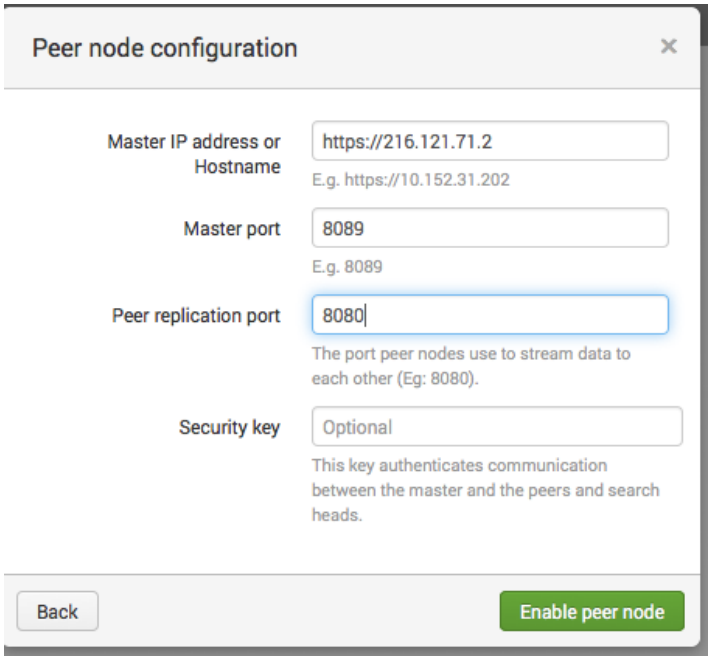
Step 2: Click on Setting tab from the top right menu

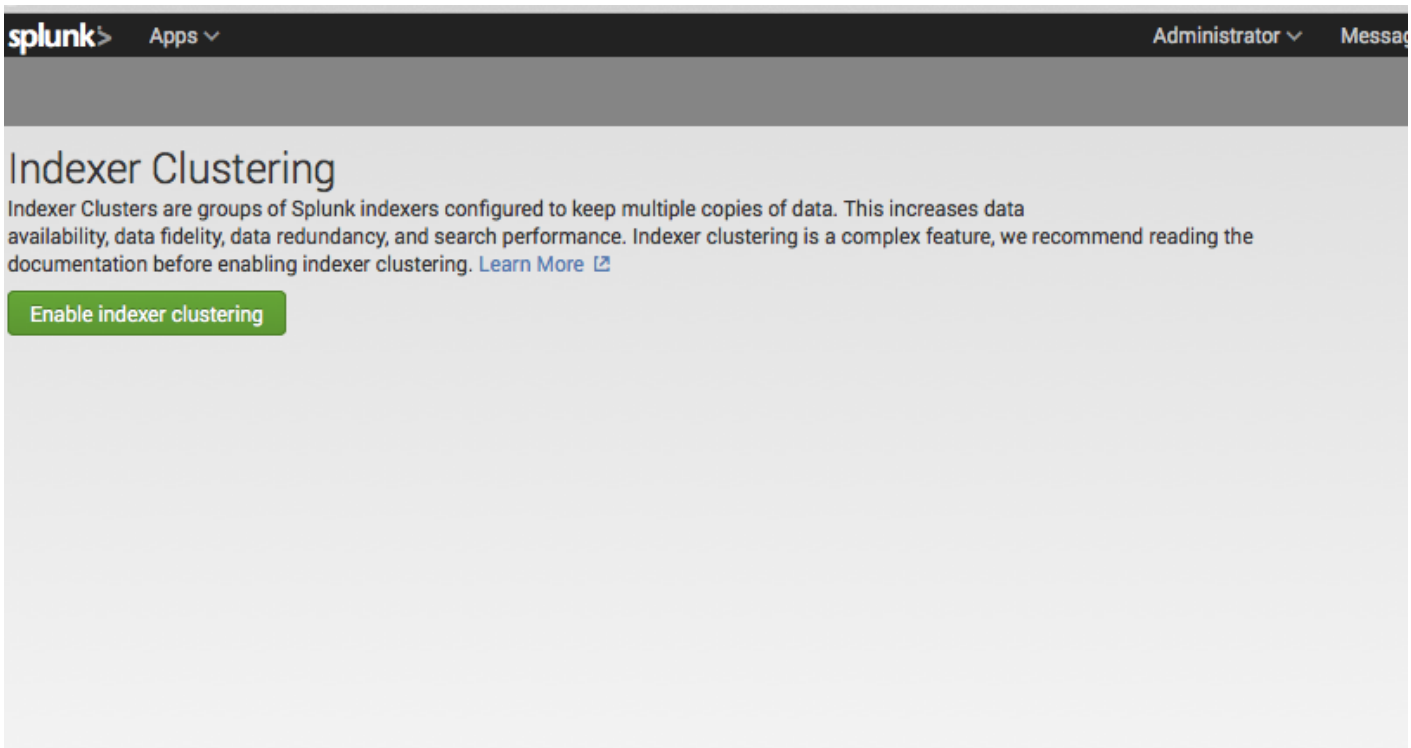
Step 3: In the DISTRIBUTED ENVIRONMENT OPTION, select indexer clustering

Step 4: select Peer node and click Next

Step 5: Enter master server details including master ip, Master port, Peer replication port keep Security Key value as Optional.

Step 6: Click on Enable Indexer Clustering





Step 7: Repeat steps 1 to 6 for all the indexers.

2. Create 3 Standard small servers (1 GB, 1 Core)

2.2 STEPS FOR INSTALLING UNIVERSAL FORWARDER ON ALL THE 3 FORWARDER SERVERS

Step 1: Downloaded latest splunk forwarder package on local machine and scp to all the forwarder server one can use the readme.txt file in the spunk package to find the link for latest package installation

install spunk using the following link
http://docs.splunk.com/Documentation/Splunk/6.2.0/Installation/

Step 2: Tar_file_install.
The below commands extract and install splunkforwarder in /opt directory

tar xvzf splunk_package_name.tgz -C /opt

ex: tar xvzf splunkforwarder-6.2.0-237341-Linux-x86_64.tgz -C /opt

Step 3: To start splunkforwarder change directory from /root to /opt/splunkforwarder/bin/

Step 4: Start splunk forwarder using the below command

./splunk start --accept-license
./splunk enable boot-start

Step 5: Repeat steps 1 to 4 for all the forwarders

2.3 STEPS FOR ADDING FORWARDERS AND MONITOR TO /var/log DIRECTORY

Step 1. Run the below command on the forwarder1

./splunk add forward-server index-IP-address:port -method autobalance

ex: ./splunk add forward-server 216.121.71.4:9997-method autobalance

it will ask for forwarder username and password

Step 2: Run the following command for verification

./splunk list forward-server

Step 3: Use the below command to add monitor to /var/log directory

./splunk add monitor /var/log

Step 4: Repeat the steps from 1 to 3 for all the forwarders.

Screenshot for adding and verifying forwarders.

```
[root@forwarder3 bin]# ./splunk add forward-server 216.121.71.4:9997
Splunk username: admin
Password:
Added forwarding to: 216.121.71.4:9997.
[root@forwarder3 bin]# ./splunk list forward-server
Active forwards:
        None
Configured but inactive forwards:
        216.121.71.4:9997
[root@forwarder3 bin]# ./splunk add forward-server 216.121.71.5:9997
Added forwarding to: 216.121.71.5:9997.
[root@forwarder3 bin]# ./splunk add forward-server 216.121.71.6:9997
Added forwarding to: 216.121.71.6:9997.
[root@forwarder3 bin]# ./splunk list forward-server
Active forwards:
        216.121.71.4:9997
Configured but inactive forwards:
        216.121.71.5:9997
        216.121.71.6:9997
[root@forwarder3 bin]#
```

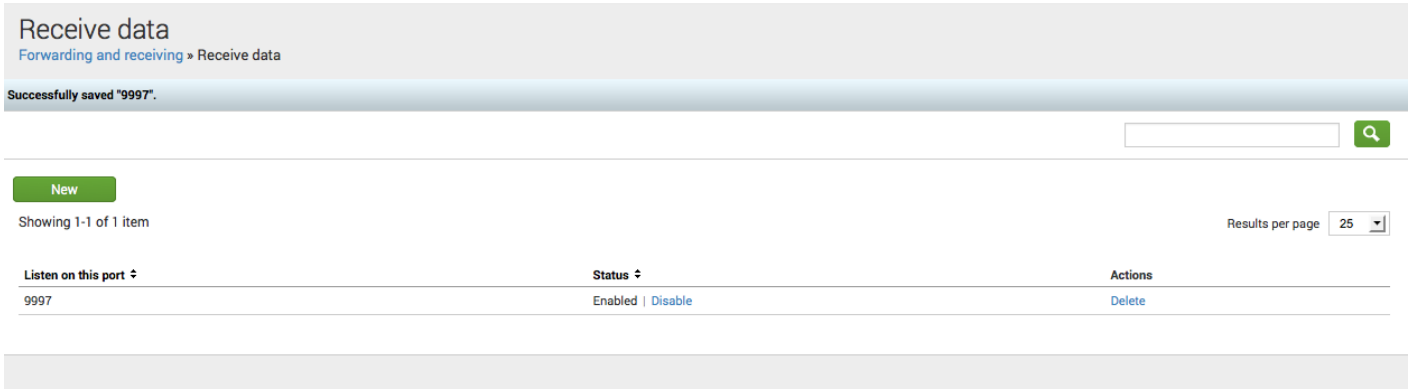
2.3.2 STEPS FOR RECEIVERS CONFIGURATION

Step 1: Log in to indexers

Step 2: From Setting select Forwarding and Receiving

Step 3: Select Configure receiving

Step 4: Click New and add port 9997



Step 5: Repeat the above steps for all the indexers.

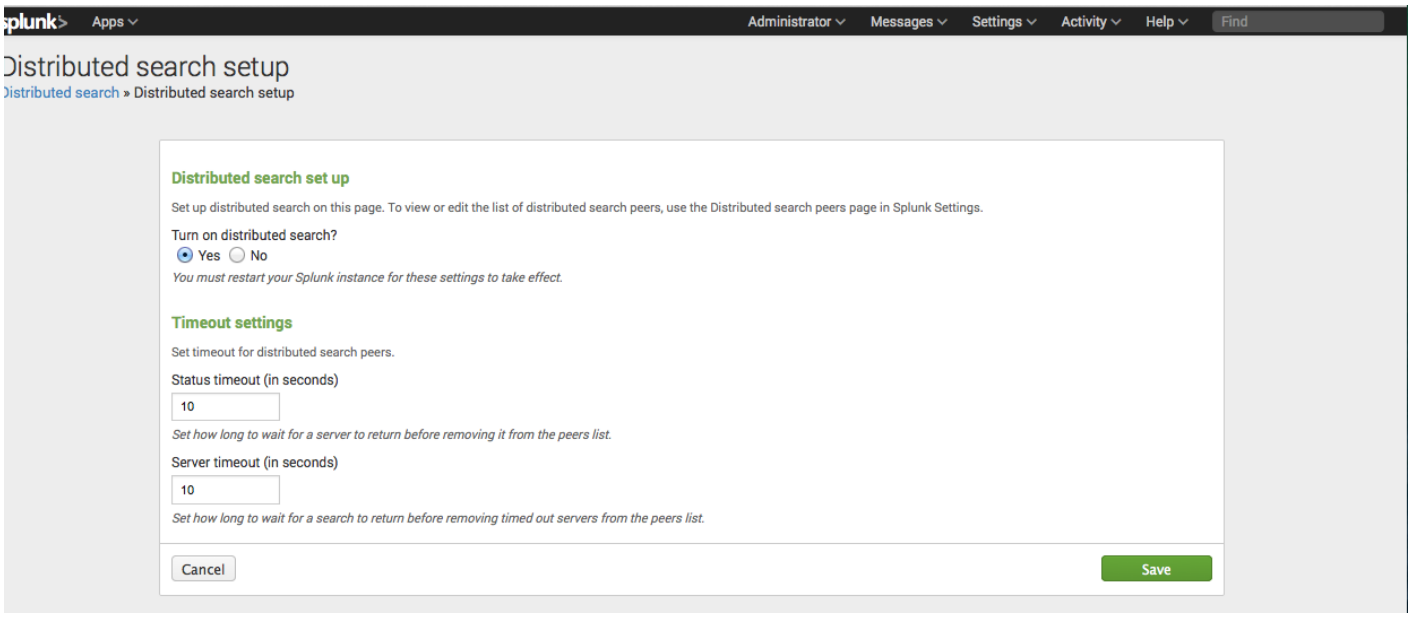
STEPS FOR ENABLING DISTRIBUTED SEARCH

Step 1: Log in to Indexer1

Step 2: Click on Settings

Step 3: From DISTRIBUTED ENVIRONMENT select Distributed Search

Step 4: Select Distributed search setup and check the configurations and save



Step 5: Select Search peers

Step 6: Create new Search peer. For indexer 1 there will be 2 Search peer indexer 2 and indexer 3

Step 7: Provide the Search peer IP and management port and username and password and click save

Step 8: Repeat the above steps for other 2 indexers.

3. STEPS FOR CREATING AND SAVING SEARCH FOR ALL THE FAILED LOGIN ATTEMPTS FOR ALL THE SERVERS WHERE /var/log is being monitored.

Create Report Named Failed Login Attempt

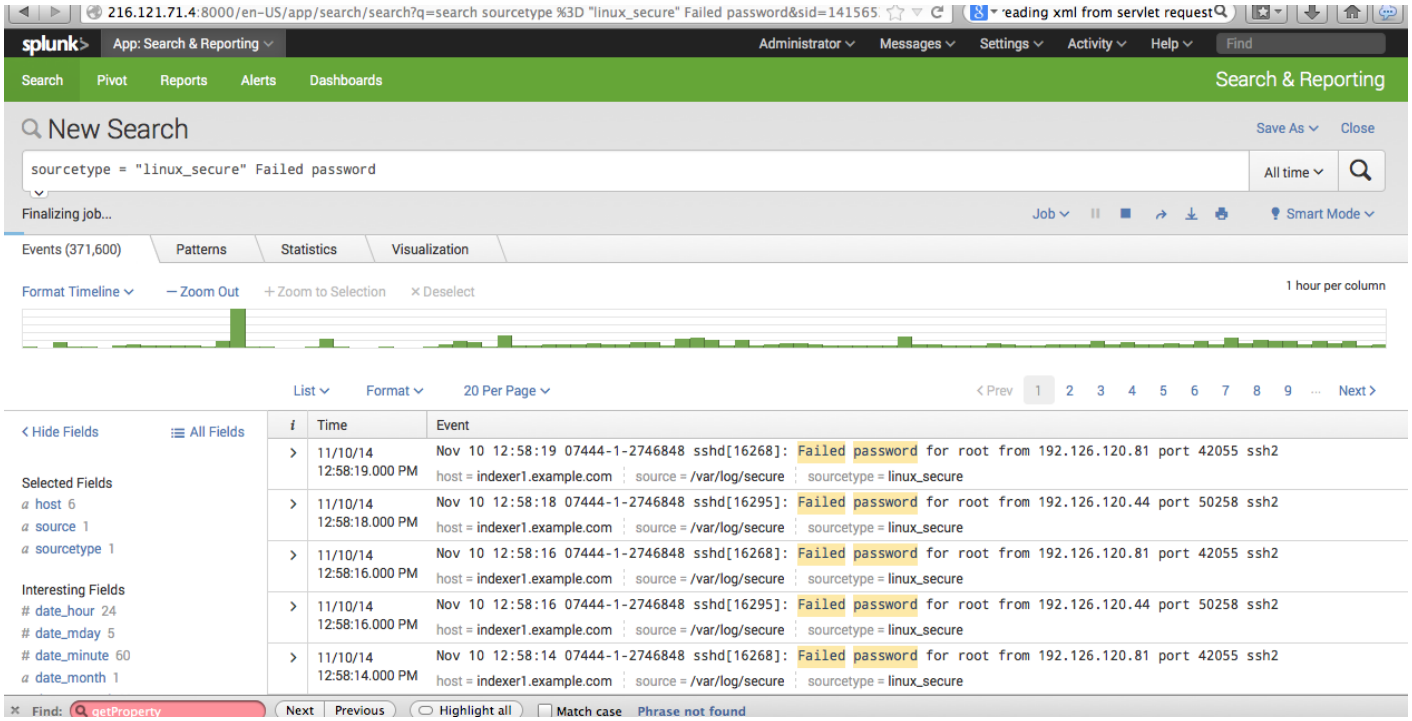
Step 1: Login to the server and select Search and Reporting from home page.

Step 2: Provide the following search string
sourcetype = "linux_secure" Failed password

Step 3. Click on Save As and Save it as a Report named **Failed Login Attempt on**

Step 4 Create and save this search on all the servers where /var/log is being monitored.

Screenshot for Failed Login attempt Search



Screenshot of the saved report Failed Login Attempt