Steps for Splunk disributed search – Search head cluster steups.

Note: 8000,8089,9000,9100,9200 posrt needs to open for ingress

1. Deployer1
2. Search-Head11(sh11)
3. Search-Head12(sh12)
4. Search-Head13(sh13)

Step-1

All above 4 machine must be running with same os. And same splunk enterpise version must be installed. Works well with Windows/Linux.

Cross-check: All 4 machines must be having splunk console running in.

Step-2

Start with deployer configuration.

Opne below file

cat /opt/splunk/etc/system/local/server.conf

[shclustering]

#Below passkey must be same for remaing 3 machine

pass4SymmKey = Mypass26sep!

#mgmt url represent deployer ip/fqsn/dns, must be https

mgmt = https://172.206.251.25:8089

shcluster\_label = shcluster1

Rest all configuration will happing over sh11.sh12,sh13

cat /opt/splunk/etc/system/local/server.conf

# Repeat below conf for all 3 cluster node

[shclustering]

# below url is deployer machine ip

conf\_deploy\_fetch\_url = http://172.206.251.25:8089

disabled = 0

#mgmt\_uri represent cluster machine ip it self

mgmt\_uri = https://172.190.82.169:8089

pass4SymmKey = Mypass26sep!

shcluster\_label = shcluster1

# here replication\_port must be changed for each and every cluster node

[replication\_port://9000]

Note: After server.conf file chage ./splunk restart must be done

Step -3:

/opt/splunk/bin/splunk init shcluster-config \

-auth admin:your\_password \

-mgmt\_uri https://192.168.1.2:8089 \

-replication\_port 9887 \

-conf\_deploy\_fetch\_url https://192.168.1.1:8089 \

-secret <Your\_Secret\_Key> \

-shcluster\_label mySearchHeadCluster

Actual cmd:

Run on sh11

./splunk init shcluster-config -auth admin:Hni26sep! -mgmt\_uri <https://172.210.32.51:8089> -replication\_port 9000 -replication\_factor 3 -conf\_deploy\_fetch\_url <http://20.163.175.236:8089> -secret $7$C/VJ429XznKsgW8qkdt5hdtl213alu2Xj2du+QQ1gtt60sR72KkvGrOUSuQ= -shcluster\_label shcluster1

Run on sh12

./splunk init shcluster-config -auth admin:Hni26sep! -mgmt\_uri <https://172.210.32.121:8089> -replication\_port 9100 -replication\_factor 3 -conf\_deploy\_fetch\_url <http://20.163.175.236:8089> -secret $7$C/VJ429XznKsgW8qkdt5hdtl213alu2Xj2du+QQ1gtt60sR72KkvGrOUSuQ= -shcluster\_label shcluster1

Run on sh13

./splunk init shcluster-config -auth admin:Hni26sep! -mgmt\_uri <https://172.210.33.120:8089> -replication\_port 9200 -replication\_factor 3 -conf\_deploy\_fetch\_url <http://20.163.175.236:8089> -secret $7$C/VJ429XznKsgW8qkdt5hdtl213alu2Xj2du+QQ1gtt60sR72KkvGrOUSuQ= -shcluster\_label shcluster1

# below cmd for cluster captain bootstrap run only on sh11

./splunk bootstrap shcluster-captain -servers\_list "https://172.210.32.51:8089,https://172.210.32.121:8089,https://172.210.33.120:8089" -auth admin:Hni26sep!

 # to find out shcluster-status

./splunk show shcluster-status -auth admin:Hni26sep!