# BASE SETTINGS

[tcpout]

defaultGroup = primary\_indexers

# These two options below are required for forwarders when clustering.

# Max queue size ensures that the forwarder has enough of a buffer while

# waiting for the ACK from the indexer; without useACK, the search head

# will spout yellow warning banners in a clustered environment.

maxQueueSize = 7MB

useACK = true

# When indexing a large continuous file that grows very large, a universal

# or light forwarder may become "stuck" on one indexer, trying to reach

# EOF before being able to switch to another indexer. The symptoms of this

# are congestion on \*one\* indexer in the pool while others seem idle, and

# possibly uneven loading of the disk usage for the target index.

# In this instance, forceTimebasedAutoLB can help!

# \*\* Do not enable if you have events > 64kB \*\*

forceTimebasedAutoLB = true

# Correct an issue with the default outputs.conf for the Universal Forwarder

# or the SplunkLightForwarder app; these don't forward \_internal events.

forwardedindex.2.whitelist = (\_audit|\_introspection|\_internal)

[tcpout:primary\_indexers]

server = server\_one:9997, server\_two:9997

# If setting compressed=true, this must also be set on the indexer.

# compressed = true

#################################################################

# DO NOT USE INDEXER DISCOVERY IF YOUR FORWARDERS ARE NOT RUNNING

# VERSION EQUAL TO OR LATER THAN 6.3.7 OR 6.4.4; A SERIOUS POTENTIAL

# FOR DUPLICATE EVENTS EXISTS.

#################################################################

# INDEXER DISCOVERY (ASK THE CLUSTER MASTER WHERE THE INDEXERS ARE)

# This particular setting identifies the tag to use for talking to the

# specific cluster master, like the "primary\_indexers" group tag here.

# indexerDiscovery = clustered\_indexers

# It's OK to have a tcpout group like the one above \*with\* a server list;

# these will act as a seed until communication with the master can be

# established, so it's a good idea to have at least a couple of indexers

# listed in the tcpout group above.

# [indexer\_discovery:clustered\_indexers]

# pass4SymmKey = <MUST\_MATCH\_MASTER>

# This must include protocol and port like the example below.

# master\_uri = https://master.example.com:8089

# SSL SETTINGS

# sslCertPath = $SPLUNK\_HOME/etc/auth/server.pem

# sslRootCAPath = $SPLUNK\_HOME/etc/auth/ca.pem

# sslPassword = password

# sslVerifyServerCert = true

# COMMON NAME CHECKING - NEED ONE STANZA PER INDEXER

# The same certificate can be used across all of them, but the configuration

# here requires these settings to be per-indexer, so the same block of

# configuration would have to be repeated for each.

# [tcpout-server://10.1.12.112:9997]

# sslCertPath = $SPLUNK\_HOME/etc/certs/myServerCertificate.pem

# sslRootCAPath = $SPLUNK\_HOME/etc/certs/myCAPublicCertificate.pem

# sslPassword = server\_privkey\_password

# sslVerifyServerCert = true

# sslCommonNameToCheck = servername

# altCommonNameToCheck = servername