Aug 22

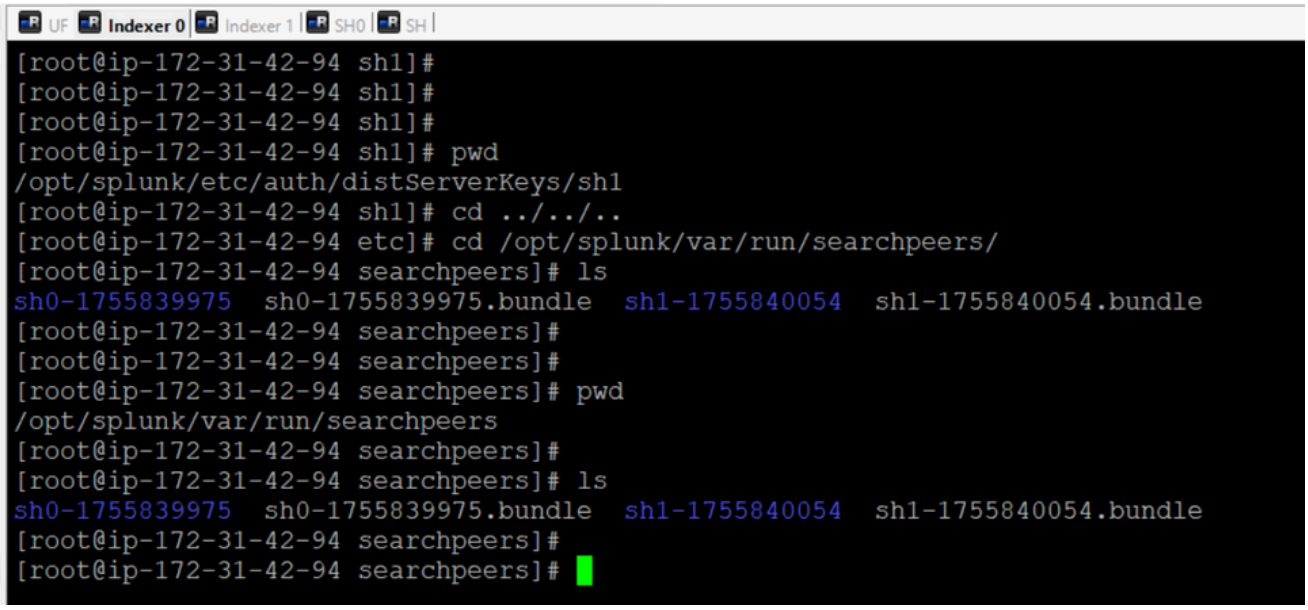
UF Indexer Search head

Commands to set default hostname and servername

```
splunk set default-hostname <NAME>

splunk set servername <NAME>

#To disable web on indexer

splunk disable webserver
```

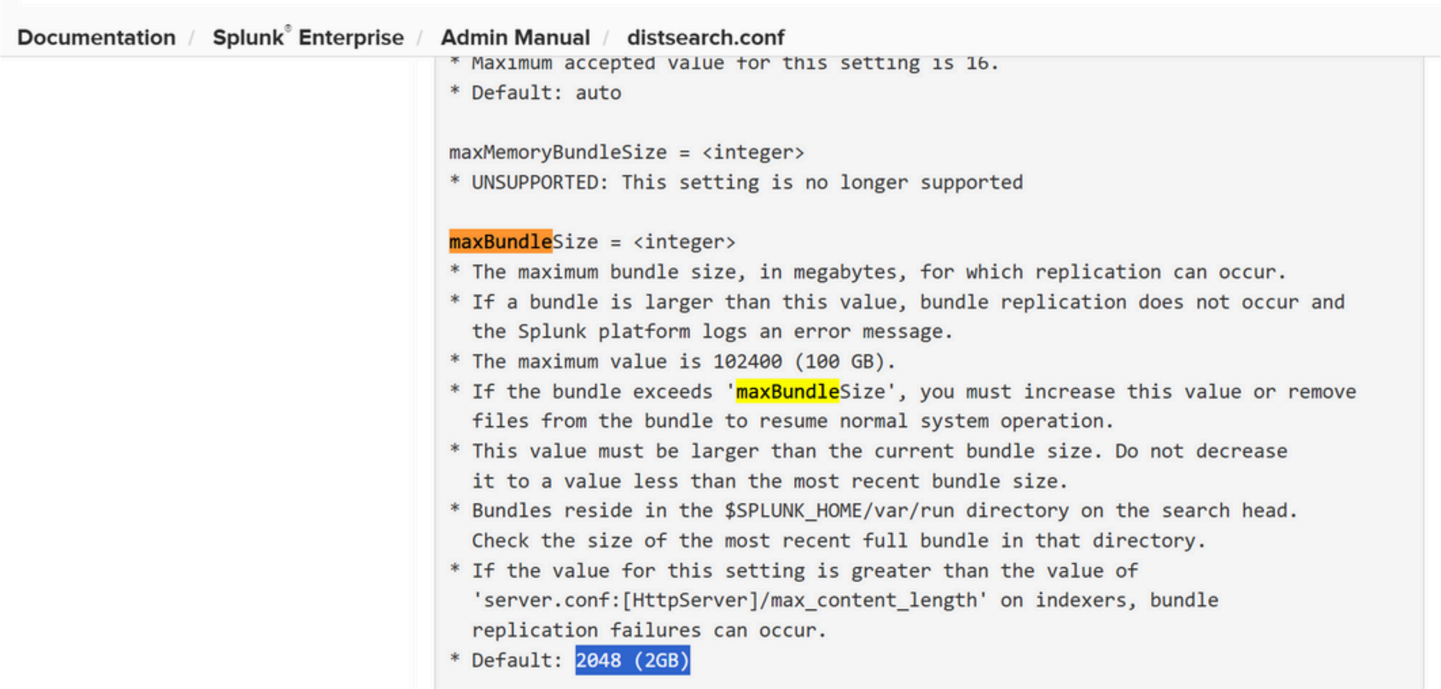
Distributed Setup

1. When SH is connected to indexer (added as search peer), search head will exchange its public key (trusted.pem) with indexer (on indexer this key will be strored in /opt/splunk/etc/auth/distServerKeys/<**SHNAME**>/trusted.pem)
2. Search head will share its KnowledgeBundle with indexer (**Knowledge Bundle replication**)
    a. it will be stored in /opt/splunk/var/run/searchpeers/* **on INDEXER**



```
[root@ip-172-31-42-94 sh1]#
[root@ip-172-31-42-94 sh1]#
[root@ip-172-31-42-94 sh1]#
[root@ip-172-31-42-94 sh1]# pwd
/opt/splunk/etc/auth/distServerKeys/sh1
[root@ip-172-31-42-94 sh1]# cd ../../..
[root@ip-172-31-42-94 etc]# cd /opt/splunk/var/run/searchpeers/
[root@ip-172-31-42-94 searchpeers]# ls
sh0-1755839975  sh0-1755839975.bundle  sh1-1755840054  sh1-1755840054.bundle
[root@ip-172-31-42-94 searchpeers]#
[root@ip-172-31-42-94 searchpeers]#
[root@ip-172-31-42-94 searchpeers]# pwd
/opt/splunk/var/run/searchpeers
[root@ip-172-31-42-94 searchpeers]#
[root@ip-172-31-42-94 searchpeers]# ls
sh0-1755839975  sh0-1755839975.bundle  sh1-1755840054  sh1-1755840054.bundle
[root@ip-172-31-42-94 searchpeers]#
[root@ip-172-31-42-94 searchpeers]#
```

https://docs.splunk.com/Documentation/Splunk/9.4.2/Admin/Distsearchconf

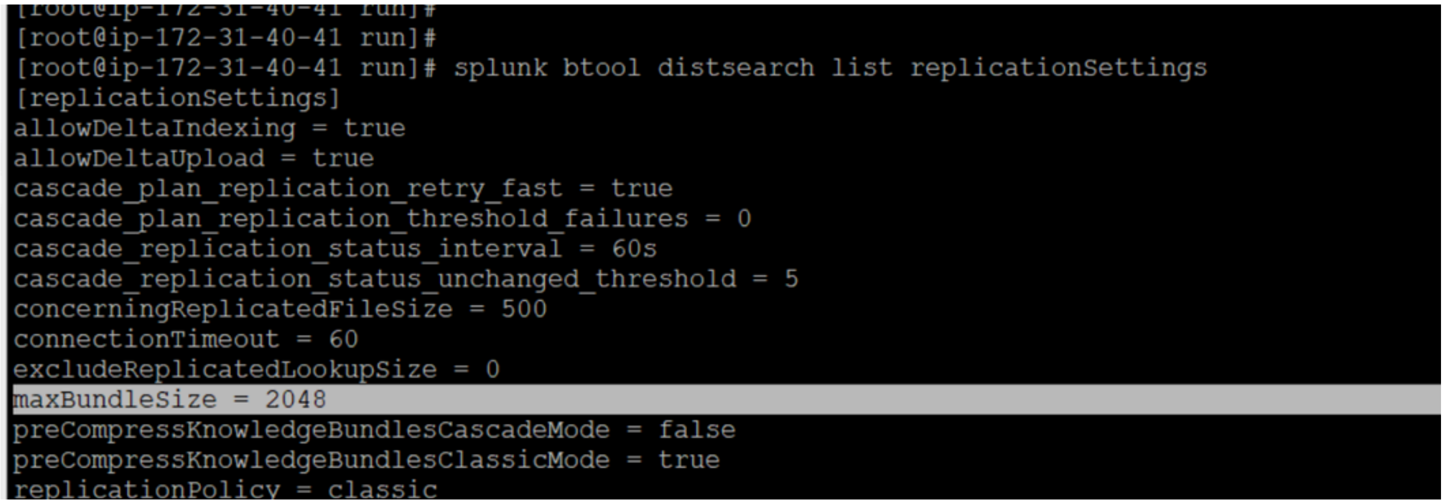

Documentation / Splunk® Enterprise / Admin Manual / distsearch.conf

```
* Maximum accepted value for this setting is 16.
* Default: auto

maxMemoryBundleSize = <integer>
* UNSUPPORTED: This setting is no longer supported

maxBundleSize = <integer>
* The maximum bundle size, in megabytes, for which replication can occur.
* If a bundle is larger than this value, bundle replication does not occur and
  the Splunk platform logs an error message.
* The maximum value is 102400 (100 GB).
* If the bundle exceeds 'maxBundleSize', you must increase this value or remove
  files from the bundle to resume normal system operation.
* This value must be larger than the current bundle size. Do not decrease
  it to a value less than the most recent bundle size.
* Bundles reside in the $SPLUNK_HOME/var/run directory on the search head.
  Check the size of the most recent full bundle in that directory.
* If the value for this setting is greater than the value of
  'server.conf:[HttpServer]/max_content_length' on indexers, bundle
  replication failures can occur.
* Default: 2048 (2GB)
```

distsearch.conf

```
[replicationSettings]
```

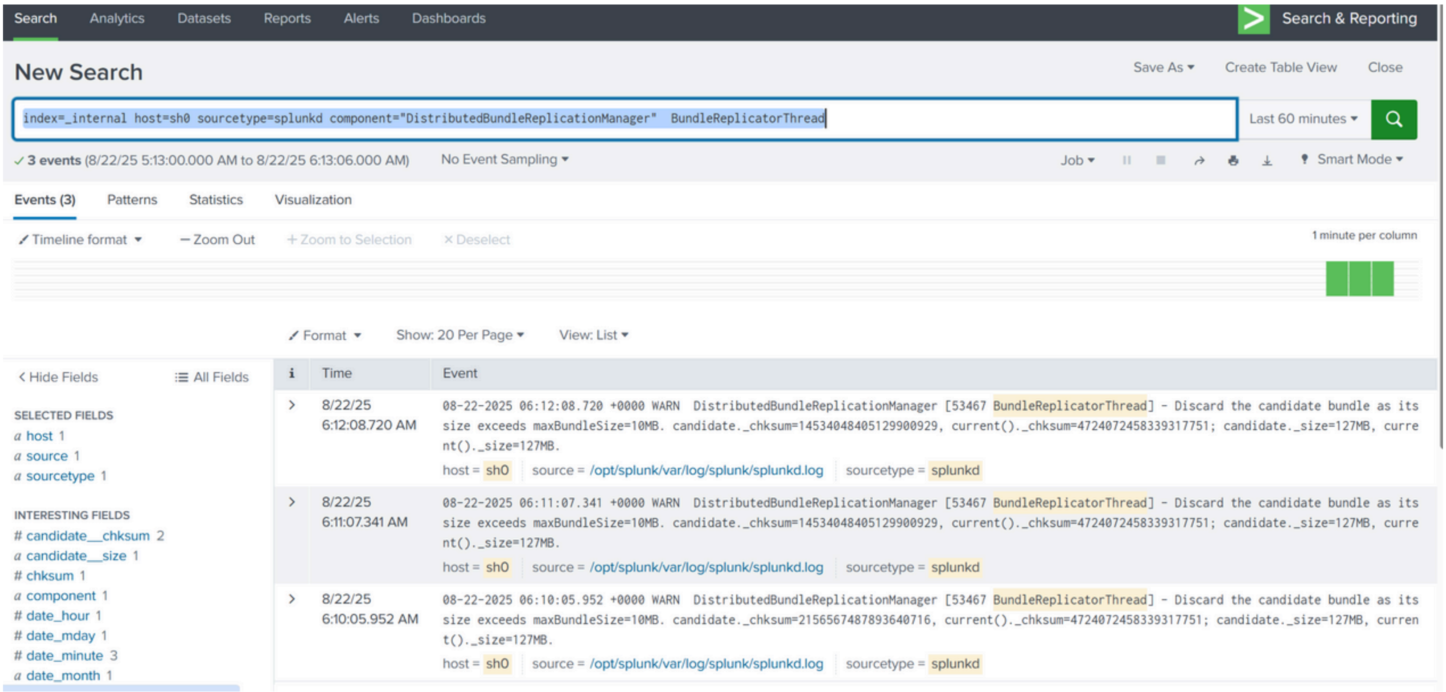
```
maxBundleSize = 2048
```



```
[root@ip-172-31-40-41 run]#
[root@ip-172-31-40-41 run]#
[root@ip-172-31-40-41 run]# splunk btool distsearch list replicationSettings
[replicationSettings]
allowDeltaIndexing = true
allowDeltaUpload = true
cascade_plan_replication_retry_fast = true
cascade_plan_replication_threshold_failures = 0
cascade_replication_status_interval = 60s
cascade_replication_status_unchanged_threshold = 5
concerningReplicatedFileSize = 500
connectionTimeout = 60
excludeReplicatedLookupSize = 0
maxBundleSize = 2048
preCompressKnowledgeBundlesCascadeMode = false
preCompressKnowledgeBundlesClassicMode = true
replicationPolicy = classic
```

`Query` to check bundle issue

index=_internal host=sh0 sourcetype=splunkd component="DistributedBundleReplicationManager" BundleReplicatorThread



```
index=_internal host=sh0 sourcetype=splunkd component="DistributedBundleReplicationManager"  BundleReplicatorThread
```

✓ 3 events (8/22/25 5:13:00.000 AM to 8/22/25 6:13:06.000 AM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# candidate__chksum 2
a candidate__size 1
# chksum 1
a component 1
# date_hour 1
# date_mday 1
# date_minute 3
a date_month 1

i	Time	Event
>	8/22/25 6:12:08.720 AM	08-22-2025 06:12:08.720 +0000 WARN DistributedBundleReplicationManager [53467 BundleReplicatorThread] - Discard the candidate bundle as its size exceeds maxBundleSize=10MB. candidate._chksum=14534048405129900929, current()._chksum=4724072458339317751; candidate._size=127MB, current()._size=127MB. host = sh0 source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	8/22/25 6:11:07.341 AM	08-22-2025 06:11:07.341 +0000 WARN DistributedBundleReplicationManager [53467 BundleReplicatorThread] - Discard the candidate bundle as its size exceeds maxBundleSize=10MB. candidate._chksum=14534048405129900929, current()._chksum=4724072458339317751; candidate._size=127MB, current()._size=127MB. host = sh0 source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	8/22/25 6:10:05.952 AM	08-22-2025 06:10:05.952 +0000 WARN DistributedBundleReplicationManager [53467 BundleReplicatorThread] - Discard the candidate bundle as its size exceeds maxBundleSize=10MB. candidate._chksum=2156567487893640716, current()._chksum=4724072458339317751; candidate._size=127MB, current()._size=127MB. host = sh0 source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd

https://docs.splunk.com/Documentation/Splunk/9.4.2/Admin/Distsearchconf#REPLICATION_DENY_LIST_OPTIONS