# Introduction

### Media Contacts:

Splunk Inc.415.848.8474[trisha@splunk.com](mailto:trisha@splunk.com)

This document gives guidance for use of the accompanying apps:

* org\_SHC\_base\_init
* org\_SHCDeployer\_base

The apps are intended to aid building Search Head Clusters patterned on the way that a deployment client works with a deployment server, but a little simpler. The apps have been tested on Splunk Enterprise versions 6.54, 6.60 and 7.0.

Assuming at least 3 **freshly installed** Splunk Enterprise instances, designate one as the Search Head Cluster Deployer and the rest as Search Head Cluster members. There are three main parts to building the Search Head Cluster (SHC) with these apps:

1. Amending the SHC initialization app and installing it to 2 or more\* Splunk Enterprise instances
2. Amending the SHC Deployer app and installing it to the SHC Deployer instance
3. Bootstrapping the SHC Captain

\*Though the SHC will work with 2 SHC members, please see related documentation [here](http://docs.splunk.com/Documentation/Splunk/6.6.0/DistSearch/SHCsystemrequirements#Required_number_of_instances).

NB: Before starting the setup, verify that all necessary ports are open.

# Part 1: Prepare the app for SHC Members

1. On each SHC member, edit the file $SPLUNK\_HOME/etc/system/local/server.conf to add the local management URI in the following format:

**[shclustering]**

mgmt\_uri = https://<FQDN\_OF\_THE\_SHC\_MEMBER>:8089

example:

**[shclustering]**

mgmt\_uri = https://search007.mi5.gov.uk:8089

1. In the app org\_SHC\_base\_init, amend the file ../default/server.conf to match your specific deployment. There are two stanzas to edit: shclustering and replication port. Man page notation is used to indicate appropriate types of parameter values in each stanza.
2. Copy the amended app org\_SHC\_base\_init to the following path on each SHC Member: $SPLUNK\_HOME/etc/apps.
3. Restart Splunk on each SHC member.
4. Copy the amended app org\_SHC\_base\_init to the following path on the *SHC Deployer*:

$SPLUNK\_HOME/etc/shcluster/apps  
  
(This ensures the config in #3 above is not lost when a bundle is pushed from the SHCD)

# Part 2: Prepare the app for the Deployer

1. In the app org\_SHCDeployer\_base amend the file ../local/server.conf to match your specific deployment. There is 1 stanza to edit: shclustering. Man page notation is used to indicate appropriate types of parameter values. The pass4SymmKey used must be the same as that in the target indexer cluster and the preceding app org\_SHC\_base\_init.
2. Copy the amended app org\_SHCDeployer\_base to the following path on the deployer: $SPLUNK\_HOME/etc/apps.
3. Restart Splunk on the SHC Deployer

# Part 3: Bootstrap the SHC Captain

These instructions are the same as the official docs and inserted here for convenience.

1. On the SHC members and deployer, change the default admin password for Splunk Enterprise, if not already done.
2. Choose one of the SHC members above to be SHC captain. It does not matter which.
3. On that SHC member, execute the following on the operating system command line:

$SPLUNK\_HOME/bin/splunk bootstrap shcluster-captain -servers\_list "<URI>:<management\_port>,<URI>:<management\_port>,..." -auth <username>:<password>

example:

$SPLUNK\_HOME/bin/splunk bootstrap shcluster-captain -servers\_list "https://search005.mi5.gov.uk:8089,https://search006.mi5.gov.uk:8089, https://search007.mi5.gov.uk:8089" -auth admin:changed

1. Verify the SHC status as follows on an SHC member other than the captain:

$SPLUNK\_HOME/bin/splunk show shcluster-status

1. Use base configs (e.g. org\_cluster\_search\_base) to connect the SHC members to indexers as appropriate. Alternatively, follow instructions to connect the SHC to indexers as follows:

<http://docs.splunk.com/Documentation/Splunk/6.6.0/DistSearch/SHCdeploymentoverview#6._Perform_post-deployment_set-up>