Sep 2024

# Splunk4Admins - Forwarder Management

Cheat Sheet for Lab Commands

## Task 1:

Follow the guide for connecting to the show instance via SSH.

## Task 2:

```
cd /opt/splunk-ds/splunk/bin
./splunk status
```

| | |
|---|---|
| Splunk version | `./splunk version` |
| Splunk Web port: | `./splunk show web-port` |
| Splunk management (splunkd) port: | `./splunk show splunkd-port` |
| Splunk App Server ports: | `./splunk show appserver-ports` |
| Splunk KV store port: | `./splunk show kvstore-port` |
| Splunk server name: | `./splunk show servername` |
| Default host name: | `./splunk show default-hostname` |

## Task 3:

```
/opt/splunk-ds/splunk/etc/system
ls README
ls default
ls local
more +39 README/server.conf.spec
ls /opt/splunk/etc/deployment-apps
more /opt/splunk/etc/deployment-apps/README
```

## Task 4:

```
mkdir all_forwarder_outputs
cd all_forwarder_outputs
mkdir metadata
mkdir local
cd metadata
vi local.meta
```

```
[]
access = read : [ * ], write : [ admin ]
export = system
```

```
cd ../local
vi outputs.conf
```

```
# BASE SETTINGS
[tcpout]
defaultGroup = primary_indexer
forceTimebasedAutoLB = true
forwardedindex.0.whitelist = (_audit|_introspection|_internal)

[tcpout:primary_indexer]
server = server_one:9997
```

```
vi limits.conf
```

```
# By default a universal or light forwarder is limited to 256kB/s
# Either set a different limit in kB/s, or set the value to zero to
# have no limit.
# Note that a full speed UF can overwhelm a single indexer.

# [thruput]
# maxKBps = 0
```

**Note**: this file doesn't do anything as everything is commented out, but the notes in the file are valuable to expose to customers and get them thinking about throughput limits.

```
vi app.conf
```

```
[install]
state = enabled

[package]
check_for_updates = false

[ui]
is_visible = false
is_manageable = false
```

# Task 5:

```
cd /opt/splunk-ds/splunk/etc/deployment-apps
mkdir all_deploymentclient
cd all_deploymentclient
mkdir metadata
mkdir local
cd metadata
vi local.meta
```

```
[]
access = read : [ * ], write : [ admin ]
export = system
```

```
vi app.conf
```

```
[install]
state = enabled

[package]
check_for_updates = false

[ui]
is_visible = false
is_manageable = false
```

```
vi deploymentclient.conf
```

```
[deployment-client]
# Set the phoneHome
# 10 minutes
# phoneHomeIntervalInSecs = 600

[target-broker:deploymentServer]
# Change the targetUri
targetUri = https://ds-ip:8089
```

# Task 6:

```
cd /opt/splunk-ds/splunk/etc/system/local
vi serverclass.conf
```

```
[serverClass:all_forwarders]
restartSplunkd = true
whitelist.0 = UF1
whitelist.1 = HF1

[serverClass:all_forwarders:app:all_forwarder_outputs]
```

```
vi serverclass.conf
```

```
[serverClass:all_deployment_clients]
restartSplunkd = true
whitelist.0 = *
```

```
[serverClass:all_deployment_clients:app:all_deploymentclient]
```

```
/opt/splunk/bin/splunk btool serverclass list --debug
```

# Task 7:

```
cd /opt/splunk-ds/splunk/etc/deployment-apps
scp -r -P 2222 all_deploymentclient/
splunk@{IPAddress}:/opt/splunkforwarder/etc/apps
scp -r -P 2222 all_deploymentclient/ splunk@{IPAddress}/opt/splunk/etc/apps
ssh username@{UF1IPAddress}
cd /opt/splunkforwarder/etc/apps/
ls -l
/opt/splunkforwarder/bin/splunk restart
ssh username@{HF1PAddress}
cd /opt/splunk/etc/apps/
ls -l
/opt/splunk/bin/splunk restart
```

# Task 8:

```
ssh username@{UF1IPAddress}
cd /opt/splunkforwarder/bin
./splunk enable boot-start
./splunk stop
./splunk clone-prep-clear-config
cd /opt
tar -czvf splunkforwarder_image.tar SplunkForwarder
scp -P 2222 /opt/splunkforwarder_image.tar.gz username@{UF2IPAddress}:/tmp
/opt/splunkforwarder/bin/splunk start
ssh username@{UF2IPAddress}
cd /tmp
ls -l
tar -xzvf splunkforwarder_image.tar.gz -C /opt
ls -l /opt
/opt/splunkforwarder/bin/splunk start
```

# Task 9:

```
ssh username@deployment-server
cd /opt/splunk-ds/splunk/etc/deployment-apps
mkdir all_linux_inputs
```

```
cd all_linux_inputs
mkdir metadata
mkdir local
cd metadata
vi local.meta

[]
access = read : [ * ], write : [ admin ]
export = system

vi app.conf

[install]
state = enabled

[package]
check_for_updates = false

[ui]
is_visible = false
is_manageable = false

vi inputs.conf

[monitor:///var/log/messages]
disabled = false
index = linux
sourcetype = syslog

cd /opt/splunk-ds/splunk/etc/system/local
vi serverclass.conf

[serverClass:all_linux]
restartSplunkd = true
whitelist.0 = *
machineTypesFilter=linux-i686, linux-x86_64

[serverClass:all_linux:app:all_linux_inputs]

/opt/splunk-ds/splunk/bin/splunk btool serverclass list --debug

/opt/splunk-ds/splunk/bin/splunk restart
```

# Task 10:

```
cd /opt/splunk-ds/splunk/etc/deployment-apps
```

```
mkdir all_apache_inputs
cd all_apache_inputs
mkdir metadata
mkdir local
cd metadata
vi local.meta
```

```
[]
access = read : [ * ], write : [ admin ]
export = system
```

```
cd ../local/
vi app.conf
```

```
[install]
state = enabled

[package]
check_for_updates = false

[ui]
is_visible = false
is_manageable = false
```

```
vi inputs.conf
```

```
[monitor:///var/log/apache2/access.log]
index = web
sourcetype = access_combined
_TCP_ROUTING = HF1
```

```
mkdir /opt/splunk-ds/splunk/etc/deployment-apps/modified_routing_outputs
cd /opt/splunk-ds/splunk/etc/deployment-apps/modified_routing_outputs
mkdir metadata
mkdir local
cd metadata
vi local.meta
```

```
[]
access = read : [ * ], write : [ admin ]
export = system
```

```
cd ../local/
vi app.conf
```

```
[install]
state = enabled
```

```
[package]
check_for_updates = false

[ui]
is_visible = false
is_manageable = false
```

```
vi outputs.conf
```

```
[tcpout:HF1]
server = <HF_IP_ADDRESS>:9997
```

```
mkdir /opt/splunk-ds/splunk/etc/deployment-apps/all_hf_props
cd /opt/splunk-ds/splunk/etc/apps/all_hf_props
mkdir metadata
mkdir local
cd metadata
vi local.meta
```

```
[]
access = read : [ * ], write : [ admin ]
export = system
```

```
cd ../local/
vi app.conf
```

```
[install]
state = enabled

[package]
check_for_updates = false

[ui]
is_visible = false
is_manageable = false
```

```
vi props.conf
```

```
[access_combined]
TRANSFORMS-set_error = set_apache_error
```

```
vi transforms.conf
```

```
[set_apache_error]
REGEX = ERROR
FORMAT = sourcetype::apache_error
DEST_KEY = MetaData:Sourcetype
```

```
cd /opt/splunk/splunk-ds/etc/system/local
vi serverclass.conf

[serverClass:all_apache]
restartSplunkd = true
whitelist.0 = UF*
blacklist.0 = HF*

[serverClass:all_apache:app:all_apache_inputs]
[serverClass:all_apache:app:modified_routing_outputs]

[serverClass:all_hf]
restartSplunkd = true
whitelist.0 = HF*
blacklist.0 = UF*

[serverClass:all_hf:app:all_hf_props]

/opt/splunk/bin/splunk btool serverclass list --debug
/opt/splunk/bin/splunk restart
```