# **AUG 23**

# **Deployment Server:**

A **deployment server** is a Splunk Enterprise instance that acts as a centralized configuration manager for any number of other instances, called "deployment clients". Any full Splunk Enterprise instance - even one indexing data locally - can act as a deployment server. A deployment server cannot be a client of itself.

A **deployment client** or **agent** is a Splunk instance remotely configured by a deployment server. Deployment clients can be universal forwarders, heavy forwarders, indexers, or search heads. Each deployment client belongs to one or more server classes.

A deployment application (app) or configuration is a set of content (including configuration files) maintained on the deployment server and deployed as a unit to clients of a server class. A deployment app might consist of just a single configuration file, or it can consist of many files. Over time, an app can be updated with new content and then redeployed to its designated clients. The deployment app can be an existing Splunk Enterprise app or one developed solely to group some content for deployment purposes.

A **server class** is a group of deployment clients that share one or more defined characteristics. For example, you can group all Windows clients into one server class and all Linux clients into another server class. You use server classes to map a group of deployment clients to one or more deployment apps. By creating a server class, you are telling the deployment server that a specific set of clients should receive configuration updates in the form of a specific set of apps.  $\rightarrow$  **serverclass.conf**  $\rightarrow$  mostly we will perform actions from Web UI

**Repository Location on DS**: \$SPLUNK\_HOME/etc/deployment-apps/

Client repository location→ \$SPLUNK\_HOME/etc/apps/

Example:

\$SPLUNK\_HOME/etc/deployment-apps/

splunk\_outputs\_app/{local,dafault}/outputs.conf

[tcpout]
defaultGroup = indexer\_grp

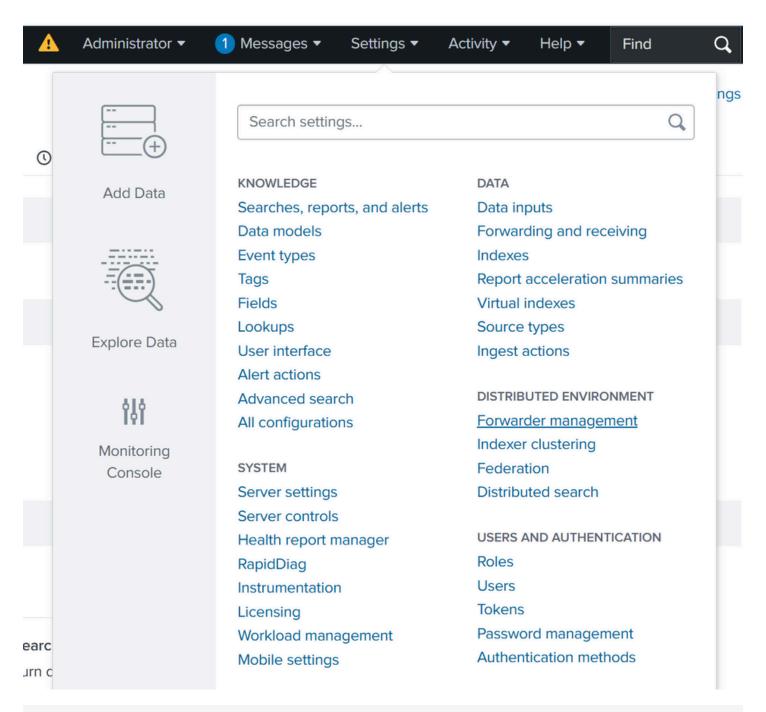
[tcpout:indexer\_grp]
server = indexer1p:9997,indexer2p:9997

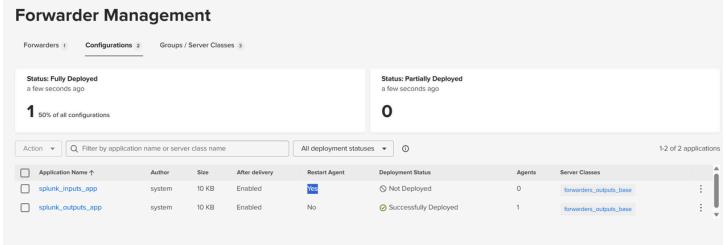
Deployment Server will not push apps/configs to Client.

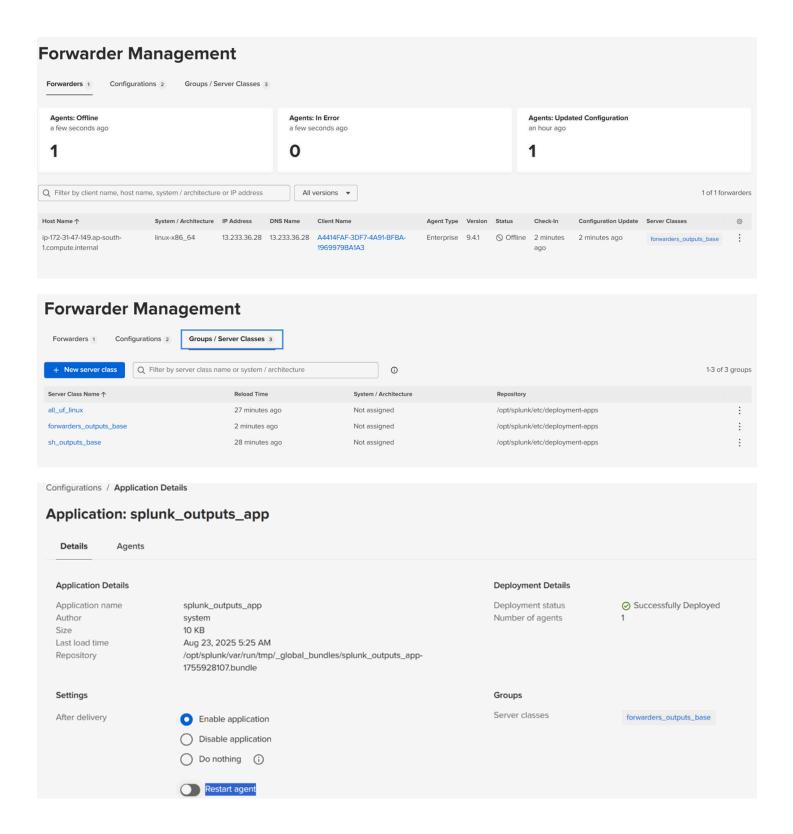
Client will download the latest available configuration by polling to DS.

Configuring Deployment Server

Settings → Forwarder management







# **Configure Deployment Client:**

it can be configured in 2 ways

### by CLI:

splunk set deploy-poll <DS\_IP/DS\_HOSTNAME>:8089

## by Configuration file:

## deploymentclient.conf

[deployment-client]

phoneHomeIntervalInSecs = 60 → can be changed based on # of client reporting to DS

[target-broker:deploymentServer]

targetUri= https://deploymentserver.splunk.buttercupgames.com:8089

```
[root@ip-172-31-47-149 local]# pwd
/opt/splunk/etc/system/local
[root@ip-172-31-47-149 local]# ls
README migration.conf restmap.conf server.conf web.conf
[root@ip-172-31-47-149 local]#
[root@ip-172-31-47-149 local]#
[root@ip-172-31-47-149 local]#
[root@ip-172-31-47-149 local] # splunk set deploy-poll 13.234.77.69:8089
WARNING: Server Certificate Hostname Validation is disabled. Please see server.co
rName for details.
Splunk username: admin
Password:
Configuration updated.
[root@ip-172-31-47-149 local]#
[root@ip-172-31-47-149 local]#
[root@ip-172-31-47-149 local]#
[root@ip-172-31-47-149 local]# ls
README deploymentclient.conf migration.conf restmap.conf server.conf web.com
[root@ip-172-31-47-149 local] # cat deploymentclient.conf
[target-broker:deploymentServer]
targetUri = 13.234.77.69:8089
[root@ip-172-31-47-149 local]#
[root@ip-172-31-47-149 local]#
[root@ip-172-31-47-149 local]#
```

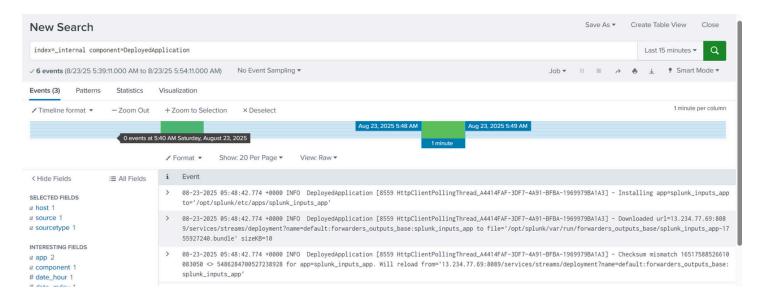
# **Deployment server configs Reload**

whenever there is a change in configurations we need to reload deployment server serverclass

#### splunk reload deploy-server -class forwarders\_outputs\_base

```
[root@ip-172-31-45-225 local]#
[root@ip-172-31-45-225 local]#
[root@ip-172-31-45-225 local]# splunk reload deploy-server -class forwarders_outputs_base
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServ
rName for details.
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServ
rName for details.
Splunk username: admin
Password:
Reloading serverclass(es).
[root@ip-172-31-45-225 local]#
```

#### Splunk Logs on Deployment client



#### **Splunk Logs on Deployment Server:**

