

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. → **serverclass.conf** → 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,default}/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


Add Data


Explore Data


Monitoring Console

Search settings... 

KNOWLEDGE

[Searches, reports, and alerts](#)

[Data models](#)

[Event types](#)

[Tags](#)

[Fields](#)

[Lookups](#)

[User interface](#)

[Alert actions](#)

[Advanced search](#)

[All configurations](#)

SYSTEM

[Server settings](#)

[Server controls](#)

[Health report manager](#)

[RapidDiag](#)

[Instrumentation](#)

[Licensing](#)

[Workload management](#)

[Mobile settings](#)

DATA

[Data inputs](#)

[Forwarding and receiving](#)

[Indexes](#)

[Report acceleration summaries](#)

[Virtual indexes](#)

[Source types](#)

[Ingest actions](#)

DISTRIBUTED ENVIRONMENT

[Forwarder management](#)

[Indexer clustering](#)

[Federation](#)

[Distributed search](#)

USERS AND AUTHENTICATION

[Roles](#)

[Users](#)

[Tokens](#)

[Password management](#)

[Authentication methods](#)

Forwarder Management

Forwarders 1 Configurations 2 Groups / Server Classes 3

Status: Fully Deployed
a few seconds ago

1
50% of all configurations

Status: Partially Deployed
a few seconds ago

0

Action ▾

Filter by application name or server class name

All deployment statuses ▾ ⓘ

1-2 of 2 applications

<input type="checkbox"/>	Application Name ↑	Author	Size	After delivery	Restart Agent	Deployment Status	Agents	Server Classes	
<input type="checkbox"/>	splunk_inputs_app	system	10 KB	Enabled	Yes	⌚ Not Deployed	0	forwards_outputs_base	⋮
<input type="checkbox"/>	splunk_outputs_app	system	10 KB	Enabled	No	✅ Successfully Deployed	1	forwards_outputs_base	⋮

Forwarder Management

Forwarders 1

Configurations 2

Groups / Server Classes 3

Agents: Offline
a few seconds ago

1

Agents: In Error
a few seconds ago

0

Agents: Updated Configuration
an hour ago

1

Q Filter by client name, host name, system / architecture or IP address

All versions ▾

1 of 1 forwarders

Host Name ↑	System / Architecture	IP Address	DNS Name	Client Name	Agent Type	Version	Status	Check-In	Configuration Update	Server Classes	
ip-172-31-47-149.ap-south-1.compute.internal	linux-x86_64	13.233.36.28	13.233.36.28	A4414FAF-3DF7-4A91-BFBA-1969979BA1A3	Enterprise	9.4.1	Offline	2 minutes ago	2 minutes ago	forwarders_outputs_base	

Forwarder Management

Forwarders 1

Configurations 2

Groups / Server Classes 3

+ New server class

Q Filter by server class name or system / architecture

1-3 of 3 groups

Server Class Name ↑	Reload Time	System / Architecture	Repository	
all_uf_linux	27 minutes ago	Not assigned	/opt/splunk/etc/deployment-apps	
forwarders_outputs_base	2 minutes ago	Not assigned	/opt/splunk/etc/deployment-apps	
sh_outputs_base	28 minutes ago	Not assigned	/opt/splunk/etc/deployment-apps	

Configurations / Application Details

Application: splunk_outputs_app

Details

Agents

Application Details

Application name
splunk_outputs_app

Author
system

Size
10 KB

Last load time
Aug 23, 2025 5:25 AM

Repository
/opt/splunk/var/run/tmp/_global_bundles/splunk_outputs_app-1755928107.bundle

Settings

After delivery

Enable application

Disable application

Do nothing ⓘ

Restart agent

Deployment Details

Deployment status
Successfully Deployed

Number of agents
1

Groups

Server classes

forwarders_outputs_base

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

Splunk Logs on Deployment client

New Search

Save As>Create Table ViewClose

index=_internal component=DeployedApplication

Last 15 minutes

6 events (8/23/25 5:39:11.000 AM to 8/23/25 5:54:11.000 AM)No Event SamplingJob|||Smart Mode

Events (3)PatternsStatisticsVisualization

Timeline formatZoom OutZoom to SelectionDeselect1 minute per column

0 events at 5:40 AM Saturday, August 23, 20251 minute

FormatShow: 20 Per PageView: Raw

Hide FieldsAll Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a app 2

a component 1

date_hour 1

Event

> 08-23-2025 05:48:42.774 +0000 INFO DeployedApplication [8559 HttpClientPollingThread_A4414FAF-3DF7-4A91-BFBA-1969979BA1A3] - Installing app=splunk_inputs_app to='/opt/splunk/etc/apps/splunk_inputs_app'

> 08-23-2025 05:48:42.774 +0000 INFO DeployedApplication [8559 HttpClientPollingThread_A4414FAF-3DF7-4A91-BFBA-1969979BA1A3] - Downloaded url=13.234.77.69:8089/services/streams/deployment?name=default:forwarders_outputs_base:splunk_inputs_app to file='/opt/splunk/var/run/forwarders_outputs_base/splunk_inputs_app-1755927240.bundle' sizeKB=10

> 08-23-2025 05:48:42.774 +0000 INFO DeployedApplication [8559 HttpClientPollingThread_A4414FAF-3DF7-4A91-BFBA-1969979BA1A3] - Checksum mismatch 16517588526610083050 <> 5486284700527238928 for app=splunk_inputs_app. Will reload from='13.234.77.69:8089/services/streams/deployment?name=default:forwarders_outputs_base:splunk_inputs_app'

Splunk Logs on Deployment Server:

```
index=_internal splunk_inputs_app source="/opt/splunk/var/log/splunk/splunkd.log"
```

Date time range ▼



✓ 14 events (8/23/25 5:40:00.000 AM to 8/23/25 5:49:00.000 AM) No Event Sampling ▾

Job Smart Mode

Events (3) Patterns Statistics Visualization

Timeline format ▾ - Zoom Out + Zoom to Selection x Deselect

1 minute per column

Aug 23, 2025 5:48 AM

Aug 23, 2025 5:49 AM

1 minute

Format Show: 20 Per Page View: List

[← Hide Fields](#)

☰ All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a app 1

a application 1

[a archiveFile 1](#)

archiveFileSize

```
# checksum 1
```

a component 3

```
# date_hour 1
```

```
# date_mday 1
```

44 data minute 4

i	Time	Event
>	8/23/25 5:48:42.778 AM	08-23-2025 05:48:42.778 +0000 INFO PackageDownloadRestHandler [16796 TcpChannelThread] ~ peer=13.233.36.28:58304 Download started and completed for path=/opt/splunk/var/run/tmp/_global_bundles/splunk_inputs_app-1755928106.bundle.gz serverclass=forwarders_outputs_base app=splunk_inputs_app host = ip-172-31-45-225.ap-south-1.compute.internal source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	8/23/25 5:48:26.998 AM	08-23-2025 05:48:26.998 +0000 INFO Application [16092 TcpChannelThread] ~ Loaded application=splunk_inputs_app fqAppPath=/opt/splunk/etc/deployment-apps/splunk_inputs_app_archiveFile=/opt/splunk/var/run/tmp/_global_bundles/splunk_inputs_app-1755928106.bundle_archiveFileSize=10240 _timestamp=1755928106 _checksum=5486284700527238928 host = ip-172-31-45-225.ap-south-1.compute.internal source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
>	8/23/25 5:48:26.948 AM	08-23-2025 05:48:26.948 +0000 INFO Serverclass [16092 TcpChannelThread] ~ Reloading application=splunk_inputs_app from location=/opt/splunk/etc/deployment-apps' host = ip-172-31-45-225.ap-south-1.compute.internal source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd