



# KPLABS Course

Splunk 2021 - Beginner to Architect

## Domain 4

**ISSUED BY**

Zeal

**REPRESENTATIVE**

[instructors@kplabs.in](mailto:instructors@kplabs.in)

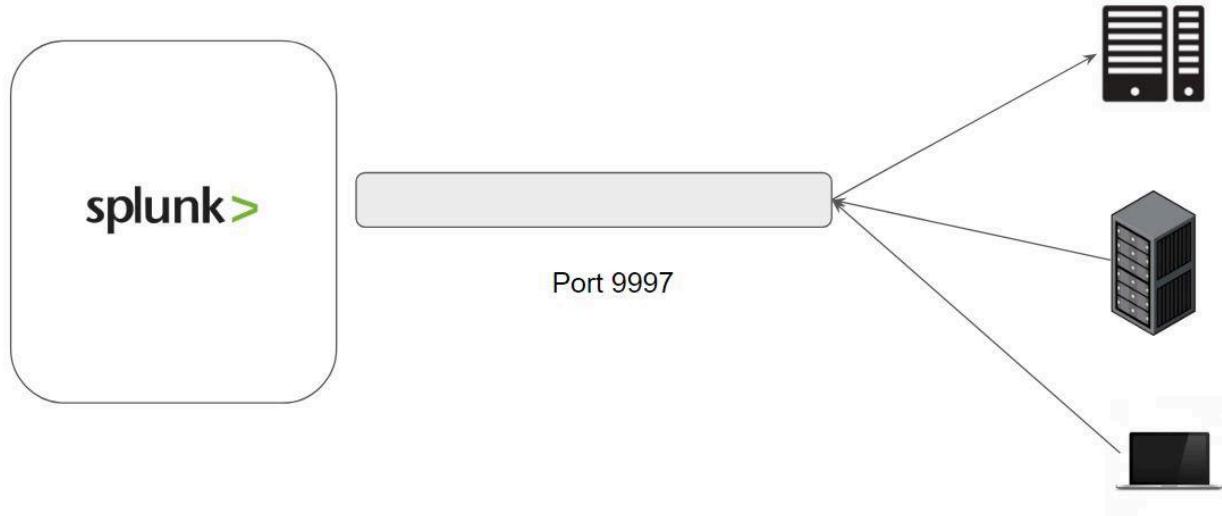
## Domain 4 - Forwarder & User Management

### Module 1: Universal Forwarder

Universal Forwarder collects data from a server and sends it to your Splunk deployment.

Splunk offers universal forwarder agent for various operating systems, including:

- Linux
- Windows
- MAC
- Solaris
- FreeBSD
- AIX



## Module 2: Challenges with Forwarder Management

### 2.1 Typical Challenges

Universal Forwarder collects data from a server and sends it to your Splunk deployment.

While installing universal forwarder, we run certain commands like:

- `./splunk add monitor /var/log`
- `./splunk add forward-server 172.17.0.2:9997`

This can be manual and can be automated with configuration management tools like Ansible.

### 2.2 Typical Use-Case

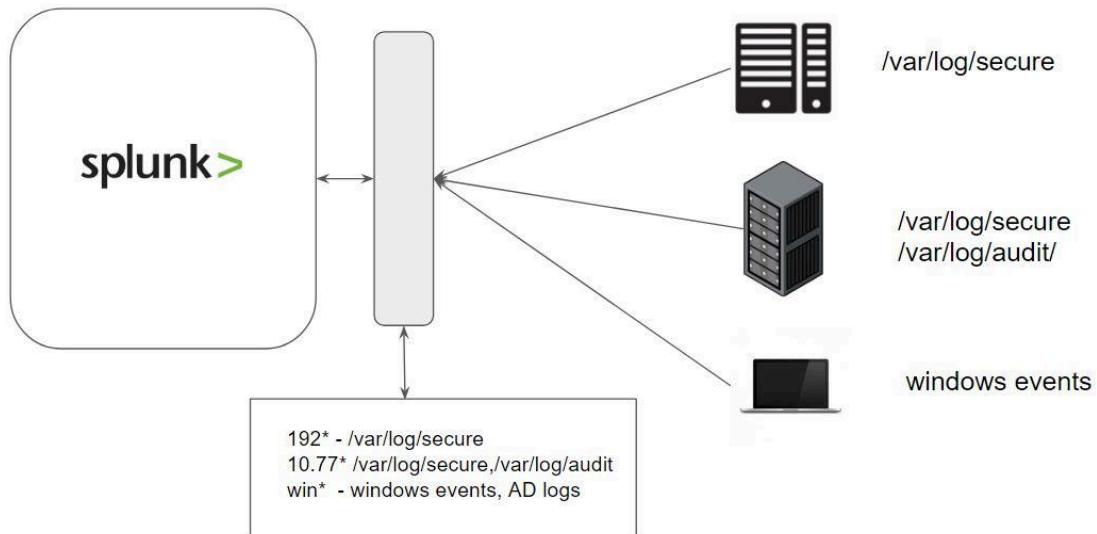
#### Some example use-cases:

Any server which belongs to subnet 192.168.10.0/24 network should have only /var/log/secure file to be monitored.

Any server which belongs to subnet 10.77.0.0/20 should have /var/log/secure and /var/log/audit directory to be monitored.

If the server hostname starts with win- , then integrate it to send all the windows events and AD logs.

## 2.3 Forwarder Management



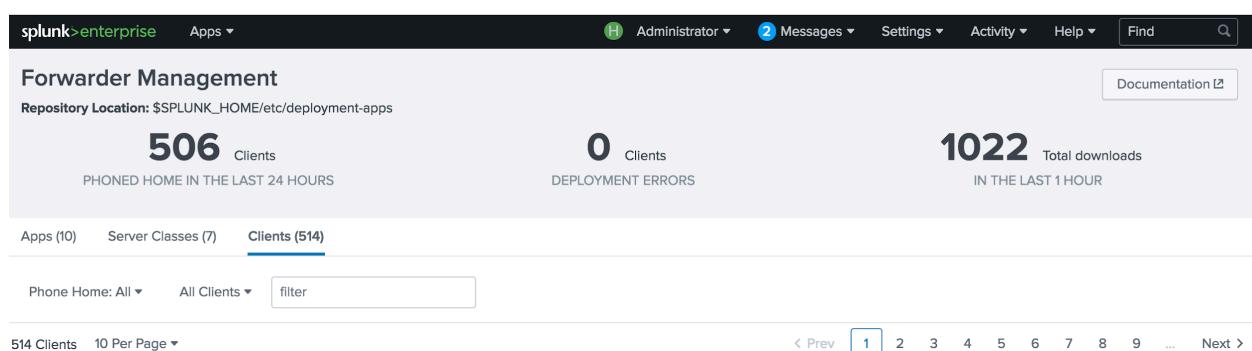
## Module 3: Introduction to Deployment Server

### 3.1 Overview of Deployment Server

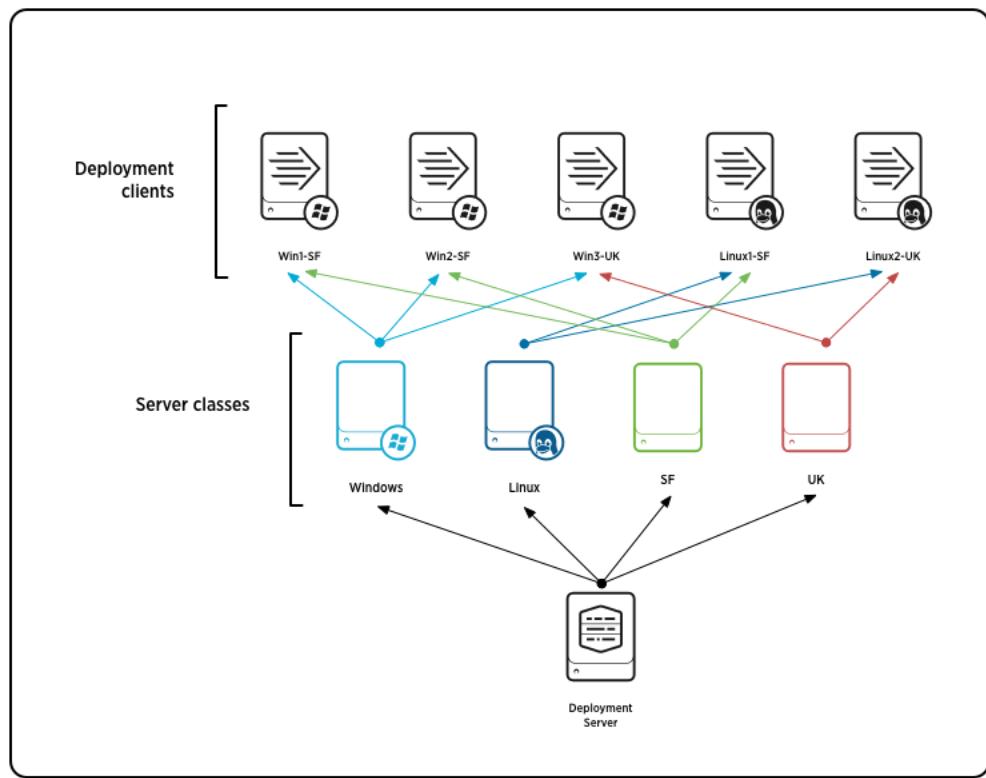
Deployment Server is a tool for distributing configuration, apps and content updates to group of splunk enterprise instances like universal forwarders, search heads and others.

Forwarder Management is a GUI built on top of deployment server that provides an easy way to configure the deployment server and monitor the status of deployment updates.

The following diagram illustrates the Forwarder Management Dashboard



The following diagram illustrates the Deployment server dashboard



### 3.2 Key Terminology of Deployment Server

**Server Class:**

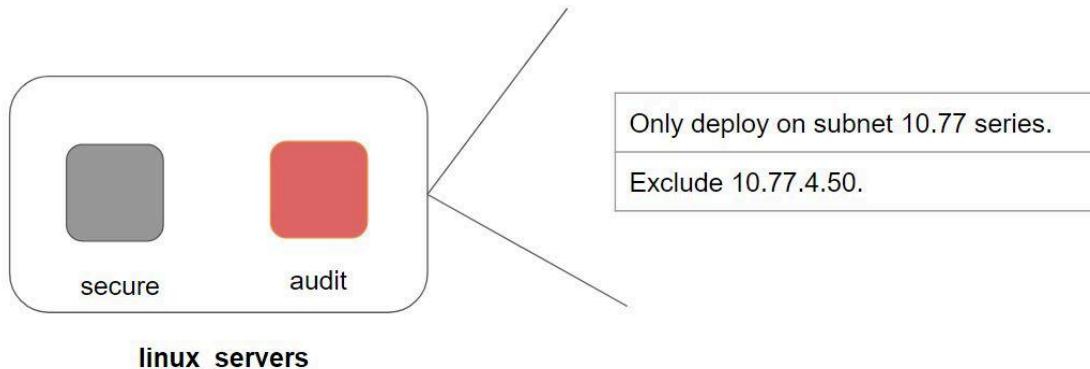
A group of common configuration which is shared by multiple instances.

**Example:**

- ServerClass called “Windows” which is common to all windows servers.
- Serverclass called “Linux” which is common for all linux servers.

## Module 4: ServerClass and Deployment Apps

Server Class is a group that can contain multiple deployment apps.



## Module 5: Creating Custom Add-Ons for deployment

There are two important files that we need to look into:

- inputs.conf
- outputs.conf

Inputs file determines which are the log files to monitor.

Outputs file determines to which destination data should be forwarded to.

### inputs.conf

```
[monitor:///var/log]
disabled = falase
index = forwarder
```

### outputs.conf

```
[tcpout]
defaultGroup = default-autolb-group

[tcpout:default-autolb-group]
server = 172.17.0.2:9997

[tcpout-server://172.17.0.2:9997]
```

