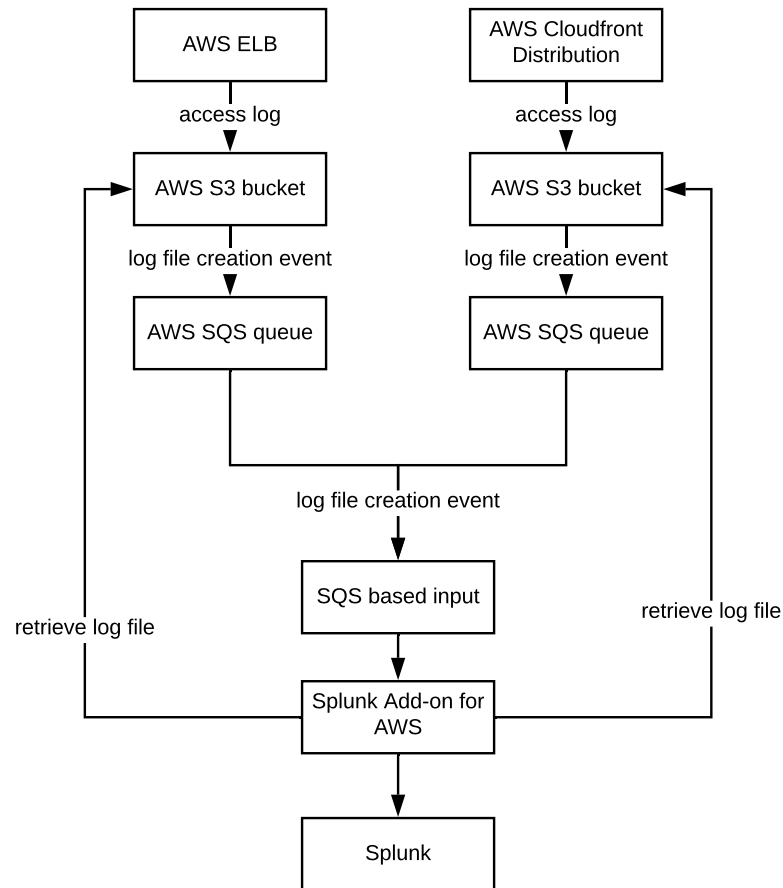ELB, Cloudfront access log transport to
Splunk via S3 and SQS

Automate SQS based input configuration
for Splunk

```
AWS ELB
```
access log
```
AWS S3 bucket
```
log file creation event
```
AWS SQS queue
```

```
AWS Cloudfront
Distribution
```
access log
```
AWS S3 bucket
```
log file creation event
```
AWS SQS queue
```

log file creation event
```
SQS based input
```

retrieve log file
```
Splunk Add-on for
AWS
```
retrieve log file

```
Splunk
```

```
AWS CLI to list SQS queues from
an AWS region
```
```
Parse queue names
```
```
Create Splunk input config file
```
```
Create Ansible playbook
1. copy input config file
2. reload input config
```
```
Run Ansible playbook
```

Ansible

```
Splunk server
```