Hosts

Webserv1
access.log
secure.log

Webserv2
access.log
secure.log

Webserv3
access.log
secure.log

localhost
Eventgen App
eventgen.conf

SPLUNK

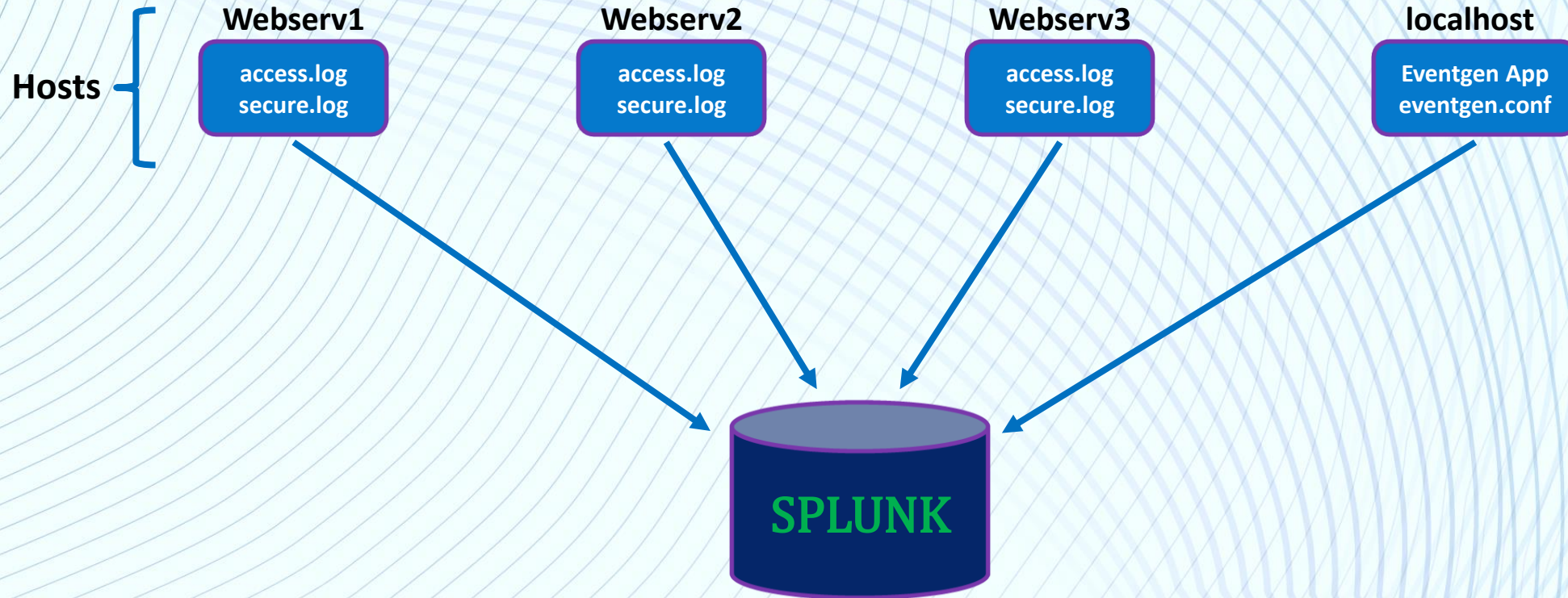**Web Access Metadata:**
index=web
sourcetype=access_combined
source=access.log
host=Webserv1,Webserv2,Webserv3

Web Security Metadata:
index=security
sourcetype=linux_secure
source=secure.log
host=Webserv1,Webserv2,Webserv3

Eventgen Metadata:
index=main
sourcetype=eventgen
source=eventgen.conf
host=localhost