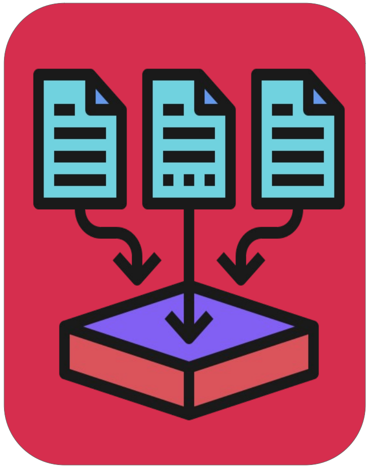
CFGS Administración de sistemas informáticos en red

Centralización y análisis de logs mediante Opensearch

ALUMNO/A: Pedro Peralta Guerrero
TUTOR/A: Javier García Estévez

Presentación del problema



Presentación del problema

SYSLOG

AUTH.LOG

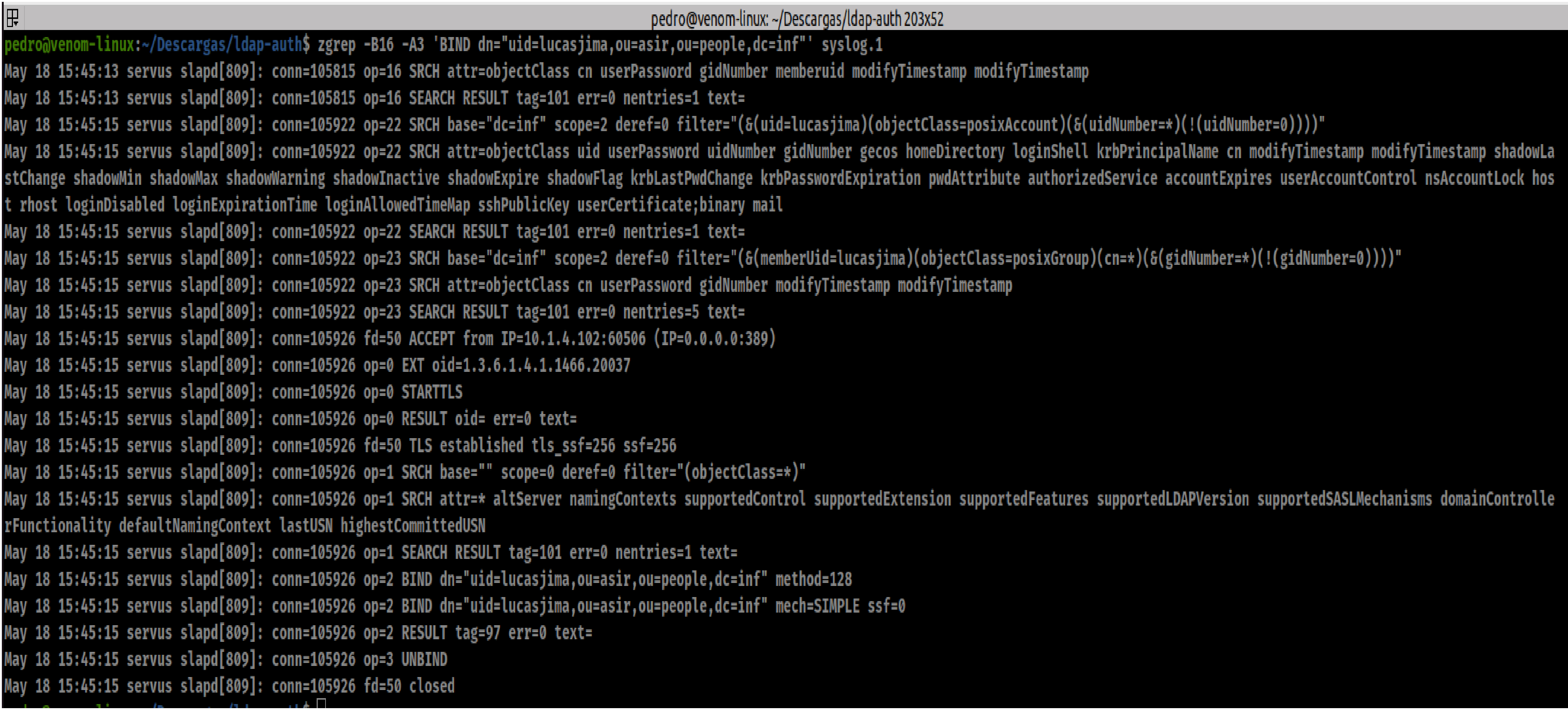
Presentación del problema

FORMATO

CONEXIONES

PARSING

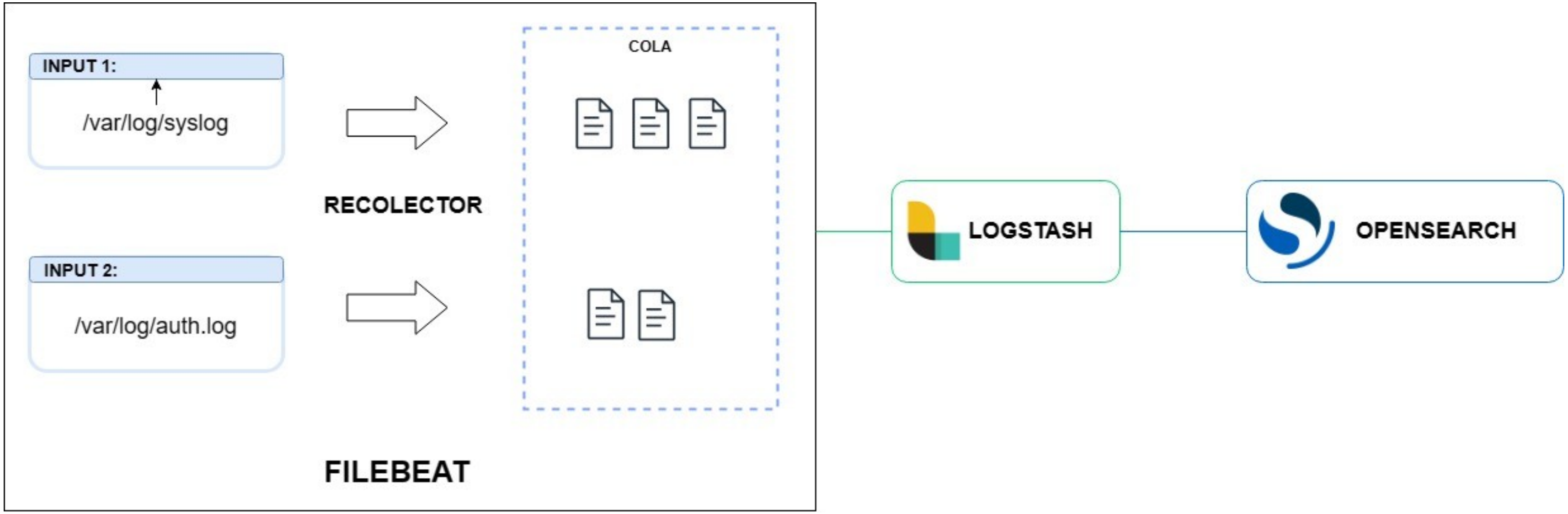
EQUIPOS



```
pedro@venom-linux:~/Descargas/ldap-auth$ zgrep -B16 -A3 'BIND dn="uid=lucasjima,ou=asir,ou=people,dc=inf"' syslog.1
May 18 15:45:13 servus slapd[809]: conn=105815 op=16 SRCH attr=objectClass cn userPassword gidNumber memberuid modifyTimestamp modifyTimestamp
May 18 15:45:13 servus slapd[809]: conn=105815 op=16 SEARCH RESULT tag=101 err=0 nentries=1 text=
May 18 15:45:15 servus slapd[809]: conn=105922 op=22 SRCH base="dc=inf" scope=2 deref=0 filter="(&(uid=lucasjima)(objectClass=posixAccount)(&(uidNumber=*)(!(uidNumber=0))))"
May 18 15:45:15 servus slapd[809]: conn=105922 op=22 SRCH attr=objectClass uid userPassword uidNumber gidNumber gecos homeDirectory loginShell krbPrincipalName cn modifyTimestamp modifyTimestamp shadowLa
stChange shadowMin shadowMax shadowWarning shadowInactive shadowExpire shadowFlag krbLastPwdChange krbPasswordExpiration pwdAttribute authorizedService accountExpires userAccountControl nsAccountLock hos
t rhost loginDisabled loginExpirationTime loginAllowedTimeMap sshPublicKey userCertificate;binary mail
May 18 15:45:15 servus slapd[809]: conn=105922 op=22 SEARCH RESULT tag=101 err=0 nentries=1 text=
May 18 15:45:15 servus slapd[809]: conn=105922 op=23 SRCH base="dc=inf" scope=2 deref=0 filter="(&(memberUid=lucasjima)(objectClass=posixGroup)(cn=*)(&(gidNumber=*)(!(gidNumber=0))))"
May 18 15:45:15 servus slapd[809]: conn=105922 op=23 SRCH attr=objectClass cn userPassword gidNumber modifyTimestamp modifyTimestamp
May 18 15:45:15 servus slapd[809]: conn=105922 op=23 SEARCH RESULT tag=101 err=0 nentries=5 text=
May 18 15:45:15 servus slapd[809]: conn=105926 fd=50 ACCEPT from IP=10.1.4.102:60506 (IP=0.0.0.0:389)
May 18 15:45:15 servus slapd[809]: conn=105926 op=0 EXT oid=1.3.6.1.4.1.1466.20037
May 18 15:45:15 servus slapd[809]: conn=105926 op=0 STARTTLS
May 18 15:45:15 servus slapd[809]: conn=105926 op=0 RESULT oid= err=0 text=
May 18 15:45:15 servus slapd[809]: conn=105926 fd=50 TLS established tls_ssf=256 ssf=256
May 18 15:45:15 servus slapd[809]: conn=105926 op=1 SRCH base="" scope=0 deref=0 filter="(objectClass=*)"
May 18 15:45:15 servus slapd[809]: conn=105926 op=1 SRCH attr=* altServer namingContexts supportedControl supportedExtension supportedFeatures supportedLDAPVersion supportedSASLMechanisms domainControlle
rFunctionality defaultNamingContext lastUSN highestCommittedUSN
May 18 15:45:15 servus slapd[809]: conn=105926 op=1 SEARCH RESULT tag=101 err=0 nentries=1 text=
May 18 15:45:15 servus slapd[809]: conn=105926 op=2 BIND dn="uid=lucasjima,ou=asir,ou=people,dc=inf" method=128
May 18 15:45:15 servus slapd[809]: conn=105926 op=2 BIND dn="uid=lucasjima,ou=asir,ou=people,dc=inf" mech=SIMPLE ssf=0
May 18 15:45:15 servus slapd[809]: conn=105926 op=2 RESULT tag=97 err=0 text=
May 18 15:45:15 servus slapd[809]: conn=105926 op=3 UNBIND
May 18 15:45:15 servus slapd[809]: conn=105926 fd=50 closed
May 18 15:45:15 servus slapd[809]: conn=105926 fd=50 ACCEPT from
IP=10.1.4.102:60506 (IP=0.0.0.0:389)

May 18 15:45:15 servus slapd[809]: conn=105926 op=2 BIND
dn="uid=lucasjima,ou=asir,ou=people,dc=inf" method=128

May 18 15:45:15 servus slapd[809]: conn=105926 op=2 BIND
dn="uid=lucasjima,ou=asir,ou=people,dc=inf" mech=SIMPLE ssf=0

May 18 15:45:15 servus slapd[809]: conn=105926 op=2 RESULT tag=97 err=0
text=

May 18 15:45:15 servus slapd[809]: conn=105926 op=3 UNBIND

May 18 15:45:15 servus slapd[809]: conn=105926 fd=50 closed
```

10.4.1.115	PC15-T1
10.4.2.21	DEPT01
10.4.2.101	PC01-T2
10.4.2.1	SERV1-T2

ARQUITECTURA PROPUESTA

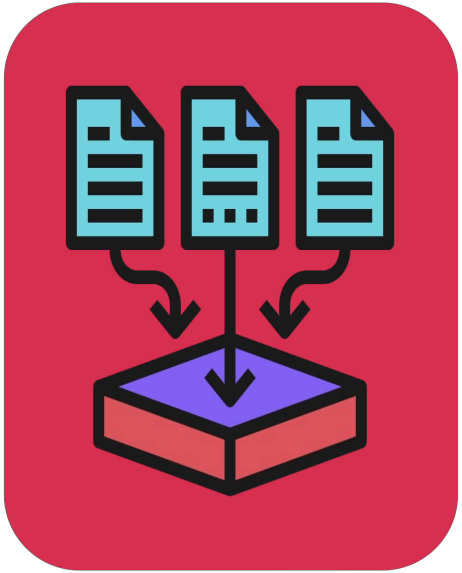


Herramientas utilizadas

Filebeat

Fluent-bit

Herramientas utilizadas



LOGSTASH

PLUGINS

Herramientas utilizadas

OPENSEARCH

ELASTICSEARCH

Herramientas utilizadas

RESULTADO FINAL