CFL - OpenLDAP

Authentication Failure Events

OpenLDAP logs AuthN failures with a specific error code, 49.

Here's a sample log sequence for an authentication failure:

```
Jul  9 13:59:54 ldap1.example.edu Jul  9 13:59:54 ldap1 slapd[29168]: conn=12495962 fd=26 ACCEPT from IP=129.
93.1.14:55256 (IP=0.0.0.0:636)
Jul  9 13:59:54 ldap1.example.edu Jul  9 13:59:54 ldap1 slapd[29168]: conn=12495962 fd=26 TLS established
tls_ssf=128 ssf=128
Jul  9 13:59:54 ldap1.example.edu Jul  9 13:59:54 ldap1 slapd[29168]: conn=12495962 op=0 BIND dn="uid=hhusker1,
ou=people,dc=unl,dc=edu" method=128
Jul  9 13:59:54 ldap1.example.edu Jul  9 13:59:54 ldap1 slapd[29168]: conn=12495962 op=0 RESULT tag=97 err=49
text=
Jul  9 13:59:54 ldap1.example.edu Jul  9 13:59:54 ldap1 slapd[29168]: conn=12495962 fd=26 closed (connection
lost)
```

The syslog aggregator must be able to group the events based on the connection ID so that you can determine the user's ID, in this case: *uid=hhusker1, ou=people,dc=unl,dc=edu*

Splunk has support for this via the *transaction* command which can group events. Sample search within Splunk for this:

```
source="idm-ldap" | transaction conn maxpause=5m | where err=49
```

This search groups events based on the conn attribute within the time range of 5 minutes, and finds those with error code 49 (invalid credentials).

Password Reset Events

OpenLDAP logs a password change as a regular modify attribute event. You must search for MOD attr=userPassword, and retain the DN of the entry which was modified.

```
Jul 12 08:12:23 ldap1.example.edu Jul 12 08:12:23 ldap1 slapd[22981]: conn=3538627 op=1 MOD dn="uid=hhusker1,
ou=people,dc=unl,dc=edu"
Jul 12 08:12:23 ldap1.example.edu Jul 12 08:12:23 ldap1 slapd[22981]: conn=3538627 op=1 MOD attr=userPassword
Jul 12 08:12:23 ldap1.example.edu Jul 12 08:12:23 ldap1 slapd[22981]: conn=3538627 op=1 RESULT tag=103 err=0
text=
```

Sample search for Splunk:

```
source="idm-ldap" MOD OR RESULT | transaction conn op maxpause=35s | search "MOD attr=userPassword" err=0
```

This search groups events using the transaction and operation values.