Open Infrastructure - Task #7545

Switch production LDAPs to cdist-managed alpine

12/31/2019 03:20 PM - Timothée Floure

Status:	Closed	**Start date:**	12/31/2019
Priority:	Normal	**Due date:**	
Assignee:	Timothée Floure	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
PM Check date:			

Description

Our production LDAP nodes do not seem to be managed by cdist (anymore?): * No relevant mention in `grep -R __ungleich_ldap dot-cdist/` or `grep -R ldap1 dot-cdist/` * Deployed configuration do not exactly match `__ungleich_ldap` type.

=> Investigate and update dot-cdist to handle production ldap{1,2}.ungleich.ch

History

#1 - 01/21/2020 10:57 AM - Timothée Floure

- Status changed from New to In Progress

#2 - 02/18/2020 10:42 AM - Timothée Floure

- Status changed from In Progress to Waiting

I cleaned up and revamped the __ungleich_ldap type to run on alpine + deployed new ldap-stagin[1,2] nodes. I'm waiting to deploy a fix to __ungleich_nftables for firewalling and monitoring of the new setup.

I would like to move the production environment to this new deployment scheme next week when I am in Glarus.

#3 - 06/15/2020 09:50 AM - Timothée Floure

- Subject changed from Investigate why production ldap{1,2}.ungleich.ch are not managed by dot-cdist to Switch production LDAPs to cdist-managed alpine

This is at the top of my TODO next time I come to Glarus, I don't want this to be delayed anymore.

#4 - 07/20/2020 11:10 AM - Timothée Floure

- Status changed from Waiting to In Progress

- ldap3.ungleich.ch has been allocated.
- cdist configuration has been simplified, now making use of __openldap_server (alpine support being upstreamed via https://code.ungleich.ch/ungleich-public/cdist/-/merge_requests/909)
- ldap3.ungleich.ch is not syncing with ldap2/ldap1 due to TLS issues (= TLS handshake fail for some reason).

#5 - 07/24/2020 01:43 PM - Timothée Floure

ldap3.ungleich.ch is now syncing with existing ldap1 and ldap2, although some objects fail to sync:

On ldap3.ungleich.ch:

```
Jul 24 11:42:57 alpine local4.debug slapd[26141]: syncrepl_message_to_entry: rid=002 mods check (objectClass:
value #4 invalid per syntax)
Jul 24 11:42:57 alpine local4.debug slapd[26141]: do_syncrepl: rid=002 rc 21 retrying
```

#6 - 07/24/2020 01:44 PM - Timothée Floure

OUs sync properly but not user entries:

```
Jul 24 11:43:50 alpine local4.debug slapd[26218]: syncrepl_entry: rid=002 be_search (0)
Jul 24 11:43:50 alpine local4.debug slapd[26218]: syncrepl_entry: rid=002 ou=customer,dc=ungleich,dc=ch
Jul 24 11:43:50 alpine local4.debug slapd[26218]: syncrepl_entry: rid=002 entry unchanged, ignored (ou=customer,dc=ungleich,dc=ch)
```

Jul 24 11:43:50 alpine local4.debug slapd[26218]: syncrepl_message_to_entry: rid=002 DN: uid=kjg,ou=users,dc=ungleich,dc=ch, UUID: b6a5cd66-6630-1038-9dc5-01997400fff6
Jul 24 11:43:50 alpine local4.debug slapd[26218]: >>> dnPrettyNormal: <uid=kjg,ou=users,dc=ungleich,dc=ch>
Jul 24 11:43:50 alpine local4.debug slapd[26218]: <<< dnPrettyNormal: <uid=kjg,ou=users,dc=ungleich,dc=ch>, <uid=kjg,ou=users,dc=ungleich,dc=ch>
Jul 24 11:43:50 alpine local4.debug slapd[26218]: syncrepl_message_to_entry: rid=002 mods check (objectClass: value #4 invalid per syntax)
Jul 24 11:43:50 alpine local4.debug slapd[26218]: daemon: activity on 1 descriptor
Jul 24 11:43:50 alpine local4.debug slapd[26218]: daemon: activity on:
Jul 24 11:43:50 alpine local4.debug slapd[26218]:
Jul 24 11:43:50 alpine local4.debug slapd[26218]: daemon: epoll: listen=7 active_threads=0 tvp=zero
Jul 24 11:43:50 alpine local4.debug slapd[26218]: daemon: epoll: listen=8 active_threads=0 tvp=zero
Jul 24 11:43:50 alpine local4.debug slapd[26218]: daemon: epoll: listen=9 active_threads=0 tvp=zero
Jul 24 11:43:50 alpine local4.debug slapd[26218]: do_syncrepl: rid=002 rc 21 retrying
```

#### #7 - 07/24/2020 02:03 PM - Timothée Floure

Issue tracked down to `objectClass: ldapPublicKey`. The schema might have to be synced by hand / put into cdist.

#### #8 - 07/24/2020 02:10 PM - Timothée Floure

Diff on files in /etc/(open)ldap/schema:

```
I /tmp » diff a b
13a14,15
> guacConfigGroup.ldif
> guacConfigGroup.schema
17a20
> ldapns.schema
23a27,28
> openssh-ldap.ldif
> openssh-ldap.schema
28d32
< xaa
```

=> Adding to cdist.

#9 - 07/24/2020 02:51 PM - Timothée Floure

ldap3.ungleich.ch is now synced to ldap1 and ldap2. I will replace ldap2 and ldap1 in a few days. I'll announce and try to do it early in the morning.

#10 - 02/10/2021 09:06 AM - Timothée Floure

- Status changed from In Progress to Waiting

- Priority changed from High to Normal

Small update: this has still to be processed.

#11 - 07/29/2021 06:08 PM - Timothée Floure

- Status changed from Waiting to Closed

This is rotten - we will move the LDAP nodes to k8s. See #9473.
```