DuckCorp Infrastructure - Bug #619

Enhancement # 615 (Rejected): new Toushirou: configuration migration

LDAP servers: install slapd

2018-04-23 18:39 - Pierre-Louis Bonicoli

Status:	Resolved	**Start date:**	2018-04-23
Priority:	Normal	**Due date:**	
Assignee:	Marc Dequènes	**% Done:**	100%
Category:	Service :: IS / AAA / PKI	**Estimated time:**	0:00 hour
Target version:			
Patch Available:		**Entity:**	DuckCorp
Confirmed:	No	**Security:**	
Branch:	ldap_config	**Help Needed:**	

Description

```
$ ansible-playbook -l Toushirou -i hosts.yml --ask-pass -v playbooks/common.yml
```

```
TASK [dc-accounts : Generate Shirka-light Configuration] *****************************************************************************************************
fatal: [Toushirou]: FAILED! => {"changed": false, "checksum": "4aa6b0fe7169098414b8fe10eb0879f4d1478859", "dest": "/etc/mp-admin/shirka.conf", "gid": 0, "group": "root", "mode": "0644", "msg": "chgrp failed: failed to look up group dc-admins", "owner": "root", "path": "/etc/mp-admin/shirka.conf", "size": 254, "state": "file", "uid": 0}
```

Should tenants/duckcorp/ldap.yml playbook be executed before tenants/duckcorp/accounts.yml ?

Related issues:

Related to DuckCorp Infrastructure - Enhancement #140: Switch to slapd.d config	**Rejected**	**2010-09-05**
Related to DuckCorp Infrastructure - Bug #594: slap_global_control: unrecogni...	**Blocked**	**2017-09-21**
Related to DuckCorp Infrastructure - Enhancement #626: Automate the WORLD!!!	**In Progress**	**2018-05-07**

History

#1 - 2018-04-23 18:39 - Pierre-Louis Bonicoli

- Description updated

#2 - 2018-04-23 18:39 - Pierre-Louis Bonicoli

- Description updated

#3 - 2018-04-23 18:51 - Pierre-Louis Bonicoli

Not related: not sure why Fetch auth service account info is used twice with same parameters:
- here
- and there ?

#4 - 2018-04-23 19:01 - Pierre-Louis Bonicoli

Isn't /etc/ldap/ldap.conf configuration missing ?

#5 - 2018-04-24 02:19 - Pierre-Louis Bonicoli

- Subject changed from dc-accounts: failed to look up group dc-admins to Toushirou: install slapd

- Parent task set to #615

> l'installation initiale du LDAP est pas gérée encore car installer le package c'est trivial mais le setup des backends et de la replication c'est plus compliqué

#6 - 2018-04-27 10:44 - Marc Dequènes

- Category changed from System :: Base to Service :: IS / AAA / PKI

The two call to `service_account_info` could indeed be factorized.

The basic installation (easy) and replication setup (harder) Ansibilization has not been done yet. I focues on the content because it was critical but indeed it needs to be done.

#7 - 2018-04-28 08:10 - Marc Dequènes

- Subject changed from Toushirou: install slapd to LDAP servers: install slapd

#8 - 2018-04-28 10:53 - Marc Dequènes

- Status changed from New to In Progress

- Assignee set to Marc Dequènes

#9 - 2018-04-28 11:45 - Marc Dequènes

- % Done changed from 0 to 10

I changed the order, good catch.

I removed the redundant call.

#10 - 2018-04-28 12:34 - Marc Dequènes

How would you suggest we do the servers' config: generating temporary LDIFs and slapadd-ing? I guess we would need to ldapsearch if this was added before, seems complicated. Or maybe generating (offline) files in the `/etc/ldap/slapd.d/` directory directly? It should be fast and only at install time, so no downtime.

I think this would also make easier to update the schema (with a very short downtime like when we update the content).

#11 - 2018-04-29 17:20 - Marc Dequènes

- Related to Enhancement #140: Switch to slapd.d config added

#12 - 2018-05-05 04:29 - Marc Dequènes

I appears to be a tad complicated. We should not have a huge amount of parameters to setup, then replication and feeking the master with the schemas. So I'll try to list what's really useful.

I saw Ansible has LDAP modules but it's lacking a few things. `ldap_entry` is used to create a new entry, and you would need to at least setup the compulsory attributes, but this module does not assert the states of the attributes is fine, which means you need to repeat yourself with `ldap_attr` to ensue their values us still right. There is also no way to query the database, which might be annoying to take proper decisions as entries' indexes might differ.

I think we should also solve #594 in the process.

#13 - 2018-05-05 04:29 - Marc Dequènes

- Related to Bug #594: slap_global_control: unrecognized control added

#14 - 2018-05-19 05:38 - Marc Dequènes

- Branch set to ldap_config

Working on a simple integration into the **dc-ldap** role for now.

#15 - 2018-05-21 07:23 - Marc Dequènes

I read copying files did not always worked out well. Also there are a lot of parameters which were converted from the conffiles and, according to upstream, **must** be cleaned up. We should also switch to mdb and it is supposed to be seamless. Moreover the root DN should not be in a database, so following the default package setup would probably be better.

Listing the useful settings:

- cn=config
  - olcLocalSSF
  - olcLogLevel
  - olcTLSCACertificateFile
  - olcTLSCertificateFile
  - olcTLSCertificateKeyFile
- cn=config/cn=module{0}
  - olcModuleLoad
- cn=config/olcDatabase={-1}frontend
  - olcMonitoring
- cn=config/olcDatabase={0}config
  - olcAccess
  - olcMonitoring
  - olcRootPW (add)
- cn=config/olcDatabase={0}config/olcOverlay={0}syncprov
  - olcSpCheckpoint
  - olcSpSessionlog
  - olcSpReloadHint
- cn=config/olcDatabase={1}monitor
  - olcMonitoring
  - olcAccess
- cn=config/olcDatabase={1}mdb
  - olcSuffix
  - olcAccess
  - olcRootDN
  - olcRootPW (remove)
  - olcMonitoring
  - olcDbIndex
  - olcLimits
  - olcDbDirectory

As for the schema, *duckcorp* seem to only need *ISPEnv2*.

#16 - 2018-05-24 05:56 - Marc Dequènes

- Status changed from In Progress to Resolved

- % Done changed from 10 to 100

With some modifications and cleanup this is done.

Also the schema file was unmaintained, so I reverse engineered from the LDIF of the database. It is again the primary source of knowledge.

Changing the schema content is still an issue, a OpenLDAP has quite some limitations. This would be worked on in the future.

There is a new playbook *regen_ldap_content.yml* to regenerate the database content only.

#17 - 2018-12-14 02:51 - Marc Dequènes

- Related to Enhancement #626: Automate the WORLD!!! added