fuss-manager - Segnalazione #856

interfaccia con LDAP asincrona per tornado

06/28/2019 01:41 PM - Elena Grandi

Status:	Chiuso	**Start date:**	06/28/2019
Priority:	Normale	**Due date:**	
Assignee:	Elena Grandi	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.7 Autenticazione e autorizzazione		
Resolution:			

Description

documentare poi come questa interfaccia esporta le informazioni ottenute da LDAP (utente e gruppi di cui fa parte) al resto del codice tornado.

Related issues:

Related to fuss-manager - Segnalazione #862: form/view di login	**Chiuso**	**06/28/2019**
Related to fuss-manager - Segnalazione #858: file di configurazione che assoc...	**Chiuso**	**06/28/2019**
Related to fuss-manager - Segnalazione #860: inserire nome utente e permessi ...	**Chiuso**	**06/28/2019**
Related to fuss-manager - Segnalazione #861: Mostrare il nome utente corrente...	**Chiuso**	**06/28/2019**
Blocks fuss-manager - Segnalazione #863: Aggiungere permission checking a ope...	**Chiuso**	**06/28/2019**

Associated revisions

Revision 372babd7 - 07/08/2019 05:23 PM - Enrico Zini

Initial LDAP wrapper class. refs: #856

Revision ea015a01 - 07/08/2019 05:32 PM - Enrico Zini

Implemented to test authentication. refs: #856

Revision c7d81823 - 07/08/2019 05:41 PM - Enrico Zini

Print auth results. refs: #856

Revision 4811999c - 07/08/2019 06:03 PM - Enrico Zini

To facilitate repeated iterations, pick the password from ldap_password if it exists. refs: #856

Revision 18228fc7 - 07/08/2019 06:07 PM - Enrico Zini

Lookup group information. refs: #856

Revision 80e8ce97 - 07/09/2019 11:08 AM - Enrico Zini

Use a dataclass to model the User object. refs: #856

Revision 3e2bfdee - 07/09/2019 11:10 AM - Enrico Zini

Moved user infrastructure in a separate submodule. refs: #856

Revision f7020d10 - 07/09/2019 11:25 AM - Enrico Zini

Added a generic infrastructure for user databases. refs: #856

Revision d9c6225b - 07/09/2019 11:50 AM - Enrico Zini

Fixed a race condition when it failed to stop a service before it had started. refs: #856

Revision 1b34327e - 07/09/2019 11:53 AM - Enrico Zini

Added a fallback local user database to work on non-ldap systems. refs: #856

Revision 222921ea - 07/09/2019 11:57 AM - Enrico Zini

Use a Group dataclass for groups. refs: #856

Revision 93f26bfe - 07/09/2019 12:05 PM - Enrico Zini

Do not stick to confusing ldap names for User and Group fields. refs: #856

Revision 146039be - 07/09/2019 12:07 PM - Enrico Zini

Revove need for ldap_bind_dn_template. refs: #856

Revision 6b30fa58 - 07/09/2019 01:07 PM - Enrico Zini

Added a mock user database, and instantiate a user database in Manager. refs: #856

Revision db81b177 - 07/09/2019 01:26 PM - Enrico Zini

Fixed mock user db. refs: #856

Revision 482e7954 - 07/09/2019 02:13 PM - Elena Grandi

Mock users only have the admin group when called root or admin. refs: #856

Revision 1aa38c03 - 07/10/2019 12:02 PM - Elena Grandi

New auth backend: master password. refs: #856

Revision 20ce2b91 - 09/24/2019 04:24 PM - Enrico Zini

Sync with master. refs: #856

Revision 6ef853c0 - 09/24/2019 04:24 PM - Enrico Zini

Merged partial work into master after review. Refs: #856

Revision f337e2d9 - 09/26/2019 12:25 PM - Elena Grandi

Start documenting the configuration file. refs: #856

Revision b70fe68e - 09/26/2019 12:42 PM - Elena Grandi

Set a sensible default for fuss as the LDAP configuration in the example. refs: #856

Revision f7069d83 - 09/26/2019 02:54 PM - Elena Grandi

Load false values for the LDAP default configuration. refs: #856

Revision 40028247 - 09/27/2019 04:07 PM - Enrico Zini

Merge branch 't856'. Refs: #856

History

#1 - 06/28/2019 01:44 PM - Elena Grandi

- Blocks Segnalazione #858: file di configurazione che associa i permessi ad utenti/gruppi added

#2 - 06/28/2019 01:45 PM - Elena Grandi

- Blocks Segnalazione #860: inserire nome utente e permessi attivi all'interno dell'HTML nel template di base added

#3 - 06/28/2019 01:46 PM - Elena Grandi

- Blocks Segnalazione #861: Mostrare il nome utente corrente nei template html added

#4 - 06/28/2019 01:48 PM - Elena Grandi

- Blocks Segnalazione #863: Aggiungere permission checking a operation e API added

#5 - 06/28/2019 01:48 PM - Elena Grandi

- Target version set to 0.7 Autenticazione e autorizzazione

#6 - 07/04/2019 10:22 AM - Mark Caglienzi

- Blocks Segnalazione #862: form/view di login added

#7 - 07/05/2019 10:44 AM - Elena Grandi

Segnalo da #742 che oltre alle utenze ldap, nelle scuole è anche in uso un utente root con la master password del fuss-server (in /etc/fuss-server/fuss-server.yaml, se presente)

#8 - 07/08/2019 05:37 PM - Enrico Zini

- Status changed from Nuovo to In elaborazione

- Assignee changed from Enrico Zini to Elena Grandi

Nel branch t856 ho committato un comando di esempio, che sarà poi da rimuovere:

```
usage: fuss-manager ldap [-h] uid

positional arguments:
  uid         user id to use to test authentication
```

Che tenta l'autenticazione con un server ldap (la password la chiede con getpass()).

In config.py ci sono 3 parametri necessari da configurare per l'autenticazione:

```
    'ldap_uri': "ldap://server:port",
    'ldap_search_base': 'dc=fuss,dc=example,dc=it',
    'ldap_bind_dn_template': 'uid={uid},dc=fuss,dc=example,dc=it',
```

L'implementazione è in manager/ldap.py, asincrona.

Ho un po' di domande:

- Cosa mettiamo come configurazione di default per lo sviluppo?
- Decidiamo un formato per passare i dati su un utente invece di una Entry ldap3?
- ldap_bind_dn_template ha un senso come parametro di configurazione per mappare come passare da username a bind DN di LDAP?

Per esportare i gruppi servirà anche fare una ulteriore query in _sync_authenticate, immagino: vediamo dopo aver deciso con quale struttura dati restituire i risultati.

#9 - 07/08/2019 06:12 PM - Enrico Zini

Ho aggiunto la lettura dei gruppi dell'utente. Per un login, e per avere informazioni su un utente, ci sono da fare 3 query LDAP: dati utente, nome gruppo primario, elenco nomi e gid gruppi secondari.

Probabilmente è possibile togliere ldap_bind_dn_template e aggiugnere sempre uid=$UID a ldap_user_search_base. Chiedo feedback a Simone.

Ho improvvisato una struttura User in ldap.py, che sarà poi da tirar fuori da ldap.py e mettere in un qualcosa di piú generico in fuss-manager. Accetto suggerimenti sul suo layout.

#10 - 07/08/2019 06:13 PM - Enrico Zini

La configurazione di esempio per LDAP ora è:

```
    'ldap_uri': "ldap://server:port",
    'ldap_bind_dn_template': 'uid={uid},ou=People,dc=fuss,dc=example,dc=it',
    'ldap_user_search_base': 'ou=People,dc=fuss,dc=example,dc=it',
    'ldap_group_search_base': 'ou=Group,dc=fuss,dc=example,dc=it',
```

#11 - 07/08/2019 06:45 PM - Simone Piccardi

Allora ldap_bind_dn_template secondo me è inutile, per ogni utente il DN sarà sempre nella forma uid=username,{{ldap_user_search_base}}.

Inoltre sul fuss-server l'albero ha sempre la seguente struttura (creata dal playbook) sulla base del dominio specificato in fase di lancio (ex. fuss.lan) ed in genere si contatta sempre su localhost, per cui l'elenco sopra lo esprimerei come (in yaml):

```
ldap_uri: "ldap://localhost:port"
ldap_base: dc=fuss,dc=lan
ldap_user_search_base: ou=Users,{{ldap_base}}
ldap_group_search_base: ou=Groups,{{ldap_base}}
```

ci son pure dei rami ou=Computers e ou=Idmap ad uso di Samba, che si possono ignorare, visto che non mi risulta usino più il fuss-server come PDC.

#12 - 07/09/2019 12:09 PM - Enrico Zini

Ho tolto ldap_bind_dn_template e uso invece ldap_user_search_base.

Ho implementato un'astrazione per User, Group, e database utenti e gruppi.

Ho implementato l'autenticazione per LDAP e per db utenti unix locale. Possiamo usare il db utenti unix locale come fallback se ldap non è configurato. Per autenticare utenti però serve essere root.

#13 - 07/09/2019 12:11 PM - Enrico Zini

A questo punto ti passo il ticket per review, e per eventualmente:

- vedere come impostare la configurazione di default
- documentare le chiavi di configurazione LDAP

#14 - 07/09/2019 12:19 PM - Enrico Zini

Per la gestione della master password si può fare un MasterPasswordMixin per i vari user database, che controlla la master password prima di fare super().authenticate(...)

#15 - 07/09/2019 01:08 PM - Enrico Zini

Ho aggiunto anche un user database mock, e l'autodetect del database da usare con lo stesso meccanismo is_viable usato per le machine data source

#16 - 07/09/2019 01:58 PM - Elena Grandi

Fatto il merge in master, mi tengo il ticket per quanto nei commenti 13 e successivi

#17 - 07/10/2019 12:03 PM - Elena Grandi

Aggiunto un nuovo backend per la master password (al posto di un mixin, sembrava più coerente col resto).

È sul branch t853, mi tengo il ticket per il resto.

#18 - 09/23/2019 03:15 PM - Elena Grandi

il branch mergiabile era t856 (typo, sorry)

#19 - 09/24/2019 04:25 PM - Enrico Zini

Fatto merge in master, grazie!

#20 - 09/26/2019 12:46 PM - Elena Grandi

- Status changed from In elaborazione to Commenti

- Assignee changed from Elena Grandi to Enrico Zini

Ho iniziato la configurazione del file di configurazione nel branch t856, per me mergiabile (le modifiche sono in doc/configuration.rst e doc/fuss_manager.yaml.example).

Per come funziona la is_viable di LDAP credo che valga la pena non mettere questi valori nei default di Config, ma impostare un /etc/fuss-manager/fuss-manager.yaml con fuss-server quando lo si installa.

In base a quanto scritto da Simone, I valori da impostare dovrebbero essere quelli usati nei file di documentazione citati sopra.

#21 - 09/26/2019 02:39 PM - Elena Grandi

- Status changed from Commenti to In elaborazione

- Assignee changed from Enrico Zini to Elena Grandi

mi riprendo il ticket, mi sono accorta che al momento non avendo un valore di default la configurazione non verrebbe caricata

#22 - 09/26/2019 02:56 PM - Elena Grandi

- Status changed from In elaborazione to Commenti

- Assignee changed from Elena Grandi to Enrico Zini

Fatto caricare valori (False), ti ripasso il ticket per review (il branch è sempre t856)

#23 - 09/27/2019 04:11 PM - Enrico Zini

- Assignee changed from Enrico Zini to Elena Grandi

Ho fatto merge in master. Il ticket dice inoltre di documentare come vengono esportati i dati utenti dall'interfaccia di db utenti: se implementare funzioni di user management non è una priorità al momento, possiamo rimandare quella parte a quando implementeremo funzioni di user management, e per il momento chiudere questo ticket sbloccando la funzionalità di login.

Te lo passo per conferma: se sei d'accordo chiudi pure.

#24 - 09/30/2019 11:39 AM - Elena Grandi

- Related to Segnalazione #862: form/view di login added

#25 - 09/30/2019 11:40 AM - Elena Grandi

- Blocks deleted (Segnalazione #862: form/view di login)

#26 - 09/30/2019 11:41 AM - Elena Grandi

- Related to Segnalazione #858: file di configurazione che associa i permessi ad utenti/gruppi added

#27 - 09/30/2019 11:41 AM - Elena Grandi

- Blocks deleted (Segnalazione #858: file di configurazione che associa i permessi ad utenti/gruppi)

#28 - 09/30/2019 11:42 AM - Elena Grandi

- Related to Segnalazione #860: inserire nome utente e permessi attivi all'interno dell'HTML nel template di base added

#29 - 09/30/2019 11:42 AM - Elena Grandi

- Blocks deleted (Segnalazione #860: inserire nome utente e permessi attivi all'interno dell'HTML nel template di base)

#30 - 09/30/2019 11:43 AM - Elena Grandi

- Related to Segnalazione #861: Mostrare il nome utente corrente nei template html added

#31 - 09/30/2019 11:43 AM - Elena Grandi

- Blocks deleted (Segnalazione #861: Mostrare il nome utente corrente nei template html)

#32 - 10/09/2019 02:35 PM - Elena Grandi

- Status changed from Commenti to Chiuso

Più che altro la documentazione era su come usare le informazioni di utenza per implementare il resto dei ticket della 0.7, ma direi che nel frattempo ci stiamo lavorando e quindi chiudo.