fuss-server - Segnalazione #189

Aggiungere supporto kerberos

02/09/2017 11:54 AM - Elena Grandi

Status:	Chiuso	**Start date:**	02/09/2017
Priority:	Normale	**Due date:**	
Assignee:	Simone Piccardi	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

cfr Documentazione_varia

History

#1 - 02/10/2017 10:11 AM - Elena Grandi

- Description updated

#2 - 02/15/2017 12:10 PM - Elena Grandi

Inizio a segnare i passaggi di quanto fatto (e sono abbastanza sicura vada fatto) sul client:

- installato nfs-common
- controllato la correttezza del fqdn
- modificato /etc/default/nfs-common per abilitare idmapd e gssd

A questo punto cercando di montare con

```
mount -t nfs4 -o sec=krb5 proxy.{{ domain }}:/home /mnt
```

si ottiene correttamente un access denied.

Proseguo e poi aggiornerò il ticket

#3 - 02/15/2017 02:24 PM - Elena Grandi

Inoltre, sul client installati krb5-user e krb5-config

#4 - 02/15/2017 02:37 PM - Elena Grandi

Sul server, dato il comando kadmin.local e poi:

```
addprinc -randkey nfs/client.fqdn@REALM
ktadd nfs/client.fqdn@REALM
```

A quel punto ho copiato le righe relative a nfs/client.fqdn dal /etc/krb5.keytab del server a quello del client, e montare come sopra funziona anche sul client.

Non mi è ancora chiaro come si possa automatizzare questa parte, che fa eseguita per ciascun client.

#5 - 02/16/2017 11:45 AM - Elena Grandi

Nota, i pacchetti di kerberos sul client sono preseedabili con krb5-config/default-realm: {{ domain | upper }}; non trovo dove venga salvata l'altra domanda di preseed (la cui risposta è il nome del server)

#6 - 02/17/2017 02:56 PM - Elena Grandi

- File add_client_principal added

Come soluzione potenziale ho iniziato a scrivere uno script che potrebbe essere installato da ansible sul server e che:

- prende l'hostname del client come parametro
- genera principal e relativa chiave, salvandola su un file per-client
- mergia le chiavi create nel keytab globale

dal client sarebbe sufficiente lanciare

```
ssh root@proxy.{{ domain }} add_client_principal `hostname`
scp root@proxy.{{ domain }}/$(hostname).keytab /etc/krb5.keytab
```

Per avere le chiavi installate nel posto giusto e poter montare

Se è una soluzione fattibile, basta solidificare un po' lo script e poi lo posso mettere sul fuss-server

#7 - 02/21/2017 11:31 AM - Elena Grandi

Riassumendo la procedura completa in un unico post:

> Controllare l'fqdn
> Installare: nfs-common krb5-user krb5-config
> da preseedarsi
>
> Configurazione dell'autenticazione Kerberos, Realm preferito ---> enter
> Configurazione dell'autenticazione Kerberos, Server Kerberos del proprio realm ----> proxy.{{ domain }}
> Configurazione dell'autenticazione Kerberos, Server amministrativo per il realm Kerberos ---> proxy.{{ domain }}
>
> Dovrebbero corrispondere, rispettivamente, a

```
> krb5-config/default_realm
> krb5-config/kerberos_servers
> krb5-config/admin_server
>
```

modificare /etc/default/nfs-common per abilitare idmapd e gssd
service nfs-common restart

ssh root@proxy.{{ domain }} add_client_principal {{ client_hostname }}
scp root@proxy.{{ domain }}:{{ client_hostname }}.keytab /etc/krb5.keytab

mount -t nfs4 -o sec=krb5 proxy.{{ domain }}:/home /mnt

#8 - 02/21/2017 11:33 AM - Elena Grandi

- Status changed from In elaborazione to Commenti

- Assignee changed from Elena Grandi to Christopher R. Gabriel

Dimenticato di riassegnare

la parte server è tutta committata dentro a fuss-server, per la parte client c'è la procedura del commento sopra

#9 - 03/01/2017 12:59 PM - Elena Grandi

E adesso anche la parte client è stata committata in fuss-client

#10 - 03/06/2017 10:30 AM - Christopher R. Gabriel

- Status changed from Commenti to In elaborazione

- Assignee changed from Christopher R. Gabriel to Elena Grandi

#11 - 03/07/2017 07:36 PM - Simone Piccardi

Altre cose da fare per mettere i dati di kerberos su LDAP:

Modificare:

```
access to attrs=userPassword
        by dn="cn=admin,dc=thisschool,dc=lan" write
        by anonymous auth
        by self write
        by * none
```

in

```
access to attrs=userPassword,userPKCS12
        by dn="cn=admin,dc=thisschool,dc=lan" write
        by anonymous auth
        by self write
        by * none
```

ed aggiungere anche:

```
index   krbPrincipalName                               eq
```

la configurazione dovrebbe essere (in /etc/krb5kdc/kdc.conf):

```
[kdcdefaults]
    kdc_ports = 750,88

[realms]
    THISSCHOOL.LAN = {
#        database_name = /var/lib/krb5kdc/principal
#        admin_keytab = FILE:/etc/krb5kdc/kadm5.keytab
#        acl_file = /etc/krb5kdc/kadm5.acl
#        key_stash_file = /etc/krb5kdc/stash
#        kdc_ports = 750,88
#        max_life = 10h 0m 0s
#        max_renewable_life = 7d 0h 0m 0s
#        master_key_type = des3-hmac-sha1
#        supported_enctypes = aes256-cts:normal arcfour-hmac:normal des3-hmac-sha1:normal des-cbc-crc:normal d
es:normal des:v4 des:norealm des:onlyrealm des:afs3
#        default_principal_flags = +preauth
         database_module = LDAP
    }

[dbmodules]
    LDAP = {
        db_library = kldap
        ldap_kerberos_container_dn = cn=krbContainer,dc=thisschool,dc=lan
        ldap_kdc_dn = cn=admin,dc=thisschool,dc=lan
        ldap_kadmind_dn = cn=admin,dc=thisschool,dc=lan
        ldap_service_password_file = /etc/krb5kdc/admin.stash
        ldap_servers = ldapi:///
    }
```

eseguire:

```
kdb5_ldap_util -D cn=admin,dc=thisschool,dc=lan create -subtrees ou=users,dc=thisschool,dc=lan -r THISSCHOOL.L
AN -s
Password for "cn=admin,dc=thisschool,dc=lan":
Initializing database for realm 'THISSCHOOL.LAN'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
```

chiede prima la password dell'admin ldap e poi due volte quella del KDC database master key, poi fare lo stash della password:

```
root@server:/etc/krb5kdc# kdb5_ldap_util -D cn=admin,dc=thisschool,dc=lan stashsrvpw cn=admin,dc=thisschool,dc
=lan
Password for "cn=admin,dc=thisschool,dc=lan":
Password for "cn=admin,dc=thisschool,dc=lan":
Re-enter password for "cn=admin,dc=thisschool,dc=lan":
```

Così kadmin.local sul server usa LDAP per salvare i dati, ma ci van comunque rimessi i principal che servono (compresi quelli per gli utenti).

#12 - 03/08/2017 07:54 PM - Simone Piccardi

Fatti ulteriori controlli, non serve mettere le configurazioni di kerberos su LDAP.

Quello che serve è invece avere un principal per ogni utente presente su LDAP, corrispondente al nome utente.

Se cioè user è un utente su LDAP/Samba, deve esistere il corrispondente principal user@DOMINIO.LAN.

Questo deve essere creato sul server con il comando kadmin.local con qualcosa del tipo:

```
kadmin.local << EOF
addprinc user@DOMINIO.LAN
pwd
pwd
EOF
```

La password **deve** essere la stessa dell'utenza su LDAP, questo va fatto per ogni utente in fase di creazione, (da octofuss, o quando lo si crea a mano).

Sul lato client invece occorre installare il pacchetto libpam-krb5 modificare due dei common-* sotto /etc/pam.d.

Il primo è /etc/pam.d/common-auth cui va aggiunto la riga:

```
auth    optional                        pam_krb5.so minimum_uid=1000 try_first_pass
```

sopra:

```
auth    required                        pam_permit.so
```

tolti i commenti /etc/pam.d/common-auth deve essere qualcosa del tipo:

```
auth    [success=2 default=ignore]    pam_unix.so nullok_secure
auth    [success=1 default=ignore]    pam_ldap.so minimum_uid=1000 use_first_pass
auth    requisite            pam_deny.so
auth    optional                        pam_krb5.so minimum_uid=1000 try_first_pass
auth    required            pam_permit.so
```

Il secondo è /etc/pam.d/common-password cui va aggiunta la riga:

```
password        optional                        pam_krb5.so minimum_uid=1000 try_first_pass use_authtok
```

sopra:

```
password        optional                        pam_krb5.so minimum_uid=1000 try_first_pass use_authtok
```

e tolti i commenti deve risultare qualcosa del tipo:

```
password        requisite                       pam_cracklib.so retry=3 minlen=8 difok=3 minclass=3
password    [success=2 default=ignore]    pam_unix.so obscure use_authtok try_first_pass sha512
password    [success=1 default=ignore]    pam_ldap.so minimum_uid=1000 try_first_pass use_authtok
password    requisite            pam_deny.so
password        optional                        pam_krb5.so minimum_uid=1000 try_first_pass use_authtok
password    required            pam_permit.so
password    optional    pam_gnome_keyring.so
```

Va verificato che nell'installazione di libpam-krb5 non venga attivata l'autenticazione ordinaria via kerberos, che non è necessaria.

In questo modo sarà possibile modificare la password dell'utente (sia su LDAP che su kerberos) via PAM (è stato verificato solo passwd, controllare con gli altri programmi).

Per cambiare la password del principal dell'utente sul server (ad uso dei programmi di gestione dell'utente sul server) si può usare il comando:

```
kadmin.local << EOF
cpw user@DOMINIO.LAN
newpw
newpw
EOF
```

#13 - 03/10/2017 02:49 PM - Christopher R. Gabriel

- Status changed from In elaborazione to Commenti

- Assignee changed from Elena Grandi to Simone Piccardi

Ho aggiunto il necessario a octofussd per la creazione utenti/cambio password, assumendo il realm di default.

Visto che tutti gli altri test sono a posto, direi che si puo' chiudere?

#14 - 03/14/2017 02:22 PM - Simone Piccardi

- Status changed from Commenti to Chiuso

Si, si può chiudere.

Files

add_client_principal	339 Bytes	02/17/2017	Elena Grandi