kadmin

Interface CLI pour l'administration de Kerberos

kadmin et kadmin.local sont des interfaces en ligne de commande pour le système d'administration de Kerberos. Ils fonctionnent de manière similaire à l'exception que kadmin.local communique directement avec le fichier de base de données.

Le client distant **kadmin** utilise Kerberos pour s'authentifier auprès de kadmind en utilisant le principal de service **kadmin/ADMINHOST**, où **ADMINHOST** est le fqdn du serveur d'administration, ou **kadmin/admin**. Si le cache d'accréditifs contient un ticket pour un de ces principaux, et que l'option **-c** est spécifié, ce ticket est utilisé pour s'authentifier à kadmind. Sinon les options **-p** et **-k** sont utilisés pour spécifier le nom du principal client utilisé pour s'authentifier. Une fois que kadmin a déterminé le nom du principal, il demande un ticket de service au KDC, et l'utilise pour s'authentifier à kadmind.

OPTIONS

-r realms Utilise de domaine spécifié par défaut

-p principal Utilise le principal spécifié pour s'authentifier. Sinon, kadmin va ajouter /admin au nom de principal primaire du ccache par défaut, la valeur de la variable d'environnement USER, ou le username obtenu par getpwuid, dans cet ordre.

-k Utilise un keytab pour déchiffrer la réponse du KDC au lieu de demander un mot de passe. Dans ce cas, le principal par défaut sera host/hostname. S'il n'y a par de keytab spécifié avec l'option -t, le keytab par défaut sera utilisé.

-t keytab Utilise keytab pour déchiffrer la réponse du KDC. Peut seulement être utilisé avec l'option -k

-n Demande un traitement anonyme. 2 types de principaux anonyme sont supportés. Pour l'anonymité complète, configurer PKINIT et utiliser l'option **-n** avec un principal sous la forme **@REALM**. Si permis par le KDC, un ticket anonyme sera retourné. Une seconde forme est supportée, et cache l'identité du client mais pas le domaine du client. Pour ce mode, utiliser kinit -n avec un principal normal. Si supporté par le KDC, le principal, mais pas le domaine, sera remplacé par le principal anonymous.

-c credentials_cache Utile de cache d'accréditifs spécifié. Le cache devrait contenir un ticket de service pour **kadmin/ADMINHOST** ou **kadmin/admin**. Si non spéifié, kadmin demande un nouveau ticket au KDC et le stocke dans son propre cache temporaire.

-w password Utilise le mot de passe au lieu de le demander

-q query Effectue le requête spécifiée et quitte.

-d dbname Spécifie le nom de la base KDC. Ne s'applique par au module de base LDAP

-s admin_server[:port] Spécifie le serveur d'administration à contacter

-m Avec kadmin.local, demande le mot de passe maître de la base au lieu de chercher un fichier stash

-e "enc :salt..." Définis la liste keysalt à utiliser pour toute nouvelle clé créée.

-O Force l'utilisation de l'ancienne authentification AUTH_GSSAPI

-N Empêche l'utilisation de l'ancienne authentification AUTH_GSSAPI

-x db_args Spécifie les arguments spécifique à la base. les options supportée pour le module de base LDAP sont :

- **-x host=hostname** Spécifie le serveur LDAP à contacter
- **-x binddn=bind_dn** DN de l'objet à utiliser par le serveur d'administration pour le bind ldap.
- **-x bindpwd=bind_password** Mot de passe pour le binddn
- **-x debug=level** Niveau de verbosité pour le client OpenLDAP.

Commandes

En utilisant le client distant, les commandes disponible peuvent être restreins en accord avec les privilèges dans kadm5.acl.

add_principal

Crée le principal spécifié, en demandant 2 fois le mot de passe. Si aucune stratégie de mot de passe n'est spécifiée, la stratégie nommée **default** est assignée au principal si elle existe. Cependant, créer une stratégie **default** ne va pas assigner automatiquement ce stratégie aux principaux déjà existant. Cette stratégie peut être supprimée avec l'option -clearpolicy

-expire expdate (chaîne getdate_time) Date d'expiration du principal

-pwexpire pwexpdate (chaîne getdate_time) Date d'expiration du mot de passe

-maxlife maxlife (chaîne getdate_time) Durée de vie de ticket max pour le principal

-maxrenewlife maxrenewlife (chaîne getdate_time) Durée de vie de renouvellement max des tickets

-kvno kvno Numéro de version de clé initial

-policy policy Stratégie de mot de passe utilisé par ce principal.

-clearpolicy Empêche l'assignation automatique d'une stratégie si non spécifiée par -policy

{-|+}allow_postdated Droit d'obtenir des tickets post-datés

{-|+}allow_forwardable Droit d'obtenir des tickets forwardable

{-|+}allow_renewable Droit d'obtenir des tickets renouvelable

{-|+}allow_proxiable Droit d'obtenir des tickets proxiable

{-|+}allow_dup_skey Droit d'effectuer une authentification user-to-user

{-|+}requires_preauth force le principal à ce pré-authentifier

{-|+}requires_hwauth Utiisation d'un hardware pour la pré-authentification

{-|+}ok_as_delegate flag okay as delegate dans les tickets fournis avec ce principal en tant que service.

{-|+}allow_svr Droit de délivrer des tickets de service pour ce principal

{-|+}allow_tgs_req Droit d'obtenir un TGS pour un ticket de service pour ce principal

{-|+}allow_tix Droit d'obtenir un ticket pour ce principal

{-|+}needchange Force le changement de mot de passe à la prochaine authentification

{-|+}password_changing_service Marque ce principal comme principal de service de changement de mot de passe

{-|+}ok_to_auth_as_delegate Droit d'obtenir des tickets forwardable à soi-même depuis des utilisateurs arbitraires

{-|+}no_auth_data_required Droit d'ajouter des données PAC ou AD-SIGNEDPATH

-randkey Définis la clé du principal à une valeur aléatoire

-nokey Crée un principal sans clé

-pw password Définis de mot de passe pour ce principal

-e enc :salt,... Utilise la liste de keysalt pour les clés de ce principal.

-x db_princ_args Options spécifique à la base :

- **-x dn=dn** Spécifie l'objet LDAP qui va contenir le principal Kerberos à créer
- **-x linkdn=dn** Spécifie l'objet LDAP pour lequel le nouveau principal Kerberos va pointer
- **-x containerdn=container_dn** Spécifie le conteneur sous lequel le principal Kerberos est créé
- **-x tktpolicy=policy** Associe une stratégie de ticket au principal Kerberos

Note

Les options **containerdn** et **linkdn** ne peuvent pas être spécifiés avec l'option **dn**. Si ces options ne sont pas spécifiées, les principaux sont créés sous le conteneur principal configurés dans le domaine. Ces options devraient pointer dans les sous-arborescences ou le conteneur principal configurés dans le domaine.

Exemple

```
kadmin: addprinc jennifer
WARNING: no policy specified for "jennifer@ATHENA.MIT.EDU";
defaulting to no policy.
Enter password for principal jennifer@ATHENA.MIT.EDU:
Re-enter password for principal jennifer@ATHENA.MIT.EDU:
Principal "jennifer@ATHENA.MIT.EDU" created.
kadmin:
```

modify_principal

Modifie le principal spécifié, en changeant les champs spécifiés. Les options de **add_principal** s'appliquent également à cette commande, excepté **-randkey**, **-pw** et **-e**. Cette commande nécessite les privilège modify. Alias : **modprinc**

-unlock Débloque un principal.

rename_principal

Renomme l'ancien principal avec le nouveau principal. Demande configuration sauf si **-force** est donné. Nécessite les privilèges add et delete. Alias : **renprinc**

delete_principal

Supprime le principal spécifié de la base. emande configuration sauf si **-force** est donné. Nécessite les privilèges delete. Alias : **delprinc**

change_password

Change le mot de passe du principal. Demande un nouveau mot de passe si **-randkey** ou **-pw** ne sont pas spécifiés. Nécessite les privilège changepw, ou que le principal qui lance ce programme est le même que le principal à changer. Aliar : **cpw**

-randkey Définis la clé du principal à une valeur aléatoire

-pw password Définis de mot de passe pour ce principal

-e enc :salt,... Utilise la liste de keysalt pour les clés de ce principal.

-keepold Conserve les clés existantes dans la base.

Exemple

```
kadmin: cpw systest
Enter password for principal systest@BLEEP.COM:
Re-enter password for principal systest@BLEEP.COM:
Password for systest@BLEEP.COM changed.
kadmin:
```

purgekeys

Purge les anciennes clé du principal. Si **-keepkvno** est spécifié, alors seul les clés avec des kvno inférieur sont purgés. Si **-all** est spécifié, purge toutes les clés. Nécessite le privilège modify

get_principal

Récupère les attributs du principal. L'option **-terce** affiche les champs en tant que chaîne séparés par des tabulations. Nécessite le privilège inquire, ou que le principal utilisant le programme soit le même que le principal cible. Alias : **getprinc**

Exemple

```
kadmin: getprinc tlyu/admin
Principal: tlyu/admin@BLEEP.COM
Expiration date: [never]
Last password change: Mon Aug 12 14:16:47 EDT 1996
Password expiration date: [none]
Maximum ticket life: 0 days 10:00:00
Maximum renewable life: 7 days 00:00:00
Last modified: Mon Aug 12 14:16:47 EDT 1996 (bjaspan/admin@BLEEP.COM)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 2
Key: vno 1, DES cbc mode with CRC-32, no salt
Key: vno 1, DES cbc mode with CRC-32, Version 4
Attributes:
Policy: [none]

kadmin: getprinc -terse systest
systest@BLEEP.COM 3 86400 604800 1
785926535 753241234 785900000
tlyu/admin@BLEEP.COM 786100034 0 0
kadmin:
```

list_principal

Récupère des noms de principal. L'expression est une expression glob qui peut contenir les caractères *****, **?** et **[]**. Tous les noms de principaux qui matche l'expression sont affichés. Sans expression, liste tous les principauix. Si l'expression ne contient pas un caractère **@**, ce caractère est ajouté avec le domaine local à l'expression. Nécessite le privilège list. Alias : **listprincs, get_principals, get_princs**

Exemple

```
kadmin: listprincs test*
test3@SECURE-TEST.OV.COM
test2@SECURE-TEST.OV.COM
test1@SECURE-TEST.OV.COM
testuser@SECURE-TEST.OV.COM
kadmin:
```

get_strings

Affiche les attributs chaîne dans le principal. Nécessite le privilège inquire. Alias : **getstr**

set_strings

Définis un attribut chaîne dans le principal. Les attributs chaîne sont utilisés pour fournir une configuration par principal au KDC et certaine modules du KDC. Nécessite le privilège modify. Alias **setstr**. Les attributs suivants sont reconnus par le KDC :

session_enctypes Spécifie les types de chiffrement supportés pour les clés session quand le principal est authentifié en tant que serveur.

del_strings

Supprime un attribut chaîne du principal. Nécessite le privilège delete. Alias : **delstr**

add_policy

Ajoute une stratégie de mot de passe à la base. Nécessite le privilège add. Alias : **addpol**

-maxlife time (chaîne getdate_time) Définis la durée de vie max d'un mot de passe

-minlife time (chaîne getdate_time) Définis la durée de vie min d'un mot de passe

-minlength length Définis la longueur maximum d'un mot de passe

-minclasses number Définis le nombre minimum de classes de caractères requis dans un mot de passe. Les 5 classes sont : minuscule, majuscule, nombres, ponctuation et espaces blancs.

-history number Définis le nombre de clé à conserver pour un principal. Non supporté avec le module LDAP

-maxfailure maxnumber Définis le nombre d'échec d'authentification avant que le principal soit bloqué. 0 le désactive.

-failurecountinterval failuretime (chaîne getdate_time) Définis le temps permis entre les échecs d'authentification.

-lockoutduration lockouttime (chaîne getdate_time) Définis la durée pour lequel le principal est bloqué. 0 signifie que le compte est bloqué jusqu'à ce qu'un administrateur le débloque.

-allowedkeysalts Spécifie les tuples key/salt supportés pour les clés à long terme en définissant ou en changeant un mot de passe de principal. Les tuples doivent être séparés par une virgule. Pour enlever le tuple de la stratégie, utiliser "-"

Exemple

```
kadmin: add_policy -maxlife "2 days" -minlength 5 guests
kadmin:
```

modify_policy

Modifie la stratégié de mot de passe spécifiée. Les options sont les même que pour add_policy. Nécessite le privilège modify. Alias : **modpol**

delete_policy

Supprime la stratégie de mot de passe spécifiée. Demande confirmation. Échoue si la stratégie est utilisée par un principal. Nécessite le privilège delete. Alias : **delpol**

Exemple

```
kadmin: del_policy guests
Are you sure you want to delete the policy "guests"?
(yes/no): yes
kadmin:
```

get_policy

Affiche les valeurs de la stratégie spécifiées. -terse affiche les champs séparés par des tabulations. Nécessite le privilège inquire. Alias : **getpol**

Exemple

```
kadmin: get_policy admin
Policy: admin
Maximum password life: 180 days 00:00:00
Minimum password life: 00:00:00
Minimum password length: 6
Minimum number of password character classes: 2
Number of old keys kept: 5
Reference count: 17

kadmin: get_policy -terse admin
admin 15552000 0 6 2 5 17
kadmin:
```

list_policies

Liste des stratégie basée sur l'expression. Nécessite le privilège list. Alias : **listpols, get_policies, getpols**

Exemple

```
kadmin: listpols
test-pol
dict-only
once-a-min
test-pol-nopw

kadmin: listpols t*
test-pol
test-pol-nopw
kadmin:
```

ktadd

Ajoute un principal, ou tous les principaux matchant l'expression de l'option glob, à chaque fichier keytab. Chaque clé de principal est

randomisé dans le processus. Nécessite les privilèges inquire et changepw. pour utiliser -glob, nécessite le privilège list.

-k [eytab] keytab Utilise le fichier keytab spécifié

-e enc :salt,... Utilise la liste keysalt spécifiée

-q mode silencieux

-norandkey Ne randomise pas les clé. Ne peut pas être utilisé avec -e.

Exemple

```
kadmin: ktadd -k /tmp/foo-new-keytab host/foo.mit.edu
Entry for principal host/foo.mit.edu@ATHENA.MIT.EDU with kvno 3,
 encryption type aes256-cts-hmac-sha1-96 added to keytab
 FILE:/tmp/foo-new-keytab
kadmin:
```

ktremove

Supprime des entrées pour le principal spécifié du keytab. Ne nécessite aucune permission. Si all est spéficié, toutes les entrées pour le principal sont supprimés ; si old est spécifié, toutes les entrée sauf le kvno le plus récent sont supprimés. Si kvno est spécifié, supprime les entrées avec ce kvno.

-k [eytab] keytab Utilise le fichier keytab spécifié

-q mode silencieux

Exemple

```
kadmin: ktremove kadmin/admin all
Entry for principal kadmin/admin with kvno 3 removed from keytab
 FILE:/etc/krb5.keytab
kadmin:
```

lock

Bloque la base. Ne fonctionne qu'avec le module DB2

unlock

Réactive la base après un lock

list_requests

Liste les demandes kadmin disponible. Alias **lr, ?**

quit

Quitte le programme. Alias **exit,q**