
kdb5_ldap_util

Utilitaire de maintenance de la base LDAP de Kerberos

OPTIONS

- D user_dn** DN de l'utilisateur pour les opérations sur le serveur
- w passwd** Mot de passe de l'utilisateur
- H ldapuri** URI du serveur LDAP à contacter.

Commandes

create [-subtrees subtree_dn_list] [-sscope search_scope] [-containerref container_reference_dn] [-k mkeytype] [-kv mkeyVNO] [ticket_flags] Crée un domaine dans l'annuaire.

- subtrees subtree_dn_list** Spécifie la liste des subtrees contenant les principaux d'un domaine, séparés par " :"
- sscope search_scope** Spécifie le scope de recherche pour les principaux sous le subtree (1 - onelevel, 2 - subtree)
- containerref container_reference_dn** DN du conteneur dans lequel les principaux d'un domaine seront créés.
- k mkeytype** Spécifie le type de clé de la clé maître dans la base.
- kv mkeyVNO** Spécifie le numéro de version de la clé maître dans la base ; défaut : 1.
- m** Spécifie que le mot de passe maître de la base devrait être lu depuis le clavier au lieu d'un fichier sur disque.
- P password** Spécifie le mot de passe maître.
- r realm** Spécifie le domaine Kerberos
- sf stashfilename** Spécifie le fichier stash pour le mot de passe maître.
- s** Spécifie que le fichier stash est à créer
- maxtktlife max_ticket_life** (chaîne getdate_time) Spécifie la durée de vie max d'un ticket pour les principaux dans ce domaine
- maxrenewlife max_renewable_ticket_life** (chaîne getdate_time) Spécifie la durée de vie max renouvelable pour les principaux dans ce domaine
- ticket_flags** Spécifie les flags global de ticket pour le domaine. voir kadmin add_principal.

Exemples

```
kdb5_ldap_util -D cn=admin,o=org -H ldaps://ldap-server1.mit.edu
create -subtrees o=org -sscope SUB -r ATHENA.MIT.EDU
Password for "cn=admin,o=org":
Initializing database for realm 'ATHENA.MIT.EDU'
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:
```

modify [-subtrees subtree_dn_list] [-sscope search_scope] [-containerref container_reference_dn] [-r realm] [-maxtktlife max_ticket_life] Modifie les attributs d'un domaine.

- subtrees subtree_dn_list** Spécifie la liste des subtrees contenant les principaux d'un domaine, séparés par " :"

-scope search_scope Spécifie le scope de recherche pour les principaux sous le subtree (1 - onelevel, 2 - subtree)
-containerref container_reference_dn DN du conteneur dans lequel les principaux d'un domaine seront créés.
-r realm Spécifie le domaine Kerberos
-maxtktlife max_ticket_life (chaîne getdate_time) Spécifie la durée de vie max d'un ticket pour les principaux dans ce domaine
-maxrenewlife max_renewable_ticket_life (chaîne getdate_time) Spécifie la durée de vie max renouvelable pour les principaux dans ce domaine
ticket_flags Spécifie les flags global de ticket pour le domaine. voir kadmin add_principal.

Exemples

```
shell% kdb5_ldap_util -D cn=admin,o=org -H
  ldaps://ldap-server1.mit.edu modify +requires_preauth -r
  ATHENA.MIT.EDU
Password for "cn=admin,o=org":
shell%
```

view [-r realm] Affiche les attribut d'un domaine. **-r** spécifie le domaine Kerberos de la base

Exemples

```
kdb5_ldap_util -D cn=admin,o=org -H ldaps://ldap-server1.mit.edu
  view -r ATHENA.MIT.EDU
Password for "cn=admin,o=org":
Realm Name: ATHENA.MIT.EDU
Subtree: ou=users,o=org
Subtree: ou=servers,o=org
SearchScope: ONE
Maximum ticket life: 0 days 01:00:00
Maximum renewable life: 0 days 10:00:00
Ticket flags: DISALLOW_FORWARDABLE REQUIRES_PWCHANGE
```

destroy [-f] [-r realm] Supprime un domaine existant. **-f** ne demande pas confirmation, **-r** spécifie de domaine de la base.

Exemples

```
shell% kdb5_ldap_util -D cn=admin,o=org -H
  ldaps://ldap-server1.mit.edu destroy -r ATHENA.MIT.EDU
Password for "cn=admin,o=org":
Deleting KDC database of 'ATHENA.MIT.EDU', are you sure?
(type 'yes' to confirm)? yes
OK, deleting database of 'ATHENA.MIT.EDU'...
shell%
```

list Liste le nom des domaines

Exemples

```
shell% kdb5_ldap_util -D cn=admin,o=org -H
  ldaps://ldap-server1.mit.edu list
Password for "cn=admin,o=org":
ATHENA.MIT.EDU
OPENLDAP.MIT.EDU
MEDIA-LAB.MIT.EDU
shell%
```

stashsrvpw [-f filename] servicedn Permet à un administrateur de stocker un mot de passe pour un objet service dans un fichier pour que le KDC et le serveur d'administration puissent l'utiliser pour s'authentifier auprès du serveur LDAP. **-f filename** est le chemin complet du fichier, **servicedn** est le DN de l'objet service.

Exemples

```
kdb5_ldap_util stashsrwpw -f /home/andrew/conf_keyfile
cn=service-kdc,o=org
Password for "cn=service-kdc,o=org":
Re-enter password for "cn=service-kdc,o=org":
```

create_policy [-r realm] [-maxtktlife max_ticket_life] [-maxrenewlife max_renewable_ticket_life] [ticket_flags] policy_name

Crée une stratégie de ticket dans l'annuaire.

-r realm Spécifie le domaine Kerberos

-maxtktlife max_ticket_life (chaîne getdate_time) Spécifie la durée de vie max d'un ticket pour les principaux dans ce domaine

-maxrenewlife max_renewable_ticket_life (chaîne getdate_time) Spécifie la durée de vie max renouvelable pour les principaux dans ce domaine

ticket_flags Spécifie les flags global de ticket pour le domaine. voir kadmin add_principal.

policy_name Nom de la stratégie de ticket

Exemples

```
kdb5_ldap_util -D cn=admin,o=org -H ldaps://ldap-server1.mit.edu
create_policy -r ATHENA.MIT.EDU -maxtktlife "1 day"
-maxrenewlife "1 week" -allow_postdated +needchange
-allow_forwardable tktpolicy
Password for "cn=admin,o=org":
```

modify_policy [-r realm] [-maxtktlife max_ticket_life] [-maxrenewlife max_renewable_ticket_life] [ticket_flags] policy_name

Modifie les attributs d'une stratégie de ticket. Les options sont les même que pour **create_policy**

Exemples

```
kdb5_ldap_util -D cn=admin,o=org -H
ldaps://ldap-server1.mit.edu modify_policy -r ATHENA.MIT.EDU
-maxtktlife "60 minutes" -maxrenewlife "10 hours"
+allow_postdated -requires_preauth tktpolicy
Password for "cn=admin,o=org":
```

view_policy [-r realm] policy_name Affiche les attributs d'une stratégie de ticket. **policy_name** est le nom de la stratégie

Exemples

```
kdb5_ldap_util -D cn=admin,o=org -H ldaps://ldap-server1.mit.edu
view_policy -r ATHENA.MIT.EDU tktpolicy
Password for "cn=admin,o=org":
Ticket policy: tktpolicy
Maximum ticket life: 0 days 01:00:00
Maximum renewable life: 0 days 10:00:00
Ticket flags: DISALLOW_FORWARDABLE REQUIRES_PWCHANGE
```

destroy_policy [-r realm] [-force] policy_name Détruit une stratégie de ticket. **-force** ne demande pas confirmation.

Exemples

```
kdb5_ldap_util -D cn=admin,o=org -H ldaps://ldap-server1.mit.edu
destroy_policy -r ATHENA.MIT.EDU tktpolicy
Password for "cn=admin,o=org":
This will delete the policy object 'tktpolicy', are you sure?
(type 'yes' to confirm)? yes
addentry articles autoadd autofind autoprod createalpha createbeta createdb createprod findentry fullpowa
generator.php genhtml genman genmd gentex html insert man md pdf regen setfor setfor2 sql temp temp-new-pc
tex threads ToDo policy object 'tktpolicy' deleted.
```

list_policy [-r realm] Liste les stratégie de ticket dans le domaine.

Exemples

```
kdb5_ldap_util -D cn=admin,o=org -H ldaps://ldap-server1.mit.edu
  list_policy -r ATHENA.MIT.EDU
Password for "cn=admin,o=org":
tktpolicy
tmppolicy
userpolicy
```