kadm5.acl

Fichier acl pour kadmind

Kadmind utilise un fichier d'acl pour gérer les droits d'accès à la base Kerberos. Pour les opérations qui affectent les principaux, le fichier d'acl contrôle également quels principaux peuvent opérer sur quels autres principaux. L'emplacement par défaut est **LOCALSTATEDIR/krb5kdc/kadm5.acl** ou la variable **acl_file** dans **kdc.conf**.

Syntaxe

Les lignes vides ou commençant par # sont ignorées. les lignes contenant une entrée acl a le format suivant :

principal permissions [target_principal [restrictions]]

Note : l'ordre des lignes est importante. La première entrée correspondante va contrôler l'accès pour un acteur principal sur un principal cible.

principal (Nom de principal complet ou partiel) Spécifie le principal dont les permissions sont définies

permissions Spécifie quels opérations peuvent être effectuées ou non par le principal. C'est une chaîne d'un ou plusieurs caractères ou leur opposé majuscule qui désactive cette permission :

- **a** ajout de principaux ou stratégies
- **c** changer les mots de passe pour les principaux
- **d** suppression de principaux ou stratégies
- **i** demandes de renseignements concernant les principaux et stratégies
- **l** lister les principaux ou stratégies
- **m** modification de principaux ou stratégies
- **p** propagation de la base de principaux
- **s** paramétrage explicite des clés pour un principal
- **x** raccourci pour admcil. Tous les privilèges

target_principal (Optionnel. Nom de principal complet ou partiel) Spécifie le principal sur lequel les permissions s'appliquent. chaque composant du nom peut être wildcarded (*). Peut également inclure des référence au principal, dans lequel ***number** matche le wilcard correspondant dans principal

restrictions (optionnel) Une chaîne de flags. Les restrictions permises sont :

- **{+|-}flagname** flag est forcé à la valeur indiquée. Les flags permissifs sont les même que les flags + et - pour les commandes **add_principal** et **modify_principal** de kadmin.
- **-clearpolicy** La stratégie est forcée à être vide
- **-policy pol** La stratégie est forcée à pol
- **-{expire, pwexpire, maxlife, maxrenewlife} time** (chaîne de temps getdate) la valeur associée est forcée à MIN(time, valeur demandée)

Ces flags agissent comme restriction sur toute opération d'ajout ou de modification qui sont permis dans la ligne d'ACL.

Attention : si le fichier d'acl est modifié, kadmind doit être redémarré pour prendre en compte les modifications.

Exemple

Exemple de fichies kadm5.acl :

```
*/admin@ATHENA.MIT.EDU *
joeadmin@ATHENA.MIT.EDU ADMCIL
joeadmin/*@ATHENA.MIT.EDU il */root@ATHENA.MIT.EDU
/root@ATHENA.MIT.EDU cil *1@ATHENA.MIT.EDU
/*@ATHENA.MIT.EDU i
/admin@EXAMPLE.COM x * -maxlife 9h -postdateable
```

ligne 1 Tout principal dans le domaine ATHENA.MIT.EDU avec une instance **admin** a tous les privilèges administratifs

ligne 2 et 3 L'utilisateur **joeadmin** a toutes les permissions avec son instance **admin**, **joeadmin/admin@ATHENA.MIT.EDU** (matche de la ligne 1), il n'a aucune permission avec son instance **joeadmin@ATHENA.MIT.EDU** (matche de la ligne 2). Ses instances **root** et autre non admin ont les permissions de lister et demander avec tout principal qui a l'instance **root** (macthe de la ligne 3).

ligne 4 Tout principal **root** dans ATHENA.MIT.EDU peut demander, lister ou changer les mots de passe de leur instance nul, mais pas les autres instance null.

ligne 5 Tout principal dans ATHENA.MIT.EDU (sauf **joeadmin@ATHENA.MIT.EDU** comme mentionné plus haut) a les privilèges demander.

ligne 6 Finallement, tout principal avec une instance **admin** dans EXAMPLE.COM a toutes les permissions, mais tout principal qu'ils créent ou modifient ne seront par capable d'obtenir de tickets post-datés ou avec une durée de vie supérieur à 9 heures.