kdc.conf

Fichier de configuration des services Kerberos

Ce fichier est un supplément à krb5.conf et est utilisé uniquement dans les KDC. Normalement, kdc.conf se trouve dans le répertoire d'état du KDC, **LOCALSTATEDIR/krb5kdc** mais peut être changé dans la variable **KRB5_KDC_PROFILE**. Noter qu'il faut redémarrer les services kdc pour prendre en comptes les changements.

Structure

Les noms de sections sont entre crochets, chaque section peut contenir 0 ou plusieurs relations, sous la forme :

foo = bar

Sections

Le fichier kdc.conf peut contenir les sections suivantes :

[kdcdefaults] Valeurs par défaut pour le fonctionnement du KDC

[realms] Configuration et paramètres de base de données spécifique au domaine

[dbdefaults] Paramètres de base de données par défaut

[dbmodules] Paramètres par base de données

[logging] Contrôle les logs des services Kerberos

[kdcdefaults]

À une exception près, les relations dans cette section spécifient les valeur par défaut pour les variable du domaine à utiliser si la sous-section [realms] ne contient par de relation pour le tag.

host_based_services

kdc_ports

kdc_tcp_ports

no_host_referral

restrict_anonymous_to_tgt

kdc_max_dgram_reply_size Spécifie la taille de packet maximum que peut être envoyé en UDP. Défaut : 4096

[realms]

Chaque tag dans cette section est le nom d'un domaine Kerberos. La valeur du tag est une sous-section où les relations définissent les paramètres du KDC pour ce domaine. L'exemple suivant montre comment définir un paramètre pour le domaine ATHENA.MIT.EDU :

```
[realms]
 ATHENA.MIT.EDU = {
  max_renewable_life = 7d 0h 0m 0s
 }
```

acl_file (chaîne). Emplacement du fichier d'acl que kadmind utilise pour déterminer quels principaux ont un accès privilégié à la base. Défaut : **LOCALSTATEDIR/krb5kdc.acl**

database_module (chaîne). Indique le nom de la section de configuration sous [dbmodules] pour les paramètres spécifiques à la base utilisé par la librairie. Défaut : le nom du domaine.

database_name (chaîne, déprécié) Spécifie l'emplacement de la base Kerberos pour ce domaine, si DB2 est utilisé et que la section de configuration [dbmodules] ne spécifie par un nom de base. Défaut : **LOCASTATEDIR/krb5kdc/principal**

default_principal_expiration (chaîne, temps absolu). Spécifie le temps d'expiration par défaut des principaux créés dans ce domaine. Défaut : 0 qui signifie aucune expiration.

default_principal_flags (Chaîne) Spécifie les attributs par défaut des principaux crées dans ce domaine. Le format est une liste de flags séparés par une ",", avec un "+" avant chaque flag à ajouter, et "-" à enlever. Défaut : les flag suivant sont permis **postdateable, forwardable, tgt-based, renewable, proxiable, dup-skey, allow-tickets, et service**. Les flags possibles sont :

allow-tickets Le KDC va fournir de tickets pour ce principal

dup-skey permet au principal d'obtenir une clé de session pour un autre utilisateur.

forwardable Permet au principal d'obtenir des tickets forwardable

hwauth Le principal doit utiliser un périphérique hardware pour la pré-authentification

no-auth-data-required Empêche les données PAC et AD-SIGNEDPATH d'être ajoutés au ticket de service pour le principal

ok-as-delegate Indique au client que les accréditifs peuvent et devraient être délégués en s'authentifiant auprès du service

ok-to-auth-as-delegate Permet au principal d'utiliser des tickets S4USelf

postdateable Permet au principal d'obtenir des tickets post-datés.

preauth Le principal doit de pré-authentifier auprès du KDC avant de recevoir un ticket. Pour un principal de service, cela signifie que les tickets de service pour ce principal seront uniquement fournis aux clients avec un TGT qui a le bit preauthenticated mis.

proxiable Permet au principal d'obtenir des tickets proxy

pwchange Force le changement de mot de passe pour ce principal

pwservice Marque ce principal comme service de changement de mot de passe. Devrait être utilisé uniquement dans des cas spéciaux, par exemple, si le mot de passe de l'utilisateur a expiré, alors l'utilisateur doit obtient des tickets pour ce principal sans passer par une authentification normal par mot de passe pour pouvoir changer le mot de passe.

renewable Permet au principal d'obtenir des tickets renouvelable.

service Permet au KDC de fournir des tickets de service pour ce principal

tgt-based Permet au principal d'obtenir des tickets basés sur un TGT au lieu de répéter le process d'authentification utilisé pour obtenir ce TGT.

dict_file (chaîne) Emplacement du fichier dictionnaire contenant les chaînes non permises pour un mot de passe.

host_based_services (liste séparée par des espaces ou des virgules) Liste des services qui vont obtenir un traitement des référants basés sur l'hôte même si le principal du serveur n'est pas marqué comme basé sur l'hôte par le client.

iprop_enable (bool) Spécifie si la propagation incrémentale de la base est permise. Défaut : false.

iprop_master_ulogsize (entier) Spécifie le nombre max d'entrées de log à retenir pour la propagation incrémentale. max : 2500, défaut : 1000

iprop_slave_poll (chaîne de temps delta) Spécifie la fréquence des mises à jours les esclaves auprès du maître. Défaut : 2m (minutes)

iprop_port (numéro de port) Spécifie le numéro de port à utiliser pour la propagation incrémentale. Requis dans les configuration des maître et esclaves.

iprop_resync_timeout (chaîne de temps delta). Spécifie le temps d'attente pour une propagation complète. Optionnel et est utilisé par les esclaves uniquement. Défaut : 5m.

iprop_logfile (Nom de fichier) Spécifie où se situe le fichier de log des mises à jours. Par défaut, utilise **database_name.ulog**

kadmind_port (numéro de port) Port d'écoute du service kadmind. Défaut : 749

key_stash_file (chaîne) Spécifie l'emplacement du fichier stash. Défaut : **LOCALSTATEDIR/krb5kdc/.k5.REALM**.

kdc_ports (liste séparée par des espaces ou des virgules) Liste de ports d'écoute du serveur Kerberos pour les requêtes UDP. Défaut : 88,750

kdc_tcp_ports (liste séparée par des espaces ou des virgules) Liste de ports d'écoute du serveur Kerberos pour les requêtes TCP (Défaut : 88).

master_key_name (chaîne) Spécifie le nom du principal associé avec la clé maître. Défaut : K/M

master_key_type (Chaîne de type de clé) Spécifie le type de clé maître. Défaut : aes256-cts-hmac-sha1-96.

max_life (chaîne de temps) Spécifie le temps maximum pour lequel un ticket peut être valide dans le domaine. Défaut : 24heures.

max_renewable_life (chaîne de temps) Spécifie le temps maximum durant lequel un ticket valide peut être renouvelé dans ce domaine. Défaut : 0

no_host_referral (liste séparée par des espaces ou des virgules) Liste

des_crc_session_supported (bool) À true, le KDC assume que les principaux de service supportent des-cbc-crc pour les type de clé de session. Défaut : true.

reject_bad_transit (bool) À true, le KDC vérifie la liste des domaines de transit pour les tickets inter-domaines avec le chemin de transit calculé depuis les noms des domaines et la section capaths de son fichier krb5.conf ; si le chemin dans le ticket contient un domaine qui n'est pas dans le chemin calculé, le ticket ne sera pas délivré. Si cette valeur est à false, de tels tickets seront toujours émis. si le flag **disable-transited-check** est mis dans la requête entrante, cette vérification n'est pas effectuée. L'option **reject_bad_transit** force de telles requête à être toujours rejetées. Défaut : true

restrict_anonymous_to_tgt (bool) À true, le KDC rejète les demandes de tickets pour des principaux anonymes au principaux de service autre que le domaine du TGS. Cette option permet les PKINIT anonymes pour les tickets FAST sans autoriser l'authentification anonyme aux services. Défaut : false.

supported_enctypes (liste de key :salt) Spécifie les combinaisons key/salt par défaut des principaux pour ce domaine. Tout principal créé via kadmin aura des clé de ce type. Défaut : **aes256-cts-hmac-sha1-96 :normal aes128-cts-hmac-sha1-96 :normal des3-cbc-sha1 :normal arcfour-hmac-md5 :normal**.

[dbdefaults]

Cette section spécifie les valeur par défaut pour certains paramètres de base, à utiliser si la sous-section dbmodules ne contient pas de relation pour ce tag.

ldap_kerberos_container_dn

ldap_kdc_dn

ldap_kadmind_dn

ldap_service_password_file

ldap_servers

ldap_conns_per_server

[dbmodules]

Cette section contient des paramètres utilisés par les bases du KDC et les modules. Chaque tag dans cette section est le nom d'un domaine Kerberos ou un nom de section spécifié par le paramètre **database_module** du domaine. L'exemple suivant montre comment définir un paramètre de base pour le domaine ATHENA.MIT.EDU :

```
[dbmodules]
ATHENA.MIT.EDU = {
 disable_last_success = true
}
```

database_name Ce tag spécifique à db2 indique l'emplacement de la base dans le système de fichier. Défaut : LOCALSTATEDIR/krb5kdc/principal

db_library Indique le nom du module de base à charger. peut être **db2** ou **kldap**

disable_last_success À true, supprime les mises à jours KDC du champ "last successful authentication" des entrées de principal nécessitant une pré-authentification. Positionner ce flag peut améliorer les performances. (Les entrées de principal qui ne nécessitent par de pré-authentification ne mettent jamais ce champ)

disable_lockout À true, supprime les champs "last failed authentication" et "failed password attempts" des entrées de principal nécessitant une pré-authentification. peut améliorer les performances.

ldap_conns_per_server Indique le nombre de connexios à maintenir par serveur LDAP

ldap_kadmind_dn Indique le bind DN par défaut pour le service kadmind. Cet objet devrait avoir les droits de lire et écrire dans la base Kerberos dans la base LDAP.

ldap_kdc_dn Indique le bind DN par défaut pour le service krb5kdc. Cet objet devrait avoir les droits de lire dans la base Kerberos dans la base LDAP et d'écrire les données sauf si **disable_lockout** et **disable_last_success** sont à true.

ldap_kerberos_container_dn Indique le DN de l'objet conteneur où les objets de domaine sont localisés.

ldap_servers Liste les serveur LDAP à contacter.

ldap_service_password_file Indique le fichier contenant les mots de passe stashed (créés par kdb5_ldap_util stashsrvpw) pour les objets **ldap_kadmind_dn** et **ldap_kdc_dn**.

db_module_dir contrôle l'emplacement les modules de base de données. devrait être un chemin absolu. Ce tag pour être spécifié directement dans la section dbmodules.

[logging]

Cette section indique comment krb5kdc et kadmind effectuent les logs. Les clés dans cette section sont les noms des services, qui peut être un parmi :

admin_server Spécifie comment kadmind effectue les logs

kdc Spécifie comment krb5kdc effectue les logs

default Spécifie comment les 2 services effectuent les logs.

Les valeurs sont sous la forme suivante :

FILE=filename ou FILE :filename Log les messages dans le fichier spécifié. si la 1ère forme est utilisée, le fichier est écrasé.

STDERR Log les message sur stderr

CONSOLE Log les messages dans la console

DEVICE=<devicename> Log les messages dans le périphérique spécifié

SYSLOG [:severity [:facility]] Los les messages dans syslog

Dans l'exemple suivant, les messages du KDC vont dans la console et dans syslog. Les messages de kadmind vont dans /var/adm/kadmin.log et dans le périphérique /dev/tty04

```
[logging]
 kdc = CONSOLE
 kdc = SYSLOG:INFO:DAEMON
 admin_server = FILE:/var/adm/kadmin.log
 admin_server = DEVICE=/dev/tty04
```

[otp]

Chaque sous-section de [opt] est le nom du type de token OTP. Les tags dans la sous-section définis la configuration requise pour forwarder une requête OTP au serveur radius. Pour chaque type de token, les tags suivants peuvent être spécifiés :

server Serveur où envoyer les requêtes RADIUS. Peut être un nom d'hôte et un port optionnel, une adresse IP ou un socket UNIX. Défaut LOCALSTATEDIR/krb5kdc/<name>.socket

secret Indique le fichier qui peut être relatif à LOCALSTATEDIR/krb5kdc contenant le secret utilisé pour chiffré les packets RADIUS. Le secret devrait apparaître sur la première ligne du fichier. Si **server** indique un socket unix, ce tag est optionnel.

timeout Entier qui spécifie le temps en secondes durant lequel de KDC devrait attendre pour contacter le serveur RADIUS. Ce tag est le temps total entre toutes les tentatives et devrait être inférieur au temps de validité de l'OTP. Défaut : 5 secondes

retries Nombre de re-tentatives auprès du serveur RADIUS. Défaut : 3

strip_realm À true, le principal sans le domaine sera passé au serveur RADIUS, sinon le domaine est inclus. Défaut : true.

Dans l'exemple suivant, les requêtes sont envoyées à un serveur distant via UDP :

```
[otp]
 MyRemoteTokenType = {
  server = radius.mydomain.com:1812
  secret = SEmfiajf42$
  timeout = 15
  retries = 5
  strip_realm = true
 }
```

Un token par défaut implicite nommé DEFAULT est définis pour les type de token non spécifiés. Sa configuration est décrite ci-dessous.

```
[otp]
 DEFAULT = {
  strip_realm = false
 }
```

Options PKINIT

Cet valeurs peuvent être spécifiées dans [kdcdefaults] comme valeur par défaut, ou dans une sous-section de [realms]. Noter qu'une valeur spécifique à un domaine remplace, n'ajoute pas, une spécification kdcdefaults. L'ordre de recherche est :

1. sous-section de [realms] :

```
[realms]
 EXAMPLE.COM = {
  pkinit_anchors = FILE:/usr/local/example.com.crt
 }
```

2. Valeur générique dans la section [kdcdefaults] :

```
[kdcdefaults]
 pkinit_anchors = DIR:/usr/local/generic_trusted_cas/
```

pkinit_anchors Spécifie l'emplacement des certificats de confiance racine que le client utilise pour signer les certificats KDC. Peut être spécifié plusieurs fois.

pkinit_dh_min_bits Taille de la clé Diffie-Hellman que le client va tenter d'utiliser. les valeur acceptable sont 1024, 2048 (défaut), et 4096.

pkinit_allow_upn Spécifie que le KDC est prêt à accepter les certificats client avec un SAN UPN. Défaut : false. Sans cette option, le KDC accepte uniquement les certificats avec id-pkinit-san comme définis dans la rfc4556. Il n'y a actuellement aucune option pour désactiver la vérification SAN dans le KDC.

pkinit_eku_checking spécifie quelle valeur d'Extended Key Usage le KDC est prêt à accepter dans les certificats client. Les valeurs reconnues sont :

kpClientAuth C'est la valeur par défaut et spécifie que les certificats client doivent avoir le id-pkinit-KDKdc EKU comme définis dans la rfc4556.

scLogin Les certificats client avec id-ms-sc-logon seront acceptés

none Les certificats client ne seront pas vérifiés pour un EKU acceptable.

pkinit_identity Spécifie l'emplacement des information d'identité X.509 du KDC. Cette option est requise si pkinit est supportée par le KDC

pkinit_kdc_ocsp Spécifie l'emplacement de l'OCSP du KDC

pkinit_mapping_file Spécifie le nom du fichier de mappage d'acl pkinit. Ce fichier map les principaux aux certificats qu'ils utilisent.

pkinit_pool Spécifie l'emplacement des certificats intermédiaires qui peuvent être utilisés par le KDC pour compléter le chaîne. Peut être spécifiée plusieurs fois

pkinit_revoke Spécifie l'emplacement de la CRL. Peut être spécifié plusieurs fois

pkinit_require_crl_checking Spécifie que la vérification de révocation est requise.

Types de chiffrement

des-cbc-crc DES cbc mode avec CRC-32 (weak)

des-cbc-md4 DES cbc mode avec RSA-MD4 (weak)

des-cbc-md5 DES cbc mode avec RSA-MD5 (weak)

des-cbc-raw DES cbc mode raw (weak)

des3-cbc-raw Triple DES cbc mode raw (weak)

des3-cbc-sha1 des3-hmac-sha1 des3-cbc-sha1-kd Triple DES cbc mode avec HMAC/sha1

des-hmac-sha1 DES avec HMAC/sha1 (weak)

aes256-cts-hmac-sha1-96 aes256-cts AES-256 CTS mode avec 96-bit SHA-1 HMAC

aes128-cts-hmac-sha1-96 aes128-cts AES-128 CTS mode avec 96-bit SHA-1 HMAC

arcfour-hmac rc4-hmac arcfour-hmac-md5 RC4 avec HMAC/MD5

arcfour-hmac-exp rc4-hmac-exp arcfour-hmac-md5-exp Exportable RC4 avec HMAC/MD5 (weak)

camellia256-cts-cmac camellia256-cts Camellia-256 CTS mode avec CMAC

camellia128-cts-cmac camellia128-cts Camellia-128 CTS mode avec CMAC

des Fammille DES : des-cbc-crc, des-cbc-md5, and des-cbc-md4 (weak)

des3 Famille triple DES : des3-cbc-sha1

aes Famille AES : aes256-cts-hmac-sha1-96 and aes128-cts-hmac-sha1-96

rc4 Famille RC4 : arcfour-hmac

camellia Famille Camellia : camellia256-cts-cmac and camellia128-cts-cmac

La chaîne **DEFAULT** peut être utilisé pour les type de jeu par défaut pour les variables en question. Les types ou familles peuvent être supprimées de la liste courante en les préfixant avec un "-". Les types ou familles peuvent être préfixés avec un "+" pour la symétrie ; il a la même signification que simplement lister le type ou la famille. Par exemple, **DEFAULT -des** sera le jeu de chiffrement par défaut avec les types DES supprimés, et **des3 DEFAULT** sera le jeu de chiffrement par défaut avec triple DES supprimé.

Alors que **aes128-cts** et **aes256-cts** sont supportés pour toutes les opérations Kerberos, ils ne sont pas supportés par d'anciennes versions de l'implémentation GSS-API.

Listes de keysalt

Les clés Kerberos pour les utilisateurs sont généralement dérivés des mots de passe. Les commandes et les paramètres de configuration Kerberos qui affectent la génération de clés prennent la liste des paires enctype-salttype, appelés "liste keysalt". Chaque paire keysalt est un nom de type de chiffrement suivi par un nom de salttype, dans le format enc :salt. Par exemple :

kadmin -e aes256-cts :normal,aes128-cts :normal

va lancer kadmin pour qu'il génère par défaut des clé dérivés pour les types de chiffrement **aes256-cts** et **aes128-cts**, en utilisant un salt **normal**.

Pour s'assurer que les gens qui utilisent le même mot de passe n'aient pas la même clé, Kerberos 5 incorpore plus d'informations dans la clé en utilisant un salt. Les types de salt supportés sont les suivant :

normal Défaut pour Kerberos v5

v4 Utilisé uniquement par Kerberos v4 (pas de salt)

norealm Idem au défaut, sans utiliser d'information de domaine.

onlyrealm Utilise seulement les information de domaine comme salt

afs3 AFS version 3, utilisé uniquement pour la compatibilité avec Kerberos v4

special Génère un salt aléatoire.

Exemple

Exemple de fichier de configuration kdc.conf

```
[kdcdefaults]
 kdc_ports = 88

[realms]
 ATHENA.MIT.EDU = {
  kadmind_port = 749
  max_life = 12h 0m 0s
  max_renewable_life = 7d 0h 0m 0s
  master_key_type = des3-hmac-sha1
  supported_enctypes = des3-hmac-sha1:normal des-cbc-crc:normal des-cbc-crc:v4
  database_module = openldap_ldapconf
 }

[logging]
 kdc = FILE:/usr/local/var/krb5kdc/kdc.log
 admin_server = FILE:/usr/local/var/krb5kdc/kadmin.log

[dbdefaults]
 ldap_kerberos_container_dn = cn=krbcontainer,dc=mit,dc=edu

[dbmodules]
 openldap_ldapconf = {
  db_library = kldap
  disable_last_success = true
  ldap_kdc_dn = "cn=krbadmin,dc=mit,dc=edu"
  ldap_kadmind_dn = "cn=krbadmin,dc=mit,dc=edu"
  ldap_service_password_file = /etc/kerberos/service.keyfile
  ldap_servers = ldaps://kerberos.mit.edu
  ldap_conns_per_server = 5
 }
```