Kerberos - Formats

Formats et données diverses

Format de temps supportés

Le format **time_duration** est utilisé pour exprimé une durée de temp dans les fichiers de configuration Kerberos est les commandes utilisateur. Les formats permis sont :

Format	Exemple	valeure
h:m[:s]	36:00	36 hours
NdNhNmNs	8h30s	8 hours 30 seconds
N	3600	1 hour

Note : l'interval de temps ne devrait pas excéder 2147483647 secondes.

Le format **getdate_time** spécifie une date. Les formats permis sont :

Date	mm/dd/yy	07/27/12
	month dd, yyyy	Jul 27, 2012
	yyyy-mm-dd	2012-07-27
Absolute time	HH:mm[:ss]pp	08:30 PM
	hh:mm[:ss]	20:30
Relative time	N tt	30 sec
Time zone	Z	EST
	z	-0400

Le format **absolute_time**, rarement utilisé peut être noté selon un des formats suivants :

Format	Example	Value
yyyymmddhhmmss	20141231235900	One minute before 2015
yyyy.mm.dd.hh.mm.ss	2014.12.31.23.59.00	
yymmddhhmmss	141231235900	
yy.mm.dd.hh.mm.ss	14.12.31.23.59.00	
dd-month-yyyy:hh:mm:ss	31-Dec-2014:23:59:00	
hh:mm:ss	20:00:00	8 o'clock in the evening

Types de chiffrement

Kerberos peut utiliser divers algorithmes de chiffrement pour protéger des données. Un type de chiffrement Kerberos est une combinaison spécifique d'un algorithme de chiffrement avec un algorithme d'intégrité pour fournir la confidentialité et l'intégrité des données. Les clients effectuent 2 types de demandes (KDC-REQ) au KDC : AS-REQ et TGS-REQ. Le client utilise l'AS-REQ pour obtenir des tickets initiaux (appelés TGT), et utilisent TGS-REQ pour obtenir des tickets de service. Le KDC utilise 3 types de clé différentes en fournissant un ticket au client.

La clé long-terme du service : Le KDC l'utilise pour chiffrer le ticket de service actuel. Le KDC utilise la première clé long-terme dans le kvno le plus récent.

La clé de session : Le KDC choisis aléatoirement cette clé et place une copie dans le ticket et une autre copie dans la partie chiffrée de la réponse.

La clé de chiffrement de réponse : Le KDC l'utilise pour chiffrer la réponse qu'il envoie au client. Pour les réponses AS, c'est une clé long-terme du client. Pour les réponses TGS, c'est soit la clé de session du ticket authentifiant, ou une clé de sous-session.

Chaque type de demande permet au client d'envoyer une liste de type de chiffrement qu'il accepte. Pour AS-REQ, cette liste affecte la sélection de la clé de session et la clé de chiffrement de la réponse. Pour TGS-REQ, cette liste affecte uniquement la sélection de la clé de session.

Compatibilité des types de chiffrement :

des-cbc-crc_____weak____all_____>=2000

des-cbc-md5_____weak____all__ __>=2000

arcfour-hmac_____ _____>=1.3___>=2000

aes128-cts-hmac-sha1-96_ _____>=1.3___>=Vista

camellia128-cts-cmac____ _____>=1.9___none

Variables d'environnement

KRB5_CONFIG Spécifie l'emplacement de krb5.conf

KRB5_KDC_PROFILE Spécifie l'emplacement de kdc.conf

KRB5_KTNAME Fichier keytab par défaut

KRB5_CLIENT_KTNAME Fichier keytab client par défaut

KRB5CCNAME fichier du cache d'accréditifs par défaut, sous la forme type :residual

KRB5RCACHETYPE Type de cache replay par défaut. (défaut : dfl) none pour le désactiver

KRB5RCACHEDIR Répertoire du cache replay par défaut.

KPROP_PORT port kprop à utiliser. Défaut : 754

KRB5_TRACE Fichier pour les logs.