kinit

Obtenir un TGT initial

OPTIONS

-v mode verbeux

-l lifetime (Chaîne time_duration) Demande un ticket avec la durée de vie spécifiée (ex : kinit -l 5 :30 ou kinit -l 5h30m).

-s start_time (Chaîne time_duration) Demande un ticket post-daté en spécifiant le délai avant que le ticket devienne valide.

-r renewable_life (Chaîne time_duration) Demande des tickets renouvelables, avec la durée de vie totale spécifiée.

-f Demande des tickets forwardable

-F Demande des tickets non-forwardable

-p Demande des tickets proxiable

-P Demande des tickets non-proxiable

-a Demande des tickets restreins aux adresses locales de l'hôte.

-A Demande des tickets non restreins pas des adresses

-C Demande la canonisation du nom du principal, et permet au KDC de répondre avec un principal client différent.

-E Traite le nom du principal comme un nom d'entreprise

-v Demande que le TGT dans le cache (avec le flag invalid) soit passé au KDC pour validation.

-R Demande de renouveler le TGT.

-k [-i | -t keytab_file] Demande un ticket, obtenu depuis un clé dans le keytab de l'hôte. L'emplacement du keytab peut être spécifié avec **-t**, ou avec **-i** pour spécifier l'utilisation de keytab du client par défaut. Par défaut, un ticket d'hôte pour l'hôte local est requis, mais tout principal peut être spécifié. Sur le KDC, l'emplacement du keytab spécial **KDB :** peut être utilisé pour indiquer que kinit devrait ouvrir la base du KDC et rechercher la clé directement. Cela permet aux administrateur d'obtenir des tickets pour tous principal qui supporte l'authentification basé sur les clé.

-n Demande un traitement anonyme.

-I input_ccache Spécifie le nom du cache d'accréditifs qui contient déjà un ticket. En obtenant ce ticket, si les informations d'obtention de ce ticket sont également présentes dans le cache, ces informations seront utilisées pour affecter l'obtention des nouveaux tickets, incluant les méthodes d'authentification auprès du KDC.

-T armor_ccachef Spécifie le nom du cache d'accréditifs qui contient déjà un ticket. Si supporté par le KDC, ce cache sera utilisé pour protéger la demande, empêchant les attaques par dictionnaire offline et permettant d'utiliser des mécanismes de pré-authentification additionnels.

-c cache_name Utilise le cache spécifié comme cache d'accréditifs au lieu du cache par défaut spécifié par la variable **KRB5CCNAME**

-S service_name Spécifie un nom de service alternatif à utiliser pour obtenir les tickets initiaux.

-X attribute [=value] Spécifie un attribut/valeur de pré-authentification interprété par les modules de pré-authentification. Les attributs reconnus par PKINIT sont les suivants :

X509_user_identity=value Spécifie où trouver les informations d'identité X509 de l'utilisateur

X509_anchors=value Spécifie où trouver les informations de validation X509

flag_RSA_PROTOCOL [=yes] Spécifie l'utilisation de RSA au lieu de DH

Variables d'environnement

KRB5CCNAME peut contenir un nom de cache d'autorisations Kerberos5

fichiers

DEFCCNAME Emplacement par défaut pour le cache d'accréditifs Kerberos 5

DEFKTNAME Emplacement par défaut pour le keytab de l'hôte local