Configuration et dépannage de la prise en charge de client Kerberos V5

Contenu

Introduction

Ce document fournit un exemple de configuration, aussi bien que quelques solutions aux problèmes courants. Des techniques qui vous aident à dépanner toutes les questions sont également fournies dans ce document. Ce document n'adresse pas le support kerberized de telnet.

La majeure partie de ce contenu en cet article est provenue la documentation librement disponible qui est livré avec le Kerberos et de divers forums aux questions disponibles (Foires aux questions) sur le module. Les configurations sont provenues un routeur et un serveur fonctionnels du Kerberos KDC.

Ce document suppose que vous avez correctement compilé et avez installé une version en cours

de la version 5 du module de Kerberos du MIT. Référez-vous aux références à la fin de cet article pour les informations sur la façon dont obtenir, compiler, et installer le Kerberos V5.

Notez également que la version de logiciel 11.2 ou ultérieures de Cisco IOS® est exigée pour le support du Kerberos V5. Ceci fournit le support complet de l'authentification client du Kerberos V, qui inclut l'expédition de créance. Les systèmes qui ont des infrastructures du Kerberos V peuvent employer leurs centres serveurs de distribution de clé (KDCs) afin d'authentifier des utilisateurs pour l'accès de réseau ou de routeur. C'est une implémentation de client et pas une implémentation du Kerberos KDC.

Le Kerberos est considéré un service de sécurité existant et est le plus salutaire dans les réseaux qui utilisent déjà le Kerberos.

Référez-vous aux notes en version de Logiciel Cisco IOS version 11.2 pour plus d'informations détaillées dont les versions incluent ce support.

Pour le support de Kerberos dans des versions logicielles ultérieures de Cisco IOS, référez-vous au conseiller de logiciel (clients enregistrés seulement).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco IOS version 11.2 et plus tard

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Introduction au Kerberos

Le Kerberos est un protocole d'authentification de réseau pour l'usage sur les réseaux physiquement non sécurisés. Le Kerberos est basé sur le modèle de la distribution de clé présenté par Needham et Schroeder. (Voir le numéro 9 dans la section de références de ce document. Il est conçu pour fournir l'authentification poussée pour le client/serveurs d'application en employant le chiffrement de secret-key. Il permet les entités qui communiquent au-dessus des réseaux pour prouver leur identité entre eux tandis qu'elle empêche écouter clandestinement ou

attaques par relecture. Il prévoit également l'intégrité de flux de données (telle que la détection de la modification) et le secret (tel que la prévention de la lecture non autorisée) avec l'aide des systèmes de chiffrement tels que le DES.

Plusieurs des protocoles utilisés en Internet ne fournissent aucune Sécurité. Les outils utilisés « pour renifler » des mots de passe hors fonction du réseau sont d'usage courant par des casseurs de systèmes. Ainsi, les applications qui envoient un mot de passe au-dessus du réseau décrypté sont vulnérables. En outre, d'autres client/serveurs d'application comptent sur le programme client pour être « honnêtes » au sujet de l'identité de l'utilisateur qui l'utilise. D'autres applications se fondent sur le client pour limiter ses activités à ceux qu'on lui permet de faire, sans l'autre application par le serveur.

Tentative de quelques sites d'employer des Pare-feu afin de résoudre leurs problèmes de sécurité des réseaux. Les Pare-feu supposent que « les mauvais garçons » sont sur l'extérieur, qui est souvent une supposition non valide. Cependant, la majorité des incidents de criminalité informatique qui endommagent plus ont été effectuées par des initiés. Les Pare-feu ont également un inconvénient significatif du fait ils limitent comment vos utilisateurs peuvent utiliser l'Internet.

Le Kerberos a été créé par le MIT comme solution à ces problèmes de sécurité des réseaux. Le protocole de Kerberos utilise le chiffrement fort, de sorte qu'un client puisse prouver son identité à un serveur (et vice versa) à travers une connexion réseau non sécurisée. Après qu'un client et serveur ait utilisé le Kerberos afin de prouver leur identité, ils peuvent également chiffrer toutes leurs transmissions afin d'assurer l'intimité et l'intégrité des données pendant qu'ils vont environ leur entreprise.

Le Kerberos est librement disponible du MIT, sous un avis d'autorisation de copyright qui est semblable à celui utilisé pour l'opération BSD et le système de fenêtrage X11. Le MIT fournit le Kerberos sous la forme source. Ceci est fait de sorte que n'importe qui qui souhaite l'utiliser puisse regarder au-dessus du code pour eux-mêmes et s'assurer que le code est digne de confiance. En outre, pour ceux qui préfèrent compter sur un produit professionnellement pris en charge, le Kerberos est disponible comme produit de beaucoup de différents constructeurs.

Le support de client du Kerberos V5 est basé sur le système d'authentification Kerberos développé au MIT. Sous le Kerberos, un client (généralement un utilisateur ou un service) envoie une demande d'un ticket au centre serveur de distribution de clé (KDC). Le KDC crée un ticket distribué (TGT) pour le client, le chiffre avec l'aide du mot de passe du client comme clé, et envoie le TGT chiffré de nouveau au client. Les tentatives de client puis de déchiffrer le TGT, avec l'aide de son mot de passe. Si le client déchiffre avec succès le TGT par exemple, si le client donne le mot de passe correct), il garde le TGT déchiffré. Ceci indique la preuve de l'identité du client.

Le TGT, qui expire à un temps spécifié, permet au client pour obtenir les tickets supplémentaires, qui donnent l'autorisation pour des services spécifiques. Les demandes et les concessions de ces tickets supplémentaires est utilisateur-transparente.

Puisque le Kerberos négocie authentifié, est sur option chiffré, et communique entre deux points quelconques sur l'Internet, il fournit une couche de Sécurité qui ne dépend pas de quel côté d'un Pare-feu l'un ou l'autre de client se trouve. Le Kerberos est principalement utilisé dans les protocoles de niveau application (niveau modèle OIN 7), tel que le telnet ou le FTP, afin de fournir l'utilisateur pour héberger la Sécurité. Il est également utilisé, bien que moins fréquemment, comme système d'authentification implicite de flux de données (tel que SOCK_STREAM) ou de mécanismes RPC (niveau modèle OIN 6). Il peut également être utilisé à un niveau plus bas pour le degré de sécurité d'hôte à hôte, dans les protocoles tels que l'IP, l'UDP, ou le TCP (niveaux modèles OIN 3 et 4). Bien que, de telles réalisations soient rares, si elles existent du tout.

Il prévoit l'authentification mutuelle et la communication protégée entre les principaux sur un réseau ouvert par la fabrication des clés secrètes pour n'importe quel demandeur. Un mécanisme pour que ces clés secrètes soient sans risque propagées par le réseau est également fourni. Le Kerberos ne prévoit pas l'autorisation ou la comptabilité. Cependant, applications qui souhaitent à l'utilisation de boîte leurs clés de secret afin de remplir ces fonctions sécurisé.

Définitions

- **Authentification** — Assurez-vous que vous êtes qui vous dites que vous êtes, et que nous savons qui vous êtes.
- **Client** — Une entité qui peut obtenir un ticket. Cette entité est habituellement un utilisateur ou un hôte.
- **Qualifications** — Les mêmes que des tickets.
- **Démon** — Un programme, habituellement un qui fonctionne sur un hôte UNIX, ce entretient des demandes réseau pour l'authentification.
- **Hôte** — Un ordinateur qui peut être accédé à au-dessus d'un réseau.
- **Exemple** — La deuxième partie d'un principal Kerberos. Il fournit les informations qui qualifient le primaire. L'exemple peut être nul. Dans le cas d'un utilisateur, l'exemple est employé souvent afin de décrire l'utilisation destinée des qualifications correspondantes. Dans le cas d'un hôte, l'exemple est entièrement - l'adresse Internet qualifiée.
- **Kerberos** — En mythologie grecque, le chien à tête de trois qui garde l'entrée à la pègre. Dans le monde des ordinateurs, le Kerberos est un module de sécurité des réseaux qui a été développé au MIT.
- **KDC** — Centre serveur de distribution de clé. Un ordinateur ce tickets Kerberos de questions.
- **Keytab** — Un fichier de table principal qui contient un ou plusieurs clés. Un hôte ou un service utilise un fichier de keytab de la même manière qu'un utilisateur utilise leur mot de passe.
- **NAS** — Un serveur d'accès à distance (une case de Cisco) ou toute autre chose qui font l'authentification et les demandes d'autorisation TACACS+, ou envoie des paquets de comptabilité.
- **Principal** — Une chaîne qui nomme une entité spécifique à laquelle un ensemble de qualifications peut être assigné. Il a généralement trois parts nommées Primary, exemple, et ROYAUME.Le format typique d'un principal Kerberos typique est **primaire/instanceREALM**.
- **Primaire** — La première partie d'un principal Kerberos. Dans le cas d'un utilisateur, c'est le nom d'utilisateur. Dans le cas d'un service, c'est le nom du service.
- **ROYAUME** — Le réseau logique a servi par une base de données Kerberos simple et un ensemble de centres serveurs de distribution de clé. Par la convention, les noms de royaume sont généralement toutes les lettres majuscules, pour différencier le royaume du domaine de l'Internet.
- **Service** — Tout programme ou ordinateur que vous accédez à au-dessus d'un réseau. Les exemples des services incluent :« hôte » — un hôte, (par exemple, quand vous utilisez le telnet et le rsh)« FTP » — FTPauthentification de « krbtgt » — ; comme le ticket distribué« bruit » — Courrier électronique
- **Ticket** — Un ensemble provisoire de qualifications électroniques qui vérifient l'identité d'un client pour un service particulier.
- **TGT** — Ticket distribué. Un ticket Kerberos spécial qui permet au client pour obtenir les tickets Kerberos supplémentaires dans le même royaume de Kerberos.Une bonne analogie pour le ticket distribué est un passage de trois jours de ski qui est bon à quatre stations de vacances différentes. Vous affichez le passage à n'importe quelle station de vacances vous

décidez d'aller (jusqu'à ce qu'elle expire), et vous recevez un ticket d'ascenseur pour cette station de vacances. Une fois que vous avez le ticket d'ascenseur, vous pouvez skier tous que vous voulez à cette station de vacances. Si vous allez à une autre station de vacances le next day, vous affichez de nouveau votre passage, et vous obtenez un ticket supplémentaire d'ascenseur pour la nouvelle station de vacances. La différence est que le Kerberos V5 programme l'avis que vous avez le passage de ski de fin de semaine, et obtenez le ticket d'ascenseur pour vous, ainsi vous ne devez pas exécuter les transactions vous-même.

Gotcha

Cette section répertorie plusieurs éléments dont vous devez se rendre compte :

- Veillez-vous pour enlever tous les espaces de remorquage dans les fichiers de configuration. Les espaces de remorquage peuvent poser des problèmes avec le serveur krb5kdc. Autrement, vous pouvez recevoir un message qui indique, "krb5kdc ne pouvez pas commencer la base de données pour le royaume. »
- Assurez-vous que l'horloge sur le routeur est réglée au même temps que l'hôte UNIX qui exécute le serveur KDC. Afin d'empêcher des intrus de remettre à l'état initial leurs horloges système afin de continuer à utiliser les tickets expirés, le Kerberos V5 est installé pour rejeter des demandes de ticket de n'importe quel hôte dont l'horloge n'est pas dans la distorsion maximum spécifiée d'horloge du KDC (comme spécifié dans le fichier kdc.conf). De même, des hôtes sont configurés pour rejeter des réponses de n'importe quel KDC dont l'horloge n'est pas dans la distorsion maximum spécifiée d'horloge de l'hôte (comme spécifié dans le fichier krb5.conf). La valeur par défaut pour la distorsion maximum d'horloge est de 300 secondes (cinq minutes).
- Assurez-vous les travaux de DN correctement. Plusieurs aspects de Kerberos se fondent sur le service de nom. Pour que le Kerberos fournisse son haut niveau de sécurité, il est plus sensible aux problèmes de service de nom que quelques autres parties de votre réseau. Il est important que vos entrées de Système de noms de domaine (DNS) et vos hôtes aient les informations correctes. Chaque canonique du nom d'hôte doit être le nom d'hôte plein-qualifié (qui inclut le domaine), et chaque adresse IP de l'hôte doit inverse-résolution au nom canonique.
- Le support du Kerberos V5 de Cisco IOS ne permet pas l'utilisation des noms de royaume minuscules et le code de Kerberos dans le Cisco IOS n'authentifie pas des utilisateurs si le royaume est en minuscules. Ceci a été réparé dans le Logiciel Cisco IOS version 11.2(7).Référez-vous à l'ID de bogue Cisco CSCdj10598 (clients enregistrés seulement).Le seul contournement est d'utiliser des noms de ROYAUME majuscules (qui est conventionnel).Les royaumes minuscules fonctionnent afin de récupérer un TGT, mais pas un laisser-passer de service. Puisque Cisco emploie leur nouveau TGT afin de récupérer un laisser-passer de service (utilisé pour empêcher l'attaque de détournement de trafic KDC) pendant se connecter l'authentification, l'authentification Kerberos que les royaumes minuscules d'utilisations échoue toujours.
- Le Kerberos V5 pour le PPP PAP et le CHAP peut tomber en panne le routeur. Ceci a été réparé dans le Logiciel Cisco IOS version 11.2(6).Référez-vous à l'ID de bogue Cisco CSCdj08828 (clients enregistrés seulement).Le contournement pour ceci est de forcer la procédure de connexion d'exécutif dans le routeur par l'intermédiaire de l'**async mode interactive** sans pendant-**procédure de connexion d'autoselect** et puis d'avoir le PPP de début

d'utilisateur manuellement :`aaa authentication ppp default if-needed krb5 local`

- Le Kerberos V5 ne fait pas l'autorisation ou la comptabilité. Vous avez besoin d'un autre code afin de faire ceci.

Configuration de routeur Cisco IOS

La configuration dans cette section dépeint un routeur AS5200 saturé qui fait le Kerberos V5. Le routeur dans cette configuration utilise le serveur de Kerberos afin d'authentifier les sessions et les utilisateurs VTY qui se connectent pour faire le PPP avec l'authentification PAP.

Config AS5200 avec le Kerberos V5

```
version 11.2
service timestamps debug datetime msec
!
hostname cisco5200
!
aaa new-model
aaa authentication login cisco2 krb5 local
aaa authentication ppp cisco krb5 local
enable secret
enable password
!
username cisco password cisco
ip host-routing
ip domain-name cisco.edu
ip name-server 10.10.1.25
ip name-server 10.10.20.3
kerberos local-realm CISCO.EDU
kerberos srvtab entry host/cisco5200.cisco.edu@CISCO.EDU
0 861289666 2
1 80:>:11338>531159=
!
 !--- You do not actually enter the previous line. !---
Enter "kerberos srvtab remote 10.10.1.8 /ts/krb5.keytab"
and the !--- the router TFTPs the key entry on its own.
kerberos server CISCO.EDU 10.10.1.8 kerberos credentials
forward isdn switch-type primary-5ess clock timezone GMT
-6 clock summer-time CDT recurring ! controller T1 0
framing esf clock source line primary linecode b8zs pri-
group timeslots 1-24 ! controller T1 1 framing esf clock
source line secondary linecode b8zs pri-group timeslots
1-24 ! interface Ethernet0 ip address 10.10.110.245
255.255.255.0 no ip mroute-cache ! interface Serial0 no
ip address no ip mroute-cache shutdown ! interface
Serial1 no ip address no ip mroute-cache shutdown !
interface Serial0:23 ip unnumbered Ethernet0 no ip
mroute-cache encapsulation ppp isdn incoming-voice modem
no cdp enable ! interface Serial1:23 ip unnumbered
Ethernet0 no ip mroute-cache encapsulation ppp isdn
incoming-voice modem no cdp enable ! interface Group-
Async1 ip unnumbered Ethernet0 no ip mroute-cache
encapsulation ppp async mode interactive peer default ip
address pool mypool dialer in-band dialer idle-timeout
9999 dialer-group 1 no cdp enable ppp authentication pap
cisco group-range 1 48 ! ip local pool mypool
10.10.110.97 10.10.110.144 no ip classless ip route
0.0.0.0 0.0.0.0 10.10.110.254 ! dialer-list 1 protocol
ip permit ! line con 0 login authentication test line 1
48 autoselect ppp login authentication cisco2 modem
```

```
InOut transport input all line aux 0 modem InOut
transport input all flowcontrol hardware line vty 0 10
exec-timeout 0 0 login authentication cisco2 ! end
```

Configuration du Kerberos KDC

Veillez-vous pour avoir les ports appropriés installés pour l'**inetd**.

Remarque: Cet exemple utilise des wrappers. Si vous voulez le telnet chiffré, vous devez remplacer le telnet normal par le telnet kerberized, ainsi ces fichiers ont une apparence différente.

Ports d'installation pour l'inetd

```
# cat /etc/services
-----------------------------------------------------------------
#
# Syntax:  ServiceName PortNumber/ProtocolName [alias\_1,...,alias\_n] [#comments]
#
# ServiceNameofficial Internet service name
# PortNumber the socket port number used for the service
# ProtocolNamethe transport protocol used for the service
# alias                 unofficial service names
# #comments             text following the comment character (#) is ignored
#
tftp69/udp

kerberos88/udpkdc
kerberos88/tcpkdc

kxct549/tcp

klogin      543/tcp         # Kerberos authenticated rlogin
kshell 544/tcp         cmd # and remote shell
kerberos-adm 749/tcp          # Kerberos 5 admin/changepw
kerberos-adm 749/udp        # Kerberos 5 admin/changepw
kerberos-sec 750/udp         kdc    # Kerberos authentication--udp
kerberos-sec   750/tcp         kdc   # Kerberos authentication--tcp
krb5\_prop    754/tcp          # Kerberos slave propagation
eklogin       2105/tcp         # Kerberos auth. & encrypted rlogin
krb524        4444/tcp         # Kerberos 5 to 4 ticket translator
-----------------------------------------------------------------

#cat /etc/inetd.conf

ident   stream  tcp     nowait  root    /usr/local/etc/in.identd in.identd
ftp     stream  tcp     nowait  root    /usr/sbin/tcpd          ftpd
telnet  stream  tcp     nowait  root    /usr/sbin/tcpd          telnetd
#shell   stream  tcp     nowait  root    /usr/sbin/tcpd          rshd
shell   stream  tcp     nowait  root    /usr/sbin/rshd          rshd
#login   stream  tcp     nowait  root    /usr/sbin/tcpd          rlogind
login   stream  tcp     nowait  root    /usr/sbin/rlogind       rlogind
exec    stream  tcp     nowait  root    /usr/sbin/rexecd        rexecd
# Run as user "uucp" if you don't want uucpd's wtmp entries.
#uucp   stream  tcp     nowait  root    /usr/sbin/uucpd         uucpd
#finger  stream  tcp     nowait  root    /usr/sbin/tcpd          fingerd
# tftp was /tmp and is now /ts for terminal server macros
tftp    dgram   udp     wait    nobody  /usr/sbin/tcpd          tftpd /ts
comsat  dgram   udp     wait    root    /usr/sbin/comsat        comsat
-----------------------------------------------------------------
```

Fichiers de configuration de Kerberos d'installation

Ensuite, vous devez installer quelques fichiers de configuration de Kerberos que le serveur KDC indique. Pour plus d'informations sur ce que signifient ces paramètres, référez-vous au Kerberos installent le guide ou le guide d'admin de système .

```
# cat /etc/krb5.conf

[libdefaults]
        default_realm =  CISCO.EDU
        ticket_lifetime = 600
        default_tgs_enctypes = des-cbc-crc
        default_tkt_enctypes = des-cbc-crc

[realms]
        CISCO.EDU = {
        kdc =  ciscoaxa.cisco.edu:88
        admin_server =  ciscoaxa.cisco.edu
        default_domain =  CISCO.EDU
        }

[domain_realm]
        .cisco.edu = CISCO.EDU
        cisco.edu  = CISCO.EDU

[logging]
        kdc = FILE:/var/log/krb5kdc.log
        admin_server = FILE:/var/log/kadmin.log
        default = FILE:/var/log/krb5lib.log


# cat /usr/local/var/krb5kdc/kdc.conf

[kdcdefaults]
      kdc_ports = 88,750

[realms]
      CISCO.EDU = {
         database_name = /usr/local/var/krb5kdc/principal
         admin_keytab = FILE:/usr/local/var/krb5kdc/kadm5.keytab
         acl_file = /usr/local/var/krb5kdc/kadm5.acl
         acl_file = /usr/local/var/krb5kdc/kadm5.dict
         key_stash_file = /usr/local/var/krb5kdc/.k5.CISCO.EDU
         kadmind_port = 749
         max_life = 10h 0m 0s
         max_renewable_life = 7d 0h 0m 0s
         master_key_type = des-cbc-crc
         supported_enctypes = des-cbc-crc:normal des:normal des:v4
des:norealm des:onlyrealm des:afs3
     }
```

Installez la base de données pour le serveur KDC

Ensuite, vous devez créer la base de données que le serveur KDC utilise.

1. Sélectionnez la commande **kdb5_util** :`# kadmin/dbutil/kdb5_util Usage: kdb5_util cmd [-r realm] [-d dbname] [-k mkeytype] [-M mkeyname] [-m] [cmd options] create [-s] destroy [-f] stash [-f keyfile] dump [-old] [-ov] [-b6] [-verbose] [filename [princs...]] load [-old] [-ov] [-b6] [-verbose] [-update] filename dump_v4 [filename] load_v4 [-t] [-n] [-v] [-K] [-s stashfile] inputfile ---------- # kadmin/dbutil/kdb5_util destroy -r cisco.edu kdb5_util: No such file or directory while`

```
setting active database to "/usr/local/var/krb5kdc/principal" # kadmin/dbutil/kdb5_util
create -r CISCO.EDU -s Initializing database '/usr/local/var/krb5kdc/principal' for realm
'CISCO.EDU', master key name 'K/M@CISCO.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:
```

C'est nécessaire afin de récupérer le mot de passe de **srvtab du** routeur par l'intermédiaire du TFTP avec la commande de **kerberos srvtab remote**.

```
# kadmin/dbutil/kdb5_util stash -r CISCO.EDU Enter KDC database master key:
```

2. Afin d'ajouter des directeurs et des utilisateurs à la base de données, utilisez la **commande kadmin.local** :

```
# kadmin/cli/kadmin.local kadmin.local: listprincs kadmin/admin@CISCO.EDU
kadmin/changepw@CISCO.EDU K/M@CISCO.EDU krbtgt/CISCO.EDU@CISCO.EDU kadmin/history@CISCO.EDU
kadmin.local: kadmin.local: ? Available kadmin.local requests: add_principal, addprinc, ank
Add principal delete_principal, delprinc Delete principal modify_principal, modprinc Modify
principal change_password, cpw Change password get_principal, getprinc Get principal
list_principals, listprincs, get_principals, getprincs List principals add_policy, addpol
Add policy modify_policy, modpol Modify policy delete_policy, delpol Delete policy
get_policy, getpol Get policy list_policies, listpols, get_policies, getpols List policies
get_privs, getprivs Get privileges ktadd, xst Add entry(s) to a keytab ktremove, ktrem
Remove entry(s) from a keytab list_requests, lr, ? List available requests. quit, exit, q
Exit program. ----------------------------------------
```

3. Ajoutez un utilisateur :

```
kadmin.local:  ank cisco1@CISCO.EDU
Enter password for principal "cisco1@CISCO.EDU":
Re-enter password for principal "cisco1@CISCO.EDU":
Principal "cisco1@CISCO.EDU" created.
```

4. Obtenez une liste de la base de données en cours :

```
kadmin.local:  listprincs
kadmin/admin@CISCO.EDU
kadmin/changepw@CISCO.EDU
cisco1@CISCO.EDU
K/M@CISCO.EDU
krbtgt/CISCO.EDU@CISCO.EDU
kadmin/history@CISCO.EDU
```

5. Ajoutez l'entrée pour le routeur de Cisco :

```
kadmin.local:  ank
host/cisco5200.cisco.edu@CISCO.EDU
Enter password for principal "host/cisco5200.cisco.edu@CISCO.EDU":

Re-enter password for principal "host/cisco5200.cisco.edu@CISCO.EDU":
Principal "host/cisco5200.cisco.edu@CISCO.EDU" created.
```

6. Extrayez une clé à la table pour le routeur de Cisco :

```
kadmin.local:  ktadd
host/cisco5200.cisco.edu@CISCO.EDU
Entry for principal host/cisco5200.cisco.edu@CISCO.EDU with kvno 2,
   encryption type DES-CBC-CRC added to keytab WRFILE:/etc/krb5.keytab.
```

7. Prenez des autres regardent la base de données :

```
kadmin.local:  listprincs
kadmin/admin@CISCO.EDU
kadmin/changepw@CISCO.EDU
cisco1@CISCO.EDU
K/M@CISCO.EDU
krbtgt/CISCO.EDU@CISCO.EDU
kadmin/history@CISCO.EDU
host/cisco5200.cisco.edu@CISCO.EDU

kadmin.local:  quit
```

8. Déplacez le fichier de keytab à un endroit où le routeur peut obtenir à lui :

```
# cp
/etc/krb5.keytab /ts/
# chmod 777 /ts/krb5.keytab
```

9. Mettez en marche le serveur KDC :

```
# kdc/krb5kdc
#
```

10. Vérifiez pour s'assurer qu'il fonctionne réellement :

```
# ps -A | grep  'krb5'
   6043 ??       I        0:00.01 kdc/krb5kdc
  23427 ttypf    S  +     0:00.05 grep krb5
```

11. Forcez le routeur pour lire son entrée de table principale :

```
cisco5200(config)#kerberos srvtab
```

remote 10.10.1.8 /ts/krb5.keytab Loading /ts/krb5.keytab from 10.10.1.8 (via Ethernet0): ! [OK - 229/1000 bytes]

12. Vérifiez le routeur pour s'assurer que tout est prêt :cisco5200#**write terminal** aaa new-model aaa authentication login cisco2 krb5 local aaa authentication ppp cisco krb5 local kerberos local-realm CISCO.EDU kerberos srvtab entry host/cisco5200.cisco.edu@CISCO.EDU 0 861289666 2 1 8 0:>:11338>531159= kerberos server CISCO.EDU 10.10.1.8 kerberos credentials forward
13. Activez l'élimination des imperfections et l'essayez de se connecter dans le routeur :cisco5200#**terminal monitor** cisco5200#**debug kerberos** Kerberos debugging is on cisco5200#**debug aaa authen** AAA Authentication debugging is on cisco5200#**show clock** 10:16:41.797 CDT Thu Apr 17 1997 cisco5200# Apr 17 15:16:58.965: AAA/AUTHEN: create_user user='' ruser='' port='tty51' rem_addr='12.12.109.64' authen_TYPE=ASCII service=LOGIN priv=1 Apr 17 15:16:58.969: AAA/AUTHEN/START (0): port='tty51' list='cisco2' ACTION=LOGIN service=LOGIN Apr 17 15:16:58.969: AAA/AUTHEN/START (1957396): found list Apr 17 15:16:58.973: AAA/AUTHEN/START (1667706374): METHOD=KRB5 Apr 17 15:16:58.973: AAA/AUTHEN (1667706374): status = GETUSER Apr 17 15:17:02.493: AAA/AUTHEN/CONT (1667706374): continue_login Apr 17 15:17:02.493: AAA/AUTHEN (1667706374): status = GETUSER Apr 17 15:17:02.497: AAA/AUTHEN (1667706374): METHOD=KRB5 Apr 17 15:17:02.497: AAA/AUTHEN (1667706374): status = GETPASS Apr 17 15:17:05.401: AAA/AUTHEN/CONT (1667706374): continue_login Apr 17 15:17:05.405: AAA/AUTHEN (1667706374): status = GETPASS Apr 17 15:17:05.405: AAA/AUTHEN (1667706374): METHOD=KRB5 Apr 17 15:17:05.413: Kerberos: Requesting TGT with expiration date of 861319025 Apr 17 15:17:05.417: Kerberos: Sending TGT request with no pre-authorization data. Apr 17 15:17:05.441: Kerberos: Sent TGT request to KDC Apr 17 15:17:06.405: Kerberos: Received TGT reply from KDC Apr 17 15:17:06.465: Domain: query for 245.110.10.10.in-addr.arpa to 10.10.1.25 Reply received ok Apr 17 15:17:06.569: Kerberos: Sent TGT request to KDC Apr 17 15:17:06.769: Kerberos: Received TGT reply from KDC Apr 17 15:17:06.881: Kerberos: Received valid credential with endtime of 861232625 Apr 17 15:17:06.897: AAA/AUTHEN (1667706374): status = PASS

Exemple de sortie de débogage

Voici un utilisateur de PPP qui authentifie avec succès.

cisco5200#**debug ppp auth** Apr 17 15:47:15.285: Async6: Dialer received incoming call from <unknown> %LINK-3-UPDOWN: Interface Async6, changed state to up Apr 17 15:47:17.293: Async6: Dialer received incoming call from <unknown> Apr 17 15:47:17.909: PPP Async6: PAP receive authenticate request cisco1 Apr 17 15:47:17.913: PPP Async6: PAP authenticating peer cisco1 Apr 17 15:47:17.917: AAA/AUTHEN: create_user user='cisco1' ruser='' port='Async6' rem_addr='async/6151010' authen_TYPE=PAP service=PPP priv=1 Apr 17 15:47:17.917: AAA/AUTHEN/START (0): port='Async6' list='cisco' ACTION=LOGIN service=PPP Apr 17 15:47:17.921: AAA/AUTHEN/START (4706358): found list Apr 17 15:47:17.921: AAA/AUTHEN/START (712179591): METHOD=KRB5 Apr 17 15:47:17.929: Kerberos: Requesting TGT with expiration date of 861320837 Apr 17 15:47:17.933: Kerberos: Sending TGT request with no pre-authorization data. Apr 17 15:47:17.957: Kerberos: Sent TGT request to KDC Apr 17 15:47:18.765: Kerberos: Received TGT reply from KDC Apr 17 15:47:18.893: Kerberos: Sent TGT request to KDC Apr 17 15:47:19.097: Kerberos: Received TGT reply from KDC Apr 17 15:47:19.205: Kerberos: Received valid credential with endtime of 861234437 Apr 17 15:47:19.221: AAA/AUTHEN (712179591): status = PASS Apr 17 15:47:19.225: PPP Async6: Remote passed PAP authentication sending Auth-Ack. Apr 17 15:47:19.225: Async6: authenticated host cisco1 with no matching dialer map %LINEPROTO-5-UPDOWN: Line protocol on Interface Async6, changed state to up

Dépannez

Cette section contient de divers scénarios pour des problèmes potentiels. Ceux-ci met au point l'aide vous pour voir rapidement un problème.

Nom de royaume faux

```
cisco5200#
cisco5200#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
cisco5200(config)#kerberos local-realm junk.COM cisco5200# Apr 17 15:19:16.089: AAA/AUTHEN:
create_user user='' ruser='' port='tty51' rem_addr='12.12.109.64' authen_TYPE=ASCII
service=LOGIN priv=1 Apr 17 15:19:16.093: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
ACTION=LOGIN service=LOGIN Apr 17 15:19:16.097: AAA/AUTHEN/START (1957396): found list Apr 17
15:19:16.129: AAA/AUTHEN/START (56280416): METHOD=KRB5 Apr 17 15:19:16.129: AAA/AUTHEN
(56280416): status = GETUSER Apr 17 15:19:21.721: AAA/AUTHEN/CONT (56280416): continue_login Apr
17 15:19:21.721: AAA/AUTHEN (56280416): status = GETUSER Apr 17 15:19:21.725: AAA/AUTHEN
(56280416): METHOD=KRB5 Apr 17 15:19:21.725: AAA/AUTHEN (56280416): status = GETPASS Apr 17
15:19:26.057: AAA/AUTHEN/CONT (56280416): continue_login Apr 17 15:19:26.057: AAA/AUTHEN
(56280416): status = GETPASS Apr 17 15:19:26.061: AAA/AUTHEN (56280416): METHOD=KRB5 Apr 17
15:19:26.065: Kerberos: Requesting TGT with expiration date of 861319166 Apr 17 15:19:26.069:
Kerberos: Sending TGT request with no pre-authorization data. Apr 17 15:19:26.089: Kerberos:
Received invalid credential. ~~~~~~~~~~~~~~~~~~~ Apr 17 15:19:26.093: AAA/AUTHEN (56280416):
password incorrect Apr 17 15:19:26.097: AAA/AUTHEN (56280416): status = FAIL Apr 17
15:19:28.169: AAA/AUTHEN: free user cisco1 tty51 12.12.109.64 authen_TYPE=ASCII service=LOGIN
priv=1 Apr 17 15:19:28.173: AAA/AUTHEN: create_user user='' ruser='' port='tty51'
rem_addr='12.12.109.64' authen_TYPE=ASCII service=LOGIN priv=1 Apr 17 15:19:28.177:
AAA/AUTHEN/START (0): port='tty51' list='cisco2' ACTION=LOGIN service=LOGIN Apr 17 15:19:28.177:
AAA/AUTHEN/START (1957396): found list Apr 17 15:19:28.181: AAA/AUTHEN/START (126312328):
METHOD=KRB5 Apr 17 15:19:28.181: AAA/AUTHEN (126312328): status = GETUSER
```

Les DN ne fonctionne pas

```
Apr 10 17:22:15.370: Kerberos:  Requesting TGT with expiration date
    of 860721735
Apr 10 17:22:15.374: Kerberos:  Sending TGT request with no
pre-authorization data.
Apr 10 17:22:15.398: Kerberos:  Sent TGT request to KDC
Apr 10 17:22:16.034: Kerberos:  Received TGT reply from KDC
Apr 10 17:22:16.090: Domain: query for 245.110.10.10.in-addr.arpa
        to 255.255.255.255 Reply received empty
                                          ~~~~
```

Horloge de routeur non correcte

```
pppcisco1#
Apr 18 20:41:41.011: AAA/AUTHEN: create_user user='' ruser=''
     port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
Apr 18 20:41:41.011: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
     ACTION=LOGIN service=LOGIN
Apr 18 20:41:41.015: AAA/AUTHEN/START (1957396): found list
Apr 18 20:41:41.015: AAA/AUTHEN/START (4036314657): METHOD=KRB5
Apr 18 20:41:41.019: AAA/AUTHEN (4036314657): status = GETUSER
Apr 18 20:41:43.835: AAA/AUTHEN/CONT (4036314657): continue_login
Apr 18 20:41:43.839: AAA/AUTHEN (4036314657): status = GETUSER
Apr 18 20:41:43.839: AAA/AUTHEN (4036314657): METHOD=KRB5
Apr 18 20:41:43.843: AAA/AUTHEN (4036314657): status = GETPASS
Apr 18 20:41:48.835: AAA/AUTHEN/CONT (4036314657): continue_login
Apr 18 20:41:48.839: AAA/AUTHEN (4036314657): status = GETPASS
Apr 18 20:41:48.839: AAA/AUTHEN (4036314657): METHOD=KRB5
Apr 18 20:41:48.847: Kerberos:  Requesting TGT with expiration date
     of 861424908
Apr 18 20:41:48.851: Kerberos:  Sending TGT request with no
     pre-authorization data.
Apr 18 20:41:48.875: Kerberos:  Sent TGT request to KDC
Apr 18 20:41:49.675: Kerberos:  Received TGT reply from KDC
Apr 18 20:41:49.795: Kerberos:  Sent TGT request to KDC
Apr 18 20:41:50.119: Kerberos:  Received TGT reply from KDC
Apr 18 20:41:50.155: AAA/AUTHEN (4036314657): password incorrect
Apr 18 20:41:50.159: AAA/AUTHEN (4036314657): status = FAIL
Apr 18 20:41:52.235: AAA/AUTHEN: free user cisco1  tty51 171.68.109.64
```

```
                    authen_TYPE=ASCII service=LOGIN priv=1
Apr 18 20:41:52.239: AAA/AUTHEN: create_user user='' ruser=''
     port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
Apr 18 20:41:52.243: AAA/AUTHEN/START (0): port='tty51' list='cisco2' A
     CTION=LOGIN service=LOGIN
Apr 18 20:41:52.243: AAA/AUTHEN/START (1957396): found list
Apr 18 20:41:52.247: AAA/AUTHEN/START (1817975874): METHOD=KRB5
Apr 18 20:41:52.247: AAA/AUTHEN (1817975874): status = GETUSER
Apr 18 20:42:08.143: AAA/AUTHEN/ABORT: (1817975874) because
     Carrier dropped.
Apr 18 20:42:08.147: AAA/AUTHEN: free user   tty51 171.68.109.64
     authen_TYPE=ASCII service=LOGIN priv=1
----------------------
```

Voici ce que l'utilisateur voit :

```
$telnet 10.10.110.245 Trying 10.10.110.245 ... Connected to 10.10.110.245. Escape character is
'^]'. User Access Verification Username: cisco1 Password: Kerberos: Failed to retrieve temporary
service credentials! Kerberos: Failed to validate TGT! % Access denied Username:
```

Client pas dans la base de données Kerberos

```
Apr 18 19:04:49.983: AAA/AUTHEN: create_user user=''
     ruser='' port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
Apr 18 19:04:49.987: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
     ACTION=LOGIN service=LOGIN
Apr 18 19:04:49.987: AAA/AUTHEN/START (1957396): found list
Apr 18 19:04:49.991: AAA/AUTHEN/START (3962282505): METHOD=KRB5
Apr 18 19:04:49.995: AAA/AUTHEN (3962282505): status = GETUSER
Apr 18 19:04:53.475: AAA/AUTHEN/CONT (3962282505): continue_login
Apr 18 19:04:53.479: AAA/AUTHEN (3962282505): status = GETUSER
Apr 18 19:04:53.479: AAA/AUTHEN (3962282505): METHOD=KRB5
Apr 18 19:04:53.483: AAA/AUTHEN (3962282505): status = GETPASS
Apr 18 19:04:56.283: AAA/AUTHEN/CONT (3962282505): continue_login
Apr 18 19:04:56.283: AAA/AUTHEN (3962282505): status = GETPASS
Apr 18 19:04:56.287: AAA/AUTHEN (3962282505): METHOD=KRB5
Apr 18 19:04:56.291: Kerberos:  Requesting TGT with expiration date
     of 861419096
Apr 18 19:04:56.295: Kerberos:  Sending TGT request with no
     pre-authorization data.
Apr 18 19:04:56.323: Kerberos:  Sent TGT request to KDC
Apr 18 19:04:56.355: Kerberos:  Received TGT reply from KDC
Apr 18 19:04:56.363: Kerberos:  Client not found in Kerberos database
                                ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Apr 18 19:04:56.371: Kerberos:  Received invalid credential.
Apr 18 19:04:56.375: AAA/AUTHEN (3962282505): password incorrect
Apr 18 19:04:56.379: AAA/AUTHEN (3962282505): status = FAIL
Apr 18 19:04:58.679: AAA/AUTHEN: free user cisco3  tty51 171.68.109.64
                         authen_TYPE=ASCII service=LOGIN priv=1
Apr 18 19:04:58.687: AAA/AUTHEN: create_user user='' ruser=''
     port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
Apr 18 19:04:58.687: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
     ACTION=LOGIN service=LOGIN
Apr 18 19:04:58.691: AAA/AUTHEN/START (1957396): found list
Apr 18 19:04:58.743: AAA/AUTHEN/START (1209738018): METHOD=KRB5
Apr 18 19:04:58.747: AAA/AUTHEN (1209738018): status = GETUSER
Apr 18 19:05:04.863: AAA/AUTHEN/ABORT: (1209738018) because
     Carrier dropped.
Apr 18 19:05:04.863: AAA/AUTHEN: free user   tty51 171.68.109.64
     authen_TYPE=ASCII service=LOGIN priv=1
```

Le client est dans la base de données mais le mot de passe incorrect d'utilisations

```
Apr 18 19:06:05.427: AAA/AUTHEN: create_user user='' ruser=''
     port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
Apr 18 19:06:05.427: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
     ACTION=LOGIN service=LOGIN
Apr 18 19:06:05.431: AAA/AUTHEN/START (1957396): found list
Apr 18 19:06:05.431: AAA/AUTHEN/START (3693437965): METHOD=KRB5
Apr 18 19:06:05.435: AAA/AUTHEN (3693437965): status = GETUSER
Apr 18 19:06:07.763: AAA/AUTHEN/CONT (3693437965): continue_login
Apr 18 19:06:07.763: AAA/AUTHEN (3693437965): status = GETUSER
Apr 18 19:06:07.767: AAA/AUTHEN (3693437965): METHOD=KRB5
Apr 18 19:06:07.767: AAA/AUTHEN (3693437965): status = GETPASS
Apr 18 19:06:14.895: AAA/AUTHEN/CONT (3693437965): continue_login
Apr 18 19:06:14.899: AAA/AUTHEN (3693437965): status = GETPASS
Apr 18 19:06:14.899: AAA/AUTHEN (3693437965): METHOD=KRB5
Apr 18 19:06:14.907: Kerberos:  Requesting TGT with expiration date
     of 861419174
Apr 18 19:06:14.907: Kerberos:  Sending TGT request with no
     pre-authorization data.
Apr 18 19:06:14.935: Kerberos:  Sent TGT request to KDC
Apr 18 19:06:15.643: Kerberos:  Received TGT reply from KDC
Apr 18 19:06:15.683: Kerberos:  Received invalid credential.
Apr 18 19:06:15.687: AAA/AUTHEN (3693437965): password incorrect
                                              ~~~~~~~~~~~~~~~~~
Apr 18 19:06:15.691: AAA/AUTHEN (3693437965): status = FAIL
Apr 18 19:06:17.695: AAA/AUTHEN: free user cisco1  tty51 171.68.109.64
     authen_TYPE=ASCII service=LOGIN priv=1
Apr 18 19:06:17.699: AAA/AUTHEN: create_user user='' ruser=''
     port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
Apr 18 19:06:17.703: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
     ACTION=LOGIN service=LOGIN
Apr 18 19:06:17.703: AAA/AUTHEN/START (1957396): found list
Apr 18 19:06:17.707: AAA/AUTHEN/START (1568599595): METHOD=KRB5
Apr 18 19:06:17.707: AAA/AUTHEN (1568599595): status = GETUSER
Apr 18 19:06:22.751: AAA/AUTHEN/ABORT: (1568599595) because
     Carrier dropped.
Apr 18 19:06:22.755: AAA/AUTHEN: free user   tty51 171.68.109.64
     authen_TYPE=ASCII service=LOGIN priv=1
```

L'utilisateur voit cette sortie :

```
Trying 10.10.110.245 ...
Connected to 10.10.110.245.
Escape character is '^]'.


User Access Verification

Username: cisco1 Password: % Access denied Username:
```

Entrée SRVTAB non correcte sur le routeur

```
pppcisco1#
%SYS-5-CONFIG_I: Configured from console by vty0 (171.68.109.64)
Apr 18 19:08:55.799: AAA/AUTHEN: create_user user='' ruser=''
     port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
Apr 18 19:08:55.803: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
     ACTION=LOGIN service=LOGIN
Apr 18 19:08:55.807: AAA/AUTHEN/START (1957396): found list
Apr 18 19:08:55.807: AAA/AUTHEN/START (3369934519): METHOD=KRB5
Apr 18 19:08:55.811: AAA/AUTHEN (3369934519): status = GETUSER
Apr 18 19:08:59.011: AAA/AUTHEN/CONT (3369934519): continue_login
```

```
Apr 18 19:08:59.011: AAA/AUTHEN (3369934519): status = GETUSER
Apr 18 19:08:59.015: AAA/AUTHEN (3369934519): METHOD=KRB5
Apr 18 19:08:59.015: AAA/AUTHEN (3369934519): status = GETPASS
Apr 18 19:09:02.219: AAA/AUTHEN/CONT (3369934519): continue_login
Apr 18 19:09:02.219: AAA/AUTHEN (3369934519): status = GETPASS
Apr 18 19:09:02.223: AAA/AUTHEN (3369934519): METHOD=KRB5
Apr 18 19:09:02.231: Kerberos:  Requesting TGT with expiration date
     of 861419342
Apr 18 19:09:02.231: Kerberos:  Sending TGT request with no
     pre-authorization data.
Apr 18 19:09:02.259: Kerberos:  Sent TGT request to KDC
Apr 18 19:09:02.311: Kerberos:  Received TGT reply from KDC
Apr 18 19:09:02.435: Kerberos:  Sent TGT request to KDC
Apr 18 19:09:02.555: Kerberos:  Received TGT reply from KDC
Apr 18 19:09:02.643: AAA/AUTHEN (3369934519): password incorrect
Apr 18 19:09:02.643: AAA/AUTHEN (3369934519): status = FAIL
Apr 18 19:09:04.779: AAA/AUTHEN: free user cisco1  tty51 171.68.109.64
                     authen_TYPE=ASCII service=LOGIN priv=1
Apr 18 19:09:04.783: AAA/AUTHEN: create_user user='' ruser=''
     port='tty51' rem_addr='171.68.109.64' authen_TYPE=ASCII
     service=LOGIN priv=1
Apr 18 19:09:04.787: AAA/AUTHEN/START (0): port='tty51' list='cisco2'
     ACTION=LOGIN service=LOGIN
Apr 18 19:09:04.791: AAA/AUTHEN/START (1957396): found list
Apr 18 19:09:04.843: AAA/AUTHEN/START (2592922252): METHOD=KRB5
Apr 18 19:09:04.843: AAA/AUTHEN (2592922252): status = GETUSER
Apr 18 19:09:11.751: AAA/AUTHEN/ABORT: (2592922252) because
     Carrier dropped.
Apr 18 19:09:11.755: AAA/AUTHEN: free user   tty51 171.68.109.64
     authen_TYPE=ASCII service=LOGIN priv=1
```

Voici ce que l'utilisateur voit :

```
Trying 10.10.110.245 ...
Connected to 10.10.110.245.
Escape character is '^]'.


User Access Verification

Username: cisco1 Password: Failed to retrieve SRVTAB key! Kerberos: Failed to validate TGT! %
Access denied Username:
```

Références

1. *Le guide d'administrateur système du* Kerberos V5 (est livré dans un fichier goudronné et g-fermé la fermeture éclair)
2. *Guide d'installation du* Kerberos V5
3. *Le guide de l'utilisateur du* Kerberos V5 *UNIX*
4. Kerberos : L'authentification Protocol de réseau
5. Le service d'authentification de réseau de Kerberos (groupe de GOST USC/ISI)
6. Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller. « Kerberos : Un service d'authentification pour des systèmes de réseau ouvert », USENIX en mars 1988
7. S. P. Miller, BC Neuman, système de J.I. Schiller, et de J.H. Saltzer, « d'authentification Kerberos et d'autorisation, », 12/21/87
8. R. M. Needham et M.D. Schroeder, « utilisant le cryptage pour l'authentification dans de grands réseaux d'ordinateurs, » transmissions de l'ACM, vol. 21(12), Pp. 993-999 (décembre, 1978)
9. V. L. Voydock et S.T. Kent, « mécanismes de sécurité dans des protocoles réseau de haut

niveau, » *calculant des analyses*, vol. 15(2), ACM (juin 1983)
10. Gong de Li, « un risque de sécurité de selon les horloges synchronisées », *examen de systèmes d'exploitation*, vol. 26, #1, pp 49-53
11. C. Neuman et J. Kohl, « le service d'authentification de réseau de Kerberos (RFC 1510 de V5),", septembre 1993
12. B. Clifford Neuman et Theodore Ts'o, « Kerberos : Un service d'authentification pour des réseaux informatiques, » transmissions d'IEEE, 32(9), septembre 1994**Remarque:** Plusieurs de ces documents, cela inclut celui par Neuman, Schiller, et Steiner (#9) sont également disponible par l'intermédiaire du FTP du système MIT Athéna -- Documentation de Kerberos . Afin d'obtenir des copies des RFC, référez-vous aux RFC et aux documents obtenants de normes.

Informations connexes

- Page d'assistance de Kerberos
- Support technique - Cisco Systems