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

Contenu

Introduction

Ce document fournit un exemple de configuration, ainsi que quelques solutions à des problèmes courants. Des techniques qui vous aident à résoudre des problèmes sont également fournies dans ce document. Ce document ne traite pas de la prise en charge de Telnet par noyau.

La majeure partie de ce matériel dans cet article provient de la documentation gratuite qui est fournie avec Kerberos et de diverses foires aux questions (FAQ) disponibles sur le paquet. Les configurations provenaient d'un routeur fonctionnel et d'un serveur KDC Kerberos.

Ce document suppose que vous avez correctement compilé et installé une version actuelle de la version 5 du paquet Kerberos du MIT. Reportez-vous aux références à la fin de cet article pour plus d'informations sur la façon d'obtenir, compiler et installer Kerberos V5.

Notez également que le logiciel Cisco IOS® version 11.2 ou ultérieure est requis pour la prise en charge de Kerberos V5. Cela fournit une prise en charge complète de l'authentification du client Kerberos V, qui inclut le transfert des informations d'identification. Les systèmes disposant d'une infrastructure Kerberos V peuvent utiliser leurs centres de distribution de clés (KDC) afin d'authentifier les utilisateurs finaux pour l'accès au réseau ou au routeur. Il s'agit d'une implémentation client et non d'une implémentation KDC Kerberos.

Kerberos est considéré comme un service de sécurité hérité et est particulièrement utile dans les réseaux qui utilisent déjà Kerberos.

Reportez-vous aux notes de version du logiciel Cisco IOS version 11.2 pour plus d'informations sur les versions qui incluent cette prise en charge.

Pour la prise en charge de Kerberos dans les versions ultérieures du logiciel Cisco IOS, reportez-vous à Software Advisor (clients enregistrés uniquement).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- Logiciel Cisco IOS Version 11.2 et ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Introduction à Kerberos

Kerberos est un protocole d'authentification réseau à utiliser sur les réseaux physiquement non sécurisés. Kerberos est basé sur le modèle de distribution clé présenté par Needham et Schroeder. (Voir le numéro 9 dans la section Références de ce document. Il est conçu pour fournir une authentification forte pour les applications client/serveur en utilisant la cryptographie à clé secrète. Elle permet aux entités qui communiquent sur des réseaux de prouver leur identité l'une à l'autre tout en empêchant l'écoute électronique ou la relecture d'attaques. Il assure également l'intégrité du flux de données (détection de modifications) et le secret (prévention de la lecture non autorisée, par exemple) à l'aide de systèmes de cryptographie tels que DES.

La plupart des protocoles utilisés sur Internet ne fournissent aucune sécurité. Les outils utilisés pour « détecter » les mots de passe hors du réseau sont couramment utilisés par les pirates de

systèmes. Ainsi, les applications qui envoient un mot de passe sur le réseau non chiffré sont vulnérables. En outre, d'autres applications client/serveur s'appuient sur le programme client pour être « honnête » quant à l'identité de l'utilisateur qui l'utilise. D'autres applications s'appuient sur le client pour limiter ses activités à celles qu'il est autorisé à effectuer, sans autre application de la part du serveur.

Certains sites tentent d'utiliser des pare-feu afin de résoudre leurs problèmes de sécurité réseau. Les pare-feu supposent que « les méchants » sont à l'extérieur, ce qui est souvent une hypothèse non valide. Cependant, la majorité des incidents informatiques qui causent plus de dégâts ont été commis par des tiers. Les pare-feu présentent également un inconvénient important en ce qu'ils limitent la manière dont vos utilisateurs peuvent utiliser Internet.

Kerberos a été créé par le MIT comme solution à ces problèmes de sécurité du réseau. Le protocole Kerberos utilise une cryptographie forte, afin qu'un client puisse prouver son identité à un serveur (et vice versa) via une connexion réseau non sécurisée. Une fois qu'un client et un serveur ont utilisé Kerberos pour prouver leur identité, ils peuvent également chiffrer toutes leurs communications afin d'assurer la confidentialité et l'intégrité des données dans l'exercice de leurs activités.

Kerberos est disponible gratuitement auprès du MIT, sous réserve d'une autorisation de copyright similaire à celle utilisée pour le BSD et le système de fenêtrage X11. Le MIT fournit Kerberos sous forme source. Ceci est fait pour que quiconque souhaite l'utiliser puisse regarder le code par lui-même et s'assurer que le code est digne de confiance. En outre, pour ceux qui préfèrent se fier à un produit pris en charge par un professionnel, Kerberos est disponible en tant que produit auprès de nombreux fournisseurs différents.

Le support client Kerberos V5 est basé sur le système d'authentification Kerberos développé au MIT. Sous Kerberos, un client (généralement un utilisateur ou un service) envoie une demande de ticket au centre de distribution de clés (KDC). Le contrôleur de domaine KDC crée un ticket d'octroi de tickets (TGT) pour le client, le chiffre à l'aide du mot de passe du client en tant que clé et renvoie le TGT chiffré au client. Le client tente ensuite de déchiffrer le TGT à l’aide de son mot de passe. Si le client décrypte correctement le TGT (par exemple, si le client donne le mot de passe correct), il conserve le TGT décrypté. Ceci indique la preuve de l'identité du client.

Le TGT, qui expire à un moment donné, permet au client d'obtenir des billets supplémentaires, qui donnent l'autorisation de services spécifiques. Les demandes et les subventions de ces billets supplémentaires sont transparentes pour l'utilisateur.

Puisque Kerberos négocie authentifié, est éventuellement chiffré et communique entre deux points sur Internet, il fournit une couche de sécurité qui ne dépend pas du côté d'un pare-feu où se trouve un client. Kerberos est principalement utilisé dans les protocoles de niveau application (modèle ISO niveau 7), tels que Telnet ou FTP, afin de fournir la sécurité de l'utilisateur à l'hôte. Il est également utilisé, quoique moins fréquemment, comme système d'authentification implicite de flux de données (tel que SOCK_STREAM) ou mécanismes RPC (modèle ISO niveau 6). Il peut également être utilisé à un niveau inférieur pour la sécurité hôte-hôte, dans des protocoles tels que IP, UDP ou TCP (niveaux 3 et 4 du modèle ISO). Bien que de telles mises en oeuvre soient rares, si elles existent.

Il permet une authentification mutuelle et une communication sécurisée entre les principaux sur un réseau ouvert en fabriquant des clés secrètes pour tout demandeur. Un mécanisme permettant de propager ces clés secrètes en toute sécurité sur le réseau est également fourni. Kerberos ne prévoit pas d'autorisation ou de comptabilité. Cependant, les applications qui souhaitent utiliser leurs clés secrètes peuvent utiliser ces fonctions de manière sécurisée.

Définitions

- **Authentification** - Assurez-vous que vous êtes celui que vous déclarez être et que nous savons qui vous êtes.
- **Client** : entité pouvant obtenir un ticket. Cette entité est généralement un utilisateur ou un hôte.
- **Informations d'identification** : identique aux tickets.
- **Démon** : programme, généralement exécuté sur un hôte UNIX, qui traite les demandes d'authentification du réseau.
- **Hôte** : ordinateur accessible via un réseau.
- **Instance** : deuxième partie d'un principal Kerberos. Il fournit des informations qui qualifient le principal. L'instance peut être null. Dans le cas d'un utilisateur, l'instance est souvent utilisée pour décrire l'utilisation prévue des informations d'identification correspondantes. Dans le cas d'un hôte, l'instance est le nom d'hôte complet.
- **Kerberos** - Dans la mythologie grecque, le chien à trois têtes qui garde l'entrée du monde souterrain. Dans le monde des ordinateurs, Kerberos est un paquet de sécurité réseau développé par le MIT.
- **KDC** : centre de distribution de clés. Une machine qui émet des tickets Kerberos.
- **Keytab** : fichier de table de clés contenant une ou plusieurs clés. Un hôte ou un service utilise un fichier keytab de la même manière qu'un utilisateur utilise son mot de passe.
- **NAS** : un serveur d'accès au réseau (un boîtier Cisco) ou tout autre élément qui fait des demandes d'authentification et d'autorisation TACACS+, ou qui envoie des paquets de comptabilité.
- **Principal** : chaîne qui nomme une entité spécifique à laquelle un ensemble d'informations d'identification peut être affecté. Il comporte généralement trois parties nommées Primary, Instance et REALM.Le format type d'un principal Kerberos type est **primary/instanceREALM**.
- **Principal** : première partie d'une entité Kerberos. Dans le cas d'un utilisateur, il s'agit du nom d'utilisateur. Dans le cas d'un service, il s'agit du nom du service.
- **REALM** : réseau logique desservi par une base de données Kerberos unique et un ensemble de centres de distribution clés. Par convention, les noms de domaine sont généralement des lettres majuscules, pour différencier le domaine du domaine Internet.
- **Service** : tout programme ou ordinateur auquel vous accédez via un réseau. Voici quelques exemples de services :«host » : un hôte (par exemple, lorsque vous utilisez Telnet et rsh)«ftp »—FTP«krbtgt » : authentification ; par exemple, billet d'émission de billets«pop » : courrier électronique
- **Billet** : ensemble temporaire d'informations d'identification électroniques qui vérifient l'identité d'un client pour un service particulier.
- **TGT** : Billet d'octroi de billets. Un ticket Kerberos spécial qui permet au client d'obtenir des tickets Kerberos supplémentaires dans le même domaine Kerberos.Une bonne analogie avec le billet d'entrée est un forfait de ski de trois jours qui convient à quatre stations différentes. Vous montrez le pass à n'importe quel endroit où vous décidez d'aller (jusqu'à son expiration), et vous recevez un billet d'ascenseur pour ce resort. Une fois que vous avez le billet de remontée mécanique, vous pouvez skier tout ce que vous voulez dans cette station. Si vous allez dans un autre resort le lendemain, vous remontez votre pass et vous obtenez un billet d'ascenseur supplémentaire pour le nouveau resort. La différence est que les programmes Kerberos V5 remarquent que vous avez le forfait de ski de fin de semaine, et obtenir le billet de remontée pour vous, de sorte que vous n'avez pas à effectuer les transactions vous-même.

J'ai eu

Cette section répertorie plusieurs éléments que vous devez connaître :

- Assurez-vous de supprimer tous les espaces de fin dans les fichiers de configuration. Les espaces de fin peuvent causer des problèmes avec le serveur krb5kdc. Sinon, vous pouvez obtenir un message disant, « krb5kdc ne peut pas démarrer la base de données du domaine. »
- Assurez-vous que l'horloge du routeur est définie à la même heure que l'hôte UNIX qui exécute le serveur KDC. Afin d'empêcher les intrus de réinitialiser leurs horloges système afin de continuer à utiliser des tickets expirés, Kerberos V5 est configuré pour rejeter les requêtes de tickets de tout hôte dont l'horloge n'est pas dans la limite maximale d'horloge spécifiée du KDC (comme spécifié dans le fichier kdc.conf). De même, les hôtes sont configurés pour rejeter les réponses de tout KDC dont l'horloge n'est pas dans la plage d'horloge maximale spécifiée de l'hôte (comme spécifié dans le fichier krb5.conf). La valeur par défaut pour le décalage d'horloge maximal est de 300 secondes (cinq minutes).
- Assurez-vous que DNS fonctionne correctement. Plusieurs aspects de Kerberos reposent sur le service de noms. Pour que Kerberos puisse fournir un niveau de sécurité élevé, il est plus sensible aux problèmes de service de noms que d'autres parties de votre réseau. Il est important que vos entrées DNS (Domain Name System) et vos hôtes disposent des informations correctes. Chaque canonique du nom d'hôte doit être le nom d'hôte complet (qui inclut le domaine), et chaque adresse IP de l'hôte doit se résoudre à l'envers par le nom canonique.
- La prise en charge de Cisco IOS Kerberos V5 n'autorise pas l'utilisation de noms de domaines minuscules et le code Kerberos dans Cisco IOS n'authentifie pas les utilisateurs si le domaine est en minuscules. Ceci a été corrigé dans le logiciel Cisco IOS Version 11.2(7).Reportez-vous à l'ID de bogue Cisco CSCdj10598 (clients enregistrés uniquement).La seule solution consiste à utiliser des noms REALM majuscules (ce qui est conventionnel).Les domaines minuscules fonctionnent afin de récupérer une TGT, mais pas une identification de service. Puisque Cisco utilise son nouveau TGT afin de récupérer des informations d'identification de service (utilisées pour empêcher l'attaque d'usurpation de KDC) pendant l'authentification de journalisation, l'authentification Kerberos qui utilise des domaines en minuscules échoue toujours.
- Kerberos V5 pour PPP PAP et CHAP peuvent bloquer le routeur. Ceci a été corrigé dans le logiciel Cisco IOS Version 11.2(6).Reportez-vous à l'ID de bogue Cisco CSCdj08828 (clients enregistrés uniquement).La solution de contournement pour cela est de forcer la connexion exec au routeur via le **mode asynchrone interactif** sans **sélection automatique lors de la connexion**, puis de demander à l'utilisateur de démarrer PPP manuellement :
  ```
  aaa authentication ppp default if-needed krb5 local
  ```
- Kerberos V5 ne fait pas d'autorisation ou de comptabilité. Vous avez besoin d'un autre code pour faire ceci.

Configuration du routeur Cisco IOS

La configuration de cette section décrit un routeur AS5200 entièrement configuré qui fait partie de Kerberos V5. Le routeur dans cette configuration utilise le serveur Kerberos afin d'authentifier à la fois les sessions VTY et les utilisateurs qui se connectent pour faire PPP avec l'authentification

PAP.

Configuration AS5200 avec 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 KDC Kerberos

Assurez-vous que les ports appropriés sont configurés pour **inetd**.

Remarque : cet exemple utilise des wrappers. Si vous voulez chiffrer Telnet, vous devez remplacer le Telnet normal par le Telnet kerbérisé, de sorte que ces fichiers ont une apparence différente.

Configuration des ports pour ineted

```
# 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
-----------------------------------------------------------------
```

Configuration des fichiers de configuration Kerberos

Ensuite, vous devez configurer quelques fichiers de configuration Kerberos que le serveur KDC lit. Pour plus d'informations sur la signification de ces paramètres, reportez-vous au Guide d'installation de Kerberos ou au Guide d'administration du 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
     }
```

Configuration de la base de données pour le serveur KDC

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

1. Entrez 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:
```

Ceci est nécessaire pour récupérer le mot de passe **srvtab** à partir du routeur via TFTP avec la commande **kerberos srvtab remote**.

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

2. Afin d'ajouter des identités 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. Ajouter 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. Obtenir la liste de la base de données actuelle :

```
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 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 de la table pour le routeur 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. Reportez-vous à 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 keytab vers un emplacement où le routeur peut y accéder :

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

9. Démarrez le serveur KDC :

```
# kdc/krb5kdc
#
```

10. Vérifiez qu'il fonctionne réellement :

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

11. Forcer le routeur à lire son entrée de table clé :

```
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 vous 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 le débogage et essayez de vous connecter au 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 PPP qui s'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
```

Dépannage

Cette section contient différents scénarios de problèmes potentiels. Ces débogages vous aident à voir rapidement un problème.

Nom de domaine incorrect

```
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
```

DNS 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 du routeur incorrecte

```
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 Non 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 utilise un mot de passe incorrect

```
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 ce résultat :

```
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 incorrecte 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. *Guide de l'administrateur système* Kerberos V5 (fourni dans un fichier chiffré et compressé)
2. *Guide d'installation* de Kerberos V5
3. *Guide de l'utilisateur* Kerberos V5 *UNIX*
4. Kerberos : Le protocole d'authentification réseau
5. Le service d'authentification réseau Kerberos (groupe GOST USC/ISI)
6. Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller. "Kerberos : An Authentication Service for Open Network Systems « , USENIX mars 1988
7. S. P. Miller, B. C. Neuman, J. I. Schiller et J. H. Saltzer, « Kerberos Authentication and Authorization System », 21/12/87
8. R. M. Needham et M. D. Schröder, « Using Encryption for Authentication in Large Networks of Computers », Communications of the ACM, vol. 21(12), p. 993-999 (décembre 1978)
9. V. L. Voydock et S. T. Kent, " Security Mechanisms in High-Level Network Protocols « , *Computing Surveys*, vol. 15(2), ACM (juin 1983)
10. Li Gong, « A Security Risk of Dependent on Synchronized Clocks », *Operating Systems Review*, Vol 26, #1, p. 49 à 53
11. C. Neuman et J. Kohl, « The Kerberos Network Authentication Service (V5)« , RFC 1510, septembre 1993
12. B. Clifford Neuman et Theodore Ts'o, " Kerberos : An Authentication Service for Computer Networks, IEEE Communications, 32(9), septembre 1994**Note :** Bon nombre de ces documents, y compris celui de Neuman, Schiller et Steiner (#9), sont également disponibles par FTP à partir du système Athena du MIT — documentation de Kerberos. Pour obtenir des copies des documents RFC, reportez-vous à la section Obtention des documents RFC et des documents de normes.

Informations connexes

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