Ondersteuning van Kerberos V5-client voor probleemoplossing en -configuratie

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie, evenals een aantal oplossingen voor gemeenschappelijke problemen. Technieken die u helpen bij het oplossen van problemen worden ook in dit document gegeven. Dit document heeft geen betrekking op de ondersteuning van telnet met kerberos.

Het grootste deel van dit materiaal in dit artikel kwam van de vrij beschikbare documentatie die bij Kerberos geleverd wordt en van diverse beschikbare vaak gestelde vragen (FAQ's) op de verpakking. De configuraties kwamen van een functionele router en Kerberos KDC server.

Dit document gaat ervan uit dat u correct een huidige versie van Versie 5 van het pakket Kerberos van MIT hebt gecompileerd en geïnstalleerd. Raadpleeg de referenties aan het einde van dit

artikel voor informatie over het verkrijgen, compileren en installeren van Kerberos V5.

Let ook op dat Cisco IOS® softwarerelease 11.2 of hoger vereist is voor Kerberos V5-ondersteuning. Dit biedt volledige ondersteuning voor Kerberos V client authenticatie, hetgeen ook het doorsturen van kredieten omvat. Systemen die een Kerberos V-infrastructuur hebben kunnen hun Key Distribution Centers (KDC's) gebruiken om eindgebruikers voor netwerk- of routertoegang te authentiseren. Dit is een clientimplementatie en geen Kerberos KDC-implementatie.

Kerberos wordt beschouwd als een erfenis veiligheidsdienst en is het meest voordelig in netwerken die reeds Kerberos gebruiken.

Raadpleeg de Releaseopmerkingen van Cisco IOS-softwarerelease 11.2 voor meer informatie waarvan versies deze ondersteuning omvatten.

Raadpleeg voor Kerberos-ondersteuning in latere Cisco IOS-softwarereleases de Softwareadviseur (alleen geregistreerde klanten).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS-softwarerelease 11.2 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Inleiding tot Kerberos

Kerberos is een protocol voor netwerkverificatie voor gebruik op fysiek onveilige netwerken. Kerberos is gebaseerd op het belangrijkste distributiemodel dat door Needham en Schroeder werd gepresenteerd. (Zie nummer 9 in het gedeelte Referenties van dit document. Het is ontworpen om een sterke authenticatie te bieden voor client/server applicaties door het gebruik van geheime sleutelcryptografie. Het laat entiteiten toe die over netwerken communiceren om hun identiteit aan elkaar te bewijzen terwijl het afluisteren of opnieuw afspelen van aanvallen voorkomt. Het voorziet ook in de integriteit van gegevensstromen (zoals detectie van modificatie) en geheimhouding (zoals het voorkomen van onbevoegd lezen) met behulp van cryptografiesystemen zoals DES.

Veel van de protocollen die op het internet worden gebruikt, bieden geen beveiliging. Gereedschappen die zijn gebruikt om wachtwoorden van het netwerk te 'doorsnuiven', worden doorgaans gebruikt door systeemkrakers. Toepassingen die een wachtwoord via het netwerk niet versleuteld, zijn dus kwetsbaar. Andere client/server applicaties vertrouwen erop dat het clientprogramma "eerlijk" is over de identiteit van de gebruiker die het gebruikt. Andere toepassingen steunen op de cliënt om zijn activiteiten te beperken tot die welke het mag doen, zonder andere controle door de server.

Sommige sites proberen firewalls te gebruiken om hun problemen met de netwerkbeveiliging op te lossen. Firewalls gaan ervan uit dat de "slechteriken" aan de buitenkant zijn, wat vaak een ongeldige veronderstelling is. Maar de meeste computerincidenten die meer schade veroorzaken, zijn wel uitgevoerd door insiders. Firewalls hebben ook een groot nadeel omdat ze de manier waarop uw gebruikers het internet kunnen gebruiken beperken.

Kerberos werd door het MIT gecreëerd als oplossing voor deze problemen op het gebied van netwerkbeveiliging. Het protocol van Kerberos gebruikt sterke cryptografie, zodat een cliënt zijn identiteit aan een server (en omgekeerd) over een onveilige netwerkverbinding kan bewijzen. Nadat een client en server Kerberos heeft gebruikt om hun identiteit aan te tonen, kunnen zij al hun communicatie ook versleutelen om de privacy en de gegevensintegriteit te garanderen terwijl ze hun bedrijf voortzetten.

Kerberos is vrij beschikbaar bij MIT, onder een copyrightvermelding die lijkt op de mededeling die gebruikt wordt voor het BSD-systeem en het X11-Windows-systeem. MIT biedt Kerberos in bronvorm. Dit gebeurt zodat iedereen die het wil gebruiken, de code zelf kan bekijken en zichzelf kan verzekeren dat de code betrouwbaar is. Bovendien is Kerberos, voor degenen die liever op een professioneel ondersteund product vertrouwen, verkrijgbaar als product van vele verschillende verkopers.

Ondersteuning van Kerberos V5-clients is gebaseerd op het bij MIT ontwikkelde Kerberos-detectiesysteem. Onder Kerberos stuurt een klant (over het algemeen een gebruiker of een service) een aanvraag voor een ticket naar het Key Distribution Center (KDC). De KDC creëert een ticket voor het toekennen van een ticket (TGT) voor de client, versleutelt het met de hulp van het wachtwoord van de client als de sleutel en stuurt de gecodeerde TGT terug naar de client. De client probeert de TGT te decrypteren met behulp van zijn wachtwoord. Als de client de TGT bijvoorbeeld decrypteert (als de client het juiste wachtwoord geeft), houdt deze de gedecrypteerde TGT in. Dit geeft het bewijs van de identiteit van de cliënt aan.

De TGT, die op een bepaald tijdstip afloopt, staat de klant toe extra tickets te verkrijgen, die toestemming geven voor specifieke diensten. De verzoeken en subsidies van deze aanvullende tickets zijn transparant voor de gebruiker.

Omdat Kerberos geauthentiseerd onderhandelt, naar keuze gecodeerd is en tussen om het even welke twee punten op het internet communiceert, verstrekt het een laag van veiligheid die niet afhankelijk is van welke kant van een firewall of een client gelegen is. Kerberos wordt hoofdzakelijk gebruikt in toepassing-level protocollen (ISO model Level 7), zoals telnet of FTP, om gebruiker te voorzien van veiligheid. Het wordt ook, zij het minder vaak, gebruikt als het impliciete authenticatiesysteem van gegevensstromen (zoals SOCK_STREAM) of RPC - mechanismen (ISO - model Niveau 6). Het kan ook op een lager niveau voor host-to-host beveiliging worden gebruikt, in protocollen zoals IP, UDP of TCP (ISO-modelniveaus 3 en 4). Hoewel dergelijke implementaties zeldzaam zijn, als ze überhaupt bestaan.

Het voorziet in wederzijdse authenticatie en veilige communicatie tussen hoofden op een open netwerk door de productie van geheime sleutels voor elke aanvrager. Er wordt ook voorzien in een

mechanisme om deze geheime sleutels veilig door het netwerk te laten verspreiden. Kerberos voorziet niet in een vergunning of een boekhouding. Toepassingen die hun geheime toetsen willen gebruiken om die functies veilig te kunnen uitvoeren.

Definities

- **Verificatie** - Zorg ervoor dat je bent wie je zegt dat je bent, en dat we weten wie je bent.
- **client**-Een entiteit die een ticket kan verkrijgen. Deze entiteit is meestal een gebruiker of een host.
- **Credentials**, hetzelfde als tickets.
- **Daemon**-A programma, meestal één dat op een UNIX-host draait, dat het servicenetwerk om authenticatie vraagt.
- **Host**-A computer die via een netwerk toegankelijk is.
- **Instantie**-het tweede deel van een Kerberos-directeur. Het geeft informatie die geschikt is voor de primaire. De instantie kan ongeldig zijn. In het geval van een gebruiker wordt de instantie vaak gebruikt om het beoogde gebruik van de overeenkomstige geloofsbrieven te beschrijven. In het geval van een host is de instantie de volledig gekwalificeerde hostname.
- **Kerberos** - In de Griekse mythologie, de driekoppige hond die de ingang naar de onderwereld bewaken. In de wereld van computers is Kerberos een pakket voor netwerkbeveiliging dat bij MIT is ontwikkeld.
- **KDC**—Key Distribution Center. Een machine die Kerberos tickets geeft.
- **sleuteltabblad** - Een belangrijk tabelbestand met een of meer toetsen. Een host of service gebruikt een sleuteltabbestand op dezelfde manier als een gebruiker gebruikt zijn wachtwoord.
- **NAS**-A Network Access Server (een Cisco-vakje) of iets anders dat TACACS+ verificatie- en autorisatieverzoeken maakt of accounting pakketten verstuurt.
- **Principal**-A string die een specifieke entiteit aanduidt waaraan een reeks aanmeldingsgegevens kan worden toegewezen. Het heeft over het algemeen drie delen die Primair, Instantie, en REALM heten.Het typische formaat van een typische Kerberos-opdrachtgever is **primair/instantieREALM**.
- **Primair**-het eerste deel van een Kerberos-directeur. Bij een gebruiker is het de gebruikersnaam. In het geval van een dienst is het de naam van de dienst.
- **REALM**-Het logische netwerk dat door één enkel Kerberos gegevensbestand en een reeks Belangrijkste Verdelingscentra wordt gediend. Bij conventie zijn realm-namen meestal alle hoofdletters, om het gebied te onderscheiden van het internet-domein.
- **Service**: elk programma of computer waartoe u via een netwerk toegang hebt. Voorbeelden van diensten zijn:"host"-een host (bijvoorbeeld wanneer u Telnet en rsh gebruikt)FTP"kroon"—authenticatie; zoals ticket"pop"-e-mail
- Een tijdelijke reeks elektronische geloofsbrieven die de identiteit van een cliënt voor een bepaalde dienst verifiëren.
- **TGT**—Ticket voor het geven van vergunningen. Een speciaal Kerberos-ticket waarmee de client binnen hetzelfde Kerberos-gebied extra Kerberos-tickets kan verkrijgen.Een goede analogie voor het ticket dat de tickets geeft is een skipasje van drie dagen dat goed is in vier verschillende vakanties. U laat de pas zien in welk middel u ook beslist om naar te gaan (tot die verstrijkt), en u ontvangt een lift voor dat hotel. Als je eenmaal de lift hebt, kun je in dat resort alles skiën wat je wilt. Als je de volgende dag naar een ander middel gaat, laat je je pas weer zien, en dan krijg je een extra lift voor de nieuwe vakantie. Het verschil is dat de Kerberos V5-programma's opmerken dat je het weekend skypas hebt en het lift-ticket voor je

hebt, dus je hoeft de transacties niet zelf uit te voeren.

Gotcha

In deze sectie worden een aantal items opgesomd waarvan u op de hoogte moet zijn:

- Zorg ervoor dat u alle resterende ruimtes in de configuratiebestanden verwijdert. Trainingsruimtes kunnen problemen met de krb5kdc server veroorzaken. Anders krijg je een bericht dat zegt: "krb5kdc kan de database voor het domein niet starten."
- Zorg ervoor dat de kloktijd op de router op hetzelfde tijdstip is ingesteld als de UNIX-host waarop de KDC-server wordt uitgevoerd. Om te voorkomen dat indringers hun systeemklokken opnieuw instellen om verlopen tickets te blijven gebruiken, is Kerberos V5 ingesteld om kaartverzoeken af te wijzen van elke host waarvan de klok niet binnen de gespecificeerde maximale klokscheefheid van de KDC (zoals gespecificeerd in het kdc.conf-bestand) valt. Op dezelfde manier zijn hosts ingesteld om reacties van iedere KDC af te wijzen, wiens kloktijd niet binnen de opgegeven maximale klokscheefheid van de host valt (zoals aangegeven in het krb5.conf-bestand). De standaardwaarde voor een maximale klokscheefheid is 300 seconden (vijf minuten).
- Controleer of de DNS correct werkt. Verscheidene aspecten van Kerberos zijn afhankelijk van de naamdienst. Om Kerberos zijn hoog niveau van veiligheid te bieden, is het gevoeliger om dienstenproblemen te noemen dan sommige andere delen van uw netwerk. Het is belangrijk dat uw DNS-items (Domain Name System) en uw hosts de juiste informatie hebben. Elke canonical van de host-naam moet de volledig-gekwalificeerde host-naam zijn (die het domein omvat), en elk IP-adres van de host moet de canonische naam omgekeerd oplossen.
- Cisco IOS Kerberos V5-ondersteuning staat het gebruik van kleine veldnamen niet toe en de Kerberos-code in Cisco IOS authenticeert gebruikers niet als het gebied in kleine letters is. Dit is vastgesteld in Cisco IOS-softwarerelease 11.2(7)ST.Raadpleeg Cisco bug-ID CSCdj10598 (alleen geregistreerde klanten).Het enige alternatief is om hoofdletters REALM-namen te gebruiken (wat conventioneel is).De kleine gebieden werken om een TGT terug te krijgen, maar geen service gecrediteerd. Aangezien Cisco hun nieuwe TGT gebruikt om een servicekrediet terug te krijgen (gebruikt om de KDC-tapingsaanval te voorkomen) tijdens de houtkapverificatie, mislukt Kerberos-verificatie die lagere case-realms gebruikt altijd.
- Kerberos V5 voor PPP PAP en CHAP kunnen de router crashen. Dit is vastgesteld in Cisco IOS-softwarerelease 11.2(6)E.Raadpleeg Cisco bug-ID CSCdj0828 (alleen geregistreerde klanten).Het alternatief is om extra inloggen in de router te forceren via **asynchrone modus interactief** zonder **automatische selectie tijdens-inloggen** en vervolgens handmatig de gebruiker start PPP:
  ```
  aaa authentication ppp default if-needed krb5 local
  ```
- Kerberos V5 verleent geen vergunning noch administratieve verantwoording. Je hebt nog een code nodig om dit te doen.

Cisco IOS-routerconfiguratie

De configuratie in deze sectie toont een volledig gevormd router AS5200 die Kerberos V5 doet. De router in deze configuratie gebruikt de server Kerberos om zowel VTY sessies als gebruikers te authentiseren die binnen om PPP met PAP authenticatie te doen draaien.

AS5200 configuratie met 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
```

Configuratie van Kerberos KDC

Zorg ervoor dat u de juiste poorten voor **internet** hebt ingesteld.

Opmerking: Dit voorbeeld gebruikt pakjes. Als u gecodeerd telnet wilt, moet u het normale telnet met het kerberichte telnet vervangen, zodat deze bestanden een andere verschijning hebben.

Instellen poorten voor internet

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

Configuratie-bestanden van Kerberos instellen

Vervolgens moet u een paar Kerberos-configuratiebestanden instellen die de KDC-server leest. Raadpleeg voor meer informatie over de betekenis van deze parameters de Kerberos Install Guide of de System Admin Guide .

```
# 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
     }
```

Stel de database voor de KDC-server in

Daarna moet je de database maken die de KDC server gebruikt.

1. Typ de opdracht **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:
```

Dit is nodig om het wachtwoord **van de srvtab** uit de router via TFTP op te halen met de **afstandsbediening** van **kerberos srvtab**.

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

2. Om hoofden en gebruikers aan de database toe te voegen, gebruikt u de opdracht **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. Voeg een gebruiker toe:

```
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. Ontvang een lijst van de huidige database:

```
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. Voeg de ingang voor de router van Cisco toe:

```
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. Haal een sleutel tot de tabel voor de Cisco-router uit:

```
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. Kijk nog eens naar de database:

```
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. Verplaats het bestand van het sleuteltabblad naar een plaats waar de router het kan benaderen:

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

9. Start de KDC-server:

```
# kdc/krb5kdc
#
```

10. Controleer of deze ook echt draait:

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

11. Dwing de router om zijn belangrijkste tabelingang te lezen:

```
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. Controleer de router om er zeker van te zijn dat alles klaar is:

```
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. Zet de debugging aan en probeer in de router te loggen:

```
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
```

Voorbeeld van output van foutopsporing

Hier is een PPP-gebruiker die authenticeert.

```
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
```

Problemen oplossen

Deze paragraaf bevat verschillende scenario's voor mogelijke problemen. Deze debugs helpen je om snel een probleem te zien.

Fout bij registreren naam

```
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 werkt niet

```
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
                                        ~~~~
```

Routerklok niet corrigeren

```
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
----------------------
```

Dit is wat de gebruiker ziet:

```
$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 niet in Kerberos Database

```
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
```

Cliënt is in databank maar gebruikt onjuist wachtwoord

```
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
```

De gebruiker ziet deze uitvoer:

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


User Access Verification

Username: cisco1
Password:
% Access denied

Username:
```

SRVTAB-ingang niet gecorrigeerd op router

```
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
```

Dit is wat de gebruiker ziet:

```
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:
```

Referenties

1. *Systeembeheerdershandleiding* van Kerberos V5 (bevindt zich in een geaard, zipt bestand)
2. Kerberos V5-*installatiehandleiding*
3. Gebruikershandleiding Kerberos V5 *UNIX*
4. Kerberos: Het netwerkverificatieprotocol
5. De Kerberos-netwerkverificatieservice (UCS/ISI's GOST-groep)
6. Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller. "Kerberos: An Authentication Service for Open Network Systems ", USENIX maart 1988
7. S. P. Miller, B. C. Neuman, J. I. Schiller, en J. H. Saltzer, "Kerberos Authentication and Authorization System", 12/21/87
8. R. M. Needham en M. D. Schroeder, "Use Encryption for Authentication in Large Networks of Computers," Communications of the ACM, Vol. 21(12), blz. 993-999 (december, 1978)
9. V.L. Voydock en S.T. Kent, "Security Mechanisms in High-Level Network Protocols," *Computing Surveys*, Vol. 15(2), ACM (juni 1983)
10. Li Gong, "A Security Risk of Afhankelijk of Synchronized Clock", *Operating Systems Review*, VOL 26, #1, pp 49-53
11. C. Neuman en J. Kohl, "The Kerberos Network Authentication Service (V5)," RFC 1510, september 1993
12. B. Clifford Neuman en Theodore Ts'o, "Kerberos: Een verificatieservice voor computernetwerken," IEEE Communications, 32(9), september 1994**Opmerking:** Veel van deze documenten, waaronder die van Neuman, Schiller en Steiner (#9), zijn ook via FTP beschikbaar bij MIT Athena System — Kerberos Documentation . Raadpleeg voor het verkrijgen van kopieën van RFC's de Verzamelde RFC's en Standards Documents.

Gerelateerde informatie

- Categoriepagina voor Kerberos-ondersteuning
- Technische ondersteuning - Cisco-systemen