Fehlerbehebung und Konfiguration des Kerberos V5 Client-Supports

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration sowie einige Lösungen für häufige Probleme. In diesem Dokument finden Sie auch Verfahren, die Ihnen bei der Fehlerbehebung helfen. Dieses Dokument behandelt nicht die kerberisierte Telnet-Unterstützung.

Die meisten dieser Materialien in diesem Artikel stammen aus der kostenlos verfügbaren Dokumentation, die Kerberos beiliegt, und aus verschiedenen verfügbaren häufig gestellten Fragen (FAQs) zum Paket. Die Konfigurationen stammen von einem funktionierenden Router und einem Kerberos KDC-Server.

In diesem Dokument wird davon ausgegangen, dass Sie eine aktuelle Version 5 des Kerberos-Pakets vom MIT korrekt kompiliert und installiert haben. Informationen zum Abrufen, Kompilieren

und Installieren von Kerberos V5 finden Sie in den Referenzen am Ende dieses Artikels.

Beachten Sie außerdem, dass die Kerberos V5-Unterstützung Cisco IOS® Softwareversion 11.2 oder höher erfordert. Dies bietet volle Unterstützung für die Kerberos V Client-Authentifizierung, die auch die Weiterleitung von Anmeldeinformationen beinhaltet. Systeme mit Kerberos V-Infrastruktur können ihre Key Distribution Center (KDCs) verwenden, um Endbenutzer für den Netzwerk- oder Router-Zugriff zu authentifizieren. Dies ist eine Client-Implementierung und keine Kerberos KDC-Implementierung.

Kerberos gilt als veralteter Sicherheitsservice und ist besonders in Netzwerken von Vorteil, die bereits Kerberos verwenden.

In den Versionshinweisen zur Cisco IOS Software 11.2 finden Sie weitere Informationen zu den Versionen, die diese Unterstützung enthalten.

Informationen zur Kerberos-Unterstützung in späteren Versionen der Cisco IOS Software finden Sie im Software Advisor (nur registrierte Kunden).

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS Software, Version 11.2 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Einführung in Kerberos

Kerberos ist ein Netzwerkauthentifizierungsprotokoll für physisch unsichere Netzwerke. Kerberos basiert auf dem von Needham und Schröder vorgestellten zentralen Vertriebsmodell. (Siehe Nummer 9 im Abschnitt Referenzen dieses Dokuments. Es wurde entwickelt, um eine starke Authentifizierung für Client-/Serveranwendungen durch Verwendung von geheimer Verschlüsselung bereitzustellen. Sie ermöglicht es Einheiten, die über Netzwerke kommunizieren, ihre Identität untereinander nachzuweisen und verhindert gleichzeitig das Abhören oder Wiederholen von Angriffen. Darüber hinaus wird mithilfe von Kryptografiesystemen wie DES die

Integrität des Datenstroms (z. B. die Erkennung von Änderungen) und die Geheimhaltung (z. B. die Verhinderung unbefugter Lesevorgänge) gewährleistet.

Viele der im Internet verwendeten Protokolle bieten keine Sicherheit. Tools, mit denen Kennwörter aus dem Netzwerk "gesnickt" werden, werden häufig von Systemknackern verwendet. Daher sind Anwendungen, die ein Kennwort unverschlüsselt über das Netzwerk senden, angreifbar. Andere Client-/Serveranwendungen verlassen sich darauf, dass das Clientprogramm "ehrlich" über die Identität des Benutzers ist, der es verwendet. Andere Anwendungen verlassen sich darauf, dass der Client seine Aktivitäten auf die Aktivitäten beschränkt, die ihm erlaubt sind, ohne dass der Server eine andere Durchsetzung durchführt.

Einige Standorte versuchen, ihre Sicherheitsprobleme mithilfe von Firewalls zu beheben. Firewalls gehen davon aus, dass "die Bösewichte" draußen sind, was oft eine ungültige Annahme ist. Die meisten Computerkriminalvorfälle, die mehr Schaden verursachen, wurden jedoch von Insidern durchgeführt. Firewalls haben auch einen erheblichen Nachteil, da sie die Nutzung des Internets durch Ihre Benutzer einschränken.

Kerberos wurde vom MIT als Lösung für diese Netzwerksicherheitsprobleme entwickelt. Das Kerberos-Protokoll verwendet eine starke Verschlüsselung, sodass ein Client seine Identität einem Server (und umgekehrt) über eine unsichere Netzwerkverbindung nachweisen kann. Nachdem ein Client und Server Kerberos zum Nachweis seiner Identität verwendet hat, können sie auch alle ihre Kommunikation verschlüsseln, um die Privatsphäre und Datenintegrität während der Geschäftsaktivitäten zu gewährleisten.

Kerberos ist vom MIT unter einem Urheberrechtshinweis frei erhältlich, der dem für das BSD-Betriebssystem und das X11-Windows-System verwendeten ähnelt. MIT stellt Kerberos als Quellcode zur Verfügung. Dies geschieht, damit jeder, der es verwenden möchte, den Code selbst übersehen und sich versichern kann, dass der Code vertrauenswürdig ist. Für diejenigen, die lieber auf ein professionell unterstütztes Produkt setzen möchten, ist Kerberos zudem als Produkt von vielen verschiedenen Anbietern erhältlich.

Kerberos V5 Client Support basiert auf dem Kerberos Authentifizierungssystem, das am MIT entwickelt wurde. Unter Kerberos sendet ein Client (in der Regel ein Benutzer oder ein Service) eine Ticket-Anfrage an das Key Distribution Center (KDC). Der KDC erstellt ein Ticket zur Ticketgewährung (TGT) für den Client, verschlüsselt es mithilfe des Passworts des Clients als Schlüssel und sendet das verschlüsselte TGT zurück an den Client. Der Client versucht dann mithilfe seines Kennworts, das TGT zu entschlüsseln. Wenn der Client z. B. das TGT erfolgreich entschlüsselt, wenn der Client das richtige Kennwort vorgibt), behält er das entschlüsselte TGT bei. Dies weist auf die Identität des Clients hin.

Das TGT, das zu einem bestimmten Zeitpunkt abläuft, ermöglicht es dem Client, zusätzliche Tickets zu erhalten, die die Berechtigung für bestimmte Dienste erteilen. Die Anfragen und Zuwendungen dieser zusätzlichen Tickets sind benutzertransparent.

Da Kerberos authentifiziert aushandelt, optional verschlüsselt ist und zwischen zwei beliebigen Punkten im Internet kommuniziert, bietet es eine Sicherheitsebene, die nicht davon abhängig ist, auf welcher Seite einer Firewall sich der Client befindet. Kerberos wird hauptsächlich in Protokollen auf Anwendungsebene (ISO-Modell Level 7), wie Telnet oder FTP, verwendet, um die Sicherheit für den Benutzer zu gewährleisten. Es wird auch, wenn auch weniger häufig, als das implizite Authentifizierungssystem von Datenstrom (wie SOCK_STREAM) oder RPC Mechanismen (ISO-Modell Level 6). Sie kann auch auf einer niedrigeren Ebene für die Sicherheit von Host zu Host in Protokollen wie IP, UDP oder TCP (ISO-Modell Level 3 und 4) verwendet werden. Obwohl solche Implementierungen selten sind, wenn überhaupt vorhanden.

Sie ermöglicht die gegenseitige Authentifizierung und sichere Kommunikation zwischen Auftraggebern in einem offenen Netzwerk durch die Herstellung von geheimen Schlüsseln für jeden Antragsteller. Es wird auch ein Mechanismus bereitgestellt, mit dem diese geheimen Schlüssel sicher über das Netzwerk verteilt werden können. Kerberos bietet keine Autorisierung oder Buchhaltung. Anwendungen, die ihre geheimen Schlüssel verwenden möchten, können diese Funktionen jedoch sicher ausführen.

Definitionen

- **Authentifizierung**: Vergewissern Sie sich, dass Sie der sind, der Sie sagen, dass Sie sind, und dass wir wissen, wer Sie sind.
- **Client**: Eine Einheit, die ein Ticket abrufen kann. Diese Entität ist normalerweise entweder ein Benutzer oder ein Host.
- **Anmeldeinformationen** - Entspricht Tickets.
- **Daemon** - Ein Programm, das normalerweise auf einem UNIX-Host ausgeführt wird und das das Netzwerk nach Authentifizierung fragt.
- **Host** - Ein Computer, auf den über ein Netzwerk zugegriffen werden kann.
- **Instanz** - Der zweite Teil eines Kerberos-Prinzips. Sie liefert Informationen, die die Primär-Qualifikation ausmachen. Die Instanz kann NULL sein. Im Fall eines Benutzers wird die Instanz häufig verwendet, um die beabsichtigte Verwendung der entsprechenden Anmeldeinformationen zu beschreiben. Bei einem Host ist die Instanz der vollqualifizierte Hostname.
- **Kerberos** - In der griechischen Mythologie, der dreiteilige Hund, der den Eingang in die Unterwelt bewacht. In der Welt der Computer ist Kerberos ein Netzwerksicherheitspaket, das am MIT entwickelt wurde.
- **KDC** - Zentrales Distribution Center. Eine Maschine, die Kerberos-Tickets ausstellt.
- **Keytab** - Eine Schlüsseltabelldatei, die mindestens eine Taste enthält. Ein Host oder Dienst verwendet eine Schlüsselregisterdatei auf die gleiche Weise wie ein Benutzer sein Kennwort verwendet.
- **NAS**: Ein Netzwerkzugriffsserver (eine Cisco Box) oder alles andere, was TACACS+-Authentifizierungs- und Autorisierungsanfragen ausführt oder Accounting-Pakete sendet.
- **Principal** (Prinzip): Eine Zeichenfolge, die eine bestimmte Entität benennt, der eine Gruppe von Anmeldeinformationen zugewiesen werden kann. Er besteht in der Regel aus drei Teilen mit dem Namen Primär, Instanz und REALM.Das typische Format eines typischen Kerberos-Prinzips ist **Primary/InstanceREALM**.
- **Primary (Primär)**: Der erste Teil eines Kerberos-Prinzips. Bei einem Benutzer ist dies der Benutzername. Bei einem Dienst ist dies der Name des Dienstes.
- **REALM** (**REALM**): Das logische Netzwerk, das von einer einzelnen Kerberos-Datenbank und einer Reihe von Key Distribution Centern bedient wird. Nach der Konvention sind Bereichsnamen in der Regel alle Großbuchstaben, um den Bereich von der Internet-Domäne zu unterscheiden.
- **Service** - Jedes Programm oder jeder Computer, auf den Sie über ein Netzwerk zugreifen. Beispiele für Services:"Host" - ein Host (z. B. wenn Sie Telnet und rsh verwenden)"ftp" - FTP"krbtgt" - Authentifizierung; z. B. Ticket-ErteilungPop - E-Mail
- **Ticket** - Ein temporärer Satz elektronischer Anmeldeinformationen, der die Identität eines Clients für einen bestimmten Dienst überprüft.
- **TGT** - Ticket-Gewährung. Ein spezielles Kerberos Ticket, mit dem der Client zusätzliche Kerberos-Tickets im selben Kerberos-Bereich erhalten kann.Eine gute Analogie zum Ticket-

Ticket ist ein 3-Tage-Skipass, der in vier verschiedenen Resorts gut ist. Sie zeigen den Pass an, in welchem Resort Sie sich entscheiden (bis er abläuft), und Sie erhalten ein Lift Ticket für diesen Resort. Sobald Sie die Liftkarte haben, können Sie in diesem Skigebiet alles Ski fahren, was Sie wollen. Wenn Sie am nächsten Tag in ein anderes Resort fahren, zeigen Sie erneut Ihren Pass, und Sie erhalten eine zusätzliche Fahrkarte für das neue Resort. Der Unterschied ist, dass die Kerberos V5 Programme bemerken, dass Sie den Wochenendskipass haben und Sie das Lift Ticket für Sie bekommen, sodass Sie die Transaktionen nicht selbst durchführen müssen.

Gotcha

In diesem Abschnitt sind mehrere Elemente aufgeführt, die Sie beachten müssen:

- Stellen Sie sicher, dass Sie alle Leerzeichen in den Konfigurationsdateien entfernen. Leerzeichen können Probleme mit dem krb5kdc Server verursachen. Andernfalls erhalten Sie die Meldung "krb5kdc kann die Datenbank für den Bereich nicht starten."
- Stellen Sie sicher, dass die Uhr am Router auf die Uhrzeit des UNIX-Hosts eingestellt ist, der den KDC-Server ausführt. Um zu verhindern, dass Eindringlinge ihre Systemuhren zurücksetzen, um weiterhin abgelaufene Tickets zu verwenden, ist Kerberos V5 so eingerichtet, dass Ticket-Anfragen von einem Host abgelehnt werden, dessen Uhr nicht innerhalb der angegebenen maximalen Taktverzerrung des KDC liegt (wie in der Datei kdc.conf angegeben). Ebenso werden Hosts so konfiguriert, dass sie Antworten von einem KDC ablehnen, dessen Uhrzeit nicht innerhalb der angegebenen maximalen Taktverzerrung des Hosts liegt (wie in der Datei krb5.conf angegeben). Der Standardwert für maximale Zeitdifferenz beträgt 300 Sekunden (fünf Minuten).
- Stellen Sie sicher, dass DNS ordnungsgemäß funktioniert. Einige Aspekte von Kerberos basieren auf Namensdienst. Damit Kerberos ein hohes Maß an Sicherheit bieten kann, ist es empfindlicher auf Serviceprobleme als andere Teile Ihres Netzwerks. Es ist wichtig, dass Ihre DNS-Einträge (Domain Name System) und Ihre Hosts die richtigen Informationen haben. Bei jedem Canonical des Hostnamens muss es sich um den vollqualifizierten Hostnamen (der die Domäne enthält) handeln, und jede IP-Adresse des Hosts muss zum kanonischen Namen zurückaufgelöst werden.
- Die Unterstützung von Cisco IOS Kerberos V5 erlaubt keine Verwendung von Kleinbuchstaben-Namen, und der Kerberos-Code im Cisco IOS authentifiziert Benutzer nicht, wenn der Bereich in Kleinbuchstaben angegeben ist. Dies wurde in Version 11.2(7) der Cisco IOS-Software behoben.Weitere Informationen finden Sie unter Cisco Bug ID CSCdj10598 (nur registrierte Kunden).Die einzige Problemumgehung besteht in der Verwendung von großgeschriebenen REALM-Namen (die konventionell ist).Die Kleinrealms können verwendet werden, um einen TGT abzurufen, aber keine Servicebeschreibung. Da Cisco sein neues TGT verwendet, um eine Service-Anmeldeinformationen abzurufen (um den KDC-Spoofing-Angriff zu verhindern), während die Authentifizierung protokolliert wird, schlägt die Kerberos-Authentifizierung, die Kleinrealms verwendet, immer fehl.
- Kerberos V5 für PPP PAP und CHAP kann zum Absturz des Routers führen. Dies wurde in Version 11.2(6) der Cisco IOS-Software behoben.Weitere Informationen finden Sie unter Cisco Bug ID CSCdj08828 (nur registrierte Kunden).Die Problemumgehung hierfür besteht darin, die exec-Anmeldung beim Router im **async-Modus** zu erzwingen, ohne **bei der Anmeldung automatisch** die **Auswahl** zu **treffen**, und den Benutzer dann dazu zu veranlassen,

PPP manuell zu starten:
`aaa authentication ppp default if-needed krb5 local`

- Kerberos V5 hat keine Autorisierung oder Buchhaltung. Dazu benötigen Sie noch einen anderen Code.

Konfiguration des Cisco IOS Routers

Die Konfiguration in diesem Abschnitt zeigt einen vollständig konfigurierten AS5200-Router mit Kerberos V5. Der Router in dieser Konfiguration verwendet den Kerberos-Server, um sowohl VTY-Sitzungen als auch Benutzer zu authentifizieren, die sich für PPP mit PAP-Authentifizierung einwählen.

AS5200-Konfiguration mit 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
```

Kerberos KDC-Konfiguration

Stellen Sie sicher, dass Sie die richtigen Ports für **Inetd** eingerichtet haben.

Hinweis: In diesem Beispiel werden Wrapper verwendet. Wenn Sie verschlüsseltes Telnet benötigen, müssen Sie das normale Telnet durch das kerberisierte Telnet ersetzen, sodass diese Dateien ein anderes Erscheinungsbild haben.

Einrichten von Ports für beabsichtigte Verbindungen

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

Einrichten von Kerberos-Konfigurationsdateien

Als Nächstes müssen Sie einige Kerberos-Konfigurationsdateien einrichten, die der KDC-Server liest. Weitere Informationen zu diesen Parametern finden Sie im Kerberos-Installationsleitfaden oder im System-Administratorhandbuch .

```
# 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
     }
```

Einrichten der Datenbank für den KDC-Server

Als Nächstes müssen Sie die Datenbank erstellen, die der KDC-Server verwendet.

1. Geben Sie den Befehl **kdb5_util ein**:

```
# 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:
```

   Dies ist erforderlich, um das **srvtab**-Passwort über TFTP mit dem **Kerberos srvtab Remote**-Befehl vom Router abzurufen.

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

2. Um der Datenbank Prinzipale und Benutzer hinzuzufügen, verwenden Sie den Befehl **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. Benutzer hinzufügen:

```
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. Abrufen einer Liste der aktuellen Datenbank:

```
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. Fügen Sie den Eintrag für den Cisco Router hinzu:

```
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. Extrahieren Sie einen Schlüssel in die Tabelle für den Cisco Router:

```
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. Sehen Sie sich die Datenbank noch einmal an:

```
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. Verschieben Sie die Schlüsselregisterdatei an eine Stelle, an die der Router zugreifen kann:

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

9. Starten Sie den KDC-Server:

```
# kdc/krb5kdc
#
```

10. Stellen Sie sicher, dass die Funktion tatsächlich ausgeführt wird:

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

11. Erzwingen Sie den Router, seinen Schlüsseltabelleneintrag zu lesen:

```
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. Überprüfen Sie den Router, um sicherzustellen, dass alles bereit ist:

```
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. Aktivieren Sie das Debuggen, und versuchen Sie, sich beim Router anzumelden:

```
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
```

Beispielausgabe für Debugging

Hier ist ein PPP-Benutzer, der sich erfolgreich authentifiziert.

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält verschiedene Szenarien für potenzielle Probleme. Diese Debugger helfen Ihnen, ein Problem schnell zu erkennen.

Falscher Bereichsname

```
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 funktioniert nicht

```
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
                                          ~~~~
```

Router-Uhr nicht korrekt

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

Der Benutzer sieht Folgendes:

```
$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 nicht in Kerberos-Datenbank

```
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
```

Der Client ist in der Datenbank, verwendet jedoch ein falsches Kennwort.

```
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
```

Der Benutzer sieht diese Ausgabe:

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


User Access Verification

Username: cisco1
Password:
% Access denied

Username:
```

SRVTAB-Eintrag auf Router nicht korrekt

```
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
```

Der Benutzer sieht Folgendes:

```
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:
```

Referenzen

1. Kerberos V5 *Handbuch für Systemadministratoren* (im Lieferumfang einer gezippten Datei enthalten)
2. Kerberos V5 *Installationshandbuch*
3. Kerberos V5 *UNIX - Benutzerhandbuch*
4. Kerberos: Das Netzwerkauthentifizierungsprotokoll
5. Der Kerberos Network Authentication Service (USC/ISI's GOST Group)
6. Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller. "Kerberos: An Authentication Service for Open Network Systems ", USENIX März 1988
7. S. P. Miller, B. C. Neuman, J. I Schiller und J. H. Saltzer, "Kerberos Authentication and Authorization System", 21.12.87

8. R. M. Needham und M. D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers", Communications of the ACM, Band 21(12), 993-999 (Dezember 1978)
9. V. L. Voydock und S. T. Kent, "Security Mechanismen in High-Level Network Protocols", *Computing Surveys*, Band 15(2), ACM (Juni 1983)
10. Li Gong, "A Security Risk of Abhängig von synchronisierten Uhren", *Operating Systems Review*, Band 26, #1, 49-53
11. C. Neuman und J. Kohl, "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993
12. B. Clifford Neuman und Theodore Ts'o, "Kerberos: An Authentication Service for Computer Networks", IEEE Communications, 32(9), September 1994**Hinweis:** Viele dieser Dokumente, darunter das von Neuman, Schiller und Steiner (Nr. 9), sind auch über FTP vom MIT Athena System verfügbar - Kerberos-Dokumentation . Informationen zum Abrufen von Kopien von RFCs finden Sie unter RFCs und Standarddokumente beziehen.

Zugehörige Informationen

- Support-Seite für Kerberos
- Technischer Support - Cisco Systems