Kerberos V5 클라이언트 지원 문제 해결 및 구성

목차

소개

이 문서에서는 컨피그레이션의 예와 일반적인 문제에 대한 몇 가지 솔루션을 제공합니다.문제를 해결하는 데 도움이 되는 기술도 이 문서에서 제공됩니다.이 문서에서는 Kerberos 텔넷 지원을 다루지 않습니다.

이 문서의 대부분은 Kerberos와 함께 제공되는 무료 문서 및 패키지에 있는 다양한 FAQ(자주 묻는 질문)에서 제공됩니다.이 구성은 기능 라우터와 Kerberos KDC 서버에서 가져온 것입니다.

이 문서에서는 MIT에서 버전 5 버전의 Kerberos 패키지를 올바르게 컴파일하고 설치했다고 가정합니다.Kerberos V5를 취득, 컴파일 및 설치하는 방법에 대한 자세한 내용은 이 문서의 끝 부분에 있는 참조를 참조하십시오.

또한 Kerberos V5 지원에 Cisco IOS® Software Release 11.2 이상이 필요합니다.이는 자격 증명 전달을 포함하는 Kerberos V 클라이언트 인증을 완벽하게 지원합니다.Kerberos V 인프라가 있는 시

스템은 네트워크 또는 라우터 액세스에 대한 최종 사용자를 인증하기 위해 KDC(Key Distribution Center)를 사용할 수 있습니다.이는 Kerberos KDC 구현이 아니라 클라이언트 구현입니다.

Kerberos는 레거시 보안 서비스로 간주되며 이미 Kerberos를 사용하는 네트워크에서 가장 유용합니다.

이 지원을 포함하는 버전에 대한 자세한 내용은 Cisco IOS Software 릴리스 11.2 릴리스 정보를 참조하십시오.

후속 Cisco IOS Software 릴리스에서 Kerberos 지원을 받으려면 Software Advisor(등록된 고객만 해당)를 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Software 릴리스 11.2 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

Kerberos 소개

Kerberos는 물리적으로 안전하지 않은 네트워크에서 사용하기 위한 네트워크 인증 프로토콜입니다.Kerberos는 Needham 및 Schroeder가 제공하는 키 배포 모델을 기반으로 합니다.(이 문서의 참조 섹션에서 9번을 참조하십시오.비밀 키 암호화를 사용하여 클라이언트/서버 애플리케이션에 강력한 인증을 제공하도록 설계되었습니다.이를 통해 네트워크를 통해 통신하는 엔티티가 서로 자신의 ID를 입증하는 동시에 도청 또는 재생 공격을 방지할 수 있습니다.또한 DES와 같은 암호화 시스템의 도움을 받아 데이터 스트림 무결성(예: 수정 탐지) 및 기밀성(예: 무단 읽기 방지)을 제공합니다.

인터넷에서 사용되는 프로토콜 중 상당수는 어떤 보안도 제공하지 않습니다.네트워크에서 비밀번호를 "sniff" 하는 데 사용되는 툴은 시스템 크래커에서 공통적으로 사용됩니다.따라서 암호화되지 않은 네트워크를 통해 비밀번호를 전송하는 애플리케이션은 취약합니다.또한 다른 클라이언트/서버 애플리케이션은 클라이언트 프로그램을 사용하는 사용자의 ID에 대해 "정직한" 클라이언트 프로그램에 의존합니다.다른 응용 프로그램은 클라이언트에 의존하여 서버의 다른 시행 없이 허용된 작업을 제한합니다.

일부 사이트는 네트워크 보안 문제를 해결하기 위해 방화벽을 사용하려고 합니다.방화벽은 "나쁜 사람들"이 외부에 있다고 가정합니다. 이는 잘못된 가정인 경우가 많습니다.하지만 내부자들 사이

에 피해가 더 큰 컴퓨터 범죄 사건의 대다수는 내부자에 의해 수행되고 있다.또한 방화벽은 사용자가 인터넷을 사용할 수 있는 방법을 제한한다는 점에서 큰 단점이 있습니다.

MIT에서 이러한 네트워크 보안 문제를 해결하기 위해 Kerberos를 만들었습니다.Kerberos 프로토콜은 강력한 암호화를 사용하므로 클라이언트가 비보안 네트워크 연결을 통해 서버에 ID를 증명할 수 있습니다(또는 그 반대의 경우도).클라이언트와 서버가 자신의 ID를 증명하기 위해 Kerberos를 사용한 후에는 모든 통신을 암호화하여 비즈니스를 수행하는 동안 개인 정보 및 데이터 무결성을 보장할 수 있습니다.

Kerberos는 BSD 운영 및 X11 Windowing 시스템에 사용되는 것과 유사한 저작권 권한 알림으로 MIT에서 자유롭게 사용할 수 있습니다.MIT는 Kerberos를 소스 형식으로 제공합니다.이 작업은 코드를 사용하려는 사용자가 코드를 직접 살펴보고 해당 코드가 신뢰할 수 있음을 확인할 수 있도록 합니다.또한 전문적인 지원 제품에 의존하는 것을 선호하는 사용자에게는 다양한 공급업체의 제품으로 Kerberos를 사용할 수 있습니다.

Kerberos V5 클라이언트 지원은 MIT에서 개발한 Kerberos 인증 시스템을 기반으로 합니다 .Kerberos에서 클라이언트(일반적으로 사용자 또는 서비스)는 KDC(Key Distribution Center)에 티켓 요청을 보냅니다. KDC는 클라이언트에 대한 TGT(Ticket-Granting Ticket)를 생성하고, 클라이언트의 비밀번호를 키로 사용하여 암호화하고, 암호화된 TGT를 클라이언트로 다시 전송합니다.그런 다음 클라이언트는 비밀번호의 도움을 받아 TGT를 해독하려고 시도합니다.클라이언트가 TGT를 성공적으로 해독할 경우(예: 클라이언트가 올바른 비밀번호를 제공할 경우), 해독된 TGT를 유지합니다.이는 클라이언트의 ID 증명을 나타냅니다.

지정된 시간에 만료되는 TGT는 클라이언트가 특정 서비스에 대한 권한을 부여하는 추가 티켓을 얻을 수 있도록 허용합니다.이러한 추가 티켓의 요청과 부여는 사용자가 투명하게 이루어집니다.

Kerberos는 인증되고, 선택적으로 암호화되며, 인터넷상의 두 지점 간에 통신하므로, 어떤 클라이언트가 있는 방화벽의 어느 쪽에 종속되지 않는 보안 계층을 제공합니다.Kerberos는 주로 텔넷 또는 FTP와 같은 애플리케이션 레벨 프로토콜(ISO 모델 레벨 7)에서 사용되어 사용자에게 호스트 보안을 제공합니다.또한 데이터 스트림(예: SOCK_**STREAM**) 또는 RPC 메커니즘(ISO 모델 레벨 6)의 암시적 인증 시스템으로 덜 자주 사용됩니다. 또한 IP, UDP 또는 TCP(ISO 모델 레벨 3 및 4)와 같은 프로토콜에서 호스트 간 보안에 대해 하위 레벨에서 사용할 수 있습니다. 그러나 이러한 구현은 드물지만, 실제로 구현되는 경우는 거의 없습니다.

또한 요청자를 위한 비밀 키를 만들어 개방형 네트워크의 주도자 간에 상호 인증 및 보안 통신을 제공합니다.이러한 비밀 키가 네트워크를 통해 안전하게 전파될 수 있는 메커니즘도 제공됩니다 .Kerberos는 권한 부여 또는 어카운팅을 제공하지 않습니다.그러나 이러한 기능을 안전하게 수행하기 위해 비밀 키를 사용할 수 있는 애플리케이션입니다.

정의

- **인증**— 여러분이 누구인지, 그리고 우리가 여러분이 누구인지 알고 있는지 확인합니다.
- **클라이언트** - 티켓을 가져올 수 있는 엔티티입니다.이 엔티티는 일반적으로 사용자 또는 호스트입니다.
- **자격 증명**—티켓과 동일합니다.
- **Daemon**—일반적으로 UNIX 호스트에서 실행되는 프로그램으로, 네트워크 인증 요청을 서비스하는 프로그램입니다.
- **호스트** - 네트워크를 통해 액세스할 수 있는 컴퓨터입니다.
- **인스턴스** - Kerberos 주체의 두 번째 부분입니다.1차 하위 구성요소에 적합한 정보를 제공합니다.인스턴스는 null일 수 있습니다.사용자의 경우 해당 자격 증명의 사용 용도를 설명하기 위해 인스턴스가 자주 사용됩니다.호스트의 경우 해당 인스턴스는 정규화된 호스트 이름입니다.

- **Kerberos**—그리스 신화에서 지하세계의 출입구를 지키는 세 개의 머리가 달린 개.컴퓨터 세계에서 Kerberos는 MIT에서 개발한 네트워크 보안 패키지입니다.
- **KDC**—키 배포 센터.Kerberos 티켓을 발급하는 시스템입니다.
- **Keytab** - 하나 이상의 키를 포함하는 키 테이블 파일입니다.호스트나 서비스는 사용자가 비밀번호를 사용하는 것과 동일한 방식으로 keytab 파일을 사용합니다.
- **NAS**—Network Access Server(Cisco 박스) 또는 TACACS+ 인증 및 권한 부여를 요청하거나 어카운팅 패킷을 전송하는 기타 모든 제품입니다.
- **Principal**(보안 주체) - 자격 증명 집합을 할당할 수 있는 특정 엔터티의 이름을 지정하는 문자열입니다.일반적으로 Primary, Instance, REALM이라는 세 부분으로 구성됩니다.일반적인 Kerberos 주체의 일반적인 형식은 **primary/instanceREALM입니다**.
- **Primary**(기본) - Kerberos 주체의 첫 번째 부분입니다.사용자의 경우 사용자 이름입니다.서비스의 경우 서비스 이름입니다.
- **REALM**—단일 Kerberos 데이터베이스 및 키 배포 센터 집합에서 제공하는 논리적 네트워크입니다.일반적으로 영역 이름은 모두 대문자이며, 영역을 인터넷 도메인과 구별합니다.
- **서비스** - 네트워크를 통해 액세스하는 모든 프로그램 또는 컴퓨터입니다.서비스의 예는 다음과 같습니다."host" - 호스트(예: 텔넷 및 rsh 사용 시)"ftp" - FTP"krbtgt"—인증티켓 부여"pop" - 이메일
- **티켓** - 특정 서비스에 대한 클라이언트의 ID를 확인하는 임시 전자 자격 증명 집합입니다.
- **TGT**—Ticket-Granting Ticket.클라이언트가 동일한 Kerberos 영역 내에서 추가 Kerberos 티켓을 얻을 수 있도록 하는 특수 Kerberos 티켓.티켓 부여 티켓의 좋은 비유로 4개의 다른 스키장에서 좋은 3일 스키패스를 들 수 있습니다.어느 리조트로 가든 (그것이 만료될 때까지) 통행권을 보여주면, 당신은 그 휴양지에 대한 리프트 티켓을 받습니다.일단 리프트 티켓이 있으면 그 리조트에서 원하는 모든 것을 스키를 탈 수 있다.다음 날 다른 리조트로 가면 다시 한번 패스를 보여드리고 새로 생긴 리조트를 이용할 수 있는 리프트 티켓을 드립니다.차이점은 Kerberos V5 프로그램은 주말 스키 패스를 가지고 있다는 것을 인식하고 리프트 티켓을 받으므로 직접 트랜잭션을 수행할 필요가 없습니다.

고차

이 섹션에서는 다음 사항을 숙지해야 합니다.

- 컨피그레이션 파일에서 모든 후행 공백을 제거해야 합니다.후행 공백은 krb5kdc 서버에 문제를 일으킬 수 있습니다.그렇지 않으면 "krb5kdc가 영역에 대한 데이터베이스를 시작할 수 없습니다."라는 메시지가 표시될 수 있습니다.
- 라우터의 클록이 KDC 서버를 실행하는 UNIX 호스트와 동일한 시간으로 설정되었는지 확인합니다.침입자가 만료된 티켓을 계속 사용하기 위해 시스템 클럭을 재설정하지 못하도록 하기 위해 Kerberos V5는 클럭이 KDC의 지정된 최대 클록 스큐 내에 있지 않은 호스트의 티켓 요청을 거부하도록 설정됩니다(kdc.conf 파일에 지정). 마찬가지로, 호스트의 지정된 최대 클럭 스큐(krb5.conf 파일에 지정된 대로) 내에 클럭이 없는 KDC의 응답을 거부하도록 호스트가 구성됩니다. 최대 클럭 기울기의 기본값은 300초(5분)입니다.
- DNS가 제대로 작동하는지 확인합니다.Kerberos의 몇 가지 기능은 이름 서비스에 의존합니다.Kerberos가 높은 수준의 보안을 제공하려면 네트워크의 다른 부분보다 이름 서비스 문제에 더 민감합니다.DNS(Domain Name System) 항목과 호스트에 올바른 정보가 있어야 합니다.호스트 이름의 각 정식 호스트 이름은 정규화된 호스트 이름(도메인을 포함)이어야 하며, 호스트의 각 IP 주소는 정식 이름으로 역확인해야 합니다.
- Cisco IOS Kerberos V5 지원에서는 소문자 영역 이름을 사용할 수 없으며 Cisco IOS의 Kerberos 코드는 영역이 소문자인 경우 사용자를 인증하지 않습니다.이는 Cisco IOS Software

릴리스 11.2(7)에서 수정되었습니다.Cisco 버그 ID CSCdj10598(등록된 고객만 해당)을 참조하십시오.유일한 해결 방법은 대문자 REALM 이름(기존 이름)을 사용하는 것입니다.소문자 영역은 서비스 자격 증명이 아니라 TGT를 검색하기 위해 작동합니다.Cisco는 로깅 인증 중에 새로운 TGT를 사용하여 서비스 자격 증명(KDC 스푸핑 공격을 방지하는 데 사용됨)을 검색하기 때문에 소문자 영역을 사용하는 Kerberos 인증은 항상 실패합니다.

- PPP PAP 및 CHAP용 Kerberos V5는 라우터를 충돌할 수 있습니다.이는 Cisco IOS Software 릴리스 11.2(6)에서 수정되었습니다.Cisco 버그 ID CSCdj08828(등록된 고객만 해당)을 참조하십시오.이를 위한 해결 방법은 **자동**을 **로그인** 중에 선택하지 않고 **비동기 모드**를 통해 라우터에 exec에 강제로 로그인하고 사용자가 수동으로 PPP를 시작하도록 하는 것입니다.
  ```
  aaa authentication ppp default if-needed krb5 local
  ```
- Kerberos V5는 권한 부여 또는 계정을 수행하지 않습니다.이 작업을 수행하려면 다른 코드가 필요합니다.

Cisco IOS 라우터 컨피그레이션

이 섹션의 컨피그레이션에서는 Kerberos V5를 수행하는 완전히 구성된 AS5200 라우터를 보여 줍니다. 이 컨피그레이션의 라우터는 VTY 세션과 PAP 인증을 사용하여 PPP를 수행하기 위해 전화를 거는 사용자를 모두 인증하기 위해 Kerberos 서버를 사용합니다.

AS5200 Config with 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 컨피그레이션

올바른 포트가 입력되도록 설정되어 있는지 **확인합니다**.

참고: 이 예제에서는 래퍼를 사용합니다.암호화된 텔넷을 원하는 경우 정상적인 텔넷을 Kerberos 텔넷으로 교체해야 이러한 파일의 모양이 다릅니다.

입력 포트 설정

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

Kerberos 구성 파일 설정

그런 다음 KDC 서버가 읽는 Kerberos 컨피그레이션 파일을 몇 개 설정해야 합니다.이러한 매개변수의 의미에 대한 자세한 내용은 Kerberos 설치 가이드 또는 시스템 관리 설명서를 참조하십시오.

```
# 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
```

```
}
```

KDC 서버의 데이터베이스 설정

그런 다음 KDC 서버가 사용하는 데이터베이스를 만들어야 합니다.

1. 다음 명령을 **입력합니다**.

```
# 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:
```

이는 **kerberos srvtab remote** 명령을 사용하여 TFTP를 통해 라우터에서 srvtab 비밀번호**를 검색하려면** 필요합니다.

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

2. 주도자와 사용자를 데이터베이스에 추가하려면 **kadmin.local** 명령을 사용합니다.

```
# 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. 사용자 추가:

```
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. 현재 데이터베이스 목록 가져오기:

```
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. Cisco 라우터의 항목을 추가합니다.

```
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. Cisco 라우터의 테이블에 대한 키를 추출합니다.

```
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. 데이터베이스를 한 번 더 살펴보십시오.

```
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. keytab 파일을 라우터가 액세스할 수 있는 위치로 이동합니다.

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

9. KDC 서버를 시작합니다.

```
# kdc/krb5kdc
#
```

10. 실제로 실행되는지 확인합니다.

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

11. 라우터가 키 테이블 항목을 읽도록 합니다.

```
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. 라우터를 확인하여 모든 것이 준비되었는지 확인합니다.

```
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. 디버깅을 켜고 라우터에 로그인합니다.

```
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
```

디버그 출력 샘플

다음은 성공적으로 인증한 PPP 사용자입니다.

```
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
```

문제 해결

이 섹션에서는 잠재적 문제에 대한 다양한 시나리오를 제공합니다.이러한 디버그를 사용하면 문제를 신속하게 확인할 수 있습니다.

잘못된 영역 이름

```
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
```

DNS가 작동하지 않음

```
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
                                          ~~~~
```

라우터 클럭이 올바르지 않음

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

사용자에게 표시되는 내용은 다음과 같습니다.

```
$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:
```

클라이언트가 Kerberos 데이터베이스에 없음

```
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
```

클라이언트가 데이터베이스에 있지만 잘못된 암호를 사용합니다.

```
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
```

사용자는 다음 출력을 볼 수 있습니다.

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


User Access Verification

Username: cisco1
Password:
% Access denied

Username:
```

라우터에서 SRVTAB 항목이 올바르지 않음

```
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
```

사용자에게 표시되는 내용은 다음과 같습니다.

```
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:
```

참조

1. Kerberos V5 *시스템 관리자 가이드*(대상 g-zip 파일로 제공)
2. Kerberos V5 *설치 가이드*
3. Kerberos V5 *UNIX 사용 설명서*
4. Kerberos:네트워크 인증 프로토콜
5. Kerberos 네트워크 인증 서비스(USC/ISI의 GOST 그룹)
6. 제니퍼 G. 슈타이너, 클리포드 뉴먼, 제프리 I. 쉴러"Kerberos:An Authentication Service for

Open Network Systems ", USENIX 1988
7. S. P. 밀러, B. C. 뉴먼, J. I. Schiller, J. H. Saltzer, "Kerberos 인증 및 권한 부여 시스템", 12/21/87
8. R. M. Needham 및 M. D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers", ACM의 통신, Vol. 21(12), pp 993-999(1978년 12월)
9. V. L. Voydock and S. T. Kent, "Security Mechanism in High-Level Network Protocols," *컴퓨팅 설문조사*, Vol. 15(2), ACM(1983년 6월)
10. 리공, "동기화된 시계에 따른 보안 위험", *운영 체제 검토*, 권 26, #1, pp 49-53
11. C. Neuman 및 J. Kohl, "The Kerberos Network Authentication Service (V5)", RFC 1510, 1993년 9월
12. B. 클리포드 뉴먼과 테오도르 티오, "Kerberos:An Authentication Service for Computer Networks," IEEE Communications, 32(9), 1994년 9월**참고:** Neuman, Schiller 및 Steiner(#9)에 의한 문서를 포함한 이러한 문서 중 상당수는 MIT Athena System — Kerberos Documentation의 FTP를 통해 제공됩니다 .RFC의 사본을 얻으려면 RFC 및 표준 문서 가져오기를 참조하십시오.

관련 정보

- Kerberos 지원 페이지
- Technical Support - Cisco Systems