Pesquisando defeitos e configurando o suporte ao cliente do Kerberos V5

Índice

Introdução

Este documento fornece um exemplo de configuração, assim como algumas soluções aos problemas comuns. As técnicas que o ajudam a pesquisar defeitos todas as edições são fornecidas igualmente neste documento. Este documento não endereça o suporte a telnet kerberizado.

A maioria deste material neste artigo vieram da documentação livremente disponível que vem com Kerberos e das várias perguntas mais frequentes disponíveis (FAQ) no pacote. As configurações vieram de um roteador funcional e de um servidor KDC de Kerberos.

Este documento supõe que você corretamente compilou e instalou uma versão atual da versão 5 do pacote do Kerberos do MIT. Refira as referências na extremidade deste artigo para obter

informações sobre de como obter, compilar, e instalar o Kerberos V5.

Igualmente note que a liberação 11.2 do Cisco IOS ® Software ou mais atrasado está exigida para o apoio do Kerberos V5. Isto fornece o apoio total da authenticação do cliente do Kerberos V, que inclui o encaminhamento de credencial. Os sistemas que têm infra-estruturas do Kerberos V podem usar seus centros de distribuição chave (KDC) a fim autenticar utilizadores finais para a rede ou o acesso de roteador. Esta é uma implementação de cliente e não uma aplicação do Kerberos KDC.

O Kerberos é considerado um serviço de segurança do legado e é o mais benéfico nas redes que já usam o Kerberos.

Refira os Release Note do Cisco IOS Software Release 11.2 para mais informação detalhada de que as versões incluem este apoio.

Para o apoio do Kerberos em Cisco IOS Software Release subsequentes, refira o Software Advisor (clientes registrados somente).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco IOS Software Release 11.2 e Mais Recente

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Introdução ao Kerberos

O Kerberos é um protocolo de autenticação de rede para o uso fisicamente em redes inseguras. O Kerberos é baseado no modelo da distribuição chave apresentado por Needham e por Schroeder. (Veja o número 9 na seção de referências deste documento. É projetado fornecer a autenticação forte para o cliente/aplicativos de servidor pelo uso da criptografia de chave secreta. Permite as entidades que se comunicam sobre redes para provar entre si sua identidade quando impedir bisbilhotar ou ataques de replay. Igualmente prevê a integridade do fluxo de dados (tal como a detecção de modificação) e o secretismo (tal como a prevenção da leitura não autorizada) com a ajuda dos sistemas de criptografia tais como o DES.

Muitos dos protocolos usados no Internet não fornecem nenhuma Segurança. As ferramentas usadas “para aspirar” senhas fora da rede são de uso comum por invasores de sistemas. Assim, os aplicativos que enviam uma senha sobre a rede sem criptografia são vulneráveis. Também, outros cliente/aplicativos de servidor confia no programa de cliente para ser “honestos” sobre a identidade do usuário que a usa. Outros aplicativos confiam no cliente para restringir suas atividades àquelas que é permitida fazer, sem a outra aplicação pelo server.

Alguns locais tentam usar Firewall a fim resolver seus problemas de segurança de rede. Os Firewall supõem que “os rapazes incorreto” estão na parte externa, que é frequentemente uma suposição inválida. Contudo, a maioria dos incidentes do crime de computador que causam mais dano foi realizada por membros. Os Firewall igualmente têm uma desvantagem significativa que restringem como seus usuários podem usar o Internet.

O Kerberos foi criado pelo MIT como uma solução a estes problemas de segurança de rede. O protocolo Kerberos usa a criptografia forte, de modo que um cliente possa provar sua identidade a um server (e vice-versa) através de uma conexão de rede insegura. Depois que um cliente e servidor usou o Kerberos a fim provar sua identidade, pode igualmente cifrar todas suas comunicações a fim assegurar a privacidade e a integridade de dados enquanto vai aproximadamente seu negócio.

O Kerberos está livremente disponível do MIT, sob uma observação da permissão dos direitos reservados que seja similar a essa usada para o funcionamento BSD e o Sistema de janelas X11. O MIT fornece o Kerberos na forma de origem. Isto é feito de modo que qualquer um que deseja o usar possa olhar sobre o código para se e se assegurar que o código é de confiança. Além, para aqueles que preferem confiar profissionalmente em uns produtos suportados, o Kerberos está disponível como um produto de muitos vendedores diferentes.

O suporte ao cliente do Kerberos V5 é baseado no sistema de autenticação de Kerberos desenvolvido no MIT. Sob o Kerberos, um cliente (geralmente um usuário ou um serviço) envia um pedido para um bilhete ao Key Distribution Center (KDC). O KDC cria um ticket-granting ticket (ingresso que concede ingresso) (TGT) para o cliente, cifra-o com a ajuda da senha do cliente como a chave, e envia-o o TGT cifrado de volta ao cliente. O cliente tenta então decifrar o TGT, com a ajuda de sua senha. Se o cliente decifra com sucesso o TGT por exemplo, se o cliente dá a senha correta), mantém o TGT decifrado. Isto indica a prova da identidade do cliente.

O TGT, que expira em um tempo especificado, permite o cliente obter os bilhetes adicionais, que dão a permissão para serviços específicos. Os pedidos e as concessões destes bilhetes adicionais são USER-transparentes.

Desde que o Kerberos negocia autenticado, é cifrado opcionalmente, e comunica-se entre todos os dois pontos no Internet, ele fornece uma camada de Segurança que não é dependente de que lado de um Firewall um ou outro cliente é encontrado. O Kerberos é usado primeiramente nos protocolos de nível de aplicativo (nível modelo 7 ISO), como o telnet ou o FTP, a fim fornecer o usuário para hospedar a Segurança. É usado igualmente, embora menos frequentemente, como o sistema de autenticação implícito de fluxo de dados (tal como SOCK_STREAM) ou de mecanismos RPC (nível modelo 6 ISO). Pode igualmente ser usado em um nível inferior para a Segurança do host-à-host, nos protocolos tais como o IP, o UDP, ou o TCP (níveis modelo 3 e 4 ISO). Embora, tais aplicações sejam raras, se existem de todo.

Prevê a autenticação mútua e a comunicação segura entre principais em uma rede aberta pela fabricação de chaves secretas para todo o solicitador. Um mecanismo para que estas chaves secretas sejam propagadas com segurança através da rede é fornecido igualmente. O Kerberos não prevê a autorização ou a contabilidade. Contudo, aplicativos que desejam ao uso da lata

suas chaves secretas a fim executar firmemente aquelas funções.

Definições

- **Autenticação** — Assegure-se de que você seja quem você diz que você é, e que nós conhecemos quem você é.
- **Cliente** — Uma entidade que possa obter um bilhete. Esta entidade é geralmente um usuário ou um host.
- **Credenciais** — O mesmos que bilhetes.
- **Demônio** — Um programa, geralmente um que é executado em um host Unix, esse presta serviços de manutenção a requisições de rede para a autenticação.
- Computador do **Host-a** que pode ser alcançado sobre uma rede.
- **Exemplo** — O segundo parte de um Kerberos principal. Dá a informação que qualifica o preliminar. O exemplo pode ser nulo. No caso de um usuário, o exemplo é usado frequentemente a fim descrever o uso pretendido das credenciais correspondentes. No caso de um host, o exemplo é o hostname totalmente qualificado.
- **Kerberos** — Na mitologia grega, o cão três-dirigido que guarda a entrada ao submundo. No mundo de computadores, o Kerberos é um pacote da segurança de rede que seja desenvolvido no MIT.
- **KDC** — Key Distribution Center. Uma máquina essa bilhetes do Kerberos das edições.
- **Keytab** — Um arquivo de tabela chave que contenha umas ou várias chaves. Um host ou um serviço usam um arquivo de keytab de forma similar a um usuário usam sua senha.
- **NAS** — Um servidor do acesso de rede (uma caixa de Cisco) ou qualquer outra coisa que façam a autenticação TACACS+ e os pedidos de autorização, ou enviam pacotes da contabilidade.
- **Principal** — Uma corda que nomeie uma entidade específica a que um grupo de credenciais pode ser atribuído. Tem geralmente três porções nomeadas Preliminar, exemplo, e REINO.O formato típico de um principal de Kerberos típico é **preliminar/instanceREALM**.
- **Preliminar** — O primeiro parte de um Kerberos principal. No caso de um usuário, é o username. No caso de um serviço, é o nome do serviço.
- **REINO** — A rede lógica serviu por um único base de dados de Kerberos e por um grupo de centros de distribuição chave. Por convenção, os nomes de esfera são geralmente todas as letras maiúsculas, para diferenciar o reino do domínio de internet.
- **Serviço** — Algum programa ou computador que você alcançar sobre uma rede. Os exemplos dos serviços incluem:“host” — um host, (por exemplo, quando você usar o telnet e o rsh)“ftp” — FTPautenticação do “krbtgt” —; como o ticket-granting ticket (ingresso que concede ingresso)“PNF” — Email
- **Bilhete** — Um conjunto temporário de credenciais eletrônicas que verifica a identidade de um cliente para um serviço particular.
- **TGT** — Ticket-granting ticket (ingresso que concede ingresso). Um bilhete especial do Kerberos que permita o cliente obter o Kerberos adicional tickets dentro da mesma esfera de kerberos.Uma boa analogia para o ticket-granting ticket (ingresso que concede ingresso) é uma passagem de três dias do esqui que seja boa em quatro recursos diferentes. Você mostra a passagem em qualquer recurso você decide ir (até que expire), e você recebe um bilhete do elevador para esse recurso. Uma vez que você tem o bilhete do elevador, você pode esquiar tudo que você quer nesse recurso. Se você vai a um outro recurso o next day, você mostra mais uma vez sua passagem, e você obtém um bilhete adicional do elevador para o recurso novo. A diferença é que o Kerberos V5 programa a observação que você tem

a passagem do esqui do fim de semana, e obtém o bilhete do elevador para você, assim que você não tem que executar as transações você mesmo.

Gotcha

Esta seção alista diversos artigos de que você precisa de estar ciente:

- Certifique-se de você remover todos os espaços de trailing nos arquivos de configuração. Os espaços de trailing podem causar problemas com o server krb5kdc. Se não, você pode receber uma mensagem que diga, "krb5kdc não pode começar o base de dados para o reino."
- Certifique-se que o pulso de disparo no roteador está ajustado ao mesmo tempo que o host Unix que executa o servidor de KDC. A fim impedir que os intrusos restaurem seus relógios de sistema a fim continuar a usar bilhetes expirados, o Kerberos V5 estabelece-se para rejeitar pedidos do bilhete de todo o host cujo o pulso de disparo não estiver dentro do desvio de relógio máximo especificado do KDC (como especificado no arquivo kdc.conf). Similarmente, os anfitriões são configurados para rejeitar respostas de todo o KDC cujo o pulso de disparo não estiver dentro do desvio de relógio máximo especificado do host (como especificado no arquivo krb5.conf). O valor padrão para o desvio máximo de relógio é 300 segundos (cinco minutos).
- Certifique-se de trabalhos DNS corretamente. Diversos aspectos do Kerberos confiam no serviço de nome. Para que o Kerberos forneça seu alto nível de segurança, é mais sensível aos problemas do serviço de nome do que algumas outras partes de sua rede. É importante que suas entradas do Domain Name System (DNS) e seus anfitriões têm a informação correta. Cada canônico do nome de host deve ser o nome de host totalmente qualificado (de que inclui o domínio), e cada endereço IP de Um ou Mais Servidores Cisco ICM NT do host deve reverso-resolução ao nome canônico.
- O apoio do Kerberos V5 do Cisco IOS não permite o uso de nomes de esfera minúscula e o código do Kerberos no Cisco IOS não autentica usuários se o reino está no lowercase. Isto foi fixado no Cisco IOS Software Release 11.2(7).Refira a identificação de bug Cisco CSCdj10598 (clientes registrados somente).A única ação alternativa é usar nomes de esfera caixas (que é convencional).As esferas minúsculas trabalham a fim recuperar um TGT, mas não umas credenciais do serviço. Desde que Cisco usa seu TGT novo a fim recuperar umas credenciais do serviço (usadas para impedir o ataque de falsificação KDC) durante a autenticação de registro, a autenticação de Kerberos que usa esferas minúsculas falha sempre.
- O Kerberos V5 para PPP PAP e RACHADURA pode causar um crash o roteador. Isto foi fixado no Cisco IOS Software Release 11.2(6).Refira a identificação de bug Cisco CSCdj08828 (clientes registrados somente).A ação alternativa para esta é forçar o login exec no roteador através do **modo assíncrono interativo** sem durante-**início de uma sessão do autoselect** e então ter o começo PPP do usuário manualmente:`aaa authentication ppp default if-needed krb5 local`
- O Kerberos V5 não faz a autorização ou a contabilidade. Você precisa algum outro código a fim fazer este.

Configuração do roteador do Cisco IOS

A configuração nesta seção descreve um roteador AS5200 inteiramente configurado que faça o Kerberos V5. O roteador nesta configuração usa o servidor Kerberos a fim autenticar as sessões de VTY e os usuários que discam dentro para fazer o PPP com autenticação pap.

Configuração AS5200 com 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
```

Configuração KDC de Kerberos

Certifique-se de você ter as portas adequadas estabelecidas para o **inetd**.

Nota: Este exemplo usa envoltórios. Se você quer o telnet cifrado, você precisa de substituir Telnet normal com o telnet com kerberos, assim que estes arquivos têm uma aparência diferente.

Portas estabelecidas para o inetd

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

kerberos88/udpkdc
kerberos88/tcpkdc

kxct549/tcp

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

#cat /etc/inetd.conf

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

Arquivos de configuração estabelecidos do Kerberos

Em seguida, você precisa de estabelecer alguns arquivos de configuração do Kerberos que o servidor de KDC lê. Para obter mais informações sobre do que estes parâmetros significam, refira o Kerberos instalam o guia ou o guia do System Admin .

```
# 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
     }
```

Estabelecer o base de dados para o servidor de KDC

Em seguida, você precisa de criar o base de dados que o servidor de KDC usa.

1. Inscreva o comando 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:` Isto é precisado a fim recuperar a senha do srvtab do roteador através do TFTP com o comando kerberos srvtab remote.`# kadmin/dbutil/kdb5_util stash -r CISCO.EDU Enter KDC database master key:`
2. A fim adicionar diretores e usuários ao base de dados, use o comando 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. Adicionar um usuário:`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. Obtenha uma lista do base de dados atual:`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. Adicionar a entrada para o roteador Cisco:`kadmin.local:  ank`
```
host/cisco5200.cisco.edu@CISCO.EDU
Enter password for principal "host/cisco5200.cisco.edu@CISCO.EDU":

Re-enter password for principal "host/cisco5200.cisco.edu@CISCO.EDU":
Principal "host/cisco5200.cisco.edu@CISCO.EDU" created.
```
6. Extraia uma chave à tabela para o roteador Cisco:`kadmin.local:  ktadd`
```
host/cisco5200.cisco.edu@CISCO.EDU
Entry for principal host/cisco5200.cisco.edu@CISCO.EDU with kvno 2,
   encryption type DES-CBC-CRC added to keytab WRFILE:/etc/krb5.keytab.
```
7. Tome um outro olhar no base de dados:`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. Mova o arquivo de keytab para um lugar onde o roteador possa lhe obter:`# cp`
```
/etc/krb5.keytab /ts/
# chmod 777 /ts/krb5.keytab
```
9. Ligue o servidor de KDC:`# kdc/krb5kdc`
```
#
```
10. Verifique para certificar-se que é executado realmente:`# ps -A | grep  'krb5'`
```
 6043 ??       I        0:00.01 kdc/krb5kdc
23427 ttypf    S  +     0:00.05 grep krb5
```
11. Force o roteador a ler sua entrada de tabela chave:`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. Verifique o roteador para certificar-se que tudo está pronto:`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. Gire sobre debugar e tente-o registrar no roteador:`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
```

Exemplo de debug

Está aqui um usuário PPP que autentique com sucesso.

```
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
```

Troubleshooting

Esta seção contém várias encenações para problemas potenciais. Estes debugam a ajuda você para ver rapidamente um problema.

Nome de esfera errado

```
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
```

O DNS não trabalha

```
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
                                          ~~~~
```

Relógio do roteador não correto

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

Éaqui o que o usuário vê:

```
$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:
```

Cliente não no base de dados de Kerberos

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

O cliente está no base de dados mas os usos lesam a senha

```
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
```

O usuário vê esta saída:

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


User Access Verification

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

Entrada SRVTAB não correta no roteador

```
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
```

Éaqui o que o usuário vê:

```
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:
```

Referências

1. *O guia de administrador de sistema do* Kerberos V5 (vem em um arquivo tarred, g-fechado)
2. *Guia de Instalação do* Kerberos V5
3. *O guia de usuário do* Kerberos V5 *UNIX*
4. Kerberos: O protocolo de autenticação de rede
5. O serviço de autenticação de rede de kerberos (grupo do GOST USC/ISI)
6. Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller. “Kerberos: Um serviço de autenticação para sistemas de rede aberta ”, USENIX março de 1988
7. S. P. Miller, B.C. Neuman, J.I. Schiller, e J.H. Saltzer, “autenticação de Kerberos e sistema de autorização,”, 12/21/87
8. R. M. Needham e M.D. Schroeder, “usando a criptografia para autenticação nas redes grandes dos computadores,” comunicações do ACM, Vol. 21(12), pp. 993-999 (dezembro, 1978)
9. V. L. Voydock e S.T. Kent, “mecanismos de segurança nos protocolos de rede de alto nível,” *análises de computação*, Vol. 15(2), ACM (junho 1983)
10. Gongo de Li, “um risco de segurança segundo de relógios sincronizados”, *revisão de sistemas operacionais*, Vol 26, #1, pp 49-53
11. C. Neuman e J. Kohl, “o serviço de autenticação de rede de kerberos (RFC 1510 de V5),", em setembro de 1993
12. B. Clifford Neuman e Theodore Ts'o, “Kerberos: Um serviço de autenticação para redes de computador,” comunicações IEEE, 32(9), em setembro de 1994**Nota:** Muitos destes documentos, isso incluem esse por Neuman, Schiller, e Steiner (#9) está igualmente

disponível através do FTP do sistema MIT Athena -- Documentação de kerberos . A fim obter cópias dos RFC, refira os RFC e os documentos de obtenção dos padrões.

Informações Relacionadas

- Página de suporte do Kerberos
- Suporte Técnico - Cisco Systems