Устранение неисправностей и настройка поддержки клиентов Kerberos V5

Содержание

Введение

Этот документ предоставляет пример конфигурации, а также некоторые решения типичных проблем. Способы, которые помогают вам решать любые проблемы, также предоставлены в этом документе. Этот документ не обращается к поддержке Telnet на основе Kerberos.

Большая часть этого материала в этой статье прибыла из документации в свободном доступе, которая идет с Kerberos и из различных доступных часто задаваемых вопросов (часто задаваемые вопросы) на пакете. Конфигурации прибыли из функционального маршрутизатора и сервера Kerberos KDC.

Этот документ предполагает, что вы правильно скомпилировали и установили текущий релиз Версии 5 пакета Kerberos от MIT. См. ссылки в конце этой информационной статьи о

том, как получить, скомпилируйте и установите Kerberos V5.

Также обратите внимание, что Выпуск 11.2 программного обеспечения Cisco IOS или позже требуется для поддержки Kerberos V5. Это предоставляет полную поддержку Kerberos V аутентификаций клиента, которые включают пересылку учетных данных. Системы, которые имеют Kerberos V инфраструктур, могут использовать свои Key Distribution Center (KDC) для аутентификации конечных пользователей для сети или доступа к маршрутизатору. Это - реализация клиента и не реализация KDC Kerberos.

Kerberos считают устаревшим сервисом безопасности и является самым выгодным в сетях, это уже использует Kerberos.

См. Комментарии к выпуску программного обеспечения Cisco IOS версии 11.2 для более подробной информации, которой версии включают эту поддержку.

Для поддержки Kerberos в последующих Cisco IOS Software Release обратитесь к Software Advisor (только зарегистрированные клиенты).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Программное обеспечение Cisco IOS версии 11.2 и позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Введение в Kerberos

Kerberos является сетевым протоколом аутентификации для использования на физически ненадежных сетях. Kerberos основывается на модели распределения ключей, представленной Нидхэмом и Шредером. (См. Номер 9 в Ссылочном разделе этого документа. Это разработано для обеспечения строгой проверки подлинности для клиент-серверных приложений при помощи шифрования с секретным ключом. Это позволяет объекты, которые связываются по сетям для удостоверения их личности друг другу, в то время как это предотвращает подслушивание или атаки с повторением пакетов. Это также

обеспечивает целостность потока данных (такую как обнаружение изменения) и тайна (такая как предотвращение неавторизованное показания) с помощью систем шифрования, таких как DES.

Многие протоколы, используемые в Интернете, не предоставляют безопасности. Программные средства, используемые для "осуществления сниффинг" паролей прочь сети, распространены взломщиками систем. Таким образом приложения, которые передают пароль по по сети незашифрованный пароль, уязвимы. Кроме того, другие клиент-серверные приложения полагаются на программу клиента, чтобы быть "честными" о личности пользователя, который использует его. Другие приложения полагаются на клиента для ограничения его действий теми, которых позволено сделать без другого осуществления сервером.

Некоторые узлы пытаются использовать межсетевые экраны для решения их проблем сетевой безопасности. Межсетевые экраны предполагают, что "злоумышленники" находятся на внешней стороне, которая часто является неверным предположением. Однако большинство инцидентов компьютерного преступления, которые наносят больший ущерб, было выполнено посвященными лицами. Межсетевые экраны также имеют значительный недостаток в этом, они ограничивают, как ваши пользователи в состоянии использовать Интернет.

Kerberos был создан MIT как решение этих проблем сетевой безопасности. Протокол Kerberos использует сильную криптографию, так, чтобы клиент мог удостоверить ее личность к серверу (и наоборот) через небезопасное сетевое подключение. После того, как клиент и сервер использовал Kerberos для удостоверения их личности, они могут также зашифровать всю свою связь для уверения конфиденциальности и целостности данных, когда они идут о своем бизнесе.

Kerberos в свободном доступе от MIT под предупреждением разрешений авторского права, которое подобно тому, используемому для работы BSD и системы организации окон X11. MIT предоставляет Kerberos в исходной форме. Это сделано так, чтобы любой, кто хочет использовать его, мог просмотреть код для себя и убедиться, что код защищен. Кроме того, для тех, кто предпочитает полагаться профессионально поддерживаемый продукт, Kerberos доступен как продукт от многих других поставщиков.

Поддержка клиентов Kerberos V5 основывается на системе проверки подлинности Kerberos, разработанной в MIT. Под Kerberos клиент (обычно или пользователь или сервис) отправляет запрос для билета к Key Distribution Center (KDC). KDC создает разрешение на получение разрешения (TGT) для клиента, шифрует его с помощью пароля клиента как ключ и передает зашифрованный TGT обратно клиенту. Клиент тогда пытается дешифровать TGT, с помощью его пароля. Если клиент успешно дешифрует TGT, например, если клиент дает правильный пароль), это поддерживает дешифрованный TGT. Это указывает на доказательство личности клиента.

TGT, который истекает в заданное время, разрешает клиенту получать дополнительные билеты, которые дают разрешения для определенных сервисов. Запросы и предоставления этих дополнительных билетов прозрачны для пользователя.

Так как Kerberos выполняет согласование аутентифицируемый, дополнительно зашифрован и связывается между любыми двумя точками в Интернете, он предоставляет уровень безопасности, которая не зависит, на которую сторону межсетевого экрана расположен любой клиент. Kerberos прежде всего используется в протоколах уровня приложений (Уровень 7 модели ISO), таких как Telnet или FTP, для обеспечения пользователя

безопасности хоста. Это также используется, хотя менее часто, как неявная система аутентификации потока данных (такого как SOCK_STREAM) или механизмы RPC (Уровень 6 модели ISO). Это может также использоваться на более низком уровне для хоста безопасности хоста, в протоколах, таких как IP, UDP или TCP (Уровни 3 и 4 модели ISO). Несмотря на то, что такие реализации редки, если они существуют вообще.

Это обеспечивает обоюдную проверку подлинности и безопасную связь между принципалами на открытой сети изготовлением секретных ключей для любой запрашивающей стороны. Механизм для этих секретных ключей, которые безопасно распространятся через сеть, также предоставлен. Kerberos не обеспечивает авторизацию или учет. Однако приложения, которые хотят, могут использовать свои секретные ключи для выполнения тех функций надежно.

Определения

- **Аутентификация** — Гарантирует, что вы - то, кто вы говорите, что вы, и что мы знаем, кто вы.
- **Клиент** — объект, который может получить билет. Этот объект обычно является или пользователем или хостом.
- **Учетные данные** — то же как билеты.
- **Демон** — программа, обычно та, которая работает на хосте UNIX, что сетевые запросы сервисов для аутентификации.
- **Host** — Компьютер, к которому можно обратиться по сети.
- **Экземпляр** — вторая часть главной части Kerberos. Это дает информацию, которая квалифицирует основного. Экземпляр может быть пустым. В случае пользователя экземпляр часто используется для описания надлежащего использования соответствующих учетных данных. В случае хоста экземпляр является полностью квалифицированным именем хоста.
- **Kerberos** — В Греческой мифологии, трехголовая собака, которая охраняет вход преступному миру. В компьютерном мире Kerberos является пакетом сетевой безопасности, который был разработан в MIT.
- **KDC** — Key Distribution Center. Машина, которая выполняет билеты Kerberos.
- **Keytab** — Ключевой файл таблицы, который содержит один или несколько ключей. Хост или сервис используют файл keytab почти таким же способом, как пользователь использует их пароль.
- **NAS** Сервер доступа к сети (коробка Cisco) или что-либо еще, что делает TACACS + запросы проверки подлинности и авторизация или передает пакеты учета.
- **Принципал** — строка, которая называет определенный объект, на который может быть назначен ряд учетных данных. Это обычно имеет три части под названием Основной, Экземпляр и ИМЕНОВАННАЯ ОБЛАСТЬ (REALM).Типичный формат стандартной основной части Kerberos является **primary/instanceREALM**.
- **Основной** — первая часть главной части Kerberos. В случае пользователя это - имя пользователя. В случае сервиса это - название сервиса.
- **ИМЕНОВАННАЯ ОБЛАСТЬ (REALM)** — логическая сеть, подаваемая одиночной базой данных Kerberos и рядом Key Distribution Center. Условно, имена области обычно являются всеми буквами в верхнем регистре, для дифференциации области от Интернет-домена.
- **Сервис** — Любая программа или компьютер вы обращаетесь по сети. Примеры сервисов включают:"хост" — хост, (например, когда вы используете Telnet и rsh),"ftp" —

FTP"krbtgt" — authentication; такой как разрешение на получение разрешения"популярность" — Электронная почта
- **Билет** — временный набор электронных мандатов, которые проверяют личность клиента для определенного сервиса.
- **TGT** — Разрешение на получение разрешения. Специальный билет Kerberos, который разрешает клиенту получать дополнительные билеты Kerberos в той же Области "Kerberos".Хорошая аналогия для разрешения на получение разрешения является трехдневным ски-пассом, который способен к четырем другим курортам. Вы показываете проход в том, какой бы ни обращаются, вы решаете перейти (пока он не истекает), и вы получаете билет на подъемник для того курорта. Как только у вас есть билет на подъемник, можно покататься на лыжах все, что вы хотите в том курорте. Если вы переходите к другому курорту на следующий день, вы еще раз показываете свой проход, и вы получаете дополнительный билет на подъемник для нового курорта. Различие - то, что программы Kerberos V5 замечают, что вы имеете ски-пасс выходных дней и получаете билет на подъемник для вас, таким образом, вы не должны выполнять транзакции сами.

Глюк

Этот раздел перечисляет несколько элементов, о которых необходимо знать:

- Удостоверьтесь, что вы удаляете всех замыкающих пробел в файлах конфигурации. Замыкающие пробел могут вызвать проблемы с krb5kdc сервером. В противном случае можно получить сообщение, которое говорит, "krb5kdc не может запустить базу данных для области".
- Удостоверьтесь, что часы на маршрутизаторе установлены в то же время как хост UNIX, который выполняет сервер KDC. Чтобы препятствовать тому, чтобы злоумышленники перезагрузили свои системные часы, чтобы продолжить использовать истекшие билеты, Kerberos V5 установлен для отклонения запросов билета от любого хоста, часы которого не в указанной максимальной расфазировке синхронизирующих импульсов KDC (как задано в kdc.conf файле). Точно так же хосты настроены для отклонения ответов от любого KDC, часы которого не в указанной максимальной расфазировке синхронизирующих импульсов хоста (как задано в krb5.conf файле). Значение по умолчанию для максимальной расфазировки синхронизирующих импульсов составляет 300 секунд (пять минут).
- Удостоверьтесь, что DNS работает должным образом. Несколько аспектов Kerberos полагаются на сервис имен. Для Kerberos для обеспечения его высокого уровня безопасности это более чувствительно к проблемам сервиса имен, чем некоторые другие части сети. Важно, чтобы ваши записи Системы доменных имен (DNS) и ваши хосты имели корректную информацию. Каждый канонический из имени хоста должен быть полностью определенным именем хоста (который включает домен), и каждый IP-адрес хоста должен обратное решение к установленному имени.
- Поддержка Cisco IOS Kerberos V5 не позволяет использование названий области нижнего регистра, и код Kerberos в Cisco IOS не аутентифицирует пользователей, если область находится в нижнем регистре. Это было исправлено в программном обеспечении Cisco IOS версии 11.2(7).См. идентификатор ошибки Cisco CSCdj10598 (только зарегистрированные клиенты).Единственный обходной путь должен

использовать прописные Имена области (который обычен).Области нижнего регистра работают для получения TGT, но не сервисных учетных данных. Так как Cisco использует их новый TGT для получения сервисных учетных данных (использовал предотвращать спуфинговую атаку KDC) во время регистрации аутентификации, проверка подлинности Kerberos, которая использует области нижнего регистра всегда, отказывает.

- Kerberos V5 для PAP PPP и CHAP может завершиться катастрофическим отказом маршрутизатор. Это было исправлено в программном обеспечении Cisco IOS версии 11.2(6).См. идентификатор ошибки Cisco CSCdj08828 (только зарегистрированные клиенты).Обходной путь для этого должен вызвать вход exec в маршрутизатор через **async mode interactive** без **автовыбора во время входа в систему** и затем сделать, чтобы пользователь запустил PPP вручную:`aaa authentication ppp default if-needed krb5 local`
- Kerberos V5 не делает авторизации или учета. Вам нужен некоторый другой код, чтобы сделать это.

Конфигурация маршрутизатора Cisco IOS

Конфигурация в этом разделе изображает полностью настроенный маршрутизатор AS5200, который делает Kerberos V5. Маршрутизатор в этой конфигурации использует сервер Kerberos для аутентификации и Сеансов VTY и пользователей, которые набирают в сделать PPP с Аутентификацией PAP.

Config AS5200 с 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
```

Конфигурация Kerberos KDC

Удостоверьтесь, что вам устанавливали соответствующие порты для **inetd**.

Примечание: Данный пример использует обертки. Если вы хотите зашифрованную Telnet, необходимо заменить обычный сеанс сетевого теледоступа сеансом Telnet с применением технологии Kerberos, таким образом, эти файлы имеют другое появление.

Установите порты для 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
----------------------------------------------------------------------
```

Установите файлы конфигурации Kerberos

Затем, необходимо установить несколько файлов конфигурации Kerberos, которые читает сервер KDC. Для получения дополнительной информации о каком эти параметры среднее значение, обращаются к Руководству Установки Kerberos или Руководству 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
    }
```

Установите базу данных для сервера KDC

Затем, необходимо создать базу данных, которую использует сервер KDC.

1. Введите **команду 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:` Это необходимо для получения **пароля srvtab** из маршрутизатора через TFTP с **командой kerberos srvtab remote**.`# kadmin/dbutil/kdb5_util stash -r CISCO.EDU Enter KDC database master key:`
2. Для добавления принципалов и пользователей к базе данных, используйте **команду 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. Добавьте пользователя:`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. Получите список текущей базы данных:`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. Добавьте запись для маршрутизатора 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. Извлеките ключ к таблице для маршрутизатора 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. Бросьте другой взгляд на базу данных:`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. Переместите файл keytab в место, где маршрутизатор в состоянии добраться до него:
```
# cp /etc/krb5.keytab /ts/
# chmod 777 /ts/krb5.keytab
```
9. Запустите сервер KDC:
```
# kdc/krb5kdc
#
```
10. Проверьте, чтобы удостовериться, что это фактически выполняется:
```
# ps -A | grep 'krb5'
 6043 ??       I        0:00.01 kdc/krb5kdc
23427 ttypf    S  +     0:00.05 grep krb5
```
11. Вынудите маршрутизатор считать свой ключевой элемент таблицы:
```
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. Проверьте маршрутизатор, чтобы удостовериться, что все готово:
```
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. Включите отладку и попытайтесь войти в маршрутизатор:
```
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
```

Пример результата отладки

Вот пользователь PPP, который успешно аутентифицируется.

```
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
```

Устранение неполадок

Этот раздел содержит различные сценарии для потенциальных проблем. Эти отладки помогают вам быстро видеть проблему.

Неправильное имя области

```
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 не работает

```
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
                                          ~~~~
```

Синхронизация маршрутизатора, не корректная

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

Вот то, что видит пользователь:

```
$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:
```

Клиент не в базе данных 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
```

Клиент Находится В Базе данных, но использует Неправильный пароль

```
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
```

Пользователь видит эти выходные данные:

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

```
User Access Verification

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

ЗАПИСЬ SRVTAB, не корректная на маршрутизаторе

```
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
```

Вот то, что видит пользователь:

```
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:
```

Ссылки

1. *Руководство системного администратора Kerberos V5* (прибывает в просмоленное, g-zipped файл),
2. *Руководство по установке Kerberos V5*
3. *Руководство пользователя Unix Kerberos V5*
4. Kerberos: Сетевой протокол аутентификации
5. Сетевая служба проверки подлинности Kerberos (GOST Group USC/ISI)
6. Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller. Kerberos: Сервис проверки подлинности для открытых сетевых систем", март 1988 USENIX
7. S. P . Миллер, B. C . Неумен, J. Я. Шиллер и J. H. Saltzer, "Проверка подлинности Kerberos и система авторизации", 21.12.87
8. R. M. Нидхэм и доктор медицины Шредер, "Использование Шифрования для аутентификации в Больших сетях Компьютеров", Связь ACM, Издания 21 (12), стр 993-999 (декабрь 1978)
9. V. L. Voydock и S. T. Кент, "Механизмы обеспечения безопасности в сетевых протоколах высокого уровня", *компьютерные обозрения*, издание 15 (2), ACM (июнь 1983)
10. Ли Гун, "Угроза безопасности В зависимости от Синхронизированных часов", *Анализ Операционных систем*, Vol 26, #1, стр 49-53
11. C . Неумен и J. Коль, "сетевая служба проверки подлинности Kerberos (V5)", RFC 1510, сентябрь 1993
12. B. Clifford Neuman и Теодор Tc'o, "Kerberos: сервис проверки подлинности для компьютерных сетей", IEEE Communication, 32 (9), сентябрь 1994**Примечание:** Многие из этих документов, который включает тот Неуменом, Шиллером и Штейнером (#9), также доступны через FTP от Системы Athena Массачусетского технологического института (MIT) - Документация Kerberos. Для получения копий RFC обратитесь к RFC Получения и Документам Стандартов.

Дополнительные сведения

- Страница поддержки Kerberos
- Техническая поддержка - Cisco Systems