أستكشاف أخطاء دعم عميل Kerberos V5 وإصلاحها وتكوينه

المحتويات

المقدمة

يقدم هذا المستند مثالا للتكوين، بالإضافة إلى بعض الحلول للمشاكل الشائعة. يتم توفير التقنيات التي تساعدك على أستكشاف أخطاء أي مشاكل وإصلاحها في هذا المستند أيضا. لا يتناول هذا المستند دعم Kerberized Telnet.

معظم هذه المواد في هذه المقالة جاءت من الوثائق المتاحة بحرية التي تأتي مع Kerberos ومن مختلف الأسئلة المتداولة (FAQs) حول الحزمة. جاءت التكوينات من موجه وظيفي وخادم Kerberos KDC.

يفترض هذا المستند أنك قمت بتجميع إصدار حالي من حزمة Kerberos من MIT وتثبيته بشكل صحيح. ارجع إلى المراجع في نهاية هذه المقالة للحصول على معلومات حول كيفية الحصول على Kerberos V5 وتجميعه وتثبيته.

لاحظ أيضا أن برنامج Cisco IOS® الإصدار 11.2 أو إصدار أحدث مطلوب لدعم Kerberos V5. وهذا يوفر دعما كاملا لمصادقة عميل Kerberos V، والتي تتضمن إعادة توجيه بيانات الاعتماد. يمكن للأنظمة التي تحتوي على بنية

Kerberos V الأساسية إستخدام مراكز توزيع المفاتيح (KDC) لمصادقة المستخدمين النهائيين للوصول إلى الشبكة أو الموجه. هذا تطبيق عميل وليس تنفيذ Kerberos KDC.

تعد Kerberos خدمة أمان قديمة وهي أكثر فائدة في الشبكات التي تستخدم Kerberos بالفعل.

ارجع إلى ملاحظات الإصدار 11.2 من برنامج Cisco IOS Software للحصول على معلومات أكثر تفصيلا حول الإصدارات التي تتضمن هذا الدعم.

للحصول على دعم Kerberos في إصدارات برنامج Cisco IOS التالية، ارجع إلى Software Advisor (مرشد البرامج) (العملاء المسجلون فقط).

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج IOS الإصدار 11.2 من Cisco والإصدارات الأحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

مقدمة إلى Kerberos

Kerberos هو بروتوكول مصادقة الشبكة للاستخدام على الشبكات غير الآمنة ماديا. وتستند كيربيروس إلى نموذج التوزيع الرئيسي الذي قدمته نيدهام وشرودر. (راجع الرقم 9 في قسم المراجع في هذا المستند. وهو مصمم لتوفير مصادقة قوية لتطبيقات العميل/الخادم باستخدام تشفير مفتاح سري. فهي تسمح للكيانات التي تتواصل عبر الشبكات بإثبات هويتها لبعضها البعض بينما تمنع التنصت أو الهجمات المتكررة. كما ينص على سلامة تدفق البيانات (مثل اكتشاف التعديل) والسرية (مثل منع القراءة غير المصرح بها) بمساعدة أنظمة التشفير مثل DES.

لا يوفر العديد من البروتوكولات المستخدمة في الإنترنت أي أمان. الأدوات المستخدمة ل "sniff" كلمة مرور خارج الشبكة هي قيد الاستخدام من قبل أدوات النظام. وبالتالي، فإن التطبيقات التي ترسل كلمة مرور عبر الشبكة غير مشفرة تكون حساسة. كما تعتمد تطبيقات العميل/الخادم الأخرى على برنامج العميل لتكون "صادقة" بشأن هوية المستخدم الذي يستخدمها. وتعتمد تطبيقات أخرى على العميل لتقييد أنشطته بتلك التي يسمح له بها، دون أي تنفيذ آخر من قبل الخادم.

تحاول بعض المواقع إستخدام جدران الحماية لحل مشاكل أمان الشبكة الخاصة بها. وتفترض جدران الحماية أن "الأشرار" موجودون في الخارج، وهو افتراض غير صحيح في كثير من الأحيان. بيد أن معظم حوادث جرائم الحاسوب التي تتسبب في مزيد من الضرر قد قام بها أشخاص من الداخل. كذلك، تمثل جدران الحماية عائقا كبيرا لأنها تقيد قدرة المستخدمين لديك على إستخدام الإنترنت.

تم إنشاء Kerberos بواسطة MIT كحل لمشاكل أمان الشبكة هذه. يستخدم بروتوكول Kerberos تشفيرا قويا، حتى يمكن للعميل إثبات هويته للخادم (والعكس بالعكس) عبر اتصال شبكة غير آمن. بعد إستخدام العميل والخادم ل Kerberos لإثبات هويته، يمكنهم أيضا تشفير جميع إتصالاتهم لضمان الخصوصية وسلامة البيانات أثناء تنفيذ أعمالهم.

Kerberos متاح بحرية من MIT، بموجب إشعار بإذن حقوق النسخ مشابه لذلك المستخدم لنظام تشغيل BSD و X11 Windowing. يوفر MIT Kerberos في نموذج المصدر. ويجري ذلك لكي يتمكن كل من يرغب في إستعماله ان ينظر إلى الشفرة لنفسه ويتأكد ان الشفرة جديرة بالثقة. بالإضافة إلى ذلك، بالنسبة لهؤلاء الذين يفضلون الاعتماد على منتج مدعوم مهنيا، تتوفر Kerberos كمنتج من العديد من البائعين المختلفين.

يعتمد دعم عميل Kerberos V5 على نظام مصادقة Kerberos الذي تم تطويره في MIT. تحت Kerberos، يرسل عميل (بشكل عام إما مستخدم أو خدمة) طلب تذكرة إلى مركز توزيع المفاتيح (KDC). تقوم KDC بإنشاء تذكرة منح تذكرة (TGT) للعميل، وتشفيرها بمساعدة كلمة مرور العميل كمفتاح، وإرسال TGT المشفر مرة أخرى إلى العميل. ثم يحاول العميل فك تشفير TGT، بمساعدة كلمة المرور الخاصة به. إذا قام العميل بفك تشفير TGT بنجاح، على سبيل المثال، إذا أعطى العميل كلمة المرور الصحيحة)، فإنه يحتفظ ب TGT الذي تم فك تشفيره. وهذا يشير إلى إثبات هوية العميل.

ويسمح TGT، الذي ينتهي في وقت محدد، للعميل بالحصول على تذاكر إضافية، مما يسمح بتقديم خدمات محددة. طلبات ومنح هذه التذاكر الإضافية شفافة.

ونظرا لأن Kerberos يقوم بالتفاوض الذي تمت مصادقته، ويتم تشفيره إختياريا، ويتصل بين أي نقطتين على الإنترنت، فإنه يوفر طبقة أمان لا تعتمد على الجانب الذي يوجد عليه أي من جدر الحماية. يتم إستخدام Kerberos بشكل أساسي في البروتوكولات على مستوى التطبيقات (ISO طراز المستوى 7)، مثل Telnet أو FTP، من أجل توفير أمان المستخدم للمضيف. كما يتم إستخدامها، ولو بشكل أقل تكرارا، كنظام المصادقة الضمنية لتدفق البيانات (مثل **SOCK_STREAM**) أو آليات RPC (المستوى 6 من طراز ISO). كما يمكن إستخدامها على مستوى أقل للأمان من المضيف إلى المضيف، في بروتوكولات مثل IP أو UDP أو TCP (المستوى 3 و 4 من طراز ISO). وعلى الرغم من ذلك، فإن مثل هذه العمليات نادرة، إن وجدت على الإطلاق.

وهو ينص على المصادقة المتبادلة والاتصالات الآمنة بين الأساسيات على شبكة مفتوحة عن طريق تصنيع مفاتيح سرية لأي طالب. كما يتم توفير آلية لنشر هذه المفاتيح السرية بأمان من خلال الشبكة. لا يوفر Kerberos التخويل أو المحاسبة. ومع ذلك، فإن التطبيقات التي ترغب في إستخدام مفاتيحها السرية لأداء تلك الوظائف بشكل آمن.

التعاريف

- **المصادقة**— تأكد من أنك على طبيعتك، ومن معرفتك من تكون.
- **الزبون** — كيان يمكنه الحصول على تذكرة. عادة ما يكون هذا الكيان إما مستخدما أو مضيفا.
- **بيانات الاعتماد** — مثل التذاكر.
- **Daemon**—برنامج يعمل عادة على مضيف UNIX، ويقدم طلبات الشبكة للمصادقة.
- **المضيف** — جهاز كمبيوتر يمكن الوصول إليه عبر شبكة.
- **المثيل** — الجزء الثاني من مدير Kerberos. وهو يعطي معلومات تؤهل الشخص الرئيسي. يمكن أن يكون المثيل فارغا. في حالة مستخدم ما، غالبا ما يتم إستخدام المثيل لوصف الاستخدام المقصود لبيانات الاعتماد المقابلة. في حالة المضيف، يكون المثيل هو اسم المضيف المؤهل بالكامل.
- **كيربروس** — في الاساطير اليونانية، الكلب ذو الرؤوس الثلاثة الذي يحرس المدخل إلى العالم السفلي. في عالم الحواسيب، Kerberos هو حزمة أمان شبكة تم تطويرها في MIT.
- **مركز KDC** — مركز توزيع رئيسي. جهاز يصدر تذاكر Kerberos.
- **علامة التبويب KeyTab**—ملف جدول مفاتيح يحتوي على مفتاح واحد أو أكثر. يستخدم المضيف أو الخدمة ملف علامة تبويب مفاتيح بنفس الطريقة التي يستخدم بها المستخدم كلمة المرور الخاصة به.
- **NAS**—خادم وصول إلى الشبكة (مربع Cisco) أو أي شيء آخر يقوم بطلب مصادقة TACACS+ والتفويض، أو يرسل حزم المحاسبة.
- **الأساسي**—سلسلة تسمي كيانا معينا يمكن تعيين مجموعة بيانات الاعتماد إليه. وهي عموما تتألف من ثلاثة أجزاء تدعى أوليا، مثيلا، وعالم.التنسيق النموذجي لنموذج Kerberos الأساسي هو **basic/instanceREALM**.

- **أساسي** — الجزء الأول من مدير Kerberos. في حالة مستخدم، هو اسم المستخدم. وفي حالة الخدمة، يكون اسم الخدمة.
- **Realm**—الشبكة المنطقية التي تخدمها قاعدة بيانات Kerberos واحدة ومجموعة من مراكز التوزيع الأساسية. وفقا للأعراف، أسماء النطاق عموما هي حروف كبيرة، لتمييز النطاق عن مجال الإنترنت.
- **الخدمة**—أي برنامج أو جهاز كمبيوتر يمكنك الوصول إليه عبر الشبكة. وتتضمن أمثلة الخدمات ما يلي:"host"— مضيف، (على سبيل المثال، عند إستخدام Telnet و Krbtgt"FTP"—"ftp"(rsh"— المصادقة، مثل تذكرة منح التذاكر"بوب"—بريد إلكتروني
- **التذكرة** — مجموعة مؤقتة من وثائق الإعتماد الإلكترونية التي تتأكد من هوية عميل ما لخدمة معينة.
- **TGT** — تذكرة منح التذاكر. تذكرة Kerberos خاصة تسمح للعميل بالحصول على تذاكر Kerberos إضافية داخل نطاق Kerberos نفسه.والقياس الجيد لتذكرة منح التذاكر هو تصريح التزحلق لمدة ثلاثة أيام والذي يعد جيدا في أربعة منتجعات مختلفة. يمكنك عرض التصريح في أي منتجع تقرر الذهاب إليه (حتى انتهاء صلاحيته)، وتحصل على تذكرة سفر لهذا المنتجع. بمجرد أن تحصل على تذكرة الوصول، يمكنك التزلج على كل ما تريد في ذلك المنتجع. إذا ذهبت إلى منتجع آخر في اليوم التالي، تظهر لك مرة أخرى بطاقة مرورك، وتحصل على تذكرة سفر إضافية إلى المنتجع الجديد. الفرق هو أن برامج Kerberos V5 تلاحظ أنك تحصل على تصريح التزلج في نهاية الأسبوع، وتحصل على تذكرة الوصول، حتى لا تضطر إلى إجراء المعاملات بنفسك.

أمسك

يسرد هذا القسم العديد من العناصر التي يجب أن تكون على دراية بها:

- تتأكد أنت أزلت كل فراغات في التشكيل مبرد. يمكن أن تتسبب المسافات الزائدة في حدوث مشاكل مع خادم krb5kdc. وإلا، يمكنك الحصول على رسالة تقول، "Krb5kdc لا يستطيع بدء قاعدة البيانات للمجال."
- تأكد من تعيين الساعة على الموجه إلى نفس وقت مضيف UNIX الذي يشغل خادم KDC. لمنع المتسللين من إعادة تعيين ساعات النظام الخاصة بهم لمتابعة إستخدام التذاكر منتهية الصلاحية، تم إعداد Kerberos V5 لرفض طلبات التذاكر من أي مضيف لا تقع ساعته ضمن الحد الأقصى المحدد لانحراف ساعة KDC (كما هو محدد في ملف kdc.conf). بالمثل، شكلت مضيف أن يرفض جواب من أي KDC الذي ساعة ليس ضمن الحد الأقصى المحدد لساعة تشويه المضيف (كما هو محدد في ملف krb5.conf). القيمة الافتراضية لأقصى انحراف للساعة هي 300 ثانية (خمس دقائق).
- تأكد من عمل DNS بشكل صحيح. تعتمد عدة جوانب من Kerberos على خدمة الأسماء. من أجل أن توفر Kerberos مستوى الأمان العالي الخاص بها، يكون من الأكثر حساسية لتسمية مشاكل الخدمة من بعض الأجزاء الأخرى من شبكتك. من المهم أن يكون لإدخالات نظام اسم المجال (DNS) والمضيفين لديك المعلومات الصحيحة. يجب أن يكون كل عنوان من عناوين اسم المضيف هو اسم المضيف المؤهل بالكامل (الذي يتضمن المجال)، ويجب أن يعكس كل عنوان IP الخاص بالمضيف الحل إلى الاسم القانوني.
- لا يسمح دعم Cisco IOS Kerberos V5 باستخدام أسماء النطاقات الصغيرة ولا تقوم شفرة Kerberos في برنامج Cisco IOS بمصادقة المستخدمين إذا كان النطاق في حالة صغيرة. تم إصلاح هذا في برنامج Cisco IOS الإصدار 11.2(7).أحلت cisco بق CSCdj10598 id (يسجل زبون فقط).الحل الوحيد هو إستخدام أسماء النطاق الكبير (وهو تقليدي).تعمل معاملات الأحرف الصغيرة من أجل إسترداد TGT، ولكن ليس بيانات اعتماد الخدمة. بما أن Cisco يستخدم TGT الجديد الخاص بها من أجل إسترداد بيانات اعتماد الخدمة (المستخدمة لمنع هجوم انتحال KDC) أثناء مصادقة التسجيل، فإن مصادقة Kerberos التي تستخدم حقول صغيرة تفشل دائما.
- يمكن أن يقوم Kerberos V5 ل PPP PAP و CHAP بتعطيل الموجه. تم إصلاح هذا في برنامج Cisco IOS الإصدار 11.2(6).أحلت cisco بق CSCdj08828 id (يسجل زبون فقط).يتمثل الحل البديل لهذا الإجراء في فرض تسجيل دخول EXEC إلى الموجه عبر **وضع غير متزامن تفاعلي** دون **التحديد التلقائي أثناء تسجيل الدخول** ثم مطالبة المستخدم ببدء تشغيل PPP يدويا:
```
aaa authentication ppp default if-needed krb5 local
```
- لا يقوم Kerberos V5 بالتفويض أو المحاسبة. تحتاج إلى بعض التعليمات البرمجية الأخرى للقيام بذلك.

تكوين موجه IOS من Cisco

يصف التكوين الموجود في هذا القسم موجه AS5200 تم تكوينه بالكامل يقوم Kerberos V5. يستخدم الموجه في هذا التكوين خادم Kerberos لمصادقة كل من جلسات عمل VTY والمستخدمين الذين يطلبون الدخول إلى PPP باستخدام مصادقة PAP.

AS5200 config مع 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
                                               =531159<11338:<:80 1
                                                              !
 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
```

تكوين Kerberos KDC

تأكد من أن لديك المنافذ المناسبة التي تم إعدادها ل ID.

ملاحظة: يستخدم هذا المثال المغلفات. إن يريد أنت Telnet مشفر، أنت تحتاج أن يستبدل ال telnet عادي مع ال kerberized telnet، لذلك هذا مبرد يتلقى مظهر مختلف.

إعداد المنافذ ل 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
-----------------------------------------------------------------
```

إعداد ملفات تكوين Kerberos

بعد ذلك، تحتاج إلى إعداد بعض ملفات تكوين Kerberos التي يقرأها خادم KDC. لمزيد من المعلومات حول ما تعنيه هذه المعلمات، ارجع إلى دليل تثبيت Kerberos أو دليل مسؤول النظام .

```
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
                                          {
```

إعداد قاعدة البيانات لخادم KDC

بعد ذلك، تحتاج إلى إنشاء قاعدة البيانات التي يستخدمها خادم KDC.

1. دخلت الأمر **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
```

هذا مطلوب لاسترداد كلمة مرور **srvtab** من الموجه عبر TFTP باستخدام الأمر **kerberos srvtab remote**.

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

2. لإضافة مبادئ ومستخدمين إلى قاعدة البيانات، أستخدم الأمر **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. إضافة مستخدم:

```
                                                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. الحصول على قائمة بقاعدة البيانات الحالية:

```
                                                    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. أضفت مدخل ل ال cisco مسحاج تخديد:

```
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. إستخراج مفتاح للجدول لموجه 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. ألق نظرة أخرى على قاعدة البيانات:

```
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. انقل ملف علامة التبويب الرئيسية إلى مكان يمكن للموجه الوصول إليه فيه:

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

9. بدء تشغيل خادم KDC:

```
kdc/krb5kdc #
#
```

10. تحقق للتأكد من تشغيله بالفعل:

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

11. إجبار الموجه على قراءة إدخال الجدول الرئيسي الخاص به:

```
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. تحقق من الموجه للتأكد من أن كل شيء جاهز:

```
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
=531159<11338:<:0 8 1 2
kerberos server CISCO.EDU 10.10.1.8
kerberos credentials forward
```

13. قم بتشغيل تصحيح الأخطاء وحاول تسجيل الدخول إلى الموجه:

```
cisco5200#terminal monitor
cisco5200#debug kerberos
Kerberos debugging is on
cisco5200#debug aaa authen
AAA Authentication debugging is on
cisco5200#show clock
CDT Thu Apr 17 1997 10:16:41.797
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
```

إخراج تصحيح الأخطاء للعينة

فيما يلي مستخدم PPP الذي يقوم بالمصادقة بنجاح.

```
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%
```

استكشاف الأخطاء وإصلاحها

يحتوي هذا القسم على سيناريوهات مختلفة للمشاكل المحتملة. تساعدك هذه الأخطاء على رؤية المشكلة بسرعة.

اسم النطاق الخطأ

```
                                                                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 لا يعمل

```
  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
                         ~~~~
```

ساعة الموجه غير صحيحة

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

فيما يلي ما يراه المستخدم:

```
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
```

العميل غير موجود في قاعدة بيانات 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
```

العميل موجود في قاعدة البيانات لكنه يستخدم كلمة مرور غير صحيحة

```
''=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
```

يرى المستخدم هذا الإخراج:

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


                                    User Access Verification

                                        Username: cisco1
                                               :Password
                                     Access denied %

                                               :Username
```

إدخال SRVTAB غير صحيح على الموجه

```
                                                    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
```

فيما يلي ما يراه المستخدم:

```
... 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
```

المراجع

1. *دليل مسؤول النظام* Kerberos V5 (يرد في ملف مضغوط G-zipped)
2. *دليل تثبيت* Kerberos V5
3. *دليل مستخدم UNIX* Kerberos V5
4. Kerberos: بروتوكول مصادقة الشبكة
5. خدمة مصادقة شبكة Kerberos (مجموعة GOST الخاصة ب USC/ISI)
6. جينيفر جي. شتاينر، كليفورد نيومان، جيفري إ. شيلر. "Kerberos: خدمة مصادقة لأنظمة الشبكة المفتوحة "، USENIX MAR 1988
7. س. ب. ميلر، ب. س. نيومان، ج. إ. شيللر، و ج. ه. سالتزر، "نظام كربروس للتوثيق والإذن،" 87/21/12
8. ر. م. نيدهام و م. د. شرودر، "إستخدام التشفير من أجل المصادقة في شبكات كبيرة من أجهزة الكمبيوتر"، مراسلات ACM، المجلد 21(12)، الصفحات 993-999 (كانون الأول/ديسمبر 1978)
9. V. L. Voydock and S. T. Kent، "آليات الأمن في بروتوكولات الشبكة الرفيعة المستوى"، *الدراسات الاستقصائية الحاسوبية*، المجلد 15(2)، ACM (حزيران/يونيه 1983)
10. لي غونغ، "مخاطر أمنية تتعلق بالاعتماد على الساعات المتزامنة"، *إستعراض نظم التشغيل*، المجلد 26، المجلد الأول، الصفحات 49-53
11. C. Neuman and J. Kohl، "The Kerberos Network Authentication Service (V5)"، RFC 1510، أيلول/سبتمبر 1993
12. B. Clifford Newan and Thiore TsO، "Kerberos: خدمة مصادقة لشبكات الكمبيوتر" IEEE Communications، 32(9)، أيلول/سبتمبر 1994 **ملاحظة:** العديد من هذه الوثائق، التي تشمل وثيقة (Neuman، Schiller، and Steiner #9) متاحة أيضا عن طريق FTP من نظام MIT Athena - وثائق Kerberos . للحصول على نسخ من RFCs، ارجع إلى الحصول على مستندات RFCs والمعايير.

معلومات ذات صلة

- صفحة دعم Kerberos

- الدعم الفني - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).