Kerberos V5 クライアント サポートのトラブルシューティングと設定

内容

概要

このドキュメントでは、設定例および一般的な問題のソリューションを提供します。また、このドキュメントでは、問題のトラブルシューティングに役立つテクニックを紹介します。このドキュメントでは、Kerberos 対応 Telnet のサポートは扱っていません。

このドキュメントに記載されている資料の多くは、Kerberos 付属の無料で入手可能なドキュメントと、Kerberos パッケージで参照可能ないくつかの FAQ から引用したものです。設定例は、動作可能なルータと Kerberos KDC サーバからとったものです。

このドキュメントでは、MITからKerberosパッケージのバージョン5の最新リリースを正しくコンパイルしてインストールしていることを前提としています。Kerberos V5の入手、コンパイル、インストール方法については、この記事の最後にある参考資料を参照してください。

また、Kerberos V5 をサポートするには、Cisco IOS(R) ソフトウェア リリース 11.2 以降が必要です。これにより、クレデンシャル転送を含むKerberos Vクライアント認証が完全にサポートされます。Kerberos V インフラストラクチャを使用するシステムでは、ネットワーク アクセスまたはルータ アクセスのエンドユーザの認証に、それぞれの Key Distribution Center (KDC; 鍵発行局) を使用できます。これはクライアント実装であり、Kerberos KDC実装ではありません。

Kerberos は、レガシー セキュリティ サービスと考えられ、すでに Kerberos を使用しているネットワークでは特に有用です。

このサポートを実装しているバージョンの詳細については、『Cisco IOS ソフトウェア リリース 11.2 のリリース ノート』を参照してください。

それ以降のCisco IOSソフトウェアリリースでのKerberosサポートについては、Software Advisor (登録ユーザ専用) を参照してください。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS ソフトウェア リリース 11.2 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

Kerberos の概要

Kerberos は、物理的にセキュアではないネットワークで使用するためのネットワーク認証プロトコルです。Kerberos は、Needham と Schroeder の提唱による鍵配布モデルを基盤にするものです。(このドキュメントの「参考資料」セクションの番号 9 を参照してください)。Kerberos は、秘密鍵による暗号化を使用することにより、クライアント/サーバ アプリケーションに強固な認証を提供する設計になっています。Kerberos では、ネットワークで通信を行うエンティティが互いに自分の身元を証明できるようにして、盗聴やリプレイ攻撃を防止します。また、DES など暗号化システムを使用して、データ ストリームの整合性 (改ざんの検出など) や機密性 (不正読み取りの防止など) も提供します。

インターネットで使用されているプロトコルの多くでは、セキュリティが提供されません。システム クラッカーは、ネットワークからパスワードを「盗聴」するツールをよく使用します。そのため、パスワードを暗号化せずにネットワークに送信しているアプリケーションには脆弱性があ

ります。また、使用しているユーザの身元をクライアント プログラムが「ありのままに」報告することを前提にしているクライアント/サーバ アプリケーションもあります。さらに、クライアントで実行が許可されているアクティビティの制限をクライアントに依存し、サーバではその他の制限を実施していないアプリケーションもあります。

サイトによっては、ファイアウォールを使用して、ネットワークのセキュリティ問題を解決しようとしているところもあります。ファイアウォールでは「犯罪者」が外部にいることを前提にしていますが、多くの場合、この前提条件は正しくありません。これに反して、大きな被害を引き起こしたコンピュータ犯罪の事件の多くは、内部の人間の犯行によるものでした。また、ファイアウォールには、ユーザがインターネットを使用できる方法が制限されるといった大きな欠点もあります。

Kerberos は、このようなネットワーク セキュリティの問題に対するソリューションとして、MIT で開発されたものです。Kerberos プロトコルでは強固な暗号化を使用しており、セキュアではないネットワーク接続を介して、クライアントは自身の身元をサーバに (その逆も同様に) 証明します。まず、クライアントとサーバでそれぞれの身元証明に Kerberos を使用し、次に、両者が業務を遂行する際にも、すべての通信を暗号化してプライバシーとデータ整合性を保証できます。

Kerberos は MIT から無料で入手でき、著作権許諾の表記に従って使用できます。著作権許諾の表記は、BSD オペレーティング システムや X11 Windowing システムで使用されているものに類似しています。MIT では Kerberos をソース形式で提供しています。このため、使用を検討しているユーザは、自分でコードに目を通して、コードが信頼できるものであるかどうかを確認できます。さらに、専門家によるサポートのある製品を求めるユーザ向けには、Kerberos はさまざまなベンダーから製品として販売されています。

Kerberos V5 のクライアント サポートは、MIT が開発した Kerberos 認証システムが基盤になっています。Kerberos では、クライアント (一般に、ユーザまたはサービスのいずれか) が、Key Distribution Center (KDC; 鍵発行局) にチケットの要求を送信します。 KDC では、クライアントのための Ticket-Granting Ticket (TGT; チケット認可チケット) を作成し、クライアントのパスワードを鍵に使用して暗号化し、暗号化した TGT をクライアントに返信します。続いて、クライアントでは、自身のパスワードを使用して TGT の復号化を実行します。クライアントは、(たとえば、クライアントが正しいパスワードを使用したとして) TGT の復号化に成功すると、復号化した TGT を保存します。これは、クライアントの身元が証明されたことを意味します。

TGT は一定の有効期間の間、追加チケットの取得をクライアントに許可するもので、この追加チケットによって個別のサービスへのアクセスが許可されます。この追加チケットの要求と許可は、ユーザに対して透過的に実行されます。

Kerberos ではインターネットのどのような 2 地点間であっても、認証がネゴシエートされ、オプションで暗号化が実行され、通信が実行されるため、これによって提供されるセキュリティのレイヤは、クライアントがファイアウォールのどちら側に配置されているかには依存しません。Kerberos は、主に、Telnet や FTP などのアプリケーション レベルのプロトコル (ISO モデルのレベル 7) で、ユーザにホストのセキュリティを提供するために使用します。また、使用頻度は下がりますが、データ ストリーム (SOCK_STREAM など) や RPC メカニズム (ISO モデルのレベル 6) の暗黙的な認証システムとしても使用されることもあります。 また、下位レベルのホスト間セキュリティのために IP、UDP、TCP などのプロトコル (ISO モデルのレベル 3 および 4) で使用されることもあります。 ただし、このような実装は、あったとしてもまれにしかありません。

Kerberos では、すべての要求元の秘密鍵を作成することで、オープン ネットワークのプリンシパル間の相互認証とセキュアな通信を実現します。また、これらの秘密鍵が安全にネットワークで伝搬されるメカニズムも提供されます。Kerberos では、認可とアカウンティングは提供されま

せん。ただし、必要であれば、アプリケーションでこのような機能をセキュアに実行するために、秘密鍵を使用することはできます。

定義

- **認証**：自分が自分の言っている相手であること、および自分が誰であるかを私たちが知っていることを確認します。
- **Client**：チケットを取得できるエンティティ。このエンティティは、通常、ユーザかホストのいずれかです。
- **クレデンシャル**：チケットと同じです。
- **Daemon**：通常はUNIXホスト上で実行されるプログラムで、認証のネットワーク要求を処理します。
- **ホスト**：ネットワーク経由でアクセスできるコンピュータ。
- **インスタンス**:Kerberosプリンシパルの2番目の部分。プライマリを修飾する情報を提供します。インスタンスは、ヌルの場合もあります。ユーザの場合、通常、インスタンスは対応するクレデンシャルの使用目的を記述するために使用されます。ホストの場合、インスタンスは完全修飾ホスト名です。
- **Kerberos**：ギリシャ神話で、下界への入り口を保護する3頭の犬。コンピュータの分野では、Kerberos は、MIT で開発されたネットワーク セキュリティ パッケージです。
- **KDC**：キー配布センター。Kerberos チケットを発行するマシン。
- **Keytab**:1つ以上のキーを含むキーテーブルファイル。ユーザがパスワードを使用する方法とほぼ同じように、ホストまたはサービスが keytab ファイルを使用します。
- **NAS**:Network Access Server（NAS；ネットワークアクセスサーバ）（Ciscoのボックス）など、TACACS+の認証および許可要求を行う場合、またはアカウンティングパケットを送信する場合。
- **Principal**：一連のクレデンシャルを割り当てることができる特定のエンティティを指定する文字列。一般に、プライマリ、インスタンス、およびレルムという名前の 3 つの部分で構成されます。一般的な Kerberos のプリンシパルの標準形式は、<プライマリ>/<インスタンス><レルム> です。
- **プライマリ**:Kerberosプリンシパルの最初の部分。ユーザの場合、ユーザ名です。サービスの場合、サービスの名前です。
- **REALM**：単一のKerberosデータベースとキー配布センターのセットによって提供される論理ネットワーク。標準では、インターネット ドメインのレルムと区別するため、一般的にレルム名はすべて大文字です。
- **サービス**：ネットワーク経由でアクセスするプログラムまたはコンピュータ。サービスの例には、次のものがあります。「host」：ホスト（Telnetやrshを使用する場合など）「ftp」:FTP「krbtgt」：認証、チケット認可チケットなど「pop」：電子メール
- **チケット**：特定のサービスのクライアントのIDを確認する一時的な電子認証情報セット。
- **TGT**：チケット認可チケット。同じ Kerberos レルム内の Kerberos の追加チケットの取得をクライアントに許可する、特別な Kerberos チケット。チケット認可チケットのわかりやすい例は、別々の 4 つのリゾート地で優待を受けられる 3 日間のスキー パスです。（期限が切れるまでの間は）どのリゾート地に行っても、パスを見せれば、そのリゾート地のリフト券がもらえます。リフト券を手に入れたら、そのリゾート地で好きなだけスキーを楽しめます。次の日に別のリゾート地に行った場合は、もう一度パスを見せれば、新しいリゾート地の別のリフト券がもらえます。異なる点は、Kerberos V5 プログラムは、持っている週末用のスキー パスを見つけて、リフト券をもらってきてくれるため、ユーザ自身が交換のやり取りを行う必要がないことです。

ヒント

このセクションでは、注意が必要ないくつかの事項を列記します。

- 設定ファイルでは、末尾のスペースはすべて削除してください。末尾のスペースは、krb5kdc サーバで問題を引き起こす可能性があります。そうでない場合でも、「krb5kdc cannot start the database for the realm」というメッセージが返される場合もあります。
- ルータのクロックには、確実に KDC サーバが稼働している UNIX ホストと同じ時刻を設定するようにしてください。侵入者が、自分のシステム クロックをリセットして、有効期限の切れたチケットを引き続き使用することを防止するため、Kerberos V5 では、（kdc.conf ファイルで指定した）KDC の最大クロック スキューの範囲外のクロックのホストからのチケット要求は、拒否するように設定されています。 同様に、ホストでは、（krb5.conf ファイルで指定した）ホストの最大クロック スキューの範囲外のクロックの KDC からの応答は、拒否するように設定されています。 最大クロック スキューのデフォルト値は、300 秒（5 分）です。
- DNS が正しく機能するようにしてください。いくつかの面では Kerberos はネーム サービスに依存しています。Kerberos は高レベルのセキュリティを提供しているため、ネットワークの他の部分よりもネーム サービスの問題の影響を受けやすくなっています。Domain Name System（DNS; ドメイン ネーム システム）のエントリとホストに、正しい情報が設定されていることが重要です。各ホストの標準名は完全修飾ホスト名（ドメインを含む）であり、各ホストの IP アドレスは標準名に逆解決される必要があります。
- Cisco IOS の Kerberos V5 サポートでは、小文字のレルム名の使用が許可されていないため、レルムが小文字の場合は、Cisco IOS の Kerberos コードではユーザが認証されません。これについては、Cisco IOS ソフトウェア リリース 11.2(7) で修正されています。Cisco Bug ID CSCdj10598(登録ユーザ専用)を参照してください。唯一の回避策は、（標準に合わせて）大文字のレルム名を使用することです。小文字のレルムの場合、TGT の取得は正しく機能しますが、サービスのクレデンシャルは取得できません。Cisco 製品では、ロギング認証時に新しい TGT を使用して、（KDC へのスプーフィング攻撃からの保護に使用する）サービスのクレデンシャルを取得するため、小文字のレルムを使用した Kerberos 認証は必ず失敗します。
- Kerberos V5 で PPP PAP および CHAP を使用すると、ルータがクラッシュする可能性があります。これについては、Cisco IOS ソフトウェア リリース 11.2(6) で修正されています。Cisco Bug ID CSCdj08828(登録ユーザ専用)を参照してください。この問題の回避策は、次のように、async mode interactive を autoselect during-login なしで使用して、ルータへの口グインを強制的に実行して、ユーザに PPP を手動で開始させます。
  ```
  aaa authentication ppp default if-needed krb5 local
  ```
- Kerberos V5 では、認可とアカウンティングは実行されません。これらを実行するには、追加のコードが必要です。

Cisco IOS ルータの設定

このセクションの設定は、Kerberos V5を実行する完全に設定されたAS5200ルータを示しています。この設定のルータは、PAP認証を使用してダイヤルインするVTYセッションとユーザの両方を認証するためにKerberosサーバを使用します。

Kerberos V5 を使用する AS5200 の設定

```
version 11.2
service timestamps debug datetime msec
!
hostname cisco5200
!
aaa new-model
aaa authentication login cisco2 krb5 local
aaa authentication ppp cisco krb5 local
enable secret
enable password
!
username cisco password cisco
ip host-routing
ip domain-name cisco.edu
ip name-server 10.10.1.25
ip name-server 10.10.20.3
kerberos local-realm CISCO.EDU
kerberos srvtab entry host/cisco5200.cisco.edu@CISCO.EDU
0 861289666 2
1 80:>:11338>531159=
!
 !--- You do not actually enter the previous line. !---
Enter "kerberos srvtab remote 10.10.1.8 /ts/krb5.keytab"
and the !--- the router TFTPs the key entry on its own.
kerberos server CISCO.EDU 10.10.1.8 kerberos credentials
forward isdn switch-type primary-5ess clock timezone GMT
-6 clock summer-time CDT recurring ! controller T1 0
framing esf clock source line primary linecode b8zs pri-
group timeslots 1-24 ! controller T1 1 framing esf clock
source line secondary linecode b8zs pri-group timeslots
1-24 ! interface Ethernet0 ip address 10.10.110.245
255.255.255.0 no ip mroute-cache ! interface Serial0 no
ip address no ip mroute-cache shutdown ! interface
Serial1 no ip address no ip mroute-cache shutdown !
interface Serial0:23 ip unnumbered Ethernet0 no ip
mroute-cache encapsulation ppp isdn incoming-voice modem
no cdp enable ! interface Serial1:23 ip unnumbered
Ethernet0 no ip mroute-cache encapsulation ppp isdn
incoming-voice modem no cdp enable ! interface Group-
Async1 ip unnumbered Ethernet0 no ip mroute-cache
encapsulation ppp async mode interactive peer default ip
address pool mypool dialer in-band dialer idle-timeout
9999 dialer-group 1 no cdp enable ppp authentication pap
cisco group-range 1 48 ! ip local pool mypool
10.10.110.97 10.10.110.144 no ip classless ip route
0.0.0.0 0.0.0.0 10.10.110.254 ! dialer-list 1 protocol
ip permit ! line con 0 login authentication test line 1
48 autoselect ppp login authentication cisco2 modem
InOut transport input all line aux 0 modem InOut
transport input all flowcontrol hardware line vty 0 10
exec-timeout 0 0 login authentication cisco2 ! end
```

Kerberos KDC の設定

inetd のポート設定が正しいことを確認します。

注： この例では、ラッパーを使用します。.暗号化 Telnet を使用する場合は、通常の Telnet を Kerberos 対応 Telnet に置き換える必要があります。その場合、下記のファイルの表示とは異なります。

inetd ポートの設定

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

kerberos88/udpkdc
kerberos88/tcpkdc

kxct549/tcp

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

#cat /etc/inetd.conf

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

Kerberos の設定ファイルの設定

続いて、KDC サーバで読み込まれる Kerberos の設定ファイルのいくつかの設定を行う必要があります。下記のパラメータの意味については、『Kerberos Install Guide or the System Admin Guide』を参照してください。

```
# cat /etc/krb5.conf

[libdefaults]
        default_realm =  CISCO.EDU
        ticket_lifetime = 600
```

```
        default_tgs_enctypes = des-cbc-crc
        default_tkt_enctypes = des-cbc-crc

[realms]
        CISCO.EDU = {
        kdc =  ciscoaxa.cisco.edu:88
        admin_server =  ciscoaxa.cisco.edu
        default_domain =  CISCO.EDU
        }

[domain_realm]
        .cisco.edu = CISCO.EDU
        cisco.edu  = CISCO.EDU

[logging]
        kdc = FILE:/var/log/krb5kdc.log
        admin_server = FILE:/var/log/kadmin.log
        default = FILE:/var/log/krb5lib.log


# cat /usr/local/var/krb5kdc/kdc.conf

[kdcdefaults]
      kdc_ports = 88,750

[realms]
      CISCO.EDU = {
         database_name = /usr/local/var/krb5kdc/principal
         admin_keytab = FILE:/usr/local/var/krb5kdc/kadm5.keytab
         acl_file = /usr/local/var/krb5kdc/kadm5.acl
         acl_file = /usr/local/var/krb5kdc/kadm5.dict
         key_stash_file = /usr/local/var/krb5kdc/.k5.CISCO.EDU
         kadmind_port = 749
         max_life = 10h 0m 0s
         max_renewable_life = 7d 0h 0m 0s
         master_key_type = des-cbc-crc
         supported_enctypes = des-cbc-crc:normal des:normal des:v4
des:norealm des:onlyrealm des:afs3
     }
```

KDC サーバのデータベースの設定

次に、KDC サーバで使用するデータベースを作成する必要があります。

1. kdb5_util コマンドを入力します。

```
# 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:
```

次のコマンドは、kerberos srvtab remote コマンドを使用して、TFTP 経由でルータから srvtab のパスワードを取得するために必要です。

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

2. プリンシパルとユーザをデータベースに追加するためには、kadmin.local コマンドを使用します。

```
# 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. ユーザを追加します。

```
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. 現在のデータベースのリストを取得します。

```
kadmin.local:  listprincs
kadmin/admin@CISCO.EDU
kadmin/changepw@CISCO.EDU
cisco1@CISCO.EDU
K/M@CISCO.EDU
krbtgt/CISCO.EDU@CISCO.EDU
kadmin/history@CISCO.EDU
```

5. Cisco ルータのエントリを追加します。

```
kadmin.local:  ank host/cisco5200.cisco.edu@CISCO.EDU
Enter password for principal "host/cisco5200.cisco.edu@CISCO.EDU":

Re-enter password for principal "host/cisco5200.cisco.edu@CISCO.EDU":
Principal "host/cisco5200.cisco.edu@CISCO.EDU" created.
```

6. Cisco ルータのテーブルの鍵を抽出します。

```
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. データベースを再確認します。

```
kadmin.local:  listprincs
kadmin/admin@CISCO.EDU
kadmin/changepw@CISCO.EDU
cisco1@CISCO.EDU
K/M@CISCO.EDU
krbtgt/CISCO.EDU@CISCO.EDU
kadmin/history@CISCO.EDU
host/cisco5200.cisco.edu@CISCO.EDU

kadmin.local:  quit
```

8. keytab ファイルを、ルータがアクセス可能な場所に移動します。

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

9. KDC サーバを起動します。

```
# kdc/krb5kdc
#
```

10. 実際に稼働していることを確認します。

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

11. ルータに、鍵テーブルのエントリを読み込ませます。

```
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. ルータで準備がすべて完了したことを確認します。

```
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. デバッグを有効にして、ルータへのログインを試します。

```
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
```

debug 出力例

次の例は、PPP ユーザの認証が成功したときのものです。

```
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
```

トラブルシュート

このセクションでは、潜在的な問題が発生するさまざまなシナリオを紹介します。下記のデバッグは、問題を迅速に理解するのに役立ちます。

レルム名が正しくない

```
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 が機能しない

```
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
                                        ~~~~
```

ルータのクロックが正しくない

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

ユーザには、次のように表示されます。

```
$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:
```

クライアントが Kerberos データベースに存在しない

```
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
```

クライアントはデータベースに存在するが、パスワードが正しくない

```
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
```

ユーザには、次の出力が表示されます。

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


User Access Verification

Username: cisco1
Password:
% Access denied

Username:
```

ルータの SRVTAB エントリが正しくない

```
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
```

ユーザには、次のように表示されます。

```
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:
```

参考資料

1. Kerberos V5 System Administrator's Guide（tar 形式、g-zip 形式のファイルにて提供）
2. Kerberos V5 Installation Guide
3. Kerberos V5 UNIX User's Guide
4. Kerberos:ネットワーク認証プロトコル
5. The Kerberos Network Authentication Service (USC/ISI's GOST Group)
6. Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller."Kerberos:An Authentication Service for Open Network Systems』、USENIX Mar 1988
7. S. P. Miller, B. C. Neuman, J. I. Schiller, and J. H. Saltzer, "Kerberos Authentication and Authorization System", 12/21/87
8. R. M. Needham and M. D. Schroeder、『Using Encryption for Authentication in Large Networks of Computers』、Communications of the ACM、Vol. 21(12)、pp. 993-999（1978年12月）
9. V. L. Voydock and S. T. Kent、『Security Mechanism in High-Level Network Protocols』、*Computing Surveys*、Vol. 15(2)、ACM（1983年6月）
10. Li Gong 著、『A Security Risk of Depending on Synchronized Clocks』、Operating Systems Review、Vol 26、#1、pp 49-53
11. C. Neuman and J. Kohl、『The Kerberos Network Authentication Service (V5)』、RFC 1510、1993年9月
12. B. Clifford NeumanとTheodore Ts'o、「Kerberos:An Authentication Service for Computer Networks』、IEEE Communications、1994年9月32日**注：Neuman、**Schiller、およびSteiner (#9)によるドキュメントの多くは、MIT Athena System - Kerberos DocumentationからFTPで入手できます。RFC のコピーを入手するには、『RFC および標準に関する文書の入手方法』を参照してください。

関連情報

- Kerberos サポート ページ
- テクニカルサポート - Cisco Systems