Sybase のためのケルベロスの構成

著者： **Joshua Meckler**

はじめに

Adaptive Server Enterprise、Open Client/Open Server、jConnect などの Sybase 製品でケルベロス・セキュリティを使用する場合、クライアントとサーバ間の接続を正常に確立するために一連の設定タスクが必要になります。これらの設定タスクは、CyberSafe、MIT Kerberos、MicroSoft Active Directory などケルベロス・プロバイダによって異なる場合があります。
各ケルベロス・プロバイダについての詳細は Sybase ドキュメントの範囲外であるため、それぞれのケルベロス・ベンダが提供しているマニュアルを参照することをおすすめします。このホワイトペーパーでは、クライアントとサーバ間でケルベロス接続を確立するための設定手順について概説します。また、CyberSafe、MIT Kerberos、および MicroSoft Active Directory に固有の設定情報も扱います。

Sybase で動作するようケルベロスを設定する

ケルベロス・セキュリティ・ソフトウェアをインストールし、Sybase 製品で動作するよう構成するには、次の一般的な手順を踏む必要があります。

ケルベロス・ライブラリおよびケルベロス KDC (Key Distribution Center ：キー配布センタ) のソフトウェアを購入またはダウンロードする

KDC およびケルベロス admin デーモンを設定して実行する

ケルベロス構成ファイルを設定する (例えば、 krb5.conf).

KDC にケルベロス・ユーザ (ユーザ・プリンシパル) とサーバ・プリンシパル (サービス・プリンシパル) を作成する

ケルベロス接続を受け入れるよう Sybase ASE または Open Server を構成する

サーバに接続する

ケルベロス・ライブラリおよびケルベロス KDC (Key Distribution Center ：キー配布センタ) のソフトウェアを購入またはダウンロードする

Sybase のクライアントおよびサーバにはケルベロス・ソフトウェアが付属していないため、購入またはダウンロードする必要があります。このソフトウェアは次のコンポーネントで構成されています。

ケルベロス・ライブラリ： GSS (Generic Security Services ：汎用セキュリティ・サービス) ライブラリまたは libgss と呼ばれ、明確に定義された GSS API を実装します。GSS ライブラリには、CyberSafe Limited が提供しているバージョンと MIT バージョンがあります。MIT のオープ・ソース・ケルベロス・ライブラリは自由にダウンロードできますが、サポートが公開ニュース・グループに限定され、使用プラットフォーム用の MIT ソース・コードのコンパイルが必要になることがあります。これらのライブラリは、ケルベロスを使用するサーバおよびクライアント・マシンのそれぞれに必要です。

ケルベロス・キー配布センタ (KDC) サーバ：ユーザおよびサーバのための倉庫として機能します。ユーザおよびサーバの ID の検証も行います。一般に、KDC はアプリケーションやユーザ・ログインに使用されない隔離されたマシンにインストールされます。

通常、KDC は、admin 管理デーモンおよび kpasswd デーモンの 2 つのデーモンと組み合わせて実行されます。admin デーモンでは KDC データベースが管理されます。このサーバを使用することで、ユーザおよびサービス・プリンシパルの追加、パスワードの変更、keytab ファイルの抽出などの機能を実行できます。kpasswd デーモンは、ユーザが各自のパスワードを変更できるようにします。

注： MicroSoft Active Directory をケルベロス・プロバイダとして使用する場合、別途 KDC または admin デーモンをインストールする必要はありません。Active Directory が KDC および admin デーモンの両方の役割を担うからです。Active Directory の詳細については後で説明します。

KDC およびケルベロス admin デーモンを設定して実行する

この手順はベンダによって異なります。ベンダから提供されるマニュアルを読み、インストール要件に関するベンダの指示に従うことを強くおすすめします。

ケルベロス構成ファイルを設定する

MIT を始めとする一部のケルベロス・クライアントでは、ケルベロス構成ファイルを使用する必要があります。通常、このファイルには krb5.conf という名前が付けられます。構成ファイルを使用することで、たとえばデフォルト・レルム、KDC が稼働するマシンのホスト名、ケルベロス認証中に要求されるデフォルト暗号キーなどの値を設定できます。このファイルのデフォルトの保管場所はベンダによって異なります。

注： MIT ベースのケルベロス・ソフトウェアのエンドユーザは、各自の構成ファイルを独自に設定し、このファイルを指すよう環境変数を設定することができます。詳細については、ベンダのマニュアルを参照してください。

MIT バージョンのケルベロスとは異なり、CyberSafe バージョンでは krb5.conf 構成ファイルが使用されません。代わりに、デフォルトでは、MicroSoft Active Directory が DNS によってケルベロス名前マッピングを行うときと同様に、DNS レコードによって KDC アドレス・マッピングとレルム情報を見つけます。CyberSafe 製品では、krb.conf および krb.realms の 2 つのファイル内で KDC およびレルム・マッピング情報を見つけることもできます。詳細については、CyberSafe のマニュアルを参照してください。

krb5.conf ファイルの構造については、MIT ケルベロス・オンライン・マニュアル (http://web.mit.edu/kerberos/www/) を参照してください。

注：krb5.conf ファイルは、MIT ケルベロス・クライアントを使用して任意のベンダの KDC に対して認証を行う場合に必要です。また、Java クライアントを使用する場合にも必要になります。

次のコードは krb5.conf の例です。

```
#
# これは krb5.conf のサンプル・ファイルです。このファイルは、たとえば MIT
# ケルベロス・ライブラリや Sun の Java ケルベロス実装を使用する
# クライアント用です。
#
# 実際に使用する場合は、デフォルト・レルム、[realms]、および [domain_realm] 情報を
# 各自のケルベロス環境に合わせて変更してください。また、このファイルではデフォルト・
# エンコーディング・タイプが des-cbc-crc (すなわちシングル DES)に設定されている
# ことに注意してください。クライアントおよびサーバで使用しているケルベロス実装に応じて、
# 他のエンコード・タイプ (トリプル DES など) を使用することもできます。
#
# このファイルをそのまま使用しないでください。
#
#

         [libdefaults]
         # ここで独自のデフォルト・レルムを設定します。
         default_realm = MYREALM
         default_tgs_enctypes = des-cbc-crc
         default_tkt_enctypes = des-cbc-crc
         kdc_req_checksum_type = 2
         ccache_type = 2

[realms]

         MYREALM = {
            # KDC のホスト名 kdc = kdchost を入力する必要が
            あります。
        admin_s

 erver =

 kdchost

        }

 [domain_realm]

         # これらの値は、企業の DNS マッピングとデフォルト・レルムに基づいて
         # 変更してください。
         .sybase.com =

 MYREALM

         sybase.com = MYREALM

 [logging]

default = FILE:/var/krb5/kdc.log kdc = FILE:/var/krb5/kdc.log
kdc_rotate = {

 # kdc.log の循環頻度。ログはこの期間以下の頻度で循環します。
 # KDC の使用頻度が低い場合、循環頻度は低くなります。
 #
 period = 1d
 # 保持する kdc.log のバージョン数(kdc.log.0,
 # kdc.log.1, ...)
       versions = 10
       }
```

```
[appdefaults]
kinit = {
renewable = true forwardable= true
}

 #
 # eof
 #
```

KDC にケルベロス・ユーザ (ユーザ・プリンシパル) とサーバ・プリンシパル (サービス・プリンシパル) を作成する

ケルベロス・ユーザとサービス・プリンシパルの追加手順は、使用する KDC (CyberSafe、MIT、Active Directory など) によって異なります。また、ユーザとサービス・プリンシパルを作成する前に、実行パス、ライブラリ検索パス、その他ベンダ固有の環境変数の設定が必要になる場合もあります。以降に示す例の多くでは、キーに対してシングル DES 暗号化タイプを使用しています。これは、シングル DES が、クライアント、サーバ、および KDC におけるさまざまなケルベロス実装間の相互運用性に最も優れているからです。3DES (トリプル DES) や RC4-HMAC (Active Directory のデフォルト) を使用することもできますが、他の暗号化タイプを適切に使用する方法は、ご使用のケルベロス実装によって異なってきます。詳細については、各ケルベロス・プロバイダのマニュアルを参照してください。

CyberSafe

次の例は、CyberSafe kadmin ユーティリティを使用して admin デーモンに接続し、ユーザおよびサービス・プリンシパルを作成する方法を示しています。この例のケルベロス管理者は “krb5” または “krb5@MYREALM”、レルム名は MYREALM です。
この例では、kadmin が Unix コマンドラインから実行されています。Windows 用のコマンドライン版 kadmin でも同じコマンドが使用されます。この他、GUI 版の kadmin もあります。

```
mymachine% /krb5/bin/kadmin krb5
Principal - krb5@MYREALM
Enter password:
Connected to csfA5v01 in realm MYREALM.
```

ここで、ユーザ “sybuser1” を追加します。このユーザ名はサーバ上のログインと同一である必要があります (ログインを後でサーバ上に作成することも可能)。Java ケルベロス・アプリケーションとの最大限の相互運用性を確保するために、キーに対して DES エンコーディングを使用してください。詳細については、CyberSafe のマニュアルを参照してください。ユーザの追加時に特定のエンコーディングを設定しない場合、エンコーディングのデフォルトが KDC によって決定されます。

```
Command: add sybuser1
Enter password:
Re-enter password for verification: Principal added.
```

次に、サーバのエントリを追加します。ここで入力する名前は、クライアントが接続する Sybase サーバの名前と同一である必要があります。この例のサーバ名は ase1252srv です。コマンド・シーケンスはユーザの追加時に使用したものとまったく同じです。

```
Command: add ase1252srv
Enter password:
Re-enter password for verification:
Principal added.
```

> **注：** kadmin の代わりに、csfadm を使用してこれらのタスクを実行することもできます。csfadm は CyberSafe ソフトウェアに付属の GUI ツールです。ベンダのマニュアルを参照してください。

MIT

次の例は、MIT kadmin ユーティリティを使用して MIT admin デーモンに接続し、ユーザおよびサービス・プリンシパルを作成する方法を示しています。この例のケルベロス管理者は “krb” または “krb5@MITKDC”、レルム名は MITKDC です。
この例では、kadmin が Unix コマンドラインから実行されています。

```
mymachine% /work3/mitkrb5/sbin/kadmin -p krb5
Authenticating as principal krb5 with password.
Enter password:
kadmin:
```

ここで、ユーザ “sybuser1” を追加します。このユーザ名は、サーバ上のログインと同一である必要があります (ログインを後でサーバ上に作成することも可能)。この例では、ユーザがプリンシパルのキーに対してエンコーディング “des-cbc-crc:normal” を指定しています。

```
kadmin: addprinc -e des-cbc-crc:normal sybuser1
WARNING: no policy specified for sybuser1@MITKDC; defaulting to no policy
Enter password for principal "sybuser1@MITKDC":
Re-enter password for principal "sybuser1@MITKDC":
Principal "sybuser1@MITKDC" created:
```

次に、データ・サーバのサービス･プリンシパル・エントリを追加します。この名前は、クライアントが接続するサーバの名前と同一である必要があります。この例のサーバ名は ase1252srv です。コマンド・シーケンスはユーザの追加時に使用したものとまったく同じです。

```
kadmin: addprinc -e des-cbc-crc:normal ase1252srv
WARNING: no policy specified for ase1252srv@MITKDC; defaulting to no
policy
Enter password for principal "ase1252srv@MITKDC":
Re-enter password for principal "ase1252srv@MITKDC": Principal
"ase1252srv@MITKDC" created:
```

Active Directory

Active Directory でユーザおよびサービス・プリンシパルを追加するには、Active Directory サーバ・マシンで GUI ツールを使用します。
[ユーザー アカウントとグループの設定を管理します。] をクリックします。これにより、[Active Directory ユーザーとコンピュータ] メニュー画面が表示されます。次に、“Users” フォルダを右クリックし、“sybuser1” という名前の新しいユーザを作成します。
次に、サービス・プリンシパル用に別のユーザ “ase1252srv” を作成します。
Active Directory でユーザとサービス・プリンシパルを作成するときに、シングル DES キーを使用するよう指定することもできます。これを行うには、ユーザ名またはサービス・プリンシパル名を右クリックして [プロパティ] をクリックします。これにより、そのユーザのプロパティが示された画面が表示されます。[アカウント] タブをクリックし、[アカウント オプション] リストで [このアカウントに DES 暗号化を使う] という項目を見つけます。このオプションを選択すると、Active Directory でそのユーザに対してシングル DES キーが使用されるようになります。MicroSoft は、Unix プラットフォームから Active Directory アカウントを管理することのできる数種類のツールをリリースしています。詳細については、
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnactdir/html/kerberossamp.asp を参照してください。

KDC を使用してサーバの Keytab を抽出する

サーバはユーザと同様に、KDC に対してそれ自体を認証する必要があります。KDC にサーバ・サービス・プリンシパルを作成しなければならないのはそのためです。ただし、ユーザとは異なり、サーバは、ネットワークへのサインオン処理を行う代わりに、keytab ファイルを使用してそれ自体を認証します。この keytab は、サーバがそれ自体を KDC に対して識別するために使用する、暗号化によって保護されたファイルです。ケルベロスを有効にしてサーバを開始する場合、GSS ライブラリが keytab ファイルを見つけられるよう環境変数を設定する必要があります。また、この処理が行われる前に、KDC から keytab ファイルを取得し、サーバ・マシンに保管しておく必要があります。この処理を「keytab の抽出」と言います。
サーバを Unix マシンで実行する場合は、サーバを開始する Unix ユーザが keytab ファイルを読み取れるようにしてください。実稼働環境では、このファイルへのアクセスを制御する必要があります。keytab ファイルを読み取ることのできるユーザは、本当のサーバになりすますサーバを作成することができるからです。

CyberSafe での Keytab の抽出

CyberSafe KDC を使用する場合、kadmin ユーティリティを使用して admin デーモンにログインできます。前述の「KDC にケルベロス・ユーザ (ユーザ・プリンシパル) とサーバ・プリンシパル (サービス・プリンシパル) を作成する」で説明した手順に従って kadmin を実行します。次に、ext コマンドを使用して keytab をファイルに抽出します (サービス・プリンシパルの keytab を抽出)。

```
Command: ext -n ase1252srv
Service Key Table File Name (/krb5/v5srvtab): Key extracted.
Command: quit
Disconnected.
```

これにより、キーが /krb5/v5srvtab ファイルに抽出されます。このファイルを、keytab ファイル用に Sybase サーバ上に構成された場所に保管します。Sybase サーバ上の keytab ファイルの場所については、このドキュメントの次の項「ケルベロス接続を受け入れるよう ASE または Open Server を構成する」で説明します。

.

> **注：** kadmin の代わりに csfadm を使用して keytab を抽出することもできます。csfadm は CyberSafe ソフトウェアに付属の GUI ツールです。ベンダのマニュアルを参照してください。

MIT での Keytab の抽出

MIT KDC を使用する場合、前述の「KDC にケルベロス・ユーザ (ユーザ・プリンシパル) とサーバ・プリンシパル (サービス・プリンシパル) を作成する」で説明した手順に従って kadmin を実行します。次に、ktadd コマンドを使用して keytab をファイルに抽出します (サービス・プリンシパルの keytab を抽出)。

```
kadmin: ktadd -k /tmp/v5srvtab ase1252srv
Entry for principal ase1252srv with kvno 2, encryption type Triple
DES mode with HMAC/sha1 added to keytab WRFILE:/tmp/v5srvtab
Entry for principal ase1252srv with kvno 2, encryption type DES cbc
mode with CRC-32 added to keytab WRFILE:/tmp/v5srvtab
kadmin:
```

> **注：**この例では、MIT KDC により、1 つはトリプル DES エンコーディングで、もう 1 つは DES エンコーディングで、2 つの keytab が抽出され、両方のキーが /tmp/v5srvtab ファイルに保管されます。使用するケルベロス・クライアントに応じて、一方のキー・タイプのみを抽出することもできます。これを行うには、ktadd コマンドの -e オプションを使用します。詳細については、MIT のマニュアルを参照してください。

keytab ファイルは、このファイルの読み取り場所としてサーバに設定された場所に保管してください。Sybase サーバ上の keytab ファイルの場所については、次の項「ケルベロス接続を受け入れるよう ASE または Open Server を構成する」で説明します。

Active Directory での Keytab の抽出

MicroSoft は ktpass.exe という実行プログラムを提供しています。このプログラムを使用して、Active Directory Server から keytab を抽出し、ケルベロス･サービス・プリンシパル名と Active Directory のサービス・プリンシパル・アカウントをマッピングすることができます。
たとえば、Active Directory のレルム名が “ADREALM” の場合、次のようなコマンドを実行します。

```
ktpass –princ ase1252srv@ADREALM –mapuser ase1252srv -pass
my_password –out ase1252srv.keytab
```

これにより、keytab が ase1252srv.keytab という名前のファイルに出力されます。次に、この keytab ファイルを、Sybase サーバが稼働しているマシンに移動します。
コマンド構文など ktpass.exe ユーティリティの詳細については、
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B324144&Product=win2000 で公開されている MicroSoft のマニュアルを参照してください。

ケルベロス接続を受け入れるよう Sybase ASE または Open Server を構成する

この手順を完了するには、適切な Sybase マニュアルを参照する必要があります。最も重要なのは、「KDC を使用してサーバの Keytab を抽出する」で生成した keytab ファイルを適切に見つけられるようサーバを構成することです。keytab ファイルは、(ベンダ固有の) デフォルトの場所に保管することも、環境変数で指定することもできます。CyberSafe GSS の場合は、keytab ファイルを指すよう CSFC5KTNAME 変数を設定します。MIT GSS の場合は、KRB5_KTNAME 環境変数を設定します。この他、KDC に作成したユーザ・プリンシパルと同じ名前を使用して、サーバにログインとユーザを作成する必要があります。これを行うには、**sp_addlogin** および **sp_adduser** ストアド・プロシージャを使用します。

> **注：** ASE に作成するユーザ名は KDC 内のユーザ・プリンシパル名と一致している必要がありますが、ユーザを作成するときに指定するパスワードは、KDC にユーザを作成したときと異なっていてもかまいません。これは、ケルベロス・ログインでは KDC 内のユーザのパスワードのみが使用されるためです。ASE または Open Server ユーザに対して作成したパスワードは、サーバへのログイン時にケルベロスを使用するかぎり、使用されることはありません。

サーバを開始するときは、ライブラリ検索パスにある適切な GSS ライブラリを使用してください。最後に、Sybase サーバには libtcl.cfg という名前の構成ファイルがあります。このファイルには、使用する GSS ライブラリを指定するものなど、さまざまな構成オプションが保持されます。このオプションの名前は “csfkrb5” です。サーバに対して MIT GSS ライブラリを使用する場合も、オプション名は同じです。これは、Sybase サーバで使用可能な GSS ライブラリが CyberSafe GSS ライブラリのみだった頃の名前がそのまま引き継がれているためです。

クライアント・マシンで自分自身を KDC に対して認証する

KDC にログインし、自分自身の ID を検証します。ケルベロスの用語で言えば、ケルベロス TGT (Ticket Granting Ticket ：チケット認可チケット) を取得する必要があります。TGT は、ユーザの ID を検証し、サーバへのログインなどの操作を実行する権限を与えるものです。
ユーザがマシンにログインするだけで TGT が付与されるよう作業環境を構成しているシステム管理者もいます。UNIX マシンを使用し、ログイン時に自動的に TGT を受け取るよう設定されていない場合は、ケルベロス・クライアントの kinit バイナリを実行する必要があります。kinit バイナリは、ユーザを KDC に対して認証し、クライアント・マシン上の明確に定義された場所にあるファイル (クレデンシャル・キャッシュと呼ばれる) に TGT を保管します。通常、このファイルは /tmp/krb5cc_ {user_id} にあります。

Windows マシンを使用し、ログイン時に自動的に TGT を受け取るよう設定されていない場合は、[スタート] メニューから CyberSafe 認証ツールにアクセスして TGT を作成できます。その他のベンダからも kinit 実行プログラムが提供されています。たとえば、Sun は Windows クライアント・マシンから使用可能な kinit を JDK とともに提供しています。

Unix での kinit の使用

UNIX クライアントを認証するには、コマンド・ラインから次のように kinit を実行します。

```
mycomputer% kinit sybuser1@MYREALM
Password for sybuser1@MYREALM:
mycomputer%
```

注： KDC に対する認証に失敗する一般的な原因は、クライアント・マシンと KDC マシンの時刻設定の不一致です。一般に、正常な認証には、クライアント・マシンと KDC マシンに設定されている時刻の差が一定の秒数内でなければなりません。詳細については、KDC のマニュアルを参照してください。

サーバに接続する

TGT を取得したら、サーバに対してケルベロス接続を確立することができます。ケルベロスを使用した接続の詳細については、Sybase クライアントのマニュアルを参照してください。

Sybase, Inc.
Worldwide Headquarters
One Sybase Drive
Dublin, CA 94568-7902 USA Tel: +800 8 SYBASE www.sybase.com