Kerberos の設定

Kerberos によるスイッチ アクセスの制御の前提条件

次に、Kerberos を使用してスイッチ アクセスを制御するための前提条件を示します。

- リモート ユーザーがネットワーク サービスに対して認証を得るには、Kerberos レルム内のホストと KDC を設定し、ユーザーとネットワーク サービスの両方に通信を行い、相互に認証させる必要があります。これを実現するには、互いの識別が必要です。KDC 上の Kerberos データベースにホストのエントリを追加し、Kerberos レルム内のすべてのホストに KDC が生成した KEYTAB ファイルを追加します。また、KDC データベースにユーザー用のエントリも作成します。
- Kerberos サーバーには、ネットワーク セキュリティ サーバーとして設定されていて、Kerberos プロトコルを用いてユーザーを認証できるスイッチを使用できます。

ホストおよびユーザーのエントリを追加または作成する場合の注意事項は次のとおりです。

- Kerberos プリンシパル名はすべて小文字でなければなりません。
- Kerberos インスタンス名はすべて小文字でなければなりません。
- Kerberos レルム名はすべて大文字でなければなりません。

Kerberos に関する情報

ここでは、Kerberos の情報を提供します。

Kerberos とスイッチ アクセス

ここでは、Kerberosセキュリティ システムをイネーブルにして設定する方法について説明します。Kerberos セキュリティ システムは、信頼できるサードパーティを使用してネットワーク リソースに対する要求を認証します。

（注） Kerberos の設定例では、信頼できるサード パーティを、Kerberos をサポートし、ネットワーク セキュリティ サーバーとして設定され、Kerberos プロトコルを使用してユーザーを認証するスイッチとすることができます。

Kerberos の概要

Kerberos はマサチューセッツ工科大学（MIT）が開発した秘密キーによるネットワーク認証プロトコルです。データ暗号規格（DES）という暗号化アルゴリズムを暗号化と認証に使用し、ネットワーク リソースに対する要求を認証します。Kerberosは、信頼できるサードパーティという概念を使ってユーザーとサービスに対してセキュリティの検証を実行します。この信頼できるサードパーティをキー発行局（KDC）と呼びます。

Kerberosは、ユーザーが誰であるか、そのユーザーが使用しているネットワーク サービスは何であるかを検証します。これを実行するために、KDC（つまり信頼できるKerberosサーバー）がユーザーにチケットを発行します。これらのチケットには有効期限があり、ユーザー クレデンシャルのキャッシュに保存されます。Kerberosサーバーは、ユーザー名やパスワードの代わりにチケットを使ってユーザーとネットワーク サービスを認証します。

（注） Kerberos サーバーには、ネットワーク セキュリティ サーバーとして設定されていて、Kerberosプロトコルを用いてユーザーを認証できるのであれば、どのスイッチも使用できます。

Kerberosのクレデンシャル発行スキームでは、*single logon* という手順を使用します。この手順では、ユーザーを1回認証すると、ユーザー クレデンシャルが有効な間は（他のパスワードの暗号化を行わずに）セキュア認証が可能になります。

このソフトウェア リリースは Kerberos 5 に対応しています。Kerberos 5 では、すでに Kerberos 5 を使用している組織が、（UNIX サーバーや PC などの）他のネットワーク ホストが使用している KDC 上の Kerberos 認証データベースを使用できます。

Kerberos は次のネットワーク サービスをサポートしています。

- Telnet
- rlogin
- rsh

次の表に、一般的な Kerberos 関連用語とその定義を示します。

表 *1 : Kerberos* の用語

用語	定義
認証	ユーザーやサービスが他のサービスに対して自分自身の身元を証明する手順。たとえば、クライアントはスイッチに対して認証を得て、スイッチは他のスイッチに対して認証を得ます。
許可	ユーザーがネットワークやスイッチにおいてどのような権限を有しており、またどのような動作を実行できるかを、スイッチが識別する手段
クレデンシャル	認証チケット（TSG[1]、サービス クレデンシャルなど）を表す総称。Kerberos クレデンシャルで、ユーザーまたはサービスの ID を検証します。ネットワーク サービスがチケットを発行した Kerberos サーバーを信頼することにした場合、ユーザー名やパスワードを再入力する代わりにこれを使用できます。証明書の有効期限は、8 時間がデフォルトの設定です。
インスタンス	Kerberos プリンシパルの承認レベル ラベル。ほとんどの Kerberos プリンシパルは、*user@REALM* という形式です（たとえば、smith@EXAMPLE.COM）。Kerberos インスタンスのある Kerberos プリンシパルは、*user/instance@REALM* という形式です（たとえば、smith/admin@EXAMPLE.COM）。Kerberos インスタンスは、認証が成功した場合のユーザーの承認レベルを指定するために使用できます。各ネットワーク サービスのサーバーは、Kerberos インスタンスの許可マッピングを適用し実行できますが、必須ではありません。 （注） Kerberos プリンシパル名およびインスタンス名はすべて小文字でなければなりません。 （注） Kerberos レルム名はすべて大文字でなければなりません。
KDC[2]	ネットワーク ホストで稼働する Kerberos サーバーおよびデータベース プログラムで構成されるキー発行局
Kerberos 対応	Kerberos クレデンシャルのインフラストラクチャをサポートするために変更されたアプリケーションやサービスのことを指す用語
Kerberos レルム	Kerberos サーバーに登録されたユーザー、ホスト、およびネットワーク サービスで構成されるドメイン。Kerberos サーバーを信頼して、ユーザーまたはネットワーク サービスに対する別のユーザーまたはネットワーク サービスの ID を検証します。 （注） Kerberos レルム名はすべて大文字でなければなりません。

用語	定義
Kerberos サーバー	ネットワーク ホストで稼働しているデーモン。ユーザーおよびネットワーク サービスはそれぞれ Kerberos サーバーに ID を登録します。ネットワーク サービスは Kerberos サーバーにクエリーを送信して、他のネットワーク サービスの認証を得ます。
KEYTAB[3]	ネットワーク サービスが KDC と共有するパスワード。Kerberos 5 以降のバージョンでは、ネットワーク サービスは KEYTAB を使って暗号化されたサービス クレデンシャルを暗号解除して認証します。Kerberos 5 よりも前のバージョンでは、KEYTAB はSRVTAB[4]と呼ばれます。
プリンシパル	Kerberos ID とも呼ばれ、Kerberos サーバーに基づき、ユーザーが誰であるか、サービスが何であるかを表します。 （注） Kerberos プリンシパル名はすべて小文字でなければなりません。
サービス クレデンシャル	ネットワーク サービスのクレデンシャル。KDC からクレデンシャルが発行されると、ネットワーク サービスと KDC が共有するパスワードで暗号化されます。ユーザー TGT ともパスワードを共有します。
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。SRVTAB は、Kerberos 5 以降のバージョンでは KEYTAB と呼ばれています。
TGT	身分証明書のことで、KDC が認証済みユーザーに発行するクレデンシャル。TGT を受け取ったユーザーは、KDC が示した Kerberos レルム内のネットワーク サービスに対して認証を得ることができます。

[1] チケット認可チケット
[2] キー発行局
[3] キー テーブル
[4] サーバー テーブル

Kerberos の動作

リモートユーザーが device を Kerberos サーバーとして使用してネットワークサービスで認証されるには、次の手順を実行する必要があります。Kerberos をカスタマイズする方法はいくつかありますが、ネットワーク サービスにアクセスしようとするリモート ユーザーは、3 つのセキュリティ レイヤを通過しないとネットワーク サービスにアクセスできません。

リモートユーザーが device を Kerberos サーバーとして使用してネットワークサービスで認証されるには、次の手順を実行する必要があります。

境界スイッチに対する認証の取得

ここでは、リモート ユーザーが通過しなければならない最初のセキュリティ レイヤについて説明します。ユーザーは、まず境界スイッチに対して認証を得なければなりません。リモート ユーザーが境界スイッチに対して認証を得る場合、次のプロセスが発生します。

1. ユーザーが境界スイッチに対して、Kerberos 未対応の Telnet 接続を開始します。
2. ユーザー名とパスワードの入力を求めるプロンプトをスイッチが表示します。
3. スイッチが、このユーザーの TGT を KDC に要求します。
4. KDC がユーザー ID を含む暗号化された TGT をスイッチに送信します。
5. スイッチは、ユーザーが入力したパスワードを使って TGT の暗号解除を試行します。
   - 暗号解除に成功した場合は、ユーザーはスイッチに対して認証を得ます。
   - 暗号解除に成功しない場合は、ユーザー名とパスワードを再入力（Caps Lock または Num Lock のオン/オフに注意）するか、別のユーザー名とパスワードを入力してステップ 2 の手順を繰り返します。

Kerberos 未対応の Telnet セッションを開始し、境界スイッチの認証を得ているリモート ユーザーはファイアウォールの内側にいますが、ネットワーク サービスにアクセスするには、KDC から直接認証を得る必要があります。ユーザーが KDC から認証を得なければならないのは、KDC が発行する TGT はスイッチに保存されており、ユーザーがこのスイッチにログオンしないかぎり、追加の認証に使用できないからです。

KDC からの TGT の取得

ここでは、リモート ユーザーが通過しなければならない 2 番めのセキュリティ レイヤについて説明します。ユーザーは、ネットワーク サービスにアクセスするために、このレイヤで KDC の認証を得て、KDC から TGT を取得しなければなりません。

KDC に対して認証を得る方法については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Security Server Protocols」の章にある「Obtaining a TGT from a KDC」を参照してください。

ネットワーク サービスに対する認証の取得

ここでは、リモート ユーザーが通過しなければならない 3 番めのセキュリティ レイヤについて説明します。TGT を取得したユーザーは、このレイヤで Kerberos レルム内のネットワーク サービスに対して認証を得なければなりません。

ネットワーク サービスに対して認証を得る方法については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Security Server Protocols」の章の「Authenticating to Network Services」を参照してください。

Kerberos を設定する方法

Kerberos 認証済みサーバー/クライアント システムを設定する手順は、次のとおりです。

- Kerberos コマンドを使用して KDC を設定します。
- Kerberos プロトコルを使用するようにスイッチを設定します。

Kerberos 設定の監視

Kerberos 設定を表示するには、次のコマンドを使用します。

- **show running-config**
- **show kerberos creds**：現在のユーザーの認定証キャッシュに含まれる認定証を一覧表示します。
- **clear kerberos creds**：転送済みの認定証を含め、現在のユーザーの認定証キャッシュに含まれるすべての認定証を破棄します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。