CatalystスイッチでのTACACS+、RADIUS、およびKerberosの設定

内容

概要

Cisco Catalyst スイッチ ファミリ（CatOS が動作する Catalyst 4000、Catalyst 5000、および Catalyst 6000）の 2.2 コード以降では、特定の認証方式がサポートされています。新しいバージョンでは拡張機能が追加されました。TACACS+ TCP ポート 49（XTACACS User Datagram Protocol（UDP; ユーザ データグラム プロトコル）のポート 49 ではありません）、RADIUS、または Kerberos サーバの Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）のためのユーザ セットアップは、ルータ ユーザ用のものと同じです。このドキュメントでは、これらの機能をイネーブルにするために必要となる最小限のコマンドの例を紹介しています。その他のオプションについては、該当するバージョンのスイッチのマニュアル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内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。

背景説明

新しいバージョンのコードでは追加のオプションをサポートしているため、**show version** コマンドを設定してスイッチのコードのバージョンを調べる必要があります。スイッチで使用しているコードのバージョンがわかったら、この表を参考にして、装置に使用できるオプションと、設定するオプションを判断します。

認証と認可を追加する際は、常にスイッチから離れないようにしてください。誤ってロックアウトされないようにするため、テストは別のウィンドウで行ってください。

方法（最小構成）	**Cat バージョン 2.2 ~ 5.1**	**Cat バージョン 5.1 ~ 5.4.1**	**Cat バージョン 5.4.1 ~ 7.5.1**	**Cat バージョン 7.5.1 以降**
TACACS+認証または	ステップ A	ステップ A	ステップ A	ステップ A
RADIUS認証または	N/A	ステップ B	ステップ B	ステップ B
Kerberos認証または	N/A	N/A	手順 K	手順 K
ローカル ユーザ名の認証/許可	N/A	N/A	N/A	ステップ C
Plus（オプション）				
TACACS+ コマンド認可	N/A	N/A	ステップ D	ステップ D
TACACS+ exec 認可	N/A	N/A	手順 E	手順 E
RADIUS exec 認可	N/A	N/A	手順 F	手順 F
アカウンティング：TACACS+ または RADIUS	N/A	N/A	手順 G	手順 G
TACACS+ enable 認可	手順 H	手順 H	手順 H	手順 H
RADIUS enable 認	N/A	手順 I	手順 I	手順 I

証				
TACACS+ enable 認可	N/A	N/A	手順 J	手順 J

設定手順

手順 A：TACACS+ 認証

古いバージョンのコードでは、一部の新しいバージョンのコードほどコマンドは複雑ではありません。新しいバージョンでは追加のオプションがスイッチで使用できる場合があります。

1. **set authentication login local enable** コマンドを設定し、サーバがダウンした場合のスイッチへのバック ドアを確保します。
2. **set authentication login tacacs enable** コマンドを設定して、TACACS+ 認証をイネーブルにします。
3. **set tacacs server #.#.#.#** コマンドを設定して、サーバを定義します。
4. **set tacacs key your_key コマンドを設定して、サーバの鍵を定義します。サーバの鍵は TACACS+ のオプションであり、スイッチとサーバ間でデータの暗号化を行います。**使用する場合はサーバに合わせる必要があります。**注：**Cisco Catalyst OSソフトウェアは、**キー**またはパスワードの一部**として**疑問符(?)を受け付けません。疑問符はコマンド構文についてのヘルプを表示するために使用します。

手順 B：RADIUS 認証

古いバージョンのコードでは、一部の新しいバージョンのコードほどコマンドは複雑ではありません。新しいバージョンでは追加のオプションがスイッチで使用できる場合があります。

1. **set authentication login local enable** コマンドを設定し、サーバがダウンした場合のスイッチへのバック ドアを確保します。
2. **set authentication login radius enable** コマンドを設定して、RADIUS 認証をイネーブルにします。
3. サーバを定義します。他のすべての Cisco 機器では、デフォルトの RADIUS ポートは 1645/1646 (認証/アカウンティング) です。Catalystでは、デフォルトポートは 1812/1813です。Cisco Secureまたは他のシスコ機器と通信するサーバを使用する場合は、1645/1646ポートを使用します。**set radius server #.#.#.# auth-port 1645 acct-port 1646 primary** コマンドを設定してサーバを定義します。Cisco IOS での同等のコマンドは **radius-server source-ports 1645-1646** です。
4. サーバの鍵を定義します。これは、スイッチからサーバへのパスワードがRADIUS Authentication/Authorization RFC 2865およびRADIUS Accounting RFC 2866のように暗号化されるたため、必須です 。使用する場合はサーバに合わせる必要があります。**set radius key *your_key* コマンドを設定します。**

手順 C：ローカル ユーザ名の認証/認可

CatOS バージョン 7.5.1 以降、ローカル ユーザの認証に対応しています。たとえば、ローカル パスワードによる認証ではなく、Catalyst に保存されているユーザ名とパスワードを使用して認証/許可を行えます。

ローカルユーザ認証には、0または15の2つの特権レベルしかありません。レベル0は非特権EXECレベルです。▼レベル 15 は特権 enable レベルです。▽

次の例にあるこれらのコマンドを追加する場合は、ユーザ poweruser が Telnet またはコンソールでスイッチにイネーブル モードでアクセスし、ユーザ nonenable が Telnet またはコンソールでスイッチに exec モードでアクセスします。

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

注：ユーザーnonenableが**set enable password**を認識し**ている**場合は、イネーブルモードを継続できます。

設定後、パスワードは暗号化されて保存されます。

ローカル ユーザ名による認証は、リモート TACACS+ exec、コマンド アカウンティング、またはリモート RADIUS exec アカウンティングと組み合せて使用できます。また、リモート TACACS+ exec またはコマンド許可と組み合せて使用できますが、ユーザ名は TACACS+ サーバだけでなくスイッチ上にローカルに保存する必要があるため、この方法で使用するのは意味がありません。

手順 D：TACACS+ コマンド認可

この例では、TACACS+ を使用する設定コマンドだけに対して認可を要求するようにスイッチに指示します。万一 TACACS+ サーバがダウンした場合、認証は none になります。これはコンソール ポートと Telnet セッションの両方に適用されます。次のコマンドを実行します。

set authorization commands enable config tacacs none both

この例では、次のパラメータを設定した場合に許可するよう TACACS+ サーバを設定します。

```
command=set
arguments (permit)=port 2/12
```

確認のため、**set port enable 2/12** コマンドが TACACS+ サーバに送られます。

注：コマンド許可を有効にすると、enableがコマンドとは見なされないルータとは異なり、スイッチはenableコマンドを試みたら、enableコマンドをサーバに送信します。サーバが **enable** コマンドを許可するように設定されていることも確認してください。

手順 E：TACACS+ exec 認可

この例では、TACACS+ を使用する exec セッションだけに対して認可を要求するようにスイッチに指示します。万一 TACACS+ サーバがダウンした場合、認可は none になります。これはコンソール ポートと Telnet セッションの両方に適用されます。**set authorization exec enable tacacs+ none both** コマンドを設定します。

これにより、認証要求に加えて別の認可要求がスイッチから TACACS+ サーバに対して送信されます。TACACS+ サーバでユーザのプロファイルが shell/exec に対して設定されている場合、そのユーザはスイッチにアクセスできます。

これにより、サーバで shell/exec サービスが設定されていないユーザ（PPP ユーザなど）はスイッチにログインできなくなります。この場合は Exec mode authorization failed というメッセージが表示されます。ユーザに対する exec モードの許可/拒否に加えて、サーバ上で特権レベル 15 を割り当てることにより、進入時に強制的に enable モードにするようにできます。Cisco bug ID CSCdr51314（登録ユーザ専用）が修正されたコードが、サーバで稼働している必要があります。

手順 F：RADIUS exec 認可

RADIUS exec 認可をイネーブルにするコマンドはありません。代替手段として、RADIUS サーバで Service-Type（RADIUS アトリビュート 6）を Administrative（値 6）に設定し、RADIUS サーバでユーザを enable モードで起動します。Service-Type を 6-Admistrative 以外（1-Login、7-Shell、2-Framed など）に設定した場合、ユーザにはスイッチの exec プロンプトが表示されますが、enable プロンプトは表示されません。

認証と認可のために、次のコマンドをスイッチに追加します。

```
aaa authorization exec TEST group radius
 line vty 0 4
 authorization exec TEST
 login authentication TEST
```

手順 G：アカウンティング：TACACS+ または RADIUS

TACACS+ アカウンティングをイネーブルにするには、次の手順に従います。

1. スイッチ プロンプトが表示されたら、**set accounting exec enable start-stop tacacs+** コマンドを設定します。
2. スイッチから外部に Telnet するユーザでは、**set accounting connect enable start-stop tacacs+** コマンドを設定します。
3. スイッチがリブートしたら、**set accounting system enable start-stop tacacs+** コマンドを設定します。
4. コマンドを実行するユーザでは、**set accounting commands enable all start-stop tacacs+** コマンドを設定します。
5. たとえば、1分に1回レコードを更新してユーザーがまだログインしていることを確認するには、**set accounting update periodic 1コマンドを発行します。**

RADIUS アカウンティングをイネーブルにするには、次の手順に従います。

1. スイッチ プロンプトが表示されたユーザでは、**set accounting exec enable start-stop radius** コマンドを設定します。
2. スイッチから Telnet するユーザでは、**set accounting connect enable start-stop radius コマンドを設定します。**
3. スイッチがリブートしたら、**set accounting system enable start-stop radius** コマンドを設定します。
4. たとえば、1分に1回レコードを更新してユーザーがまだログインしていることを確認するには、**set accounting update periodic 1コマンドを発行します。**

TACACS+ フリーウェア レコード

次の出力はサーバで表示されるレコードの例です。

```
Fri Mar 24 13:22:41 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=5 start_time=953936729 timezone=UTC
service=shell disc-cause=2 elapsed_time=236
Fri Mar 24 13:22:50 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=15 start_time=953936975 timezone=UTC
service=shell priv-lvl=0 cmd=enable
Fri Mar 24 13:22:54 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=16 start_time=953936979 timezone=UTC
service=shell priv-lvl=15 cmd=write terminal
Fri Mar 24 13:22:59 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=17 start_time=953936984 timezone=UTC
service=shell priv-lvl=15 cmd=show version
Fri Mar 24 13:23:19 2000 10.31.1.151 pinecone telnet85
171.68.118.100 update task_id=14 start_time=953936974 timezone=UTC
service=shell
```

UNIX 上の RADIUS のレコード出力

次の出力はサーバで表示されるレコードの例です。

```
Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Start
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
Login-Host = 171.68.118.100
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Stop
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
Login-Host = 171.68.118.100
Acct-Session-Time = 9
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Received unknown attribute 49
Acct-Session-Time = 30
```

```
Acct-Delay-Time = 0
```

手順 H：TACACS+ enable 認証

次のステップを実行します。

1. **set authentication enable local enable** コマンドを設定し、サーバがダウンした場合のスイッチへのバック ドアを確保します。
2. **set authentication enable tacacs enable** コマンドを設定し、enable 要求をサーバに送るようスイッチに指示します。

ステップ I - Radius enable 認証

次のコマンドを追加して、スイッチからユーザ名 $enab15$ が RADIUS サーバに送信されるようにします。RADIUS サーバによっては、この種のユーザ名をサポートしていません。個々のユーザを enable モードで起動する別の代替手段（Service-Type を設定する（RADIUS アトリビュート 6 を Administrative に設定する）などの方法）については、「手順 E」を参照してください。

1. **set authentication enable local enable** コマンドを設定し、サーバがダウンした場合のスイッチへのバック ドアを確保します。
2. **set authentication enable radius enable** コマンドを設定し、RADIUS サーバがユーザ名 $enab15$ をサポートしている場合は enable 要求をサーバに送るようスイッチに指示します。

ステップJ - TACACS+ enable 許可

次のコマンドを追加すると、ユーザが enable を試行したときにスイッチからサーバに enable が送られます。サーバでは **enable** コマンドを許可する必要があります。次の例では、サーバがダウンした場合に備えて none へのフェールオーバーを指定します。

set author enable enable tacacs+ none both

手順 K：Kerberos 認証

スイッチに Kerberos 認証を設定する方法についての詳細は、『認証、認可、およびアカウンティングを使用したスイッチ アクセスの制御と監視』を参照してください。

パスワードの回復

パスワードの回復方法についての詳細は、『パスワード回復手順』を参照してください。

このページは Cisco 製品のパスワード回復手順インデックスページです。

ip permit コマンドによるセキュリティ強化

セキュリティ強化のため、次のように **ip permit** コマンドによって Telnet アクセスを制御するように Catalyst を設定できます。

set ip permit enable telnet

set ip permit *range mask*|*host*

これで、指定された範囲またはホストだけがスイッチに Telnet できます。

Catalyst でのデバッグ

Catalyst でのデバッグをイネーブルにする前に、サーバ ログを調べて障害の理由を確かめてください。この方が簡単であり、スイッチへの影響も少なくて済みます。初期のバージョンのスイッチでは、**デバッグ**はエンジニアリング モードで実行していました。比較的最近のバージョンのコードでは、**デバッグ** コマンドを実行するためにエンジニアリング モードにアクセスする必要はありません。

set trace tacacs|radius|kerberos 4

注：set trace tacacs|radius|kerberos 0コマンドは、Catalystをトレースなしモードに戻します。

マルチレイヤ LAN スイッチについての詳細は、『スイッチ製品に関するサポート ページ』を参照してください。

関連情報

- TACACS+ と RADIUS の比較
- Cisco IOS での RADIUS、TACACS+、および Kerberos のドキュメンテーション
- RADIUS に関するサポート ページ
- TACACS/TACACS+ サポート ページ
- Kerberos サポート ページ
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems