CiscoSecure 2.x TACACS+のセットアップおよびデバッグ

内容

概要

このドキュメントは、Cisco Secure TACACS+設定のセットアップとデバッグで初めてCisco Secure 2.xユーザを支援することを目的としています。これは、Cisco Secure機能の包括的な説明ではありません。

サーバソフトウェアとユーザ設定の詳細については、Cisco Secureのマニュアルを参照してください。ルータコマンドの詳細[については、該当するリ](#)リースのCisco IOSソフトウェア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 Secure ACS 2.x以降
- Cisco IOS(R) ソフトウェア リリース 11.3.3 以降

表記法

ドキュメント表記の詳細については、『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。

Cisco Secure のセットアップ

次のステップを実行します。

1. UNIXサーバにCisco Secureコードをインストールするには、ソフトウェアに付属の手順を必ず使用してください。
2. 製品が停止して起動することを確認するには、`cd/etc/rc0.droot./K80Cisco Secure`します（デーモンを停止します）。`cd`を`/etc/rc2.d`し、rootとして`./S80Cisco Secure`します（デーモンを起動します）。起動時に、次のようなメッセージが表示されます。
   ```
   Cisco Secure starting Processes: Fast Track Admin, FastTrack Server (Delayed Start),
   DBServer, AAA Server
   ```
   `$BASE/utils/psg`を実行し、SQLAnywhereまたは別のデータベースエンジン、Cisco Secureデータベースサーバプロセス、Netscape Web Server、Netscape Web Admin、Acme Web Server、Cisco Secure AAAプロセス、Auto restartプロセスなど、各プロセスが少なくとも1つ実行されるようにします。
3. 適切なディレクトリに入っていることを確認するには、シェル環境で環境変数とパスを設定します。ここではc-shellを使用します。**$BASEは**Cisco Secureがインストールされているディレクトリで、インストール時に選択されます。これには、DOCS、DBServer、CSUなどのディレクトリが含まれます。この例では、/opt/CSCOacsでのインストールが想定されていますが、システムによって異なる場合があります。
   ```
   setenv $BASE   /opt/CSCOacs
   ```
   $SQLANYは、インストール時に選択された、デフォルトのCisco Secureデータベースがインストールされるディレクトリです。製品に付属するデフォルトのデータベースSQLAnywhereを使用すると、database、docなどのディレクトリが含まれます。この例では、/opt/CSCOacs/SYBSsa50でのインストールが想定されていますが、システムによって異なる場合があります。
   ```
   setenv $SQLANY /opt/CSCOacs/SYBSsa50
   ```
   シェル環境でパスを追加する方法：
   ```
   $BASE/utils
   $BASE/bin
   $BASE/CSU
   $BASE/ns-home/admserv
   $BASE/Ns-home/bin/httpd
   $SQLANY/bin
   ```
4. $BASE/configへのCD**CSU.cfg**はCisco Secureサーバ制御ファイルです。このファイルのバックアップコピーを作成します。このファイルで`LIST config_license_key`は、ソフトウェアを購入した場合にライセンスプロセスで受け取ったライセンスキーを示します。4ポートのトライアルライセンスの場合は、この行を省略できます。**NAS config_nas_configセクション**には、デフォルトのネットワークアクセスサーバ(NAS)またはルータ、またはインストール時に入力したNASを含めることができます。この例のデバッグ目的では、任意のNASがキーを使用*せずに*Cisco Secureサーバと通信できるようにすることができます。たとえば、NASの名前と、NAS名を含む行からキーを削除します`*/`"と*/*NAS/Cisco Secure secret key */*です。その地域の*唯一*のスタンザは次のとおりです。
   ```
   NAS config_nas_config = {
     {
       "",          /* NAS name can go here */
   ```

```
    "",             /* NAS/Cisco Secure secret key */
    "",                         /* message_catalogue_filename */
    1,                          /* username retries */
    2,                          /* password retries */
    1                           /* trusted NAS for SENDPASS */
  }
};

AUTHEN config_external_authen_symbols = {
```

これを行う場合、Cisco Secureに対して、キーを交換せずに、すべてのNASとの通信が許可されていることを伝えます。

5. デバッグ情報を/var/log/csuslogに送りたい場合は、CSU.cfgの一番上のセクションに行が必要です。この行は、サーバにデバッグの実行量を示しています。0X7FFFFFFFは、可能なすべてのデバッグを追加します。この行を適宜追加または変更します。

```
NUMBER config_logging_configuration = 0x7FFFFFFF;
```

次の追加行は、デバッグ情報をlocal0に送信します。

```
NUMBER config_system_logging_level = 0x80;
```

また、/etc/syslog.confファイルを変更するには、次のエントリを追加します。

```
local0.debug /var/log/csuslog
```

次に、syslogdをリサイクルして再読み込みします。

```
kill -HUP `cat /etc/syslog.pid`
```

Cisco Secureサーバを再起動します。

```
/etc/rc0.d/K80Cisco Secure
/etc/rc2.d/S80Cisco Secure
```

まだ始まるはずです。

6. ブラウザを使用して、ユーザ、グループなどを追加したり、CSimportユーティリティを追加したりできます。このドキュメントの最後にあるフラットファイルのサンプルユーザは、CSimportを使用して簡単にデータベースに移動できます。これらのユーザはテスト目的で動作し、ユーザが自分のユーザを取得したら削除できます。インポートが完了すると、GUIからインポートされたユーザを確認できます。CSimport:

```
CD $BASE/utils
```

ユーザおよびグループプロファイルをシステム上の任意の場所などのファイルに保存し、次に$BASE/utilsディレクトリからデーモンを実行します(例：/etc/rc2.d/S80Cisco Secure)、ユーザrootとしてtest (-t)オプションを使用してCSimportを実行します。

```
./CSimport -t -p <path_to_file> -s <name_of_file>
```

ユーザの構文をテストします。次のようなメッセージが表示されます。

```
Secure config home directory is: /opt/CSCOacs/config/CSConfig.ini
hostname = berry and port = 9900 and clientid = 100
/home/ddunlap/csecure/upgrade.log exists, do you want to write over 'yes' or 'no' ?
yes
Sorting profiles...
Done sorting 21 profiles!
Running the database import test...
```

次のようなメッセージは受信しないでください。

```
Error at line 2: password = "adminusr"
Couldn't repair and continue parse
```

エラーが発生したかどうかを確認するには、upgrade.logを調べて、プロファイルがチェックアウトされていることを確認します。エラーが修正されたら、$BASE/utilsディレクトリからデーモンを実行し(/etc/rc2.d/S80Cisco Secure)、ユーザrootとしてCSimportをcommit (-c)オプションで実行してユーザをデータベースに移動します。

```
./CSimport -c -p <path_to_file> -s <name_of_file>
```

ここでも、画面やupgrade.logにエラーは表示されません。

7. サポートされているブラウザは、テクニカルティップの「Cisco Secure Compatibility」に記載されています。PCブラウザで、[Cisco Secure/Solaris]ボックス**http://#.#.#.#/csをポイント**

します。ここでは、#.#.#はCisco Secure/SolarisサーバのIPです。表示される画面で、ユーザにsuperuserと入力し、パスワードにchangemeと入力します。この時点でパスワードを変更しないでください。前の手順でCSimportを使用する場合は、追加されたユーザまたはグループが表示されます。または、参照ブロックをクリックしてオフにして、GUIを使用してユーザおよびグループを手動で追加できます。

認証のセットアップ

注：このルータ設定は、Cisco IOSソフトウェアリリース12.0.5.T以降が稼働するルータで開発されました。Cisco IOSソフトウェアリリース11.3.3.T以降では、**tacacsの代わりに**group tacacsが表示されます。

この時点で、ルータを設定します。

1. ルータの設定中にCisco Secureを強制終了します。
   ```
   /etc/rc0.d/K80Cisco Secure to stop the daemons.
   ```
2. ルータで、TACACS+の設定を開始します。イネーブルモードに入り、コマンドセconf tと入力します。この構文により、Cisco Secureが動作していない場合に初めてルータからロックアウトされることがなくなります。`ps -ef`と `| grep Secure`を使用して、Cisco Secureが実行されていないことを確認し、プロセスが次の場合は–9を強制終了します。

   ```
   !--- Turn on TACACS+ aaa new-model enable password whatever !--- These are lists of
   authentication methods, !--- that is, vtymethod and conmethod are !--- names of lists, and
   the methods listed on the !--- same lines are the methods in the order to be !--- tried. As
   used here, if authentication !--- fails due to Cisco Secure not being started, !--- the
   enable password is accepted !--- because it is in each list. aaa authentication login
   vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable !--- Point the
   router to the server, that is, !--- #.#.#.# is the server IP address. tacacs-server host
   #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !---
   during debugging. exec-timeout 0 0 login authentication conmethod line vty 0 4 password
   whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0
   0 login authentication vtymethod
   ```
3. 次に進む前に、Telnet およびコンソール ポート経由で引き続きルータへアクセスできること確認します。Cisco Secureが実行されていないため、イネーブルパスワードを受け入れる必要があります。**注意：コン**ソール・ポートのセッションをアクティブにしておき、イネーブルモードのままにします。このセッションをタイムアウトさせてはいけません。この時点でルータへのアクセスを制限し始め、ロックアウトせずに設定を変更できるようにする必要があります。ルータでのサーバとルータ間のインタラクションを確認するには、次のコマンドを発行します。
   ```
   terminal monitor
   debug aaa authentication
   ```
4. rootとして、サーバでCisco Secureを起動します。
   ```
   /etc/rc2.d/S80Cisco Secure
   ```
   これによりプロセスが開始されますが、S80Cisco Secureで設定されているよりも多くのデバッグを有効にしたいので、次の手順を実行します。
   ```
   ps -ef | grep Cisco Secure
   kill -9 <pid_of CS_process>

   CD $BASE/CSU
   ./Cisco Secure -cx -f $BASE/config/CSU.cfg to start the Cisco Secure process with debugging
   ```
   -xオプシすると、Cisco Secureがフォアグラウンドで動作するため、ルータとサーバ間のインタラクションを確認できます。エラーメッセージは表示されません。-xオプションが原因で、Cisco Secureプロセスが開始され、ハングします。

5. 別のウィンドウで、Cisco Secureが起動していることを確認します。`ps -ef`と入力Cisco Secureプロセスを探します。
6. これで、Telnet(vty)ユーザはCisco Secureで認証する必要があります。ルータのデバッグを使用して、ネットワークの別の部分からルータにTelnet接続します。ルータはユーザ名とパスワードのプロンプトを生成する必要があります。次のユーザIDとパスワードの組み合わせでルータにアクセスできるはずです。

   ```
   adminusr/adminusr
   operator/oper
   desusr/encrypt
   ```

   サーバとルータを監視して、インタラクション、つまり送信された内容、応答、要求などを確認します。問題がある場合は修正してから次へ進みます。
7. ユーザがCisco Secureを介して認証を受けてイネーブルモードに入る場合は、コンソールポートセッションがまだアクティブであることを確認し、次のコマンドをルータに追加します。

   ```
   !--- For enable mode, list 'default' looks to Cisco Secure !--- then enable password if
   Cisco Secure is not running. aaa authentication enable default tacacs+ enable
   ```
8. これで、Cisco Secureを使用して有効にする**必要が**あります。ルータのデバッグを使用して、ネットワークの別の部分からルータにTelnet接続します。ルータがユーザ名/パスワードの入力を求めると、オペレー/。ユーザオペレータがイネーブルモード（特権レベル15）に入ろうとすると、パスワード「cisco」が必要です。他のユーザは、特権レベルのステートメント（またはCisco Secureデーモンがダウン）がないと、イネーブルモードに入ることはできません。Cisco Secureのインタラクションが表示されるサーバとルータを監視します。たとえば、送信される場所、応答、要求などです。続行する前に問題を修正してください。
9. コンソールポートに接続したままサーバ上のCisco Secureプロセスをダウンさせ、Cisco Secureがダウンしてもユーザがルータにアクセスできることを確認します。

   ```
   'ps -ef' and look for Cisco Secure process
   kill -9 pid_of_Cisco Secure
   ```

   前の手順で行った Telnet と enable を繰り返します。ルータは、Cisco Secureプロセスが応答せず、ユーザがデフォルトのイネーブルパスワードを使用してログインおよびイネーブルモードに入ることを認識する必要があります。
10. Cisco Secureサーバを再度起動し、Cisco Secureで認証する必要があるルータへのTelnetセッションを確立します。このセッションは、Cisco Secureでコンソールポートユーザの認証を確認するためにuserid/password **operator/operを使用しま**す。コンソールポートを介してルータにログインできるまで、ルータとイネーブルモードでtelnetしたままにします。たとえば、コンソールポートを介してルータへの元の接続からログアウトし、コンソールポートに再接続します。以前のユーザIDとパスワードの組み合わせを使用してログインするコンソールポート認証は、Cisco Secureを使用する必要があります。たとえば、ユーザID/パスワード**operator/oper**、パスワード**cisco**を使用して**イネー**ズを有効にする必要があ**ります**。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用さ[れるコマンドの詳細を調べる](#)には、[Command Lookup Tool(登録](#)ユーザ専用)を使用してください。

認可の追加

認可の追加はオプションです。

デフォルトでは、ルータには次の 3 つのコマンド レベルがあります。

- 特権レベル0 (disable、enable exit、help、logoutなど)
- 特権レベル1:Telnetおよびプロンプトの通常レベルは`router>`と
- 特権レベル15：イネーブルレベルとプロンプトに`router#`

使用可能なコマンドは、Cisco IOSフィーチャセット、Cisco IOSソフトウェアリリース、ルータのモデルなどに依存するため、レベル1および15のすべてのコマンドの包括的なリストはありません。たとえば、**show ipx route**は、IPのみのフィーチャセットには存在しません。 xコードの原因は、NATが導入されていないこと、および電源と温度の監視が行われていないルータモデルには**show environment**が存在しないためです。

特定のレベルの特定のルータで使用可能なコマンドは、**?**特権レベルの場合は、ルータのプロンプトで確認します。

CSCdi82030が実装されるまで、コンソールポート認証は機能として追加されませんでした。誤ってルータからロックアウトされる可能性を減らすために、コンソールポート認証はデフォルトでオフになっています。ユーザがコンソールを通じて物理的にアクセスできる場合は、コンソール ポート認証はあまり効果的ではありません。ただし、コンソールポート認証は、**authorization exec default|WORDコマンドでCSCdi82030が実装されたCisco IOSイメージのline con 0コマンドでオンにすることができます。**

次のステップを実行します。

1. ルータは、Cisco Secureを介して、すべてのレベルまたは一部のレベルでコマンドを許可するように設定できます。次のルータ設定では、すべてのユーザに、サーバ上でのコマンド単位の認証の設定を許可しています。Cisco Secureを使用してすべてのコマンドを認可できますが、サーバがダウンしている場合は認可が必要ないため、`none`。Cisco Secureサーバがダウンしている状態で、次のコマンドを入力します。Cisco Secureで認証を有効にする要件を削除するには、次のコマンドを入力します。
   ```
   no aaa authentication enable default tacacs+ none
   ```
   次のコマンドを入力して、Cisco Secureでコマンド許可を行うよう要求します。
   ```
   aaa authorization commands 0 default tacacs+ none
   aaa authorization commands 1 default tacacs+ none
   aaa authorization commands 15 default tacacs+ none
   ```
2. Cisco Secureサーバの実行中に、ユーザID/パスワード**lonusr/lonepwd**を使用してルータにTelnet**接続します**。このユーザは、次のコマンド以外は実行できません。
   ```
   show version
   ping <anything>
   logout
   ```
   以前のユーザ**adminusr/adminusr**、**operator/oper**、**desasr/encrypt**は、`default service = permit`を使用してすべてのコマンドを実行できる必要があります。プロセスに問題がある場合は、ルータでイネーブルモードに入り、次のコマンドを使用して許可デバッグをオンにします。
   ```
   terminal monitor
   debug aaa authorization
   ```
   Cisco Secureのインタラクションが表示されるサーバとルータを監視します。たとえば、送信される場所、応答、要求などです。問題がある場合は修正してから次へ進みます。
3. ルータは、Cisco Secureを介してexecセッションを許可するように設定できます。**aaa**

authorization exec default tacacs+ noneコマンド**は、execセッションに対するTACACS+許可を**設定します。これを適用すると、ユーザの時刻/時刻、**telnet**、**todam/todam**、**todpm/todpm**、および**somerouters/somerouters**に影響が及びます。このコマンドをルータに追加し、ユーザの**time/time**としてルータに**Telnet接続した後**は、execセッションが1分間開いたままになります(set timeout = 1)。 ユーザ**telnet/telnet**はルータに入りますが、すぐに他のアドレスに送信されます(set autocmd = "telnet 171.68.118.102")。 **todam/todam**および**todpm/todpm**は、テスト中の時刻に応じて、ルータにアクセスできる、またはアクセスできない可能性があります。ユーザ**somerouters**は、ネットワーク10.31.1.xからルータkoala.rtp.cisco.comにTelnet接続することしかできません。Cisco Secureがルータ名の解決を試みます。IPアドレス10.31.1.5を使用する場合は、解決が行われない場合は有効で、名前koalaを使用する場合は解決が通過している場合は有効です。

アカウンティングの追加

アカウンティングの追加はオプションです。

1. ルータがCisco IOSソフトウェアリリース11.0より後のCisco IOSソフトウェアリリースを実行している場合、ルータで設定されていない限り、アカウンティングは実行されません。ルータでアカウンティングを有効にできます。
   ```
   aaa accounting exec default start-stop tacacs+
   aaa accounting connection default start-stop tacacs+
   aaa accounting network default start-stop tacacs+
   aaa accounting system default start-stop tacacs+
   ```
   注：Cisco Bug ID CSCdi44140でコマンドアカウンティングが壊れていましたが、これが修正されたイメージを使用している場合は、コマンドアカウンティングも有効にできます。
2. ルータにアカウンティングレコードのデバッグを追加します。
   ```
   terminal monitor
   debug aaa accounting
   ```
3. コンソールのデバッグでは、ユーザがログインすると、サーバに入るアカウンティングレコードが表示されます。
4. アカウンティングレコードをルートとして取得するには、次の手順を実行します。
   ```
   CD $BASE/utils/bin
   ./AcctExport <filename> no_truncate
   ```
   `no_truncate`タがデータベースに保持されることを意味します。

ダイヤルアップユーザの追加

次のステップを実行します。

1. ダイヤルアップユーザを追加する前に、Cisco Secureのその他の機能が動作することを確認してください。この時点より前にCisco Secureサーバとモデムが動作していなければ、この時点を過ぎると動作しません。
2. ルータ設定に次のコマンドを追加します。
   ```
   aaa authentication ppp default if-needed tacacs+
   aaa authentication login default tacacs+ enable
   aaa authorization network default tacacs+
   chat-script default "" at&fls0=1&h1&r2&c1&d2&b1e0q2 OK
   ```
   インターフェイスの設定は異なりますが、この例ではダイヤルイン回線を次の設定で使用しています。
   ```
   interface Ethernet 0
   ip address 10.6.1.200 255.255.255.0
   ```

```
! !--- CHAP/PPP authentication user: interface Async1 ip unnumbered Ethernet0 encapsulation
ppp async mode dedicated peer default ip address pool async no cdp enable ppp
authentication chap ! !--- PAP/PPP authentication user: interface Async2 ip unnumbered
Ethernet0 encapsulation ppp async mode dedicated peer default ip address pool async no cdp
enable ppp authentication pap ! !--- login authentication user with autocommand PPP:
interface Async3 ip unnumbered Ethernet0 encapsulation ppp async mode interactive peer
default ip address pool async no cdp enable ip local pool async 10.6.100.101 10.6.100.103
line 1 session-timeout 20 exec-timeout 120 0 autoselect during-login script startup default
script reset default modem Dialin transport input all stopbits 1 rxspeed 115200 txspeed
115200 flowcontrol hardware ! line 2 session-timeout 20 exec-timeout 120 0 autoselect
during-login script startup default script reset default modem Dialin transport input all
stopbits 1 rxspeed 115200 txspeed 115200 flowcontrol hardware ! line 3 session-timeout 20
exec-timeout 120 0 autoselect during-login autoselect ppp script startup default script
reset default modem Dialin autocommand ppp transport input all stopbits 1 rxspeed 115200
txspeed 115200 flowcontrol hardware ! access-list 101 deny icmp any any
```

3. Cisco Secureのユーザファイルから：chapuser:CHAP/PPP：ユーザが回線1でダイヤルインします。アドレスは、ピアのデフォルトのipアドレスプールasyncおよびip local pool async 10.6.100.101 10.6.100.103によってルータに割り当てられますchapaddr:CHAP/PPP：ユーザが回線1でダイヤルインします。アドレス10.29.1.99はサーバによって割り当てられるchapacl:CHAP/PPP：ユーザが回線1でダイヤルインします。アドレス10.29.1.100はサーバによって割り当てられ、着信アクセスリスト101が適用されます（ルータで定義する必要があります）。papuser:PAP/PPP：ユーザが回線2でダイヤルします。アドレスは、ピアのデフォルトipアドレスプールasyncおよびip local pool async 10.6.100.101 10.6.100.103によってルータに割り当てられますpapaddr:PAP/PPP：ユーザが回線2でダイヤルインします。アドレス10.29.1.98はサーバによって割り当てられるpapacl:PAP/PPP：ユーザが回線2でダイヤルします。アドレス10.29.1.100はサーバによって割り当てられ、着信アクセスリスト101が適用されます。これはルータで定義する必要がありますloginauto：ユーザがオンラインでダイヤルします3。autocommand onlineを使用したログイン認証により、ユーザは強制的にPPP接続を行い、プールからアドレスを割り当てられます
4. ユーザーloginautoを除くすべてのユーザー用のMicrosoft Windowsセットアップ[Start] > [Programs] > [Accessories] > [Dial-Up Networking]の順に選択します。Connections > Make New Connectionの順に選択します。接続の名前を入力します。モデム固有の情報を入力します。[Configure] > [General]で、モデムの最高速度を選択します。ただし、次のチェックボックスはオンにしないでください。[Configure] > [Connection]で、8データビット、パリティなし、1ストップビットを使用します。コール設定は、[ダイヤルする前にダイヤルトーンを待つ]と[接続していない場合は200秒後にコールをキャンセル]です。[詳細]で、[ハードウェアフロー制御]と[変調タイプ標準]のみを選択します。[Configure] > [Options]では、ステータス管理の下を除き、何もチェックしないでください。[OK] をクリックします。[次へ]ウィンドウで、宛先の電話番号を入力し、[次へ]をクリックして、[完了]をクリックします。新しい接続アイコンが表示されたら、それを右クリックして[プロパティ]を選択し、[サーバの種類]をクリックします。PPP:WINDOWS 95、WINDOWS NT 3.5、Internetを選択し、高度なオプションはチェックしないでください。[許可されたネットワークプロトコル]で、少なくともTCP/IPを確認します。[TCP/IP settings]で、[Server assigned IP address] 、[Server assigned name server addresses] 、[Use default gateway on remote network]の順に選択します。[OK] をクリックします。アイコンをダブルクリックして[接続先(Connect To)]ウィンドウを開き、ダイヤルするには、[ユーザ名(User name)]フィールドと[パスワード(Password)]フィールドに入力し、[接続(Connect)]をクリックする必要があります。
5. Microsoft Windows 95 Setup for User loginautoユーザloginautoの設定、autocommand PPPを使用した認証ユーザは、[Configure] > [Options]ウィンドウを除き、他のユーザと同じ設定になります。[Bring up terminal window after dialing]をオンにします。アイコンをダブルクリックして[接続先(Connect To)]ウィンドウを開き、ダイヤルすると、[ユーザ名(User

name)]フィールドと[パスワード(Password)]フィールドに入力しません。[Connect] をクリックし、ルータへの接続が確立されたら、黒いウィンドウにユーザ名とパスワードを入力します。認証が完了したら、**[Continue (F7)]をクリックします**。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

サーバ

```
./Cisco Secure -cx -f $BASE/CSU $BASE/config/CSU.cfg
```

ルータ

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

注：debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。特定のコマンドの詳細については、『Cisco IOS Debugコマンドリファレンス』を参照してください。

- **terminal monitor**：現在のターミナルおよびセッションの**debug**コマンド出力とシステムエラーメッセージを表示します。
- **debug ppp negotiation**：PPP の開始時に送信される PPP パケットを表示します。PPP の開始時には PPP オプションがネゴシエートされます。
- **debug ppp packet**：送受信されるPPPパケットを表示します。このコマンドは低レベルのパケット ダンプを表示します。
- **debug ppp chap**：チャレンジ認証プロトコル(CHAP)を実装するインターネットワークのトラフィックおよび交換に関する情報を表示します。
- **debug aaa authentication**：使用されている認証方式とその結果を確認します。
- **debug aaa authorization**：使用されている許可方式とその結果を確認します。

Cisco Secure ユーザファイル

```
group = admin {
        password = clear "adminpwd"
        service = shell {
                default cmd = permit
                default attribute = permit
        }
}

group = oper {
        password = clear "oper"
        privilege = clear "cisco" 15
```

```
        service = shell {
                default cmd = permit
                default attribute = permit
        }
}

user = adminusr {
        password = clear "adminusr"
        default service = permit
        }

user = desusr {
        password = des "QjnXYd1kd7ePk"
        default service = permit
        }

user = operator {
        member = oper
        default service = permit
        }

user = time {
        default service = permit
        password = clear "time"
        service = shell  {
                set timeout = 1
                default cmd = permit
                default attribute = permit
        }
}

user = todam {
        password = clear "todam"
        service = shell  {
                default cmd = permit
                default attribute = permit
                time = Any 0600 - 1200
        }
        }

user = todpm {
        password = clear "todpm"
        service = shell  {
                default cmd = permit
                default attribute = permit
                time = Any 1200 - 2359
        }
        }

user = telnet {
        password = clear "telnet"
        service = shell  {
                set autocmd = "telnet 171.68.118.102"
                        }
        }

user = limit_lifetime {
        password = clear "cisco" from
        "2 may 2001" until
        "4 may 2001"
        }

user = loneusr {
        password = clear "lonepwd"
```

```
        service = shell  {
                cmd = show {
                permit "ver"
                }
                cmd = ping {
                permit "."
                }
                cmd = logout {
                permit "."
                }
        }
}

user = chapuser {
        default service = permit
        password = chap "chapuser"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                }
        }
}

user = chapaddr {
        password = chap "chapaddr"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set addr = 10.29.1.99
                }
        }
}

user = chapacl {
        default service = permit
        password = chap "chapacl"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set inacl = 101
                        set addr = 10.29.1.100
                }
        }
}

user = papuser {
        default service = permit
        password = pap "papuser"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                }
        }
}

user = papaddr {
        default service = permit
        password = pap "papaddr"
        service = ppp {
                protocol = lcp {
```

```
                        }
                protocol = ip {
                        set addr = 10.29.1.98
                }
        }
}

user = papacl {
        default service = permit
        password = chap "papacl"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set inacl = 101
                        set addr = 10.29.1.100
                }
        }
}

user = loginauto {
        default service = permit
        password = clear "loginauto"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        }
        }
 }

user = somerouters {
   password = clear "somerouters"
   allow koala ".*" "10\.31\.1\.*"
   allow koala.rtp.cisco.com ".*" "10\.31\.1\.*"
   allow 10.31.1.5 ".*" "10\.31\.1\.*"
   refuse ".*" ".*" ".*"
   service=shell {
   default cmd=permit
   default attribute=permit
   }
   }
```

関連情報

- Cisco Secure ACS for UNIX製品のサポート
- セキュリティ製品に関する Field Notice（Cisco Secure UNIX を含む）