Configurando e depurando o CiscoSecure 2.x TACACS+

Contents

Introduction

Este documento destina-se a auxiliar o usuário do Cisco Secure 2.x pela primeira vez na configuração e depuração de uma configuração do Cisco Secure TACACS+. Não é uma descrição exaustiva dos recursos do Cisco Secure.

Consulte a documentação do Cisco Secure para obter informações mais completas sobre o software do servidor e a configuração do usuário. Consulte a documentação do Cisco IOS Software para obter a versão apropriada para obter mais informações sobre os comandos do roteador.

Prerequisites

Requirements

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure ACS 2.x e posterior
- Cisco IOS® Software Release 11.3.3 e Mais Recente

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurando o Cisco Secure

Conclua estes passos:

1. Certifique-se de usar as instruções fornecidas com o software para instalar o código Cisco Secure no servidor UNIX.
2. Para confirmar se o produto para e inicia, digite `cd para /etc/rc0.d` e como raiz, execute `./K80Cisco Secure` (para interromper os daemons).Digite `cd em /etc/rc2.d` e, como raiz, execute `./S80Cisco Secure` (para iniciar os daemons).Na inicialização, você deve ver mensagens como:
   ```
   Cisco Secure starting Processes: Fast Track Admin, FastTrack Server (Delayed Start),
   DBServer, AAA Server
   ```
   Execute `$BASE/utils/psg` para ter certeza de que pelo menos um dos processos individuais é executado, por exemplo, SQLAnywhere ou outro mecanismo de banco de dados, processo de servidor de banco de dados Cisco Secure, Netscape Web Server, Netscape Web Admin, Acme Web Server, processo Cisco Secure AAA ou processo de reinicialização automática.
3. Para garantir que você está nos diretórios apropriados, configure variáveis e caminhos ambientais no ambiente shell. c-shell é usado aqui.**$BASE** é o diretório onde o Cisco Secure está instalado, escolhido durante a instalação. Contém diretórios como DOCS, DBServer, CSU e assim por diante.Neste exemplo, a instalação em /opt/CSCOacs é presumida, mas isso pode ser diferente no seu sistema:
   ```
   setenv $BASE   /opt/CSCOacs
   ```
   $SQLANY é o diretório onde o banco de dados Cisco Secure padrão está instalado, escolhido durante a instalação. Se o banco de dados padrão que acompanha o produto, SQLAnywhere, foi usado, ele contém diretórios como banco de dados, documento e assim por diante.Neste exemplo, a instalação em /opt/CSCOacs/SYBSsa50 é presumida, mas isso pode ser diferente no seu sistema.
   ```
   setenv $SQLANY /opt/CSCOacs/SYBSsa50
   ```
   Adicione caminhos em seu ambiente shell para:
   ```
   $BASE/utils
   $BASE/bin
   $BASE/CSU
   $BASE/ns-home/admserv
   $BASE/Ns-home/bin/httpd
   $SQLANY/bin
   ```
4. CD para $BASE/config**CSU.cfg** é o arquivo de controle do servidor Cisco Secure. Faça uma cópia de backup deste arquivo.Neste arquivo, `LIST config_license_key` mostra a chave de licença que você recebeu através do processo de licenciamento se você adquiriu o software; se esta for uma licença de avaliação de 4 portas, você pode deixar de fora essa linha.A seção **NAS config_nas_config** pode conter um servidor de acesso à rede (NAS) ou roteador padrão, ou o NAS que você inseriu durante a instalação. Para fins de depuração neste exemplo, você pode permitir que *qualquer* NAS se comunique com o servidor Cisco Secure *sem* uma chave. Por exemplo, remova o nome do NAS e a chave das linhas que contêm o `/* nome do NAS podem ir aqui */`" e */*NAS/Cisco Secure secret key */*. A única *estrofe* naquela área diz:

```
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 = {
```

Ao fazer isso, você informa ao Cisco Secure que é permitido conversar com todos os NASs sem troca de chaves.

5. Se desejar que as informações de depuração sejam enviadas para /var/log/csuslog, você precisará ter uma linha na seção superior do CSU.cfg, que informa ao servidor quanto deve ser feito o debugging. 0X7FFFFFFF adiciona toda a depuração possível. Adicione ou modifique esta linha de acordo:
   ```
   NUMBER config_logging_configuration = 0x7FFFFFFF;
   ```
   Esta linha adicional envia as informações de depuração para local0:
   ```
   NUMBER config_system_logging_level = 0x80;
   ```
   Além disso, adicione esta entrada para modificar o arquivo /etc/syslog.conf:
   ```
   local0.debug /var/log/csuslog
   ```
   Em seguida, recicle o syslogd para ler novamente:
   ```
   kill -HUP `cat /etc/syslog.pid`
   ```
   Reciclar o servidor Cisco Secure:
   ```
   /etc/rc0.d/K80Cisco Secure
   /etc/rc2.d/S80Cisco Secure
   ```
   Ainda deve começar.
6. Você pode usar o navegador para adicionar usuários, grupos e assim por diante, ou o utilitário CSimport. Os usuários de exemplo no arquivo simples no final deste documento podem ser facilmente movidos para o banco de dados usando CSimport. Esses usuários trabalharão para fins de teste e você poderá excluí-los assim que receber seus próprios usuários. Depois de importados, você pode ver os usuários importados através da GUI.Se você decidir usar o CSimport:
   ```
   CD $BASE/utils
   ```
   Coloque os perfis de usuário e de grupo no final deste documento em um arquivo como em qualquer lugar do sistema, depois no diretório $BASE/utils, com os daemons em execução, por exemplo, /etc/rc2.d/S80Cisco Secure e como raiz de usuário, execute CSimport com a opção test (-t):
   ```
   ./CSimport -t -p <path_to_file> -s <name_of_file>
   ```
   Isso testa a sintaxe dos usuários; você deve receber mensagens como:
   ```
   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...
   ```
   Você *não* deve receber mensagens como:
   ```
   Error at line 2: password = "adminusr"
   Couldn't repair and continue parse
   ```
   Se houve ou não erros, examine o arquivo upgrade.log para verificar se os perfis foram verificados. Quando os erros forem corrigidos, no diretório $BASE/utils, com os daemons em execução (/etc/rc2.d/S80Cisco Secure) e como raiz do usuário, execute CSimport com a

opção commit (-c) para mover os usuários para o banco de dados:
```
./CSimport -c -p <path_to_file> -s <name_of_file>
```
Novamente, não deve haver erros na tela ou no arquivo upgrade.log.

7. Os navegadores suportados estão listados na dica técnica Cisco Secure Compatibility. No navegador do PC, aponte para a caixa Cisco Secure/Solaris **http://#.#.#.#.#/cs** onde **#.#.#.#** é o IP do servidor Cisco Secure/Solaris.Na tela exibida, para o usuário, digite **superuser** e, para a senha, digite **changeme**. Não altere a senha neste momento. Você deve ver os usuários/grupos adicionados se usar o CSimport na etapa anterior ou clicar no bloco de navegação **desligado** e adicionar usuários e grupos manualmente através da GUI.

Configurando a autenticação

Observação: essa configuração de roteador foi desenvolvida em um roteador que executa o Cisco IOS Software Release 11.3.3. O Cisco IOS Software Release 12.0.5.T e posterior mostra **táticas de grupo** em vez de **táticas**.

Neste ponto, configure o roteador.

1. Mate o Cisco Secure enquanto você configura o roteador.
```
/etc/rc0.d/K80Cisco Secure to stop the daemons.
```
2. No roteador, inicie a configuração do TACACS+. Entre no modo de ativação e digite `conf t` antes do conjunto de comandos. Essa sintaxe garante que você não seja bloqueado do roteador *inicialmente* desde que o Cisco Secure não esteja em execução. Digite `ps -ef | grep Secure` para verificar se o Cisco Secure não está em execução e matar -9 o processo se ele estiver:

```
!--- 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. Teste para ter certeza de que ainda pode acessar o roteador com Telnet e através da porta de console antes de continuar. Como o Cisco Secure não está em execução, a senha de ativação deve ser aceita.**Cuidado:** mantenha a sessão da porta do console ativa e permaneça no modo de ativação; esta sessão não deve expirar. Você começa a limitar o acesso ao roteador neste ponto e precisa ser capaz de fazer alterações de configuração sem se bloquear.Execute estes comandos para ver a interação servidor-roteador no roteador:
```
terminal monitor
debug aaa authentication
```
4. Como raiz, inicie o Cisco Secure no servidor:
```
/etc/rc2.d/S80Cisco Secure
```
Isso inicia os processos, mas você deseja habilitar mais a depuração do que a configurada no S80Cisco Secure, portanto:
```
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
```

Com a opção `-x`, o Cisco Secure é executado em primeiro plano para que a interação entre roteador e servidor possa ser observada. Você não deve ver mensagens de erro. O processo do Cisco Secure deve começar e travar lá devido à opção -x.

5. Em outra janela, verifique se o Cisco Secure foi iniciado. Digite `ps -ef` e procure o processo do Cisco Secure.
6. Os usuários do Telnet (vty) agora devem se autenticar através do Cisco Secure. Com debug no roteador, faça Telnet no roteador a partir de outra parte da rede. O roteador deve produzir um prompt de nome de usuário e senha. Você deve ser capaz de acessar o roteador com essas combinações de ID/senha de usuário:

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

   Observe o servidor e o roteador onde você deve ver a interação, ou seja, o que é enviado para onde, respostas, solicitações e assim por diante. Corrija todos os problemas antes de continuar.
7. Se você também quiser que seus usuários se autentiquem através do Cisco Secure para entrar no modo de ativação, verifique se a sessão da porta de console ainda está ativa e adicione este comando ao roteador:

   ```
   !--- 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. Agora você deve ter que **habilitar** através do Cisco Secure. Com debug no roteador, faça Telnet no roteador a partir de outra parte da rede. Quando o roteador solicitar nome de usuário/senha, responda com `operador/operador`.Quando o operador do usuário tenta entrar no modo de ativação (nível de privilégio 15), a senha "cisco" é necessária. Outros usuários não poderão entrar no modo de ativação sem a instrução de nível de privilégio (ou o daemon Cisco Secure desativado).Observe o servidor e o roteador onde você deve ver a interação do Cisco Secure, por exemplo, o que está sendo enviado para onde, respostas, solicitações e assim por diante. Corrija todos os problemas antes de continuar.
9. Desative o processo do Cisco Secure no servidor enquanto ainda estiver conectado à porta do console para ter certeza de que seus usuários ainda podem acessar o roteador se o Cisco Secure estiver inoperante:

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

   Repita o Telnet e habilite a etapa anterior. O roteador deve perceber que o processo do Cisco Secure não responde e permite que os usuários façam login e ativem com as senhas de ativação padrão.
10. Ative o servidor Cisco Secure novamente e estabeleça uma sessão Telnet para o roteador, que deve ser autenticado através do Cisco Secure, com userid/password **operator/oper** para verificar a autenticação dos usuários da porta de console através do Cisco Secure. Mantenha-se conectado ao roteador e no modo de ativação até ter certeza de que pode fazer login no roteador através da porta do console, por exemplo, fazer logoff da sua conexão original com o roteador através da porta do console e, em seguida, reconectar-se à porta do console. A autenticação da porta do console para fazer login com o uso das combinações de ID de usuário/senha anteriores deve ser feita através do Cisco Secure. Por exemplo, userid/password **operator/oper**, a senha **cisco** deve ser usada para **habilitar**.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Autorização de adição

A adição de autorização é opcional.

Por padrão, há três níveis de comando no roteador:

- Nível de privilégio 0—que inclui desabilitar, habilitar saída, ajuda e logoff
- Nível de privilégio 1—nível normal em um Telnet e prompt diz `router>`
- Nível de privilégio 15—nível de habilitação e prompt dizem `router#`

Como os comandos disponíveis dependem do conjunto de recursos do Cisco IOS, da versão do software Cisco IOS, do modelo do roteador e assim por diante, não há uma lista abrangente de todos os comandos nos níveis 1 e 15. Por exemplo, **show ipx route** não está presente em um conjunto de recursos somente IP, **show ip nat trans** não está no código do Cisco IOS Software Release 10.2.X porque o NAT não foi introduzido no momento e **show environment** não está presente em modelos de roteador sem fonte de alimentação e monitoramento de temperatura.

Os comandos disponíveis em um roteador específico em um nível específico podem ser encontrados ao digitar um **?** no prompt do roteador quando estiver nesse nível de privilégio.

A autorização da porta do console não foi adicionada como um recurso até que o CSCdi82030 foi implementado. A autorização da porta do console está desativada por padrão para diminuir a probabilidade de ser acidentalmente bloqueada para fora do roteador. Se um usuário tiver acesso físico ao roteador através do console, a autorização da porta do console não será extremamente eficaz. Mas, a autorização da porta de console pode ser ativada sob o comando **line con 0** em uma imagem do Cisco IOS na qual o CSCdi82030 foi implementado com o comando **exec authorization default|WORD**.

Conclua estes passos:

1. O roteador pode ser configurado para autorizar comandos através do Cisco Secure em todos ou alguns níveis. Essa configuração de roteador permite que todos os usuários tenham autorização por comando configurada no servidor. Você pode autorizar todos os comandos através do Cisco Secure, mas se o servidor estiver inoperante, nenhuma autorização será necessária, portanto, a `nenhum`.Com o servidor Cisco Secure desativado, insira estes comandos:Insira este comando para remover o requisito de habilitar a autenticação através do Cisco Secure:
   ```
   no aaa authentication enable default tacacs+ none
   ```
   Insira estes comandos para exigir que a autorização dos comandos seja feita através do Cisco Secure:
   ```
   aaa authorization commands 0 default tacacs+ none
   aaa authorization commands 1 default tacacs+ none
   aaa authorization commands 15 default tacacs+ none
   ```
2. Enquanto o servidor Cisco Secure é executado, faça Telnet no roteador com userid/password **loneusr/lonepwd**. Este usuário não deve ser capaz de executar nenhum comando diferente de:

```
show version
ping <anything>
logout
```

Os usuários anteriores, **administrador/administrador**, **operador/oper**, **dessusr/encrypt**, ainda devem ser capazes de executar todos os comandos em virtude do `serviço padrão = permit`. Se houver problemas com o processo, entre no modo enable no roteador e ative a depuração de autorização com este comando:

```
terminal monitor
debug aaa authorization
```

Observe o servidor e o roteador onde você deve ver a interação do Cisco Secure, por exemplo, o que é enviado para onde, respostas, solicitações e assim por diante. Corrija todos os problemas antes de continuar.

3. O roteador pode ser configurado para autorizar sessões exec através do Cisco Secure. O comando **aaa authorization exec default tacacs+ none** institui a autorização TACACS+ para sessões exec.Se você aplicar isso, isso afetará o tempo/tempo dos usuários, **telnet/telnet**, **todam/todam**, **todpm/todpm** e **somerouters/somerouters**. Depois de adicionar esse comando ao roteador e executar telnet para o roteador como **tempo/hora** do usuário, uma sessão exec permanece aberta por um minuto (set timeout = 1). O usuário **telnet/telnet** entra no roteador, mas é enviado imediatamente para o outro endereço (set autocmd = "telnet 171.68.118.102"). É possível que os usuários **todam/todam** e **todpm/todpm** consigam ou não acessar o roteador, que depende da hora do dia em que ele ocorre durante o teste. Os **somerouters** do usuário só podem fazer Telnet no roteador koala.rtp.cisco.com a partir da rede 10.31.1.x. O Cisco Secure tenta resolver o nome do roteador. Se você usar o endereço IP 10.31.1.5, ele será válido se a resolução não ocorrer e se você usar o nome koala, ele será válido se a resolução for aprovada.

Relatório de adição

A adição de contabilidade é opcional.

1. A contabilização não ocorre a menos que seja configurada no roteador, se o roteador executar o software Cisco IOS versão posterior ao Cisco IOS Software Release 11.0. Você pode ativar a contabilização no roteador:

```
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+
```

Observação: a contabilização de comandos foi interrompida, no bug da Cisco ID CSCdi44140, mas se você usa uma imagem na qual isso é corrigido, a contabilização de comandos também pode ser ativada.

2. Adicione a depuração de registro contábil no roteador:

```
terminal monitor
debug aaa accounting
```

3. A depuração no console deve mostrar os registros de contabilidade que entram no servidor à medida que os usuários fazem logon.
4. Para recuperar registros de contabilidade, como raiz:

```
CD $BASE/utils/bin
./AcctExport <filename> no_truncate
```

`no_truncate` significa que os dados são retidos no banco de dados.

Adicionando usuários de discagem

Conclua estes passos:

1. Certifique-se de que as outras funções do Cisco Secure funcionem antes de adicionar usuários de discagem. Se o servidor Cisco Secure e o modem não funcionaram antes deste ponto, eles não funcionarão depois deste ponto.
2. Adicione esse comando à configuração do roteador:
   ```
   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
   ```
   As configurações da interface diferem, o que depende de como a autenticação é feita, mas as linhas de discagem são usadas neste exemplo, com estas configurações:
   ```
   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. Do arquivo do usuário do Cisco Secure:capuser—CHAP/PPP—o usuário disca na linha 1; o endereço é atribuído por **peer default ip address pool async e ip local pool assíncrono 10.6.100.101 10.6.100.103** no roteadorcapaddr—CHAP/PPP—o usuário disca na linha 1; o endereço 10.29.1.99 é atribuído pelo servidorcapacl—CHAP/PPP—o usuário disca na linha 1; o endereço 10.29.1.100 é atribuído pelo servidor e a lista de acesso de entrada 101 é aplicada (que deve ser definida no roteador)papuser—PAP/PPP— o usuário disca na linha 2; o endereço é atribuído por **peer default ip address pool async e ip local pool assíncrono 10.6.100.101 10.6.100.103** no roteadorpapaddr—PAP/PPP—o usuário disca na linha 2; o endereço 10.29.1.98 é atribuído pelo servidorpapacl—PAP/PPP—o usuário disca na linha 2; o endereço 10.29.1.100 é atribuído pelo servidor e a lista de acesso de entrada 101 é aplicada, que deve ser definida no roteadorloginauto—o usuário disca na linha 3; a autenticação de login com autocomando on-line força o usuário a se conectar ao PPP e atribui o endereço do pool
4. Configuração do Microsoft Windows para todos os usuários, exceto login automático de usuárioEscolha **Iniciar > Programas > Acessórios > Rede dial-up**.Escolha **Conexões > Criar nova conexão**. digite um nome para sua conexão.Insira as informações específicas do modem. Em **Configurar > Geral**, escolha a velocidade mais alta do modem, mas não marque a caixa abaixo disso.Em **Configurar > Conexão**, use 8 bits de dados, sem paridade e 1 bit de parada. As preferências de chamada são **Aguardar o tom de discagem antes de discar** e **Cancelar a chamada se não estiver conectada após 200 segundos**.Em Avançado, escolha somente **Hardware Flow Control** e **Modulation Type Standard**.Em **Configurar > Opções**, nada deve ser verificado, exceto sob controle de status. Click **OK**.Na janela Next (Avançar), digite o número de telefone do destino, clique em **Next (Avançar)** e clique em **Finish (Concluir)**.Quando o ícone de nova conexão for exibido, clique com o botão direito do mouse

nele e escolha **Propriedades** e clique em **Tipo de servidor**.Escolha **PPP:WINDOWS 95, WINDOWS NT 3.5, Internet** e não marque nenhuma opção avançada.Nos protocolos de rede permitidos, verifique pelo menos **TCP/IP**.Nas configurações TCP/IP, escolha o **endereço IP atribuído ao servidor**, os **endereços atribuídos ao servidor** e **use o gateway padrão na rede remota**. Click **OK**.Quando você clica duas vezes no ícone para abrir a janela Conectar a para discar, preencha os campos Nome de usuário e Senha e clique em **Conectar**.

5. Configuração do Microsoft Windows 95 para Loginauto do usuárioA configuração do usuário loginauto, usuário de autenticação com autocomando PPP, é a mesma que para outros usuários, exceto na janela **Configurar > Opções**. Marque **a janela Ativar terminal depois de discar**.Quando você clica duas vezes no ícone para exibir a janela Conectar a para discar, não preencha os campos Nome de usuário e Senha. Clique em **Connect** e depois que a conexão com o roteador for estabelecida, digite o nome de usuário e a senha na janela preta exibida.Após a autenticação, clique em **Continuar(F7)**.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Servidor

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

Router

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug. Para obter mais informações sobre comandos específicos, consulte Referência de Comandos de Depuração do Cisco IOS.

- **terminal monitor**—Display **debug** command output e system error messages for the current terminal and session.
- **debug ppp negotiation** —Exibe os pacotes PPP transmitidos durante a inicialização do PPP, onde as opções do PPP são negociadas.
- **debug ppp packet** — Exibe os pacotes PPP que são enviados e recebidos. Esse comando exibe os dumps de pacote de nível baixo.
- **debug ppp chap** —Exibe informações sobre tráfego e trocas em uma internetwork implementando o Challenge Authentication Protocol (CHAP).
- **debug aaa authentication** —Veja quais métodos de autenticação estão sendo usados e quais são os resultados desses métodos.

- **debug aaa authorization** — Veja quais métodos de autorização estão sendo usados e quais são os resultados desses métodos.

Arquivo de usuários do Cisco Secure

```
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
   }
   }
```

Informações Relacionadas

- Suporte ao produto Cisco Secure ACS para UNIX
- Avisos de campo de produtos de segurança (incluindo Cisco Secure UNIX)