Cisco Secure ACS UNIX FAQ

Índice

Introdução

Este documento dá respostas às perguntas comum sobre o Serviço de controle de acesso Cisco Secure (ACS) para UNIX (CSUnix).

Geral

Q. Podem os dados ser migrados entre CSUnix e Cisco Secure ACS for Windows (ACS)?

A. Não há atualmente nenhum instrumento de apoio usado para migrar usuários de um produto a um outro produto.

Q. CSUnix autentica contra um base de dados de NT, um LDAP, ou um NDS de Novell?

A. Não, mas estas características esta presente no Cisco Secure ACS for Windows (ACS). O Cisco Access Registrar apoia o Lightweight Directory Access Protocol (LDAP).

Licenciamento e software

Q. A versão de CSUnix 2.3.6.2 é apoiada na versão do oracle 9.2.0?

A. Os Release Note para a versão de CSUnix 2.6.3.2 indicam que a versão 8.0.x do oracle enterprise, a versão 9.0.1 8i, e 9i são versões suportadas. É possível promover à versão do oracle 9.2.0. Contudo, recomenda-se que você backup seu base de dados antes que você

promova.

Q. Como eu atualizo uma chave de licença com validade vencida?

A. Para detalhes em como obter uma chave de licença, refira problemas de licenciamento para Cisco UNIX seguro.

Q. Como eu encontro minha versão do Solaris e o endereço IP de Um ou Mais Servidores Cisco ICM NT de meu sistema?

A. A fim determinar a versão do Solaris que você uso, emite o **comando uname – a**.

A fim determinar o endereço IP de Um ou Mais Servidores Cisco ICM NT no uso por seu sistema, emita o **comando ifconfig – a**.

Q. Onde posso eu obter elevações e correções de programa de software para CSUnix?

A. As elevações de software podem ser obtidas do site do software de Serviço de controle de acesso Cisco Secure (clientes registrados somente). As correções de software podem ser obtidas das correções de programa do Software Seguro Cisco - site de UNIX (clientes registrados somente).

Nota: Você deve incorporar o **cspatchunix ao** campo do código de acesso especial para alcançar as correções de programa do Software Seguro Cisco - site de UNIX (clientes registrados somente).

Os usuários que não têm um ID válido do Cisco podem obter elevações e correções de programa de software do Suporte técnico de Cisco através do email e do telefone. Refira o site dos contatos mundiais da Cisco.

Q. Posso eu promover de CSUnix a Cisco seguro para Windows ou o Cisco Access Registrar?

A. Para obter informações sobre da fixação do preço e da Disponibilidade da “de elevações lateral,” contacte seu equipe de conta da Cisco local.

Q. Como eu determino minha versão de CSUnix?

A. Emita este comando:

```
$BASE/CSU/CiscoSecure -v
```

O **$BASE** representa o diretório em que CSUnix é instalado.

Q. Como eu reciclo (fechado e começo) os serviços CSUnix?

A. Há duas maneiras diferentes de reciclar os serviços.

- Emita o comando de **/etc/rc0.d/K80CiscoSecure** fechar, a seguir emita o comando de

/etc/rc2.d/S80CiscoSecure reiniciar.OU

- Emita o **comando $BASE/utils/kcs** fechar, a seguir emita o **comando $BASE/utils/scs** reiniciar.**O $BASE** representa o diretório em que CSUnix é instalado.

Depois que os serviços são reiniciados, emita o **comando $BASE/utils/psg**. Indica uma entrada para cada serviço.

Q. Como posso eu encontrar aonde CSUnix é instalado em minha máquina?

A. A fim determinar o local de instalação do CSUnix, emita o **comando pkginfo -l CSCEacs**.

Q. Como eu sei que valores foram selecionados durante a instalação?

A. O log de instalação de CSUnix é armazenado em **$BASE/logfiles/cs_install.log, onde $BASEREPRESENTS o** diretório em que CSUnix é instalado. Este arquivo alista todos os valores selecionados durante a instalação.

Q. Que são o requisito de software e hardware para minha versão de CSUnix?

A. A informação sobre requisitos está nas instruções de instalação para sua versão de software específica. A informação sobre requisitos é resumida igualmente na compatibilidade UNIX do Cisco Secure ACS.

Q. Há alguma restrição de exportação em CSUnix?

A. Não, CSUnix é empacotado com a versão exportável do servidor fasttrack de Netscape.

Configuração do sistema

Q. Como eu mudo o endereço IP de Um ou Mais Servidores Cisco ICM NT, o hostname, ou o nome de domínio totalmente qualificado (FQDN) do servidor CSUnix?

A. O endereço IP de Um ou Mais Servidores Cisco ICM NT, o hostname, e o FQDN para o server são armazenados em diversos arquivos, com base na versão de CSUnix no uso. Por este motivo, o método suportado usado para mudar um endereço IP de Um ou Mais Servidores Cisco ICM NT, o hostname, ou o FQDN são desinstalar o software e reinstalá-lo então com as configurações desejadas. Esta operação não afeta o base de dados. Os usuários e os grupos são retidos.

Termine estas etapas para fazer mudanças aos ajustes em seu servidor CSUnix:

1. Feche o software.
2. Suporte o base de dados. O Oracle ou Sybase podem ser suportados pelo administrador da base de dados. Copie o **csecure. db e os arquivos de** csecure.log a um lugar seguro a fim suportar o SQLAnywhere. Esta é uma precaução somente, porque as tabelas não são deixadas cair durante o processo da desinstalação e da reinstalação. Além, mantenha uma cópia do **arquivo do** $BASE/config/CSU.cfg**.** Este arquivo contém a informação do dispositivo. **$BASEREPRESENTS o** diretório em que CSUnix é instalado.
3. Emita o **comando pkgrm CSCEacs** desinstalar o programa. Este comando sae do **csecure.**

db e dos arquivos de csecure.log no lugar.

4. Assegure-se de que a resolução de nome trabalhe. A fim fazer isto, emita os **comandos hostname, nslookup, e ifconfig** segundo as indicações desta saída. `# **hostname** rtp-evergreen # **nslookup rtp-evergreen** Server: redclay2.cisco.com Address: 172.18.125.3 Non-authoritative answer: Name: rtp-evergreen.cisco.com Address: 172.18.124.114 # **nslookup rtp-evergreen.cisco.com** Server: redclay2.cisco.com Address: 172.18.125.3 Non-authoritative answer: Name: rtp-evergreen.cisco.com Address: 172.18.124.114 # **nslookup 172.18.124.114** Server: redclay2.cisco.com Address: 172.18.125.3 Name: rtp-evergreen.cisco.com Address: 172.18.124.114 # **ifconfig -a** lo0: flags=849<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232 inet 127.0.0.1 netmask ff000000 le0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500 inet 172.18.124.114 netmask ffff0000 broadcast 172.18.255.255 ether 8:0:20:76:79:f9`
5. Instale o software. Emita o **comando pkgadd -d path_to_software** e indique que esta é uma instalação da upgrade segundo as indicações desta saída.
```
New CiscoSecure install             no
.
.
.
SQLAnywhere DB directory            original_path !--- Use the path in which the csecure.*
files are located. Drop existing database tables no
```
6. Depois que a instalação está completa, comece o software e assegure-se de que os serviços corrida.

Q. Eu estou tendo problemas com o Domain Name System (DNS) em minha rede. Como eu desabilito a resolução de DNS de IP a nome de host no sistema CSUnix de modo que não tente resolver nomes?

A. À revelia, CSUnix tenta resolver o IP recebido do dispositivo do cliente a um nome de domínio totalmente qualificado (FQDN) e compara então o FQDN às entradas no **arquivo csu.cfg**. Se o DNS na rede não trabalha corretamente, este pode causar a autenticação e problemas raros lentos. A fim impedir que CSUnix tente a definição, suporte o **arquivo do** $BASE/config/CSU.cfg (onde **$BASEREPRESENTS o** diretório em que CSUnix é instalado). Em seguida, altere-o adicionando esta linha à seção do começo com o outro NUMBERENTRIES:

```
NUMBER config_get_names_from_dns = 0;
```

Salvar o arquivo alterado, a seguir recicle o server.

Q. Como eu ajusto o número de falhas de tentativa de login aceitável?

A. Termine estas etapas a fim ajustar numa base global este valor para todos os usuários.

1. Abra o **arquivo do $BASE/config/CSU.cfg** (**$BASEREPRESENTS o** diretório em que CSUnix é instalado).
2. Adicionar esta linha à seção do começo com as outras **entradas de número**: `NUMBER config_max_failed_authentication = n;` Substitua *n* com o número de falhas de tentativa permissíveis.

Termine estas etapas a fim ajustar este valor em um usuário per. ou base por grupo versão de CSUnix em 2.3.5.1 ou em mais tarde:

1. Abra o **arquivo do $BASE/config/CSU.cfg**.
2. Adicionar esta linha à seção do começo com as outras **entradas de número**: `NUMBER config_allow_global_max_failed_login_session_enable = 0;`Porque o sistema usa as configurações globais à revelia, a linha dos tis é usada para desligar as autenticações

inválidas máximas globais e para reservá-los por usuário ou os máximos do por-grupo a ser ajustados.
3. No usuário ou no perfil de grupo, adicionar esta linha: `set server max-failed-login-count = n;` Substitua *n* com o número de falhas de tentativa permissíveis.

Q. Como eu mudo a porta padrão (9900) em que o base de dados escuta?

Cuidado: CSUnix não foi testado para a Interoperabilidade com outro software. Os aplicativos múltiplos que são executado no o mesmo server não são apoiados. Isto pode causar problemas de desempenho e conflitos de portas em portas diferentes da porta de servidor de dados.

Se você deseja executar múltiplas instâncias do base de dados, feche os processos csunix e altere estes arquivos para usar uma porta a não ser 9900:

- $BASE/CSU/libdb.conf
- $BASE/FastAdmin/turbo.conf
- $BASE/config/CSConfig.ini

O **$BASE** representa o diretório em que CSUnix é instalado.

Q. Como eu ver o perfil de grupo ou usuário na interface de linha de comando?

A. Emita estes comandos na alerta do diretório **$BASE/CLI/**, onde o **$BASE** representa o diretório em que CSUnix é instalado.

- Entre em **./ViewProfile - p 9900 -** *username* **u** a fim ver um perfil de usuário.Substitua o *username* com o nome de usuário para o perfil de usuário que você quer ver.
- Entre em **./ViewProfile - p 9900 -** *nome de grupo* **g** a fim ver um perfil de grupo.Substitua o *nome de grupo* com o nome para o perfil de grupo que você quer ver.

Q. Como eu ajusto o página da web de CSUnix para ser executado em uma porta a não ser a porta 80?

Cuidado: CSUnix não foi testado para a Interoperabilidade com outro software. Os aplicativos múltiplos que são executado no o mesmo server não são apoiados. Isto pode causar problemas de desempenho e conflitos de portas em portas diferentes da porta de servidor de dados.

Se você deseja executar vários servidores de web, feche os processos csunix e altere estes arquivos para usar uma porta a não ser a porta 80:

- No arquivo **$BASE/ns-home/httpd-servername/config** (onde o **$BASE** representa o diretório em que CSUnix é instalado), **porta 80 da** mudança **para mover *n***, onde *n* é a porta nova em que você a quer ser executado.
- **No arquivo $BASE/FastAdmin/turbo.conf**, mude NS_PATH **=server/cs/ao =server de** NS_Path**: n/cs, onde** n *é o* número de porta inscrito no arquivo.

Q. Eu esqueci minha senha. Como posso eu restaurar o perfil do administrador?

A. Emita estes comandos a fim restaurar a senha de administrador:

```
$BASE/CLI/DeleteProfile -p 9900 -u superuser $BASE/CLI/AddProfile -p 9900 -u superuser -a
'member = administrator \n privilege = web "password" 15 '
```

Nota: O comando second deve estar em *uma* linha.

Substitua a *senha no* comando second com sua senha nova. **O $BASE** representa o diretório em que CSUnix é instalado.

Q. Como posso eu dizer que versões dos server do FastTrack, da administração do netscape, e do Netscape Communications do Acme estão no uso com Cisco seguro?

A. Cisco seguro usa uma versão modificada da versão de servidor 1.7 datado de novembro 13 do Acme, 1996.

A fim determinar as versões do servidor netscape, emita estes comandos (onde o **$BASE** representa o diretório em que CSUnix é instalado):

```
$BASEDIR/ns-home/admserv/ns-admin -v Netscape Communications Corporation Netscape-
Administrator/2.14,sec=e $BASEDIR/ns-home/bin/httpd/ns-httpd -v Netscape Communications
Corporation Netscape-FastTrack/2.01c
```

Bancos de dados

Q. Quantos usuários o requisito de espaço em disco 500 MB suporta usando uma base de dados de sqlanywhere?

A. O requisito de espaço em disco 500 MB suporta um máximo de 5,000 usuários.

Q. Quando o arquivo do *csdblog_yy-mm-dd* é criado?

A. O arquivo do ***csdblog_yy-mm-dd*** é criado a primeira vez que DBServer começa acima e regenerado então cada 24 horas (tempo aproximado).

Q. Que é o maior número de usuários que pode razoavelmente ser mantido em um servidor CSUnix com SQLAnywhere, servidor Oracle, ou servidor de sybase?

A. O SQLAnywhere é apoiado oficialmente para até 5,000 usuários. O Oracle e Sybase foram testados com até os milhão usuários, cada um com dez pares do valor de atributo (AV). Com este muitos usuários, manutenção são mais rápidos com as utilidades do comando line interface(cli) em vez da interface HTML ou do GUI avançado com base em Java. Note que consultar através do GUI pode ser muito lenta. Pode às vezes ser mais rápida usar a opção do **achado no** GUI avançado ou a opção do **editar > visualizar na** interface HTML.

Q. Como eu começo manualmente a base de dados de sqlanywhere?

A. Termine estas etapas a fim ligar manualmente o Engine de SQLAnywhere:

1. Ajuste os variáveis de ambiente necessários para o usuário de raiz. Neste exemplo, o c-shell é usado. Também, emita estes comandos:

```
setenv SQLANY $BASE/SYBSsa50 setenv LD_LIBRARY_PATH $SQLANY/lib set PATH=($path
$SQLANY/bin)
```

2. Emita este comando a fim começar o base de dados:
   dbeng50 -n csecure *$BASE/SQLANY*/**csecure.db** Substitua o *$BASE/SQLANY* com o lugar do arquivo de base de dados de sqlanywhere.

Q. Que valor eu preciso de ajustar para as conexões do servidor de bases de dados?

A. Na versão de CSUnix 2.3, o valor padrão é 10. As Conexões ao base de dados estão compartilhadas com outros aplicativos como utilidades do comando line interface(cli) e o GUI quando executam e alcançam o base de dados. Em regra geral, o número de Conexões ao base de dados precisa de igualar por segundo as autenticações máximas, mais pelo menos 3 para outras tarefas ACS, e aproximadamente 25 por cento para o crescimento.

Há outros fatores que precisam de ser considerados. Se você usa o CLI em linha, a seguir você precisa de adicionar o número de conexões CLI paralela que são usadas. Para cada conexão CLI paralela, adicionar uma Conexão ao base de dados adicional. Com CSUnix 2.3, a proteção explicando usa até oito Conexões ao base de dados quando permitida.

Nota: O número de Conexões ao base de dados é baseado em como CSUnix é usado. Use esta informação somente como uma diretriz.

Q. Há uma maneira que eu posso ver o base de dados usando o SQL?

A. Sim, você pode usar a interface com o usuário gráfica do SQLAnywhere (ISQL) ou o **comando ExecSql na** linha de comando. Refira a utilização do ISQL para ver o base de dados seguro de Cisco para detalhes adicionais. Este documento explica a estrutura do base de dados, dá um exemplo dos registros, ilustra consultas típicas, e mostra como executar as perguntas usando o ISQL ou usando o **comando ExecSql** através do comando line interface(cli). Igualmente discute os **comandos ViewProfile e DBClient**.

Q. Como eu replicate o base de dados usando o software de base de dados padrão (SQLAnywhere) que vem com CSUnix?

A. A replicação de base de dados com SQLAnywhere não é apoiada. Cisco apoia somente a replicação com servidor adaptável de sybase e Oracle 7.3.4 e mais atrasado.

Dois métodos usados para fazer uma cópia de uma base de dados de sqlanywhere são mostrados aqui.

- Os arquivos de base de dados de sqlanywhere (**csecure. db e** csecure.log**) podem** ser copiados de um server a outro depois que os serviços são fechados no servidor de origem e no servidor de destino. As permissões e a posse dos arquivos devem ser as mesmas no servidor de origem e no servidor de destino.
- **O comando dbbackup** pode ser emitido quando o servidor de origem for cria até arquivos de backup de base de dados (**csecure. db e** csecure.log**).** Estes arquivos podem então ser copiados ao servidor de destino depois que os serviços no servidor de destino são fechados. As permissões e a posse dos arquivos devem ser as mesmas no servidor de origem e no servidor de destino.

Q. Como eu suporto a base de dados de sqlanywhere usando o comando dbbackup quando CSUnix for executado?

A. Termine estas etapas a fim emitir o **comando dbbackup** suportar a base de dados de sqlanywhere quando CSUnix ainda for executado.

Nota: Este procedimento supõe que você usa o c-shell. Se você usa um shell diferente, o **comando env** permite que você certifique-se dos variáveis de ambiente estejam ajustados como mostrado aqui.

1. Emita estes comandos a fim ajustar os variáveis de ambiente:
   `setenv SQLANY $BASE/SYBSsa50 setenv LD_LIBRARY_PATH $SQLANY/lib set path=($path $SQLANY/bin) setenv SATMP $SQLANY/tmp`
2. Emita este comando a fim executar o utilitário dbbackup:
   `dbbackup -c "ENG=csecure; UID=DBA; PWD=SQL" -x` *`target_directory`* Substitua *target_directory* com o lugar onde você quer o csecure. db e os backup de csecure.log a ser salvar.

Q. Posso eu ter servidores principal e de backup CSUnix de modo que os dispositivos possam conectar ao servidor de backup se o servidor primário está para baixo?

A. Sim, esta conexão de failover a um servidor de backup é determinada a nível do dispositivo. A maioria de dispositivos Cisco permitem o Failover quando o servidor CSUnix preliminar é não disponível. Para o Roteadores, as entradas do **host do TACACS-server** ou do **host de servidor RADIUS** são configuradas com o nome ou os endereços IP de Um ou Mais Servidores Cisco ICM NT dos vários server. A informação sobre o usuário deve estar disponível aos vários server no caso de um Failover.

Q. Posso eu estabelecer CSUnix em um ambiente distribuído, com toda a administração feita em uma instalação central e no base de dados distribuídos aos servidores csunix locais?

A. Sim, você pode estabelecer um ambiente distribuído com CSUnix usando bases de dados de Oracle e Sybase.

Q. Como faz a interface csunix com o base de dados? Permite a criação de conta dinâmica que pode então ser adicionada à base de dados csunix?

A. CSUnix fornece um comando line interface(cli) e um GUI usados para controlar usuários e grupos. Use o CLI ou o GUI para alcançar o base de dados para controlar perfis, um pouco do que de acesso direto ao base de dados com o SQL.

Q. Eu tenho atualmente um tipo de base de dados em Cisco seguro, e eu quero migrar dados do usuário ou do grupo a um tipo de base de dados diferente (por exemplo, Oracle a Sybase, SQLAnywhere ao Oracle). Como eu faço este?

A. Termine estas etapas para exportar os usuários para um arquivo plano e para importá-los em CSUnix desse arquivo.

Nota: Antes da versão 2.3.6.1, este procedimento importa somente perfis TACACS+. Até à data da versão 2.3.6.1, este procedimento igualmente trabalha para perfis de RADIUS.

1. Emita este comando a fim exportar os usuários em um arquivo plano:
   $BASEDIR/utils/CSexport -p *file_path* **-d** *export_file_name* O $BASE representa o diretório em que CSUnix é instalado.
2. Emita estes comandos a fim importar os usuários deste arquivo plano:
   $BASEDIR/utils/CSimport -t -p *file_path* **-s** *import_file_name* *!--- Run CSimport in test mode.*
   $BASEDIR/utils/CSimport -c -p *file_path* **-s** *import_file_name* *!--- Commit the changes to the database.* Nestes comandos, o *export_file_name* é o nome de arquivo exportado, o *import_file_name* é o nome de arquivo importado, e o *file_path* é o diretório em que o arquivo é ficado situado.

Q. Como eu determino o número de usuários que existem no base de dados para cada servidor CSUnix? Que sintaxe de comando sql eu preciso de usar?

A. Emita este comando do diretório **$BASE/utils/bin** (onde o **$BASE** representa o diretório em que CSUnix é instalado):

```
$BASE/utils/bin/ ./ExecSql "select count(distinct profile_id) from cs_profile"
```

Este comando conta todo o usuário e perfis de grupo. Se você quer contar somente perfis de usuário, substitua **cs_profile** com o **cs_user_profile**.

Q. Que bases de dados ou clientes de base de dados são compatíveis com minha versão de CSUnix?

A. Para obter informações sobre da compatibilidade, refira às instruções da instalação para sua versão específica ou o sumário na compatibilidade UNIX do Cisco Secure ACS.

Q. Eu tenho uma base de dados existente (ou algum [RDBMS] do sistema de gerenciamento de base de dados relacional) não relacionada a Cisco seguro que contenha minha informação sobre o usuário. CSUnix fornece uma ferramenta de importação que possa permitir que eu importe esta informação sobre o usuário?

A. CSUnix não fornece uma ferramenta que você pode se usar para importar usuários de um base de dados NON-Cisco-seguro existente. Porque todos os bases de dados têm algum mecanismo para ver e alterar dados, a “informação sobre o usuário” pode ser extraída usando o SQL. A informação perguntada da base de dados existente pode ser recolhida em um arquivo plano e ser convertida a um formato de sintaxe de CSUnix que possa então ser importado em CSUnix com o **comando CSimport** (para o TACACS+) ou o **comando CSmigrate** (para o RAIO).

Administração de GUI e Web

Q. Eu sou incapaz de ver todas as opções no ACS GUI. Como eu corrijo este problema?

A. Gire sobre o agente remoto que registra abaixo **Interface Configuration > Advanced Options**. Verifique todas as opções que você precisa.

Q. Como eu alcanço o servidor administrativo de fasttrack do netscape?

A. O servidor administrativo fasttrack é alcançado geralmente com um navegador da Web. Use este procedimento:

1. Vá a esta URL: `http://server_name:64000` Substitua o *server_name* com o nome ou o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor administrativo fasttrack.
2. Incorpore seu nome de usuário e senha como mostrado aqui. `Username: admin Password: password`
3. Se a senha não trabalha, termine estas etapas a fim restaurá-la. Edite o arquivo **$BASE/ns-home/amdpw** (onde o **$BASE** representa o diretório em que CSUnix é instalado).Encontre esta linha no arquivo: `admin:GuBqifMleNxmY`Remova o texto da senha criptografada após os dois pontos e salvar o arquivo. Você pode agora entrar como o **admin** usando uma senha vazia.
4. Se você recebe um Mensagem de Erro do `host não autorizado`, termine estas etapas. Edite o **arquivo ns-admin.conf no diretório** $BASE/ns-home/admserv/**ou** $BASE/ns-home/admin-serv/(onde **$BASEREPRESENTS o** diretório em que CSUnix é instalado). **Nota:** Pode ser possível que um destes arquivos não está atual.Suprima dos **anfitriões** e **enderece** linhas no arquivo. **Cuidado:** Seja certo suprimir somente das linhas dos **endereços** (término no **es**). Não suprima nenhum término **es**) da linha do **endereço** (.Salve o arquivo.Reinicie o servidor de administração emitindo o **comando stop-admin** e então o **comando start-admin no** diretório **$BASE/ns-home/**.

Q. Que navegadores são compatíveis com minha versão de CSUnix?

A. Para obter informações sobre da compatibilidade, refira às instruções da instalação para sua versão específica ou o sumário na compatibilidade UNIX do Cisco Secure ACS.

Servidores de tokens

Q. Posso eu adicionar o servidor de ACE do Security Dynamics Incorporated (SDI) depois que eu instalo CSUnix?

A. Sim, você pode permitir o servidor de ACE SDI com este procedimento.

Nota: Antes que você tente uma integração com CSUnix, é uma boa ideia fazer uma autenticação de teste do cliente de SDI a fim assegurar-se de que o SDI trabalhe por si só.

1. Feche CSUnix.
2. Adicionar estas linhas ao **arquivo do $BASE/config/CSU.cfg** (onde **$BASEREPRESENTS o** diretório em que CSUnix é instalado). `AUTHEN config_external_authen_symbols = {`
```
{
"./libsdi.so",
"sdi"
}
```
3. Reinicie CSUnix.

Você pode igualmente permitir o servidor de ACE SDI usando o GUI CSUnix, como mostrado aqui.

Nota: Antes que você tente uma integração com CSUnix, execute uma autenticação de teste do cliente de SDI para assegurar-se de que o SDI trabalhe por si só.

1. No menu GUI, escolha **AAA > general**.
2. Na área dos **métodos de autenticação do** tab geral, clique o botão de rádio **dinâmico seguro (do servidor de ACE)**.

Para mais informação, refira configurar Cisco UNIX seguro e Secure ID (cliente de SDI).

Q. Posso eu instalar um servidor de ACE e um CSUnix do Security Dynamics Incorporated (SDI) na mesma máquina?

A. Sim, se o TACACS+ e o RAIO são desabilitados no servidor de ACE SDI. Os erros podem ocorrer se o servidor de ACE SDI e o TACACS+ ou o RAIO são executado ao mesmo tempo. Isto é porque o servidor de ACE SDI pode usar os mesmos Protocolos de autenticação nas mesmas portas.

Q. Posso eu usar a autenticação do protocolo de autenticação de cumprimento do desafio (RACHADURA) com um servidor de ACE do Security Dynamics Incorporated (SDI)?

A. Sim, mas a senha é entrado de uma forma diferente. Para mais informação, refira configurar Cisco UNIX seguro e Secure ID (cliente de SDI).

Q. Que são cache de token e como mim o permitem?

A. Com autenticação token-baseada, os tokens são frequentemente bons por somente um período limitado de tempo e não podem ser reutilizados dentro desse período de tempo. Estas limitações podem causar problemas para o ISDN ou os usuários multilink. A autenticação do token inicial é bem sucedida, mas as reautenticações subsequentes podem falhar porque a interface do utilizador não permite que os usuários entrem tokens adicionais.

Quando o cache de token é usado, os pedidos da reautenticação estão enviados ainda a CSUnix. Então CSUnix envia para trás uma PASSAGEM se as condições da sessão ou do intervalo são estadas conformes.

Termine estas etapas a fim usar o cache de token.

1. Pôr em esconderijo do token deve ser permitido no usuário ou no perfil de grupo adicionando esta linha: `set server token-caching=enable`
2. Emita este comando a fim ajustar a circunstância ou as circunstâncias sob que a senha expira e consequentemente quanto tempo a senha permanece válida.
   `set server token-caching-expire-method= [session | timeout | both]` **a sessão** mantém a senha em cache válida para a duração da sessão original.**o intervalo** mantém a senha em cache válida para a quantidade de tempo especificada.**ambos** mantêm a senha em cache válida para a sessão e para uma quantidade de tempo especificada.
3. Se o **intervalo** ou **ambos** foram escolhidos em etapa 2, use este comando ajustar a quantidade de tempo durante que a senha permanece válida.
   `set server token-caching-timeout=120`

Q. A funcionalidade oferecida pelo CRYPTOAdmin substitui o apoio para CRYPTOCards que é incorporado em nossos produtos csunix? Como diferem?

A. O servidor de Placa CRYPTO empacotado com CSUnix fornece somente o suporte de placa de token, visto que o CRYPTOAdmin é uma ferramenta de gerenciamento fácil de usar usada para estabelecer tokens e usuários. O CRYPTOAdmin trabalha com CSUnix e fornece um cliente GUI que não venha empacotado com CSUnix. CSUnix contém o conjunto de ferramentas de CRYPTOCard. Consequentemente, o CRYPTOAdmin complementa eficazmente CSUnix. Refira o site de CRYPTOCard para obter mais informações sobre do CRYPTOAdmin.

Perfis e senhas de usuário

Q. Como eu adiciono perfis de usuário para o TACACS+ em ACS (UNIX)?

A. A fim adicionar este tipo de perfil através do **comando AddProfile**, o cliente pode usar o **AddProfile -** [-s [Filename] da opção **s**]. Os atributos podem ser postos em um arquivo e podem adicionar o usuário como considerado aqui.

```
*$BASEDIR/CLI* ./AddProfile -p 9900 -u userA -s script
```

Estes atributos são postos no arquivo de script.

```
*$BASEDIR/CL>* *vi script*

password = clear "userA"
default service=permit
service=Sandvine {
set Sandvine-HomeDir = "/tmp"
set Sandvine-Group = "sv_operator,sv_admin"
set Sandvine-Shell = "/bin/sh"
}
```

`O $BASEDIR` é o diretório onde Cisco se fixa é instalado.

Q. Que o mínimo e o número máximo de caráteres é permitido em uma senha em CSUnix?

A. Os bases de dados armazena senha até 255 caráteres. A interface GUI reforça o mínimo e o máximo. Para mais informação, refira a opção de **ajuda no** GUI CSUnix. Isto descreve as regras da senha.

Q. CSUnix permite que eu mude minha senha?

A. Sim, você pode mudar a sua senha com o início de uma sessão terminal (do shell) ou com o GUI CSUnix. A fim mudar a sua senha com o início de uma sessão terminal (do shell), termine estas etapas.

Nota: Este procedimento muda somente sua senha de texto sem formatação.

1. Use o **comando telnet** alcançar o roteador.
2. Quando alertado, dê entrada com seu nome de usuário atribuído.
3. Quando pedido a sua senha, deixe-a vazia e pressione-a **entram**. `A sequência de senha da mudança da` mensagem aparece.

4. Incorpore sua senha antiga, a seguir siga as alertas para incorporar e confirmar sua senha nova.

A fim mudar a sua senha usando o GUI CSUnix (interface HTML), termine estas etapas.

Nota: Este procedimento muda automaticamente *todas* suas senhas atribuídas. Não há nenhuma maneira de mudar somente algumas das suas senhas.

1. Adicionar esta linha a seu perfil de usuário: `privilege = web "new_password" 1` Substitua o *new_password* com a senha nova que você gostaria de usar.
2. Em um navegador da Web, vá a este lugar: `http://host_name/cs` Substitua o *host_name* com o nome ou o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor CSUnix.
3. Entre com seu nome de usuário atribuído e a senha usada em etapa 1.

Q. Faz o envelhecimento da senha de suporte csunix?

A. Sim, mas somente através da interface Telnet. Verifique estes artigos:

- O perfil de usuário tem **até que** data ajustada para a senha.
- **O arquivo CLI.cfg** tem as linhas que definem estes valores:`config_warning_period x` `config_expiry_period y`

Se todos estes artigos são verdadeiros, a seguir o usuário recebe um mensagem de expiração com os dias do telnet *x* antes do **até a** data. Quando o usuário começar a sequência da mudança da senha deixando sua placa da senha e pressionando **para entrar**, **até que a** data estiver incrementada em dias *y*. Um perfil de usuário da amostra é mostrado nesta saída, com uma explicação resumida.

```
> ./ViewProfile -p 9900 -u abcde123 !--- In this example, abcde123 is used in place of an actual user name. User Profile Information user = abcde123{ profile_id = 21 profile_cycle = 1 password = clear "********" until "8 Aug 2001" }
```

Neste exemplo, se o **arquivo csu.cfg** tem as linhas **config_warning_period 5 e o config_expiry_period 30, a seguir o** usuário nomeado "abcde123" começa receber avisos do telnet da expiração de senha o 3 de agosto (cinco dias antes do 8 de agosto). Se o usuário muda a senha na interface Telnet o 6 de agosto, o untildate no perfil está restaurado para 30 dias mais tarde. Isto conduz a uma data de expiração nova do 5 de setembro.

Q. Há um atributo que expire um usuário após um número especificado de dias de inatividade em uma conta?

A. O envelhecimento de senha é a opção a mais próxima. Veja a pergunta do envelhecimento de senha neste documento para mais detalhes. Se um usuário não entra na data em que a senha expira, a seguir a conta expira.

Nota: Porque o alteracão da senha não é apoiado usando o PPP, este significa que a expiração de usuários trabalha somente para o início de uma sessão do modo terminal.

Q. CSUnix reforça alguma limitação nas escolhas da senha? Ou seja recusa “senhas fáceis” ou “crackable”?

A. Não CSUnix não reforça nenhuma políticas de restrição de senha, incluindo verificando um dicionário ou recordando umas senhas mais velhas. O principal restrição é que as senhas devem

estar a um comprimento mínimo de seis caráteres alfanuméricos a fim para ser aceitado. Os únicos caracteres válidos de senhas são as letras alfabéticas (à Z e a com z) e numerais (0 com 9). Refira o Guia do Usuário para obter mais informações sobre das restrições de senha.

Q. Se um perfil de usuário é “fechado,” como posso eu destravar o perfil da linha de comando?

A. Termine estas etapas a fim emitir o **comando DBClient** destravar manualmente um perfil:

1. Emita este comando na linha de comando:
   `$BASEDIR/DBClient/DBClient -p 9900` O $BASE representa o diretório em que CSUnix é instalado.
2. Incorpore estes valores quando você é alertado. `username: admin_name !--- Enter your administrator user name in place of admin_name. password: admin_password !--- Enter the administrator password in place of admin_password.`
3. O tipo **destrava** e pressiona **entra**.
4. Datilografe o *user_name do* **user =**. Substitua o *user_name* com o nome do perfil de usuário que você quer destravar.
5. A imprensa **entra** duas vezes.
6. Datilografe a **saída** e pressione-a **entram** para fechar a janela de prompt de comando.

Relatório

Q. CSUnix fornece relatórios de USO de cliente por usuário?

A. CSUnix não fornece tais relatórios, mas esta informação pode ser extraída do base de dados. A informação de contabilidade da maneira prevista pelo servidor do acesso de rede (NAS) é armazenada e pode ser extraída em um arquivo de texto usando o **utilitário AcctExport**. Uma vez que a informação de conta é extraída do base de dados, um script pode ser criado para analisar gramaticalmente os dados e para gerar o relatório necessário do usuário per. Quando você emite o **comando AcctExport target**, remove os registros de contabilidade do base de dados e coloca-os no *alvo*.

Q. Que acontece se CSUnix gerencie registros de contabilidade novos quando o comando AcctExport for executado?

A. Os novos registros não são afetados desde que o **comando AcctExport** recolhe os números de ID máximos nas tabelas antes que comece sua operação da exportação.

Q. Como eu sei mesmo se o comando AcctExport é bem sucedido?

A. Se você emite o **comando AcctExport dos** dados da linha de comando, retornam a mensagem `feita com sucesso`. Se você alcança o **comando AcctExport de um** programa, um código de saída de `0` indica o sucesso, quando um código de saída de `1` indicar a falha.

Q. Se a contabilidade do comando enable I, faz CSUnix gravam o comando exato inscrito no roteador? Por exemplo, grava um comando específico como a rota 135.52.0.0 255.255.0.0 1.1.1.1 IP?

A. Quando você emite o **comando aaa accounting command 15 start-stop tacacs+ no** roteador, a sintaxe cheia dos comandos está gravada no servidor AAA. Esta informação pode ser recuperada do base de dados com o **comando AcctExport**.

Alguns registros do exemplo dos comandos de contabilidade são mostrados aqui.

```
lab-i52.cisco.com dphillip tty18 170.69.200.7 start server=ciscosecure-sun
     time=10:09:56 date=05/19/97 task_id=74service=shell

lab-i52.cisco.com dphillip tty18 170.69.200.7 stop server=ciscosecure-sun
     time=10:09:58 date=05/19/97 task_id=75 service=shell
     priv-lvl=15 cmd=configure terminal <cr>

lab-i52.cisco.com dphillip tty18 170.69.200.7 stop server=ciscosecure-sun
     time=10:10:03 date=05/19/97 task_id=76 service=shell
     priv-lvl=15 cmd=ip route 1.1.1.1 255.255.255.255 Serial 0 <cr>
```

Q. O CallerID é capturado na contabilidade?

A. Sim, o CallerID é armazenado no campo do **rem_addr**. Pode conter o Calling Line Identification (CLID) e o Dialed Number Information Service (DNIS), que são separados por uma barra (/).

Erros e depuração

Q. Como eu corrijo o erro **filtrado "acesso de usuário"**?

A. Desabilite as limitações do acesso de rede (NAR) ou configurar-las completamente para o uso.

Q. Como eu determino o que o tipo de mensagem **"Authen falhou"** significa?

A. Note a data e hora da mensagem, vá ao arquivo de registro do csauth, e à busca na data e hora. Mais explicação detalhada da mensagem é apresentada então.

Q. Quando o CSUnix instalar no núcleo 8 de Solaris, gerencie erros. Por que isso ocorre?

A. Verifique que os arquivos de pacote não faltam do núcleo instalam:

```
/usr/lib/libX11.so.4, a symlink pointing to /usr/openwin/lib/libX11.s0.4
/usr/lib/libXext.so.0, a symlink pointing to /usr/openwin/lib/libXext.so.0
/usr/ucblib/libucb.so.1
```

Q. CSUnix recebe **ERRO do** mensagem do syslog **'- incapaz de obter o nome de NAS 134.'** O que faz este meio?

A. Se há um server satisfeito do interruptor envolvido, vá-lhe e remova-o os `tacacs do` server. Adicionar `tacacs que a frequência 0` adiciona então `tacacs` de volta a esse server. Isto é similar a um ataque e um destes resolve esta edição.

Emita estes comandos a fim desabilitar manutenções de atividade de TACACS no servidor CSS:

```
CSS(config)# no tacacs-server 10.152.4.24 49 CSS(config)# tacacs-server frequency 0 CSS(config)#
tacacs-server 10.152.4.24 49 primary
```

Q. Quando eu debugo em meu roteador, eu recebo um Mensagem de Erro `truncado "protocolo"`. O que isso significa?

A. Você provavelmente não tem uma chave de licença válida no **arquivo csu.cfg**. Sem a chave, quando CSUnix alcança quatro portas, escreve um erro ao **arquivo** $BASE/logfiles/cs_startup.log (onde **$BASEREPRESENTS o** diretório em que CSUnix é instalado). Envia então um Licensednumber da `mensagem excedida portas ao` roteador. O roteador interpreta esta mensagem como protocolgarbled. `Para mais detalhes` ao licenciar, refira LicensingIssues para Cisco UNIX seguro.

Q. Que eu preciso de fazer se eu recebo uma mensagem do `"erro de segurança"` quando eu conecto ao GUI avançado?

A. Edite o **arquivo $BASE/config/CSConfig.ini** (onde **$BASEREPRESENTS o** diretório em que CSUnix é instalado), e mude a linha ValidateClients **= retificam às** ValidateClients **= falso. Recicle os** serviços de modo que a mudança tome o efeito. Este ajuste diz CSUnix para não verificar o endereço IP de Um ou Mais Servidores Cisco ICM NT do administrador recebido.

Se há uma necessidade de verificar endereços IP de Um ou Mais Servidores Cisco ICM NT, deixar as **ValidateClients =** linha **verdadeira** inalterada e de incluir as linhas no arquivo que são similares a esta saída:

```
[Valid Clients]
100=chicago.cisco.com
102=1.2.3.4
```

Q. Que eu preciso de fazer se eu recebo `"um` Mensagem de Erro de `arquivos em aberto demais no` log de startup?

A. Estes Mensagens de Erro indicam que há demasiado poucos descritores de arquivo de Solaris disponíveis.

```
Jan 21 19:44:54 secs1 : (Too many open files)
Jan 21 19:53:17 secs1 CiscoSecure: ERROR - error on accept: (Too many open files)
```

A fim corrigir e impedir estes erros, altere arquivos de configuração de CSUnix segundo as indicações destas etapas.

1. Aumente o valor do **ulimit a 4096 no arquivo $BASE/bin/DBServer.sh** (onde **$BASEREPRESENTS o** diretório em que CSUnix é instalado), como mostrado aqui. `ulimit -n 4096`
2. Aumente o valor do **ulimit ao 256 no arquivo $BASE/bin/AcmeServer.sh**, como mostrado aqui. `ulimit -n 256`
3. Ajuste o valor do **ulimit a ilimitado no** arquivo de **/etc/rc2.d/S80CiscoSecure**, como mostrado aqui. `ulimit -n unlimited`

Q. Que eu preciso de fazer se eu não posso começar CSUnix e eu ver do "uma mensagem da `falha seminit (libsec .8187)" no` arquivo de cs_startup.log?

A. Verifique as permissões no diretório de **/tmp**. Devem ser ajustados para ler, escrever, e executar (**rwx**) para usuários, grupos, e outro. A saída do **ls -** comando **ld /tmp** retorna algo similar a este:

```
drwxrwxrwt 6 sys sys 317 Jul 8 12:00 /tmp
```

Nota: A mensagem da `falha do seminit (libsec .8187)` é um Mensagem de Erro de Netscape.

Q. O que fazem mim precise de fazer se eu tento usar CSUnix e eu recebo um "TAC+: Dados incorretos recebidos Mensagem de Erro do server"?

A. Isto significa que há ou uma incompatibilidade de chave entre o servidor do acesso de rede (NAS) e CSUnix ou lá é um problema com o Domain Name System (DNS) ou o serviço de informação de rede (NIS).

A fim testar sua configuração, substitua o endereço IP de Um ou Mais Servidores Cisco ICM NT NAS ou o nome com as aspas duplas vazias (**""**) no **arquivo csu.cfg**. Esta substituição permite CSUnix de comunicar-se com todo o cliente com uma chave correta. Um exemplo das linhas no CSU.cfgfile antes e depois da substituição é mostrado aqui.

- Antes:
```
NAS config_nas_config = {
{
"192.91.124.172", /* NAS name can go here */
```
- Em seguida:
```
NAS config_nas_config = {
{
"", /* NAS name can go here */
```

Igualmente tentativa para desabilitar o DNS no **arquivo csu.cfg** adicionando esta linha à seção do começo com o outro NUMBERENTRIES:

```
NUMBER config_get_dns_names = 0
```

Refira o Guia do Usuário para mais detalhes.

Q. Que eu preciso de fazer se o console do servidor seguro Cisco é inundado com "não pode encontrar o Mensagem de Erro do perfil de servidor"?

A. Este Mensagem de Erro é geralmente cosmético e é provável ocorrer quando o base de dados é copiado de um server a outro. Se há um perfil de servidor no servidor de origem mas nenhum perfil de servidor no servidor de destino, esta mensagem está gerada.

A fim impedir este erro, você pode adicionar o perfil para o servidor CSUnix próprio no GUI avançado. Ou, se você não usa o RAIO, você pode desabilitar o RAIO com este procedimento:

1. Backup o arquivo de **/etc/rc2.d/S80CiscoSecure**.
2. Edite o arquivo de **/etc/rc2.d/S80CiscoSecure** introduzindo **- R na** linha mostrada aqui.`cd $BASE/CSU; $BASE/CSU/CiscoSecure -R -f $BASE/config/CSU.cfg >>$BASE/logfiles/cs_startup.log 2>&1`
3. Reinicie os serviços CSUnix.

Q. Como eu obtenho a informação sobre logging de protocolo e o mais debugging detalhado para baixo ao byte-nível? Eu já mudei o valor do "config_logging_configuration" no arquivo csu.cfg, mas eu ainda não obtenho o registro do protocolo.

A. O protocolo debuga a informação não é enviado ao Syslog. Em lugar de, esta informação é redigida ao erro padrão. Na configuração normal, o servidor CSUnix fecha o descritor de arquivo de erros padrão, que causa o protocolo debuga para obter jogado no bucket de bit.

A fim ver o nível de protocolo debuga, você precisam de ligar o servidor CSUnix com **- c - as** opções de linha de comando **x**. Isto faz com que o servidor AAA seja executado no primeiro plano e mantém sua saída padrão e os descritores de arquivo de erros padrão abrem. Você vê então que o protocolo debuga no console. Estes debugam podem igualmente ser capturados a um arquivo usando a reorientação do erro padrão de UNIX.

Q. Como eu encontro o número de arquivos que um processo tem aberto?

A. Emita este comando na linha de comando:

/usr/proc/bin/pfiles *process_ID*

Substitua o *process_id* com o número de ID do processo.

Informações Relacionadas

- Cisco Secure ACS para página de suporte do UNIX
- Suporte Técnico e Documentação - Cisco Systems