Configurando o CSU para UNIX (Solaris)

Índice

Introdução

O Cisco Secure ACS para o software de UNIX (CSU) ajuda a assegurar a Segurança da rede e segue a atividade dos povos que conectam com sucesso à rede. O CSU atua como um TACACS+ ou um servidor Radius e usa o Authentication, Authorization, and Accounting (AAA) para fornecer a segurança de rede.

O CSU apoia estas opções de base de dados armazenar o grupo e os perfis de usuário e a informação de contabilidade:

- SQLAnywhere (incluído com CSU).Esta versão do SQLAnywhere de Sybase não tem o cliente/suporte de servidor. Contudo, é aperfeiçoada para executar serviços essenciais AAA com o CSU.**Cuidado:** A opção da base de dados de sqlanywhere não apoia os bases de dados do perfil que excedem 5,000 usuários, replicação da informação do perfil entre locais do base de dados, ou a característica segura do Distribute Session Manager de Cisco (DSM).
- Oracle ou Sybase Relational Database Management System (RDBMS).Para apoiar bases de dados seguros do perfil de Cisco de 5,000 ou mais usuários, replicação de base de dados, ou a característica segura de Cisco DSM, você deve instalar um Oracle (versão 7.3.2, 7.3.3, ou 8.0.3) ou o servidor SQL de Sybase (versão 11) RDBMS para guardar sua informação do perfil segura de Cisco. A replicação de base de dados exige uma configuração do RDBMS

mais adicional depois que a instalação segura de Cisco está completa.
- A elevação de uma base de dados existente de uma versão (2.x) precedente do CSU.Se você promove de uma versão 2.x mais adiantada de Cisco segura, o programa de instalação seguro de Cisco promove automaticamente o base de dados do perfil para ser compatível com CSU 2.3 para UNIX.
- Importando um base de dados existente do perfil.Você pode converter o freeware existente TACACS+ ou os bases de dados ou os arquivos planos do perfil de RADIUS para o uso com esta versão do CSU.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no Cisco Secure ACS 2.3 para UNIX.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configuração CSU

Use estes procedimentos para configurar o CSU.

Comece a interface de administrador ciscosecure

Use este procedimento para entrar ao administrador seguro de Cisco.

1. De toda a estação de trabalho com uma conexão da Web ao ACS, lance seu navegador da Web.
2. Incorpore uma destas URL para a site da web de administrador segura de Cisco:Se a característica do Security Socket Layer em seu navegador não é permitida, entre:`http://your_server/cs`onde o your_server é o nome de host (ou o nome de domínio totalmente qualificado (FQDN), se o nome de host e o FQDN diferem) da SPARCstation onde você instalou o CSU. Você pode igualmente substituir o endereço IP de Um ou Mais Servidores Cisco ICM NT da SPARCstation para o your_server.Se a característica do Security Socket Layer em seu navegador é permitida, especifique “https” um pouco do que o “HTTP” como o protocolo de transmissão do hypertext. Entre:`https://your_server/cs`onde o

your_server é o nome de host (ou o FQDN, se o nome de host e o FQDN diferem) da SPARCstation onde você instalou o CSU. Você pode igualmente substituir o endereço IP de Um ou Mais Servidores Cisco ICM NT da SPARCstation para o your_server.**Nota:** As URL e os nomes do servidor são diferenciando maiúsculas e minúsculas. Devem ser datilografados com uppercase e letras minúsculas exatamente como mostrado.A página do fazer logon CSU é indicada.

3. Insira seu nome de usuário e senha. Clique em Submit.**Nota:** O nome de usuário padrão inicial é “superuser.” A senha padrão inicial é “changeme.” Após seu login inicial, você precisa de mudar imediatamente o nome de usuário e senha para a segurança máxima.Depois que você entra, a página principal CSU está indicada com a barra de menu principal ao longo da parte superior. A página principal de menu CSU é indicada somente se o usuário fornece um nome e uma senha que tenham privilégios do administrador-nível. Se o usuário fornece um nome e uma senha que tenham somente privilégios do nível de usuário, a seguir uma tela diferente é indicada.

Comece o programa de configuração avançada

Comece o programa de configuração avançada seguro com base em Java do administrador de Cisco de alguns dos página da web do administrador CSU. Da barra de menus da interface da WEB CSU, clique **avançado**, e clique-o então **avançado** outra vez.

O programa de configuração avançada seguro do administrador de Cisco é indicado. Pôde possivelmente tomar alguns minutos para carregar.

Crie um perfil de grupo

Use o programa de configuração avançada seguro do administrador de Cisco para criar e configurar perfis de grupo. Cisco recomenda que você cria perfis de grupo para configurar exigências detalhadas AAA para um grande número usuários similares. Depois que o perfil de grupo é definido, use o CSU adicionam um página da web do usuário para adicionar rapidamente perfis de usuário ao perfil de grupo. Os requisitos avançados configurados para o grupo aplicam-se a cada usuário do membro.

Use este procedimento para criar um perfil de grupo.

1. No programa de configuração avançada seguro do administrador de Cisco, selecione a aba dos **membros**. No painel de navegação, de-seleto a caixa de verificação da **consultação**. Os indicadores novos do ícone do perfil da criação.
2. No painel de navegação, faça um destes:Para criar um perfil de grupo sem o pai, encontre e clique o ícone de pasta do [Root].Para criar seu perfil de grupo como a criança de um outro perfil de grupo, encontre o grupo que você quer como o pai e clica o.Se o grupo que você quer ser o pai é um grupo filho, clique seu dobrador de grupo de pai para indicá-lo.
3. O clique **cria o perfil novo**. Os indicadores novos da caixa de diálogo do perfil.
4. Selecione a caixa de **verificação de atributo**, datilografe o nome do grupo que você quer criar, e clique a **APROVAÇÃO**. Os indicadores novos do grupo na árvore.
5. Depois que você cria o perfil de grupo, atribua o TACACS+ ou os atributos RADIUS para configurar propriedades de AAA específicas.

Crie um perfil de usuário no modo da configuração avançada

Use o modo de configuração avançada do Cisco secure administrator para criar e configurar um perfil de usuário. Você pode fazer este para personalizar com maiores detalhes a autorização e os atributos contabilidade-relacionados do perfil de usuário do que é possível com adicionar um a página de usuário.

Use este procedimento para criar um perfil de usuário:

1. No programa de configuração avançada seguro do administrador de Cisco, selecione a aba dos **membros**. No painel de navegação, localize e de-seleto **consulte**. Os indicadores novos do ícone do perfil da criação.
2. No painel de navegação, faça um destes:Encontre e clique o grupo a que o usuário pertence.Se você não quer o usuário pertencer a um grupo, clique o ícone de pasta do [Root].
3. O clique **cria o perfil**. Os indicadores novos da caixa de diálogo do perfil.
4. Certifique-se de que a caixa de **verificação de atributo de-**está selecionada.
5. Dê entrada com o nome do usuário que você quer criar e clicar a **APROVAÇÃO**. Os indicadores do novo usuário na árvore.
6. Depois que você cria o perfil de usuário, atribua o TACACS+ específico ou os atributos RADIUS para configurar propriedades de AAA específicas:Para atribuir perfis TACACS+ ao perfil de usuário, veja para atribuir atributos TACACS+ a um perfil de grupo ou usuário.Para atribuir perfis de RADIUS ao perfil de usuário, veja para atribuir atributos RADIUS a um perfil de grupo ou usuário.

Estratégias para aplicar atributos

Use a característica do perfil de grupo CSU e o TACACS+ e os atributos RADIUS para executar a authentication e autorização dos usuários de rede com o CSU.

Planeie atributos para grupos e usuários

A característica do perfil de grupo do CSU permite-o de definir o conjunto comum de requisitos de AAA para um grande número usuários.

Você pode atribuir um grupo de TACACS+ ou valores de atributo RADIUS a um perfil de grupo. Estes valores de atributo atribuídos ao grupo aplicam-se a todo o usuário que são um membro ou que for adicionado como um membro desse grupo.

Use a característica do perfil de grupo eficazmente

Para configurar o CSU para controlar números grandes e vários tipos de usuários com requisitos complexos do AAA, Cisco recomenda que você usa as características do programa de configuração avançada seguro do administrador de Cisco para criar e configurar perfis de grupo.

O perfil de grupo precisa de conter todos os atributos que não são específicos ao usuário. Isto significa geralmente todos os atributos à exceção da senha. Você pode então usar adicionar uma página de usuário do administrador seguro de Cisco para criar perfis de usuário simples com os atributos da senha e para atribuir estes perfis de usuário ao perfil de grupo apropriado. As características e os valores de atributo definidos para um grupo particular aplicam-se então a seus usuários do membro.

Grupos e grupos filho de pai

Você pode criar uma hierarquia dos grupos. Dentro de um perfil de grupo, você pode criar perfis de grupo-filho. Os valores de atributo atribuídos ao perfil de grupo do pai são valores padrão para os perfis de grupo-filho.

A administração do nível de grupo

Um administrador de sistema seguro de Cisco pode atribuir a Cisco individual o estado seguro do administrador do grupo de usuários. O estado do administrador do grupo permitem usuários individuais de administrar todos os perfis de grupo-filho e os perfis de usuário que são subordinados a seu grupo. Contudo, não permitem que administrem nenhuns grupos ou os usuários que caem fora da hierarquia do seu grupo. Assim, o administrador de sistema parcela para fora a tarefa de administrar uma rede grande a outros indivíduos sem conceder a cada um deles a autoridade igual.

Que atributos eu defino para usuários individuais?

Cisco recomenda que você atribui a usuários individuais os valores de atributo da autenticação básica que são originais ao usuário, tal como os atributos que definem o username, a senha, o tipo de senha, e o privilégio da Web. Atribua valores de atributo da autenticação básica a seus usuários com o Edit a User do CSU ou adicionar páginas de usuário.

Que atributos eu defino para perfis de grupo?

Cisco recomenda que você define a qualificação, a autorização, e atributos contabilidade-relacionados a nível do grupo.

Neste exemplo, o perfil de grupo nomeado “usuários de discagem de entrada” é atribuído os pares de valor de atributo Frame-Protocol=PPP e Service-Type=Framed.

Que são atributos absolutos?

Um subconjunto do TACACS+ e os atributos RADIUS no CSU podem ser atribuídos o status absoluto a nível do perfil de grupo. Um valor de atributo permitido para o status absoluto a nível do perfil de grupo cancela todos os valores do atributo de contenção a nível de perfil de usuário do perfil de grupo-filho ou do membro.

Dentro das redes do multi-nível com diversos níveis de administradores do grupo, os atributos absolutos permitem um administrador de sistema de ajustar os valores de atributo de grupo selecionados que agrupam administradores em níveis inferiores não podem cancelar.

Atributos que podem ser atribuídos a indicador de status absoluto uma caixa de verificação absoluta na caixa dos atributos do programa de configuração avançada seguro do administrador de Cisco. Selecione a caixa de verificação para permitir o status absoluto.

Podem os valores de atributo de grupo e os valores de atributo de usuário opor?

A resolução de conflito entre os valores de atributo atribuídos para parent perfis de grupo, perfis de grupo-filho, e perfis de usuário do membro depende sobre se os valores de atributo são

absolutos e se são TACACS+ ou atributos RADIUS:

- TACACS+ ou valores de atributo RADIUS atribuídos a um perfil de grupo com ultrapassagem do status absoluto alguns valores do atributo de contenção ajustados a grupo filho ou nível de perfil de usuário.
- Se o status absoluto de um valor de atributo TACACS+ não é permitido a nível do perfil de grupo, está cancelado por todo o valor do atributo de contenção ajustado a grupo filho ou nível de perfil de usuário.
- Se um status absoluto de valor de atributo RADIUS não é permitido a nível do grupo do pai, a seguir todos os valores do atributo de contenção ajustam-se em um resultado do grupo filho em um resultado imprevisível. Quando você define valores de atributo RADIUS para um grupo e seus usuários do membro, evite atribuir o mesmo atributo ao usuário e aos perfis de grupo.

Use a opção de proibição e permissão

Para o TACACS+, cancele a Disponibilidade de valores herdados do serviço prefixando a palavra-chave **proibem** ou **permitem à** especificação do serviço. A palavra-chave da **licença** permite serviços especificados. A palavra-chave da **proibição** recusa serviços especificados. Com o uso destas palavras-chaves junto, você pode construir “tudo exceto” configurações. Por exemplo, esta configuração permite o acesso de todos os serviços exceto o X.25:

```
default service = permit
prohibit service = x25
```

Atribua atributos TACACS+ a um perfil de grupo ou usuário

Para atribuir serviços específicos e atributos TACACS+ a um perfil de grupo ou usuário, siga estas etapas:

1. No programa de configuração avançada seguro do administrador de Cisco, selecione a aba dos **membros**. No painel de navegação, clique o ícone para o perfil de grupo ou usuário a que os atributos TACACS+ são atribuídos.
2. Caso necessário, na placa do perfil, clique o ícone do **perfil** para expandi-lo.Uma lista ou uma caixa de diálogo que contenham os atributos aplicáveis ao perfil ou ao serviço selecionado indicam no indicador no direita inferior da tela. A informação neste indicador muda baseado em que perfil ou lhe preste serviços de manutenção selecionam na placa do perfil.
3. Clique o serviço ou o protocolo que você quer adicionar e o clique **aplicam-se**. O serviço é adicionado ao perfil.
4. Incorpore ou selecione o texto necessário no indicador do atributo.As entradas válidas são explicadas nas estratégias para aplicar a seção dos atributos do CSU 2.3 para o guia de referência UNIX.**Nota:** Se você atribui um valor de atributo a nível do perfil de grupo, e o atributo que você especifica indicadores uma **caixa de verificação absoluta**, selecione essa caixa de verificação para atribuir o status absoluto do valor. Um status absoluto de valor atribuído não pode ser cancelado por nenhuns valores de afirmação atribuída a perfil de grupo subordinado ou níveis de perfil de usuário.
5. Repita etapas 1 completamente para cada serviço adicional ou protocolo que você precisa de adicionar.
6. Quando todas as mudanças são feitas, o clique **submete-se**.

Atribua atributos RADIUS a um perfil de grupo ou usuário

Para atribuir atributos RADIUS específicos a um perfil de grupo ou usuário:

1. Atribua um dicionário radius ao perfil de grupo:Na página dos membros do programa de configuração avançada seguro do administrador de Cisco, clique o ícone do **grupo** ou do **usuário**, a seguir clique o ícone do **perfil na** placa dos perfis. Na placa dos atributos, os indicadores do menu de opções.**No menu de opções**, clique o nome do dicionário radius que você quer o grupo ou o usuário se usar. (Por exemplo, RAIO - Cisco.) Clique em Apply.
2. Adicionar os itens de verificação exigidos e responda atributos ao perfil de RADIUS:**Nota:** Os itens de verificação são atributos exigidos para a autenticação, tal como o usuário - identificação e senha. Os atributos da resposta são atributos enviados ao servidor do acesso de rede (NAS) depois que o perfil passou o procedimento de autenticação, tal como o Framed-Protocol. Para lista e explicações dos itens de verificação e dos atributos da resposta, refira os pares de valor de atributo radius e o gerenciamento de dicionário no CSU 2.3 para o guia de referência UNIX.No indicador do perfil, clique o RAIO - ícone de pasta do dictionaryname. (Você precisa provavelmente de clicar o perfil + o símbolo para expandir a pasta RADIUS.) Os itens de verificação e o indicador das opções dos atributos da resposta no indicador de grupo de atributos.Para usar uns ou vários destes atributos, para clicar os atributos que você quer se usar, a seguir para clicar **aplique**. Você pode adicionar mais de um atributo de cada vez.Clique **+** símbolo para o RAIO - dictionaryname para expandir o dobrador.**Nota:** Se você seleciona a opção RADIUS-Cisco11.3, certifique-se de que a liberação do Cisco IOS ® Software 11.3.3(T) ou mais atrasado estão instalados em seus NAS de conexão e adicionar-se linhas de comando new a suas configurações de NAS. Refira inteiramente a possibilidade do dicionário RADIUS-Cisco11.3 no CSU 2.3 para o guia de referência UNIX.
3. Especifique valores para os itens de verificação adicionados e responda atributos:**Cuidado:** Para o protocolo de raio, a herança é aditiva ao contrário de hierárquico. (O protocolo TACACS+ usa a herança hierárquica). Por exemplo, se você atribui os mesmos atributos da resposta ao usuário e aos perfis de grupo, a autorização falha porque o NAS recebe duas vezes o número de atributos. Não faz o sentido dos atributos da resposta. Não atribua o mesmo atributo do item de verificação ou da resposta ao grupo e aos perfis de usuário.Clique **itens de verificação** ou **responda atributos**, ou clique ambos. Uma lista de itens de verificação e de valores de atributos aplicáveis da resposta aparece na janela direita mais baixa. Clique **+** símbolo para expandir o dobrador.Clique os valores que você quer atribuir, a seguir clique-os **aplicam-se**. Para obter mais informações sobre dos valores, refira pares de valor de atributo radius e gerenciamento de dicionário no CSU 2.3 para o guia de referência UNIX.**Nota:** Se você atribui um valor de atributo a nível do perfil de grupo, e o atributo que você especifica indicadores uma caixa de verificação absoluta, selecione essa caixa de verificação para atribuir o status absoluto do valor. Um valor atribuído o status absoluto não pode ser cancelado por nenhuns valores de afirmação atribuída a perfil de grupo subordinado ou níveis de perfil de usuário.Quando você terminou fazer mudanças, o clique **submete-se**.
4. Para usar uns ou vários destes atributos, para clicar os atributos que você quer se usar, a seguir para clicar **aplique**. Você pode aplicar mais de um atributo de cada vez.

Atribua níveis de privilégio de controle de acesso

O administrador de superusuário usa o atributo do privilégio da Web para atribuir um nível do privilégio de controle de acesso aos usuários seguros de Cisco.

1. No programa de configuração avançada seguro do administrador de Cisco, clique o usuário cujo o privilégio de controle de acesso você quer atribuir, a seguir clica o ícone do perfil na placa dos perfis.
2. No menu de opções, clique o **privilégio da Web** e selecione um destes valores.**0** - Nega ao usuário todos os privilégios de controle de acesso que incluírem a capacidade para mudar a senha segura de Cisco do usuário.**1** - Concede o acesso de usuário ao página da web de CSUser. Isto permite que a Cisco os usuários seguros mudem suas senhas seguras de Cisco. Para detalhes sobre como mudar senhas, refira as funções do nível de usuário (que mudam uma senha) no gerenciamento simples de usuário e ACS.**12** - Concede os privilégios de administrador de grupo de usuário.**15** - Concede os privilégios de administrador de sistema de usuário.**Nota:** Se você seleciona alguma opção de privilégio na Web a não ser 0, você deve igualmente especificar uma senha. Para satisfazer a requisição de senha do privilégio da Web, um único espaço em branco é minimamente aceitável.

Comece e pare o CSU

Geralmente, o CSU começa automaticamente quando você começa ou reinicia a SPARCstation onde está instalado. Contudo, você pode começar o CSU manualmente, ou fechá-lo para baixo sem fechar a SPARCstation inteira.

Início de uma sessão como o [Root] à SPARCstation onde você instalou o CSU.

Para começar manualmente o CSU, datilografe:

```
# /etc/rc2.d/S80CiscoSecure
```

Para parar manualmente o CSU, datilografe:

```
# /etc/rc0.d/K80CiscoSecure
```

Verificar

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

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Cisco Secure ACS para página de suporte do UNIX
- Página de suporte de TACACS+
- Página de suporte RADIUS
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems