

Redefina o nome de usuário e a senha do VBond/VSmart off-line

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Problema](#)

[Conceito básico](#)

[Acesso De Usuário Do Ciscotac](#)

[Solução](#)

[Etapa 1. Use o ciscocrw para acessar o vBond/vSmart através do login SSH](#)

[Etapa 2. Redefinir a senha do usuário existente](#)

[Etapa 3. Adicionar um novo usuário Netadmin \(opcional\)](#)

[Etapa 4. Desbloquear a conta bloqueada \(se aplicável\)](#)

[Etapa 5. Verificar a configuração](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como redefinir o nome de usuário e a senha do vBond/vSmart off-line da SD-WAN.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Rede de longa distância definida por software da Cisco (SD-WAN).

Componentes Utilizados

As informações neste documento são baseadas no Cisco vManager versão 20.9.4

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

O acesso a vBonds e vSmarts foi perdido. Isso acontece quando você não sabe ou não se lembra de suas credenciais ou quando o acesso é bloqueado após tentativas excessivas e malsucedidas de fazer login em qualquer interface. Ao mesmo tempo, as conexões de controle entre vManage, vSmarts e vBonds são interrompidas. Vbond e vsmart off-line não podem ser operados através da GUI do vmanage.

Conceito básico

Acesso De Usuário Do Ciscotac

O software Cisco Edge oferece dois usuários, ciscotacro e ciscotacrw, que devem ser usados somente pela equipe de suporte da Cisco. Esses usuários estão disponíveis para instalações na nuvem e no local. Eles operam em um desafio de token de consentimento e autenticação de resposta de token, em que um novo token é necessário para cada nova sessão de login. Os usuários ciscotacro e ciscotacrw podem usar esse token para fazer login no servidor Cisco SD-WAN Manager, bem como no terminal SSH no Cisco SD-WAN Manager. Esses usuários também podem acessar o Cisco SD-WAN Validator, os controladores Cisco SD-WAN e os dispositivos Cisco vEdge usando o terminal SSH no Cisco SD-WAN Manager.

Os modelos CLI padrão incluem a configuração de usuário ciscotacro e ciscotacrw. Por padrão, esses usuários estão habilitados. No entanto, como você pode desativar esses usuários, se necessário.

- Usuário do ciscotacro: este usuário faz parte do grupo de usuários do operador com privilégios somente leitura. Esse usuário pode apenas monitorar uma configuração, mas não pode executar nenhuma operação que modifique a configuração da rede.
- Usuário do ciscotacrw: este usuário faz parte do grupo de usuários do netadmin com privilégios de leitura e gravação. Esse usuário pode modificar uma configuração de rede. Além disso, somente esse usuário pode acessar o shell raiz usando um token de consentimento.

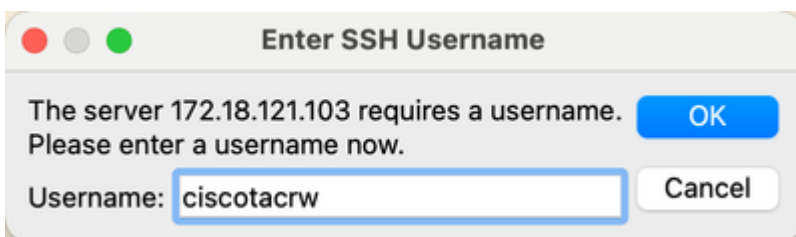


Note: A conta de usuário "ciscotac" foi apresentada e está incluída por padrão a partir das versões do software Cisco SD-WAN em torno da versão 20.x.

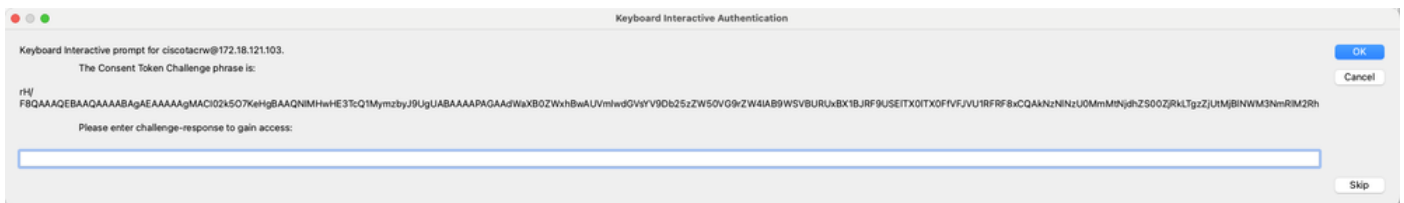
Solução

Etapa 1. Use o ciscocrw para acessar o vBond ou o vSmart através do login SSH

- Insira ciscotacrw como o nome de usuário.



- Clique em OK, a frase Desafio de token de consentimento é gerada de acordo.



- Você precisa fornecer a "frase de Desafio de Token de Consentimento" ao TAC através do caso SR. O TAC retorna o "token sdwanchallenge-response" correspondente.
- Entrada "sdwanchallenge-response token"

Etapa 2. Redefinir a senha do usuário existente

Depois de fazer login no vBond/vSmart off-line através da conta ciscotacrw (usando o token de consentimento para autenticação), você pode restaurar ou redefinir o nome de usuário e a senha.

- Entre no modo de configuração e redefina a senha para o usuário existente (como admin):

```
vBond# config terminal
```

```
vBond(config)# system aaa user admin password <new password>
vBond(config)# commit
```



Note: Após o envio, o sistema criptografa automaticamente a senha em texto simples.

Etapa 3. Adicionar um novo usuário Netadmin (opcional)

Se for necessário criar uma nova conta de administrador:

```
vBond(config)# system aaa user <new username> password <new password>
vBond(config)# system aaa user <new username> group netadmin
vBond(config)# commit
```

Etapa 4. Desbloquear a conta bloqueada (se aplicável)

Se sua conta estiver bloqueada devido a várias falhas de login, você poderá desbloqueá-la usando o comando:

```
request aaa unlock-user <username>
```

Etapa 5. Verificar a configuração

- Use o comando `show running-config system aaa` para verificar se a configuração do usuário está aplicada corretamente.
- Tente fazer login com as novas credenciais para confirmar a recuperação bem-sucedida.



Note: Como o vBond está em um estado off-line (não associado ao vManage ou desconectado), é recomendável concluir a configuração diretamente via CLI, em vez de emitir o modelo do vManage.



aviso: Após a conclusão, se você precisar restabelecer uma conexão de gerenciamento com o vManage, verifique se as credenciais são consistentes com a configuração no vManage.

Informações Relacionadas

- [Recupere o acesso vSmart e vBond da SD-WAN quando as conexões de controle forem estabelecidas](#)
- [Acesso De Usuário Do Ciscotac](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.