Procedimento de recuperação de senha para a ferramenta NAC de Cisco (acesso limpo de Cisco)

Índice

Introdução

Este documento descreve como recuperar uma senha em um Access Manager limpo de Cisco (CAM) e no servidor de acesso limpo de Cisco (CAS).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Convenções

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

Procedimentos Passo a Passo

O dispositivo do Cisco Network Admission Control (NAC) contém estas senhas de conta de usuário administrativas incorporados:

- Limpe o usuário de raiz da máquina da instalação do Access Manager

- Limpe o usuário de raiz da máquina da instalação do servidor de acesso
- Limpe o usuário admin do console de web do servidor de acesso
- Limpe o usuário admin do console de web do Access Manager

As primeiras três senhas são ajustadas inicialmente no tempo de instalação (a senha padrão é cisco123). A fim mudar mais tarde estas senhas, alcance o Access Manager limpo ou limpe a máquina do servidor de acesso pelo SSH e o início de uma sessão como o usuário cuja a senha você quer mudar. Use o **comando passwd de** Linux a fim mudar a senha do usuário. A fim recuperar a senha root para o Access Manager limpo/servidor de acesso limpo, você pode usar o procedimento de Linux para carreg ao modo do usuário único e para mudar a senha root.

LILO usado versão 3.5.x e anterior da ferramenta NAC como o Boot Loader. Os usos da versão 3.6.x e mais recente CAVAM porque o Boot Loader e daqui o procedimento de recuperação de senha é diferente. Estes são os dois procedimentos diferentes.

Versão 3.5.x e anterior da ferramenta NAC

Conclua estes passos:

1. Conecte à máquina CAM/CAS através do console.
2. Ciclo de energia a máquina a fim indicar o modo GUI.
3. Pressione o **Ctrl-x** a fim comutar ao modo de texto. Isto indica uma `bota:` prompt.
4. **No linux do** tipo imediato **único** a fim carreg a máquina no modo do usuário único.
5. Datilografe a **senha** e pressione-a **entram**.
6. Mude a senha root e recarregue a máquina usando o **comando reboot**.**Nota:** É importante fornecer senhas seguras para as contas de usuário no sistema da ferramenta NAC de Cisco, e mudá-las de vez em quando a fim manter a segurança de sistema. A série não impõe geralmente padrões para as senhas que você escolhe, mas recomenda-se que você usa senhas elaboradas. Isto é, senhas com pelo menos seis caráteres, letras misturadas e números, e assim por diante. As senhas elaboradas reduzem a probabilidade de uma senha bem sucedida que supõe o ataque contra seu sistema.

Versão 3.6.x e mais recente da ferramenta NAC

Conclua estes passos:

1. Põe acima a máquina, a ferramenta NAC, ou o server.
2. Pressione toda a chave quando a tela do Boot Loader parece com a “imprensa qualquer chave para incorporar o menu…” mensagem a fim incorporar o menu da LARVA.O menu da LARVA aparece com um artigo na lista:Acesso limpo de Cisco (2.6.11-perfigo)
3. Pressione **e** a fim editar.Estas escolhas múltiplas aparecem:
```
root (hd0,0)
kernel /vmlinuz-2.6.11-perfigo ro root=LABEL=/ console=tty0 console=ttyS0,9600n8
Initrd /initrd-2.6.11-perfigo.img
```
4. Rolo à segunda entrada (a linha que começa com `núcleo…`) e imprensa **e** a fim editar a linha.
5. A supressão **console=ttyS0,9600n8**, adiciona a palavra **única à** extremidade da linha, e pressiona-a então **entra**.A linha parece similar a este exemplo:
```
kernel /vmlinuz-2.6.11-perfigo ro root=LABEL=/ console=tty0 single
```

6. Pressione **b** a fim carreg a máquina no modo do usuário único.Você é presentado com uma alerta do shell da raiz após a inicialização.**Nota:** Você não é alertado para uma senha.
7. **Na senha do** tipo imediato, pressione **incorporam**, e seguem as instruções.
8. Depois que a senha é mudada, incorpore a **repartição** a fim recarregar a caixa.

Recuperação de senha da WEB GUI CAM

Crie um novo usuário

Não há nenhum procedimento padrão para recuperar a senha de admin. O único procedimento disponível é para a senha root CLI.

1. Conecte ao CLI e emita estes comandos:`[root@cca-3390-cam ~]#  psql -h 127.0.0.1 controlsmartdb -U postgres`
   `controlsmartdb=# select * from admin_account;`Você deve agora ver uma lista de usuários, similar a esta:
```
id |    name    |                password                |
group_name     | enable |      admin_desc
----+------------+----------------------------------------+-------------------+--------
+-----------------------
  0 | admin      | 96208ed2256706e8d8b29c1bf58d10c4a07267b4c1 |
Full-Control Admin |      1 | Primary admin account
  1 | localadmin | b0f3e23dcd1046d1dbf4e095186d5cb54e47963690 |
GuestLobby         |      1 | only local users
  2 | admin1     | 96208ed225670d688bs29c1bf58d10c4a07267b4c1 |
Full-Control Admin |      1 | admin test user
(3 rows)
```
2. Você precisa de ver o valor o mais alto identificação e de incrementá-lo (neste exemplo, o valor novo é 3).
3. Introduza o novo usuário com o comando:`insert into admin_account(id, name, password, group_name, enable)`
   `values ('3', 'recover', 'cisco123', 'Full-Control Admin', '1');`
4. Verifique se o usuário da recuperação está no DB:`controlsmartdb=# select * from admin_account;`
```
                                        id |    name
|                 password                 |     group_name     | enable
|      admin_desc
----+------------+----------------------------------------+-------------------+--------
+-----------------------
  0 | admin      | 96208ed225670688b29c1bf58d10c4a07267b4c1 |
Full-Control Admin |      1 | Primary admin account
  1 | localadmin | b0f3e23dcd10461db4e095186d5cb54e47963690 |
GuestLobby         |      1 | only local users
  2 | admin1     | 96208ed225670688b29c1bf58d10c4a07267b4c1 |
Full-Control Admin |      1 | admin test user
  3 | recover    | cisco123                                 |
Full-Control Admin |      1 |
(4 rows)
```
5. Entre ao GUI com este novo usuário.

Suprima da conta admin

Use o comando sql suprimir do usuário admin.

1. Incorpore a linha de comando sql:`[root@cca-3390-cam ~]#  psql -h 127.0.0.1 controlsmartdb -U postgres`

2. Suprima do usuário admin (id=0).
```
controlsmartdb=# delete from admin_account where id='0';
DELETE 1
```
3. Verifique que a identificação 0 esteve suprimida.
```
controlsmartdb=# select * from
admin_account;
 id |    name    |                password                |
group_name     | enable |    admin_desc
----+------------+----------------------------------------+-------------------+--------
+-----------------
  1 | localadmin | b0f3e23dcd10461db4e095186d5cb54e47963690 |
GuestLobby         |      1 | only local users
  2 | admin1     | 96208ed225670688b29c1bf58d10c4a07267b4c1 |
Full-Control Admin |      1 | admin test user
  3 | recover    | 96208ed225670688b29c1bf58d10c4a07267b4c1 |
Full-Control Admin |      1 |
(3 rows
```
4. Você pode agora criar um usuário novo “admin” no '0' identificação.
```
controlsmartdb=# insert
into
admin_account(id,name,password,group_name,enable) values('0', 'admin',
'cisco123', 'Full-Control Admin', 1);
INSERT 0 1
controlsmartdb=# select * from admin_account
controlsmartdb-# ;
 id |    name    |                password                |
group_name     | enable |    admin_desc
----+------------+----------------------------------------+-------------------+--------
+-----------------
  1 | localadmin | b0f3e23dcd10461db4e095186d5cb54e47963690 |
GuestLobby         |      1 | only local users
  2 | admin1     | 96208ed225670688b29c1bf58d10c4a07267b4c1 |
Full-Control Admin |      1 | admin test user
  3 | recover    | 96208ed225670688b29c1bf58d10c4a07267b4c1 |
Full-Control Admin |      1 |
  0 | admin      | cisco123                               |
Full-Control Admin |      1 |
(4 rows)
```
5. Verifique se o novo usuário está no DB.

Informações Relacionadas

- Documentação do produto da ferramenta NAC de Cisco
- Suporte Técnico e Documentação - Cisco Systems