

Falha na redefinição da senha do SO CUMA com o processo de "recuperação de falhas"

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Problema](#)

[Solução 1](#)

[Solução 2](#)

[Informações Relacionadas](#)

[Introduction](#)

O Cisco Unified Mobility Advantage (CUMA) faz parte da família de produtos Cisco Unified Communications. O CUMA é um software de servidor implantado por trás do firewall da empresa que conecta os celulares dos funcionários aos servidores de diretório, sistema de Comunicações IP, groupware e servidores de conferência, bem como a outros recursos da empresa. Isso estende os recursos críticos de comunicação empresarial para dispositivos portáteis e permite que todos se comuniquem com mais eficiência.

Este documento fornece as diretrizes para solucionar problemas de recuperação de senha no Cisco Unified Mobility Advantage Server.

[Prerequisites](#)

[Requirements](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

As informações neste documento são baseadas na versão 7.1.2.3 do servidor CUMA.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

[Conventions](#)

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.](#)

Problema

O problema é que você não pode fazer login com SSH, CLI ou página Plataforma. O procedimento de recuperação de energia foi tentado, mas você ainda não pode fazer login no console. Se uma senha inaceitável for inserida durante uma recuperação de energia, ela não será utilizável. Há pelo menos três tipos de senhas que não são aceitas durante uma redefinição de senha:

- A senha é muito curta
- As senhas não correspondem
- Senha no dicionário

Observação: se qualquer um desses tipos for usado, um erro será exibido. Em seguida, se uma senha correta for inserida, ela aparecerá, pois a senha foi redefinida. No entanto, a senha não pode ser usada. Qualquer tentativa de recuperação de senha não funcionará neste caso. Você não poderá fazer login na GUI ou na CLI da plataforma.

Solução 1

Se você não se lembra da senha do administrador, aqui está o procedimento para redefini-la. Há dois métodos para redefinir a senha. O primeiro é sem usar um CD de recuperação e o outro é com um CD.

1. Faça login na caixa linux com a conta raiz (esta é uma caixa linux padrão).
2. Verifique se estes serviços estão em execução: `/sbin/service cuma_db start/sbin/service cuma_admin start/sbin/service cuma_nm start`
3. Edite o arquivo usando o editor de vídeo: `/opt/cuma/conf/admin/admin.xml`.

4. Localizar esta linha:

```
<name>admin_password</name>
```

```
<value>{MD5}xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx</value>
```

E mude para:

```
<name>admin_password</name>
```

```
<value>{plain}new_password</value>
```

5. Use este comando para reiniciar o serviço:

```
/sbin/service cuma_admin restart
```

6. Faça login com "admin" e "new_password".

Solução 2

O problema é que você não pode redefinir a senha do administrador do SO ao usar o processo `pwrecovery`. Siga estas etapas para resolver o problema:

1. Inicialize o sistema com o CD de recuperação (recomendamos 7.1.2 ou posterior).
2. Verifique se ele pode detectar a instalação (impressa com o menu principal do CD de recuperação).
3. Pressione **alt+F2** para obter acesso ao shell raiz do CD de recuperação.

4. A partição ativa deve estar em `/mnt/part1`. Verifique se ele está montado corretamente.
5. Execute os comandos `chroot /mnt/part1 rpm -q master` e `chroot /mnt/part2 rpm -q master` para localizar a partição ativa.
6. Depois de executar esses comandos e encontrar a versão em funcionamento do servidor a partir dos resultados retornados, você precisa usá-la como a partição em funcionamento.
7. Digite a partição ativa por `chroot /mnt/part1`, se for uma nova instalação.
8. Se o servidor tiver sido atualizado, use esse número de peça específico (`chroot /mnt/part<no>`).
9. Em versões anteriores, execute `/root/.security/unimmunize.sh` para remover o bit imutável de `/etc/passwd`.
10. Edite `/etc/passwd` e altere `root:x:0:0:root:/root:/sbin/nologin` para `root:x:0:0:root:/root:/bin/bash` e salve as alterações.
11. Execute o comando `passwd root` e forneça uma senha no prompt e, em seguida, confirme. Agora você terá acesso raiz quando inicializar na partição ativa.
12. Pressione **Alt+F1** para obter o menu principal do CD de recuperação e digite **q** para sair. Em seguida, ejete o cd.
13. Pressione **ctrl+alt+delete** para reinicializar.
14. Depois disso, **SSH** em como raiz e defina uma senha temporária para o administrador do SO com este comando: `passwd admin`, em que admin é o nome de login de usuário do administrador do sistema operacional. **Observação:** aqui, a senha é usada apenas temporariamente. Você vai precisar fazer isso de novo.
15. Inicie a CLI com o comando `su - admin`, em que admin é o nome de login do administrador do SO.
16. Altere a senha no banco de dados com o comando CLI `set password user <admin id>`.
17. Saia da CLI.
18. Defina a senha do sistema do administrador do SO para corresponder à senha do banco de dados com este comando: `passwd admin`, em que admin é o nome de login do OS Administrator. **Observação:** isso é documentado pelo bug da Cisco ID [CSCtf25554](#) (somente clientes registrados) .

Informações Relacionadas

- [Usando o Assistente de configuração no Cisco Unified Mobility Advantage](#)
- [Problema de certificado do Cisco Unified Mobility Advantage Server com o ASA](#)
- [Suporte à Tecnologia de Voz](#)
- [Suporte aos produtos de Voz e Comunicações Unificadas](#)
- [Troubleshooting da Telefonia IP Cisco](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)