A restauração da senha do OS CUMA falha com o processo do “pwrecovery”

Índice

Introdução

O Cisco Unified Mobility Advantage (CUMA) é parte da família de produto das comunicações unificadas de Cisco. CUMA é um software do server distribuído atrás de seu Firewall da empresa que conecta os telefones celulares dos empregados a seus servidores de diretório, sistema das Comunicações IP, groupware, e server das Conferências assim como outros recursos da empresa. Isto estende capacidades críticas das comunicações empresariais aos monofones móveis e permite que todos comunique-se mais eficazmente.

Este documento fornece as diretrizes para pesquisar defeitos a recuperação de senha no server do Cisco Unified Mobility Advantage.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na versão de servidor 7.1.2.3 CUMA.

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

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

Problema

A edição é você não pode entrar com SSH ou CLI, ou página da plataforma. O procedimento do pwrecovery foi tentado, mas você ainda não pode entrar ao console. Se uma senha inaceitável é incorporada durante um pwrecovery, a senha não é útil. Há pelo menos três tipos de senhas que não são aceitadas durante uma senha restaurada:

- A senha é demasiado curto
- As senhas não combinam
- Senha no dicionário

Nota: Se qualquens um tipos são usados, um erro está indicado. Então se uma senha correta é incorporada, parece que a senha esteve restaurada. Contudo, a senha não é útil. Nenhuma tentativa de fazer uma recuperação de senha não trabalhará neste caso. Você será incapaz de entrar à plataforma GUI ou CLI.

Solução 1

Se você não recorda a senha de admin, está aqui o procedimento para restaurá-la. Há dois métodos para restaurar a senha. Primeiro é sem usar um CD da recuperação e o outro é com um CD.

1. Entre à caixa do linux com a conta raiz (esta é uma caixa padrão do linux).
2. Certifique-se que estes serviços estão sendo executado:começo do cuma_db de /sbin/servicecomeço do cuma_admin de /sbin/servicecomeço do cuma_nm de /sbin/service
3. Edite o arquivo usando o editor de VI: **/opt/cuma/conf/admin/admin.xml**.
4. Encontre esta linha:`<name>admin_password</name>`

   `<value>{MD5}xxxxxxxxxxxxxxxxxxxxxxxxxx</value>` E mude-à:`<name>admin_password</name>`

   `<value>{plain}new_password</value>`
5. Use este comando a fim reiniciar o serviço:`/sbin/service cuma_admin restart`
6. Entre com o “admin” e o “new_password”.

Solução 2

A edição é você não pode restaurar a senha de admin do OS ao usar o processo do **pwrecovery**. Siga estas etapas para resolver o problema:

1. Carreg o sistema com o CD da recuperação (7.1.2 ou mais atrasado são recomendados).
2. Certifique-se que pode detectar a instalação (que está imprimido com o menu principal do CD da recuperação).
3. Pressione **alt+F2** para obter o acesso ao shell da raiz do CD da recuperação.
4. O partição ativa deve estar em **/mnt/part1**. Certifique-se que está montado corretamente.
5. Execute o **chroot /mnt/part1 RPM - mestre q** e **chroot /mnt/part2 RPM - os** comandos

mestres q a fim encontrar o partição ativa.
6. Depois que você executa estes comandos e encontra a versão em funcionamento do server dos resultados retornados, você precisa de usá-lo como a separação de trabalho.
7. Entre no partição ativa pelo **chroot /mnt/part1**, se é uma instalação nova.
8. Se o server foi promovido, use esse part number específico (**<no> de /mnt/part do chroot**).
9. Em versões anterior, execute **/root/.security/unimmunize.sh** para remover o bit imutável de **/etc/passwd**.
10. Edite **/etc/passwd** e mude **root:x:0:0:root:/root:/sbin/nologin a root:x:0:0:root:/root:/bin/bash**, a seguir salvar as mudanças.
11. Execute o **comando root da senha** e dê uma senha na alerta, a seguir confirme-a. Agora você terá o acesso raiz quando você carreg no partição ativa.
12. Pressione **Alt+F1** para obter o menu principal do CD da recuperação e para incorporar **q** para parar. Então, ejete o CD.
13. Pressione **ctrl+alt+delete** para recarregar.
14. Após isto, o **SSH** dentro como a raiz e ajustou uma senha provisória para o OS admin com este comando: **senha admin**, onde o admin é nome de login de usuário do seu administrador do OS.**Nota:** Aqui, a senha é usada somente temporariamente. Você precisará de fazê-la outra vez.
15. Comece acima o CLI com a **SU - comando admin**, onde o admin é o nome do início de uma sessão do administrador do OS.
16. Mude a senha no base de dados com o comando CLI do *id> do <admin do* **usuário da senha do grupo**.
17. Retire do CLI.
18. Ajuste a senha de sistema do administrador do OS para combinar a senha do base de dados com este comando: **senha admin**, onde o admin é o nome do início de uma sessão do administrador do OS.**Nota:** Isto é documentado pela identificação de bug Cisco CSCtf25554 (clientes registrados somente).

Informações Relacionadas

- Usando o wizard de configuração no Cisco Unified Mobility Advantage
- Edição do certificado de servidor do Cisco Unified Mobility Advantage com ASA
- Suporte à Tecnologia de Voz
- Suporte ao Produto de Voz e Comunicações Unificadas
- Troubleshooting da Telefonia IP Cisco
- Suporte Técnico e Documentação - Cisco Systems