

Como controlar a senha no gerente integrado da interação do email (EIM)

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Procedimento](#)

Introdução

Este original descreve como mudar o usuário do base de dados do Admin Workstation de EIM (AW) (DB) ou atualizar uma senha do usuário criado no desenvolvimento EIM-inteligente da integração do gerenciamento de contato (ICM).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Empresa unificada do centro de contato (UCCE)
- EIM
- Língua de consulta estruturada (SQL) de Microsoft

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- UCCE 9.x, 10.x
- EIM 9.x

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.

Informações de Apoio

O gerente da interação de Cisco (CIM) conecta ao base de dados AW por vários motivos. Quando o CIM é integrado com UCCE, o usuário e a senha do base de dados AW estão definidos. Este usuário é tipicamente o sa que existe em corridas do servidor SQL no server AW/HDS. Uma vez que o assistente da integração é terminado, não pode ser executado outra vez.

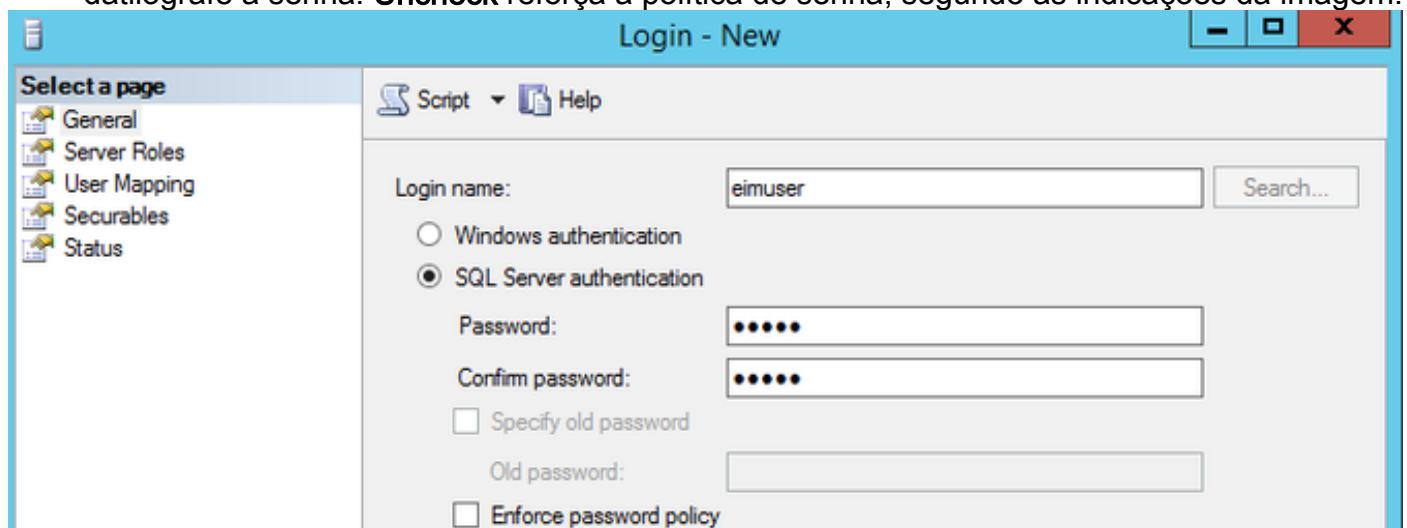
Por razões de segurança, alguns clientes não permitem que o usuário SQL sa seja usado por aplicativos. Neste caso, o novo usuário é exigido substituir o usuário SQL sa. Este procedimento explica como criar um usuário novo SQL no server AW/HDS e substituir o usuário sa com o novo usuário e atualizá-lo com a senha no lado CIM.

O procedimento similar pode ser seguido para atualizar a senha do usuário atual que não é usuário sa (por exemplo eimuser).

Procedimento

Etapa 1.

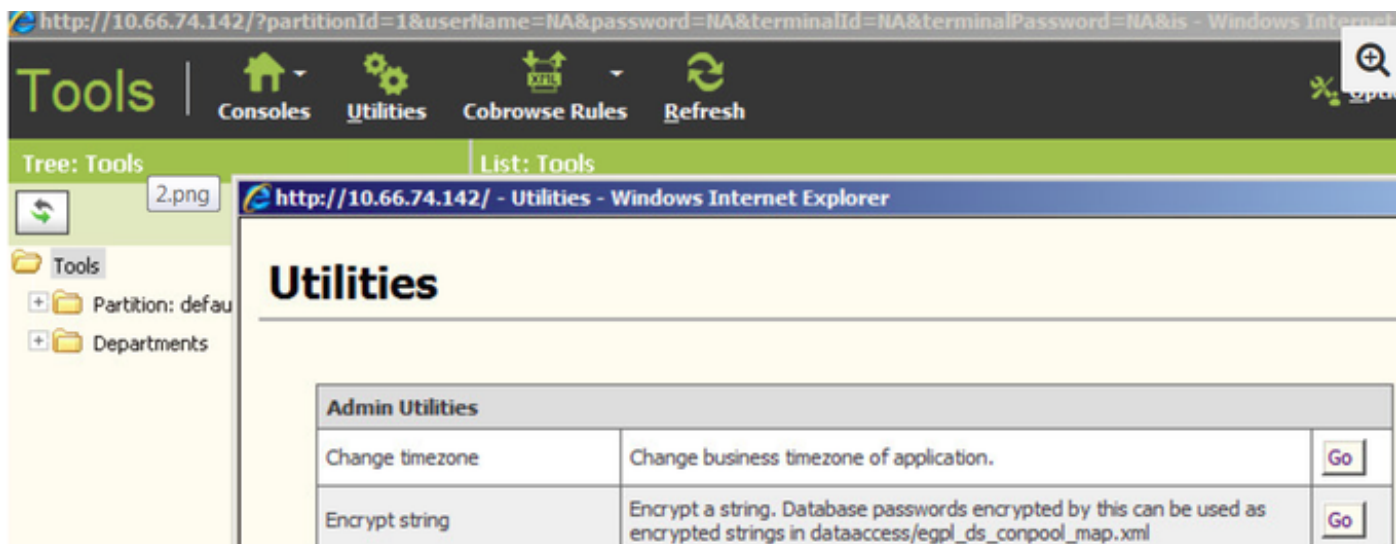
1. **Navegue a AW/HDS preliminar e abra o estúdio do Gerenciamento SQL.**
2. **Expanda a Segurança**, clicar com o botão direito em inícios de uma sessão e crie um usuário de login novo.
3. Na tela nova do início de uma sessão, selecione a **autenticação de servidor SQL** e datilografe a senha. **Uncheck** reforça a política de senha, segundo as indicações da imagem:



4. Na placa do lado esquerdo, clique sobre o **mapeamento do usuário** e verifique o `<instance>_awdb` e verifique então o papel do `db_datareader`.

Etapa 2. O assistente da integração armazena a informação do nome de usuário e senha em `egpl_ds_connpool_map.xml`. Mantenha na mente, a senha é cifrada e não pode ser alterada em linha reta em um arquivo.

1. Entre ao console EIM com **pa** e clique sobre ferramentas.
2. Clique sobre **utilidades**.
3. A utilidade do achado cifra a corda e clica sobre **Go**, segundo as indicações da imagem:



4. Datilografe a senha a ser cifrada. Recorde que esta é a mesma senha que você configurou/actualizado em AW/HDS SQL para usuário novo/existente em Step1.

Etapa 3. Ao usuário e à senha de atualização, pare o serviço Cisco.

1. Tome o backup de egpl_ds_connpool_map.xml de todos os três lugares mencionados aqui.
2. Copie a série criptografada e atualize-a no arquivo egpl_ds_connpool_map.xml situado nestes três lugares:
 - **Server> <File CIM \ eService \ instalação \ dataaccess**
 - **Server> <File CIM \ eService \ instalação \ orelha \ eService.ear \ liberal \ configurations.zip \ dataaccess **
 - **<Services Server> CIM \ eService \ liberal \ configurations.zip \ dataaccess**
3. Arquivo aberto egpl_ds_connpool_map.xml no editor de texto e busca para o awdb da palavra.
4. Encontre o ativo='y e substitua o **sa** com o novo usuário e a senha criptografada para esse pool. Além disso, se o usuário não for o **sa** já atual no arquivo, então atualize somente a senha

```

</connpool>
- <connpool name="IPCC_MSSQL_POOL_1" egid="307" active="y">
  <Type egid="3071">basic</Type>
  <CapacityIncrement egid="3072">2</CapacityIncrement>
  <DriverName egid="3073">com.microsoft.sqlserver.jdbc.SQLServerDriver</DriverName>
  <InitialCapacity egid="3074">1</InitialCapacity>
  <MaxCapacity egid="3075">10</MaxCapacity>
  <User egid="3076">sa</User>
  <Password egid="3077">C2A0C38DC2A0C2A6C399C396C2ACC2A6C284C293C296C299</Password>
  <Url egid="3078">jdbc:sqlserver://10.68.44.67:1433;DatabaseName=icm_awdb</Url>
  <Targets egid="3079"/>
  <Vendor egid="30710">MSSQL</Vendor>
  <DriverVendor egid="30711"/>
  <TableName egid="30712">sysindexes</TableName>
</connpool>
- <connpool name="IPCC_MSSQL_POOL_2" egid="308" active="n">
  <Type egid="3081">basic</Type>
  <CapacityIncrement egid="3082">2</CapacityIncrement>
  <DriverName egid="3083">com.microsoft.sqlserver.jdbc.SQLServerDriver</DriverName>
  <InitialCapacity egid="3084">1</InitialCapacity>
  <MaxCapacity egid="3085">10</MaxCapacity>
  <User egid="3086">sa</User>
  <Password egid="3087">C2A0C38DC2A0C2A6C399C396C2ACC2A6C284C293C296C299</Password>
  <Url egid="3088">jdbc:sqlserver://10.68.44.57:1433;DatabaseName=icm_awdb</Url>
  <Targets egid="3089"/>
  <Vendor egid="30810">MSSQL</Vendor>
  <DriverVendor egid="30811"/>
  <TableName egid="30812">sysindexes</TableName>
</connpool>

```

Etapa 4. Enfie o serviço Cisco e verifique trabalhos da integração muito bem. Crie o agente novo em AW/HDS no gerenciador de configuração, trace o agente novo no server CIM e verifique se o início de uma sessão do agente é bem sucedido.