Cómo manejar la contraseña en el administrador integrado de la interacción del correo electrónico (EIM)

Contenido

Introducción

Este documento describe cómo cambiar al usuario de la base de datos del Admin Workstation de EIM (AW) (DB) o poner al día una contraseña del usuario creado en el despliegue EIM-inteligente de la integración de la administración de contactos (ICM).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Empresa unificada del Centro de contacto (UCCE)
- EIM
- Lenguaje de consulta estructurado (SQL) de Microsoft

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El administrador de la interacción de Cisco (CIM) conecta con la base de datos AW por varias

razones. Cuando el CIM se integra con UCCE, definen al usuario de la base de datos y la contraseña AW. Este usuario es típicamente el sa que existe en los funcionamientos del servidor SQL en el servidor AW/HDS. Una vez que completan al Asisitente de la integración, no puede ser ejecutado otra vez.

Por razones de seguridad, algunos clientes no permiten que al usuario SQL sa utilice las aplicaciones. En este caso, requieren al usuario nuevo substituir al usuario SQL sa. Este procedimiento explica cómo crear a un nuevo usuario SQL en el servidor AW/HDS y substituir al usuario sa por el usuario nuevo y ponerlo al día es contraseña en el lado CIM.

El procedimiento similar se puede seguir para poner al día la contraseña del Usuario usuario actual que no es usuario sa (e.g eimuser).

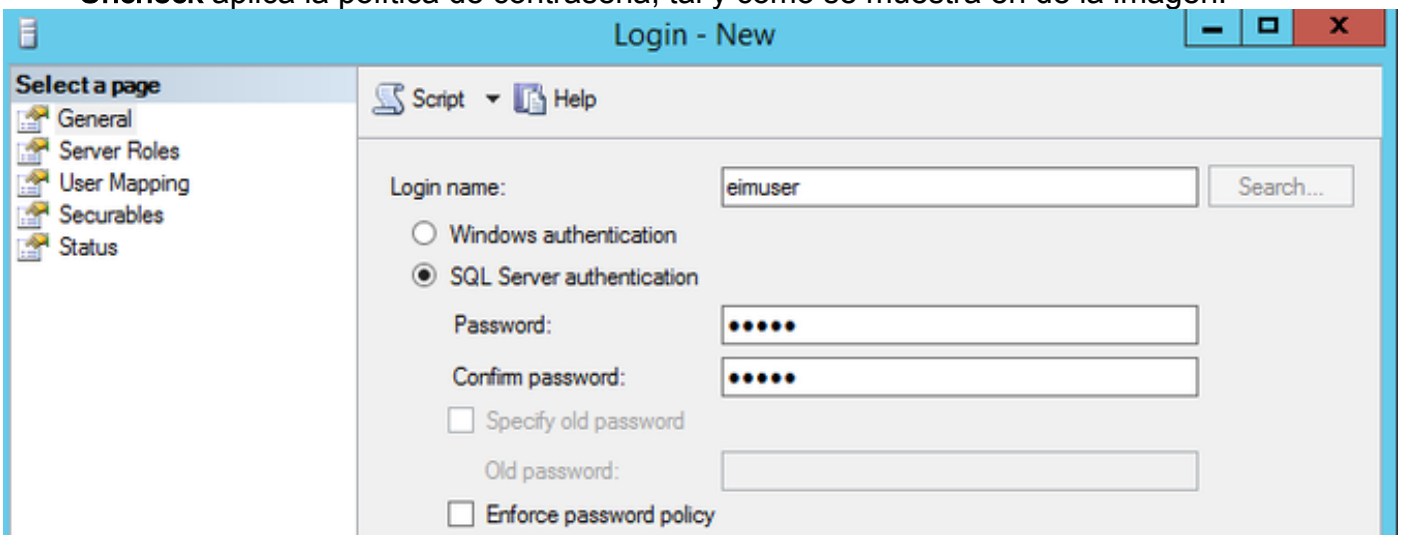
Procedimiento

Paso 1.

1. **Navegue a** AW/HDS primario y **abra el** estudio de la Administración SQL.

2. **Amplíe la** Seguridad, haga clic con el botón derecho del ratón en los logines y cree a un nuevo usuario que ingresa al sistema.

3. En la nueva pantalla del login, **autenticación de SQL Server** y contraseña selectas del tipo. **Uncheck** aplica la política de contraseña, tal y como se muestra en de la imagen:



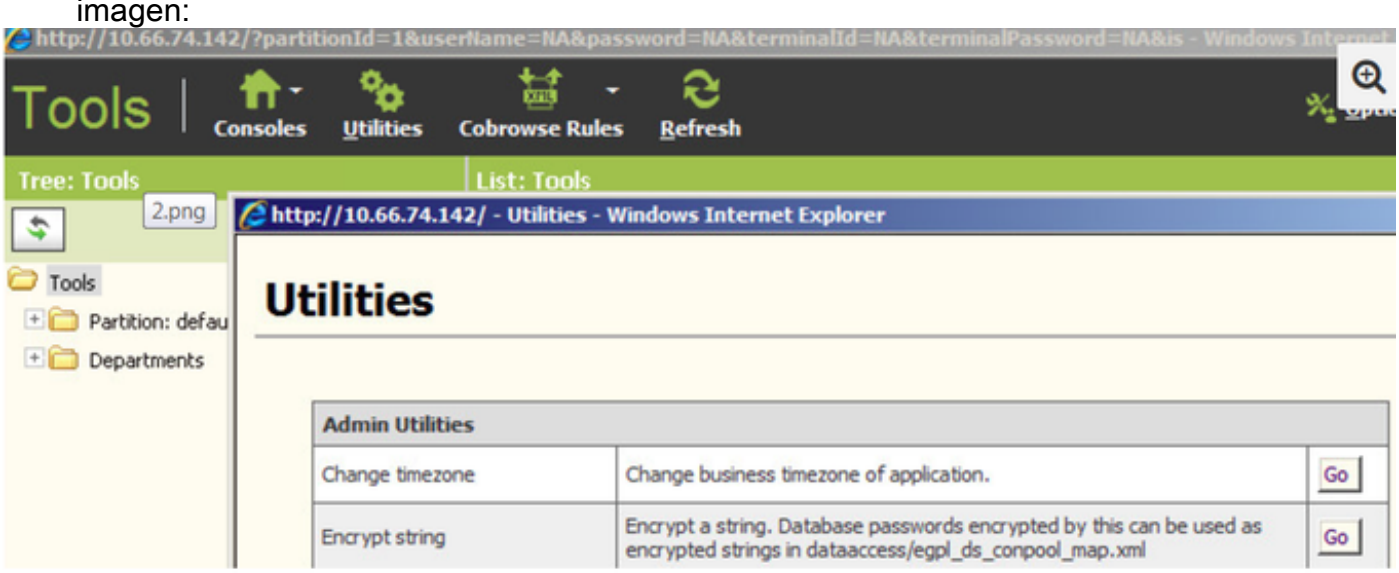
4. En el cristal del lado izquierdo, haga clic en el **<instance>_awdb el asociar del usuario** y del control y después marque el papel del **db_datareader**.

Paso 2. El Asisitente de la integración salva la información del nombre de usuario y contraseña en egpl_ds_connpool_map.xml. Tenga presente, la contraseña se cifra y no se puede modificar derecho en un archivo.

1. Inicie sesión a la consola EIM con el **PA** y haga clic en las herramientas.

2. Haga clic en las **utilidades**.

3. La utilidad del hallazgo cifra la cadena y hace clic en **va**, tal y como se muestra en de la imagen:



4. Teclee la contraseña que se cifrará. Recuerde que ésta es la misma contraseña que usted configuró/puesto al día en AW/HDS SQL para el nuevo/existente usuario en Step1.

Paso 3. Al usuario en modo actualización y a la contraseña, pare los servicios de Cisco.

1. Tome el respaldo de egpl_ds_connpool_map.xml de las tres ubicaciones mencionadas aquí.

2. Copie el string encriptada y póngase al día en el archivo egpl_ds_connpool_map.xml situado en estas tres ubicaciones:
   - **Server> <File CIM \ eService \ instalación \ dataaccess**
   - **Server> <File CIM \ eService \ instalación \ oído \ eService.ear \ liberación \ configurations.zip \ dataaccess **
   - **Server> CIM \ eService \ liberación \ configurations.zip \ dataaccess de los <Services**
3. **Archivo** abierto **egpl_ds_connpool_map.xml** en el editor de textos y la búsqueda para el awdb de la palabra.

4. Encuentre el active='y y substituya el **sa** por el usuario nuevo y la contraseña encriptada para ese pool. Si el usuario está con excepción del **sa** ya presente en el archivo, entonces ponga al día una vez más solamente la contraseña

```
</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>
```

Paso 4. Comience los servicios de Cisco y verifique los trabajos de la integración muy bien. Cree el nuevo agente en AW/HDS en el administrador de configuración, asocie el nuevo agente en el servidor CIM y verifiquelo si el login del agente es acertado.