# HP Universal CMDB Configuration Manager

Versão do software: 10.10

## Guia de proteção

Data de lançamento do documento: Novembro de 2013

Data de lançamento do documento: Novembro de 2013

# Avisos Legais

## Garantia

As únicas garantias para produtos e serviços HP estão estipuladas nas declarações de garantia expressa que acompanham esses produtos e serviços. Nenhum conteúdo deste documento deve ser interpretado como parte de uma garantia adicional. A HP não se responsabiliza por erros técnicos ou editoriais ou por omissões presentes neste documento.

As informações contidas neste documento estão sujeitas a mudanças sem aviso prévio.

## Legenda de Direitos Restritos

Software de computador confidencial. Uma licença válida da HP é necessária para posse, utilização ou cópia. Consistentes com o FAR 12.211 e 12.212, o Software de Computador Comercial, a Documentação de Software de Computador e os Dados Técnicos para Itens Comerciais estão licenciados junto ao Governo dos Estados Unidos sob a licença comercial padrão do fornecedor.

## Aviso de Direitos Autorais



## Avisos de Marcas Comerciais

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

# Atualizações da Documentação

A página inicial deste documento contém as seguintes informações de identificação:

- Número de versão do software, que indica a versão do software.
- Data de lançamento do documento, que é alterada a cada vez que o documento é atualizado.
- Data de lançamento do software, que indica a data de lançamento desta versão do software.

Para verificar as atualizações recentes ou se você está utilizando a edição mais recente, vá para: **http://h20230.www2.hp.com/selfsolve/manuals**

Esse site exige que você se registre para obter um HP Passport e para se conectar. Para se registrar e obter uma ID do HP Passport, vá para: **http://h20229.www2.hp.com/passport-registration.html**

Ou clique no link **New users - please register** (Registro de novos usuários) na página de logon do HP Passport.

Você também receberá edições novas ou atualizadas se assinar o serviço de suporte adequado ao produto. Entre em contato com seu representante de vendas HP para saber mais detalhes.

# Suporte

Visite o site de Suporte Online da HP Software em: **http://www.hp.com/go/hpsoftwaresupport**

Esse site fornece informações de contato e detalhes sobre produtos, serviços e suporte oferecidos pela HP Software.

O suporte on-line da HP Software fornece recursos de auto-ajuda aos clientes. Ele oferece uma maneira rápida e eficiente de acessar ferramentas de suporte técnico interativas necessárias para gerenciar seus negócios. Como um estimado cliente de suporte, você pode aproveitar o site de suporte para:

- Pesquisar documentos com informações de interesse
- Enviar e rastrear os casos de suporte e solicitações de aperfeiçoamentos
- Fazer download dos patches de software
- Gerenciar contratos de suporte
- Procurar contatos de suporte HP
- Revisar informações sobre os serviços disponíveis
- Participar de discussões com outros clientes de software
- Pesquisar e registrar-se para treinamentos de software

A maior parte das áreas de suporte exige que você se registre como usuário de um HP Passport e, em seguida, se conecte. Muitas também requerem um contrato de suporte ativo. Para se cadastrar e obter uma ID do HP Passport, acesse:

**http://h20229.www2.hp.com/passport-registration.html**

Para mais informações sobre níveis de acesso, vá para:

**http://h20230.www2.hp.com/new_access_levels.jsp**

**HP Software Solutions Now** acessa o site de portal HPSW Solution and Integration. Este site permite que você explore as páginas de HP Product Solutions, que inclui uma lista completa das integrações entre os produtos HP, bem como uma lista de processos ITIL. A URL para este site é **http://h20230.www2.hp.com/sc/solutions/index.jsp**

# Conteúdo

# Capítulo 1: Introdução à proteção

Este capítulo inclui:



# Visão geral da proteção

Esta seção apresenta o conceito de um aplicativo seguro do HP Universal CMDB e discute o planejamento e a arquitetura necessários para implementar a segurança. É extremamente recomendável que você leia esta seção antes de prosseguir para a discussão sobre proteção nas seções seguintes.

O HP Universal CMDB foi projetado para ser parte de uma arquitetura segura, podendo, portanto, enfrentar o desafio de lidar com as ameaças à segurança às quais pode ser exposto.

As diretrizes de proteção lidam com a configuração necessária para implementar um HP Universal CMDB mais seguro (protegido).

As informações de proteção fornecidas destinam-se principalmente aos administradores do HP Universal CMDB, que devem se familiarizar com as configurações e recomendações antes de iniciar os procedimentos de proteção.

É altamente recomendável que você use um proxy reverso com o HP Universal CMDB para obter uma arquitetura segura. Para ver detalhes sobre a configuração de um proxy reverso para uso com o HP Universal CMDB, consulte "Usando um proxy reverso" Na página38.

Se você deve usar outro tipo de arquitetura segura com o HP Universal CMDB que não seja o descrito neste documento, contate o Suporte ao Software HP para determinar qual arquitetura é a melhor para você usar.

Para ver detalhes sobre a proteção do Data Flow Probe, consulte "Proteção do Data Flow Probe" Na página71.

**Observação:**

- Os procedimentos de proteção baseiam-se na premissa de que você esteja implementando somente as instruções fornecidas nestes capítulos e que não esteja executando outras etapas de proteção documentadas em outro lugar.
- Nas situações em que os procedimentos de proteção se concentram em uma determinada arquitetura distribuída, isso não implica que essa seja a melhor arquitetura para as necessidades da sua organização.
- Pressupõe-se que os procedimentos incluídos nos capítulos a seguir sejam executados em computadores dedicados ao HP Universal CMDB. O uso dos computadores para outras finalidades além do HP Universal CMDB pode gerar resultados problemáticos.
- As informações de proteção fornecidas nesta seção não têm o objetivo de ser um guia para a realização de uma avaliação do risco à segurança dos seus sistemas informatizados.

# Preparações para proteção

- Avaliar o risco/estado de segurança da sua rede geral e usar as conclusões ao decidir como integrar o HP Universal CMDB à rede da melhor forma.
- Desenvolver uma boa compreensão da estrutura técnica do HP Universal CMDB e dos recursos de segurança do HP Universal CMDB.
- Examinar todas as diretrizes de proteção.
- Verificar se o HP Universal CMDB está totalmente funcional antes de iniciar os procedimentos de proteção.
- Seguir as etapas do procedimento de proteção cronologicamente em cada capítulo. Por exemplo, se você decidir configurar o servidor do HP Universal CMDB para suporte a SSL, leia "Habilitando comunicação SSL" Na página17 e depois siga todas as instruções cronologicamente.
- O HP Universal CMDB não fornece suporte para autenticação básica com senhas em branco. Não use uma senha em branco ao definir os parâmetros de conexão com autenticação básica.

**Dica:** imprima os procedimentos de proteção e vá conferindo-os à medida que forem sendo implementados.

# Implantando o UCMDB em uma arquitetura segura

Diversas medidas são recomendadas para implantar seus servidores do HP Universal CMDB de forma segura:

- **Arquitetura DMZ usando um firewall**

  A arquitetura segura mencionada neste documento é uma arquitetura DMZ típica usando um dispositivo como firewall. O conceito básico de tal arquitetura é criar uma separação completa e evitar acesso direto entre os clientes do HP Universal CMDB e o servidor do HP Universal CMDB.

- **Navegador seguro**

  O Internet Explorer e o Firefox em um ambiente Windows devem ser configurados para lidar com scripts Java, miniaplicativos e cookies de forma segura.

- **Protocolo de comunicação SSL**

  O protocolo SSL (Secure Sockets Layer) protege a conexão entre o cliente e o servidor. URLs que exigem uma conexão SSL usam uma versão segura do protocolo HTTP (HTTPS). Para obter detalhes, consulte "Habilitando comunicação SSL" Na página17.

- **Arquitetura de proxy reverso**

  Uma das soluções mais seguras e recomendadas sugere a implantação do HP Universal CMDB usando um proxy reverso. O HP Universal CMDB oferece total suporte para a arquitetura segura de proxy reverso. Para obter detalhes, consulte "Usando um proxy reverso" Na página38.

# Acesso ao Sistema

## Proteção ao acesso Java JMX

**Observação:** O procedimento descrito aqui também pode ser usado para o JMX do Data Flow Probe.

Para garantir que a porta RMI do JMX seja acessada somente ao fornecer credenciais do usuário, realize o seguinte procedimento:

1. No arquivo **wrapper.conf** do servidor, localizado em **C:\hp\UCMDB\UCMDBServer\bin**, defina o seguinte:

   **wrapper.java.additional.16=-Dcom.sun.management.jmxremote.authenticate=true**

   Essa configuração requer que o JMX solicite autenticação.

   - **Para o JMX do Data Flow Probe**, faça o seguinte:

     Nos arquivos **WrapperGateway.conf** e **WrapperManager.conf**, localizados em

**C:\hp\UCMDB\DataFlowProbe\bin**, defina o seguinte:

**wrapper.java.additional.17=-Dcom.sun.management.jmxremote.authenticate=true**

2. Renomeie o arquivo **jmxremote.password.template** (localizado em: **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) to **jmxremote.password**.

   **Observação:** Para o JMX do Data Flow Probe, esse arquivo está localizado em: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

3. Em **jmxremote.password**, adicione senhas para as funções **monitorRole** e **controlRole**.

   Por exemplo:

   **monitorRole QED**

   **controlRole R&D**

   atribuiria a senha **QED** a **monitorRole** e a senha **R&D** a **controlRole**.

   **Observação:** Verifique se apenas o proprietário tem permissões de gravação e leitura em **jmxremote.password**, uma vez que ele contém as senhas em texto claro. O proprietário do arquivo deve ser o mesmo usuário no qual o servidor do UCMDB está em execução.

4. No arquivo **jmxremote.access** (localizado em **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**), atribua acesso a **monitorRole** e **controlRole**.

   Por exemplo:

   **monitorRole readonly**

   **controlRole readwrite**

   atribuiria acesso de somente leitura a **monitorRole** e acesso somente de leitura-gravação a **controlRole**.

   **Observação:** Para o JMX do Data Flow Probe, esse arquivo está localizado em: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

5. Proteger arquivos da seguinte maneira:

   - **Apenas para Windows:** Execute os seguintes comandos na linha de comando para proteger arquivos:

**cacls jmxremote.password /P <username>:F**

**cacls jmxremote.access /P <username>:R**

onde **<nome de usuário>** é o proprietário do arquivo visível nas propriedades dos dois arquivos. Abra as propriedades desses arquivos e verifique se eles estão corretos e têm somente um proprietário.

- **Para sistemas operacionais Solaris e Linux:** Defina as permissões do arquivo para o arquivo de senha executando:

  **chmod 600 jmxremote.password**

6. **Para upgrades de Service Pack, migrações de servidor e recuperação de desastres:** Altere a propriedade do arquivo **jmxremote.access** (localizado em **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) para o usuário do sistema operacional que executa o upgrade ou a instalação da migração.

**Observação:**

- Para o JMX do Data Flow Probe, esse arquivo está localizado em: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.
- Antes de desinstalar o produto, edite as permissões do arquivo para **<pasta de instalação do UMCDB>\bin\jre\lib\management\jmxremote.password** para que o usuário com o qual você está conectado possa editá-lo.

# Alterando o nome de usuário ou senha do sistema para o console JMX

O console JMX utiliza usuários do sistema, ou seja, usuários de vários clientes em um ambiente multicliente. Você pode fazer logon no console JMX com qualquer nome de usuário do sistema. O nome de usuário e senha padrão são **sysadmin/sysadmin**.

Você altera a senha através do console JMX ou da ferramenta Gerenciamento de Servidor.

**Para alterar o nome de usuário ou senha do sistema padrão através do console JMX:**

1. inicie um navegador da Web e insira o seguinte endereço: **http://localhost.<nome_ domínio>:8080/jmx-console**.
2. Insira as credenciais de autenticação do console JMX.
3. Localize **UCMDB:service=Authorization Services** e clique no link para abrir a página Operations.
4. Localize a operação **resetPassword**.

- No campo **userName**, insira **sysadmin**.
- No campo **password**, insira uma nova senha.

5. Clique em **Invoke** para salvar a alteração.

**Para alterar o nome de usuário ou senha do sistema padrão através da ferramenta Gerenciamento de Servidor:**

1. **Para o Windows:** execute o seguinte arquivo: **C:\hp\UCMDB\UCMDBServer\tools\server_management.bat.**

   **Para o Linux:** Execute **server_management.sh**, localizado na seguinte pasta: **/opt/hp/UCMDB/UCMDBServer/tools/**.

2. Faça logon na ferramenta com as credenciais de autenticação: **sysadmin/sysadmin**.
3. Clique no link Usuários.
4. Selecione o usuário do sistema e clique em **Alterar senha para usuário conectado**.
5. Insira a senha antiga e a nova, e clique em **OK**.

# Alterando o usuário do serviço do servidor do HP Universal CMDB

Em uma plataforma Windows, o serviço do HP Universal CMDB, que executa todos os serviços e processos do HP Universal CMDB, é instalado quando você executa o utilitário Configuração de Servidor e Banco de Dados. Por padrão, esse serviço é executado sob o usuário do sistema local. Entretanto, você pode precisar atribuir um usuário diferente para executar o serviço (por exemplo, se estiver usando autenticação NTLM).

O usuário que você atribui para executar o serviço deve ter as seguintes permissões:

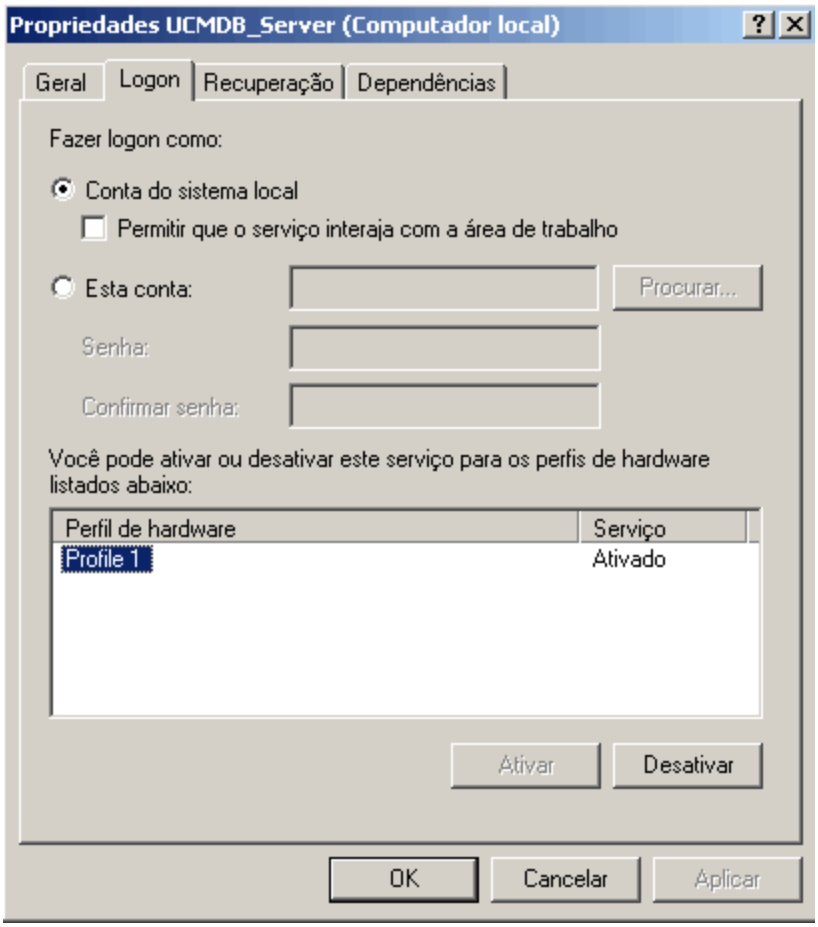
- permissões de banco de dados suficientes (conforme definido pelo administrador do banco de dados)
- permissões de rede suficientes
- permissões de administrador no servidor local

**Para alterar o usuário do serviço:**

1. Desabilite o HP Universal CMDB através do menu Iniciar (**Iniciar > Todos os Programas > HP UCMDB > Parar Servidor do HP Universal CMDB**) ou parando o serviço do Servidor do HP Universal CMDB. Para obter detalhes, consulte a seção que descreve como iniciar e parar o Serviço do Servidor UCMDB no *Guia de Administração do HP Universal CMDB*.

2. Na janela **Serviços** do Windows, clique duas vezes em **UCMDB_Server**. A caixa de diálogo **Propriedades do Servidor do UCMDB (Computador Local)** será aberta.

3. Clique na guia Logon.




4. Selecione **Esta conta** e navegue para escolher outro usuário na lista de usuários válidos no computador.

5. Insira a senha do Windows do usuário selecionado e confirme essa senha.

6. Clique em **Aplicar** para salvar suas configurações e em **OK** para fechar a caixa de diálogo.

7. Habilite o HP Universal CMDB através do menu Iniciar (**Iniciar > Todos os Programas > HP UCMDB > Iniciar Servidor do HP Universal CMDB**) ou iniciando o serviço do Servidor do HP Universal CMDB. Para obter detalhes, consulte a seção que descreve como iniciar e parar o Serviço do Servidor UCMDB no *Guia de Administração do HP Universal CMDB*.

# Criptografar a senha do banco de dados para o Configuration Manager

A senha do banco de dados do CM é armazenada no arquivo **<*Configuration_Manager_installation_directory*>\conf\database.properties**. Se desejar criptografar a senha, nosso algoritmo de criptografia padrão é compatível com os padrões de FIPS 140-2.

A criptografia é realizada por meio de uma chave, através da qual a senha é criptografada. A própria chave é então criptografada usando outra chave, conhecida como chave mestra. Ambas as chaves são criptografadas usando o mesmo algoritmo. Para ver detalhes sobre os parâmetros usados no processo de criptografia, consulte "Parâmetros para criptografia da senha do banco de dados para o Configuration Manager" abaixo.

**Cuidado:** se você modificar o algoritmo de criptografia, nenhuma das senhas criptografadas anteriormente poderá mais ser usada.

**Para modificar a criptografia da sua senha do banco de dados:**

1. Abra o arquivo **<*Configuration_Manager_installation_directory*>\conf\database.properties** e edite os campos a seguir:
   - **engineName.** Insira o nome do algoritmo de criptografia.
   - **keySize.** Insira o tamanho da chave mestra do algoritmo selecionado.
2. Execute o script **generate-keys.bat**, que cria o arquivo **<*Configuration_Manager_installation_directory*>\security\encrypt_repository** e gera a chave de criptografia.
3. Execute o utilitário **bin\encrypt-password.bat** para criptografar a senha. Defina o sinalizador **-h** para ver as opções disponíveis.
4. Copie o resultado do utilitário de criptografia da senha e cole a criptografia resultante no arquivo **conf\database.properties**.

# Parâmetros para criptografia da senha do banco de dados para o Configuration Manager

A tabela a seguir lista os parâmetros incluídos no arquivo **encryption.properties** usado para a criptografia da senha do banco de dados do CM. Para obter detalhes sobre a criptografia da senha do banco de dados, consulte "Criptografar a senha do banco de dados para o Configuration Manager" acima.

| Parâmetro | Descrição |
|---|---|
| cryptoSource | Indica a infraestrutura que implementa o algoritmo de criptografia. As opções disponíveis são:<br>• **lw.** Usa implementação leve da Bouncy Castle (opção padrão)<br>• **jce.** Aprimoramento da Criptografia Java (infraestrutura de criptografia Java padrão) |
| storageType | Indica o tipo do armazenamento de chave.<br>Atualmente, só há suporte para **arquivo binário**. |
| binaryFileStorageName | Indica o lugar no arquivo onde a chave mestra fica armazenada. |
| cipherType | O tipo da criptografia. Atualmente, só há suporte para **symmetricBlockCipher**. |
| engineName | O nome do algoritmo de criptografia.<br>As seguintes opções estão disponíveis:<br>• **AES.** American Encryption Standard. Esta criptografia é compatível com FIPS 140-2. (opção padrão)<br>• **Blowfish**<br>• **DES**<br>• **3DES.** (compatível com FIPS 140-2)<br>• **Nulo**. Sem criptografia |
| keySize | O tamanho da chave mestra. O tamanho é determinado pelo algoritmo:<br>• **AES.** 128, 192 ou 256 (a opção padrão é 256)<br>• **Blowfish.** 0-400<br>• **DES.** 56<br>• **3DES.** 156 |
| encodingMode | A codificação ASCII dos resultados da criptografia binária.<br>As seguintes opções estão disponíveis:<br>• **Base64** (opção padrão)<br>• **Base64Url**<br>• **Hexa** |

| Parâmetro | Descrição |
|---|---|
| algorithmModeName | O modo do algoritmo. Atualmente, só há suporte para **CBC**. |
| algorithmPaddingName | O algoritmo de preenchimento utilizado.<br>As seguintes opções estão disponíveis:<br>• **PKCS7Padding** (opção padrão)<br>• **PKCS5Padding** |
| jceProviderName | O nome do algoritmo de criptografia JCE.<br>**Observação:** Relevante apenas quando crytpSource é jce. Para lw, é usado engineName. |

# Capítulo 2: Habilitando comunicação SSL

Este capítulo inclui:



# Habilitar o SSL no computador servidor com um certificado autoassinado - UCMDB

Estas seções explicam como configurar o HP Universal CMDB para suporte a comunicação usando o canal SSL (Secure Sockets Layer).

1. **Pré-requisitos**

   a. Antes de iniciar o procedimento a seguir, remova o arquivo **server.keystore** antigo localizado em **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**.

   b. Coloque o repositório de chaves (tipo JKS) do HP Universal CMDB na pasta **C:\hp\UCMDB\UCMDBServer\conf\security**.

2. **Gerar um repositório de chaves de servidor**

   a. Crie um repositório de chaves (tipo JKS) com um certificado autoassinado e chave privada correspondente:

   - De **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**, execute o seguinte comando:

     ```
     keytool -genkey -alias hpcert -keystore
     C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
     ```

     A caixa de diálogo do console será aberta.

   - Insira a senha do repositório de chaves. Se a senha tiver sido alterada, execute a operação JMX **changeKeystorePassword** em **UCMDB:service=Security Services**. Se a senha não tiver sido alterada, use a senha **hppass** padrão.

   - Responda a pergunta **What is your first and last name?** Insira o nome do servidor Web do HP Universal CMDB. Insira os outros parâmetros de acordo com a sua organização.

   - Insira uma senha de chave. Ela DEVE ser igual à senha do repositório de chaves.

     Um repositório de chaves JKS chamado **server.keystore** será criado com um certificado de servidor chamado **hpcert**.

   **b.** Exporte o certificado autoassinado para um arquivo:

   De **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**, execute o seguinte comando:

   ```
   keytool -export -alias hpcert -keystore
   C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <sua
   senha> -file hpcert
   ```

3. **Colocar o certificado no repositório confiável do cliente**

   Após gerar o **server.keystore** e exportar o certificado de servidor, para cada cliente que precisar se comunicar com o HP Universal CMDB por SSL usando este certificado autoassinado, coloque o certificado nos repositórios confiáveis do cliente.

   **Observação:** só pode haver um certificado de servidor no **server.keystore**.

4. **Desabilitar a porta HTTP 8080**

   Para obter detalhes, consulte "Habilitar ou desabilitar portas HTTP/HTTPS" Na página31.

   **Observação:** verifique se a comunicação HTTPS funciona antes de fechar a porta HTTP.

5. **Reiniciar o servidor**

6. **Exibir HP Universal CMDB**

   Para verificar se o Servidor do UCMDB está seguro, insira a seguinte URL no navegador da Web: **https://<nome do servidor UCMDB ou endereço IP>:8443/ucmdb-ui**.

# Habilitar o SSL no computador servidor com um certificado autoassinado - Configuration Manager

Esta seção explica como configurar o Configuration Manager para suporte a autenticação e criptografia usando o canal SSL (Secure Sockets Layer).

O Configuration Manager usa o Tomcat 7.0.19 como servidor de aplicativos.

1. **Pré-requisitos** (não relevante se estiver instalando pela primeira vez)

   Antes de iniciar o procedimento a seguir, remova o arquivo **tomcat.keystore** antigo localizado na pasta **<*Configuration_Manager_installation_directory*>\java\windows\x86_64\lib\security** ou **<*Configuration_Manager_installation_directory*>\java\linux\x86_64\lib\security** (a que for relevante), se existir.

2. **Gerar um repositório de chaves de servidor**

   Crie um repositório de chaves (tipo JKS) com um certificado autoassinado e chave privada correspondente:

   - A partir de **<*Configuration_Manager_installation_directory*>\java\windows\x86_64\bin** ou **<*Configuration_Manager_installation_directory*>\java\linux\x86_64\bin**, execute o comando a seguir:

     ```
     keytool -genkey -alias tomcat -keyalg RSA -keystore ..\lib\
     security\tomcat.keystore
     ```

     A caixa de diálogo do console será aberta.

   - Insira a senha do repositório de chaves. Se a senha tiver sido alterada, altere-a manualmente no arquivo.

   - Responda a pergunta **What is your first and last name?** Insira o nome do servidor Web do Configuration Manager. Insira os outros parâmetros de acordo com a sua organização.

   - Insira uma senha de chave. Ela DEVE ser igual à senha do repositório de chaves.

     Um repositório de chaves JKS chamado **tomcat.keystore** será criado com um certificado de servidor chamado **hpcert**.

3. **Colocar o certificado no repositório confiável do cliente**

Adicione o certificado aos repositórios confiáveis do cliente no Internet Explorer no seu computador (**Ferramentas > Opções da Internet > Conteúdo > Certificados**). Se você não o fizer, será solicitado que o faça na primeira vez que tentar usar o Configuration Manager.

**Limitação**: só pode haver um certificado de servidor no **tomcat.keystore**.

4. **Modificar o arquivo server.xml**

   Abra o arquivo **server.xml**, localizado em **<*Configuration_Manager_installation_directory*>\servers\server-0\conf**. Localize a seção que começa com

   ```
   Connector port="8143"
   ```

   que aparece nos comentários. Ative o script removendo o caractere de comentário e adicione os seguintes atributos ao conector HTTPS:

   ```
   keystoreFile="<local do arquivo tomcat.keystore>" (ver etapa 2)
   keystorePass="<password>"
   ```

   Comente a seguinte linha:

   ```
   <Listener className="org.apache.catalina.core.AprLifecycleListener"
   SSLEngine="on" />
   ```

   **Observação:** você não deve bloquear a porta de conexão HTTP. Se você deseja bloquear a comunicação HTTP, pode usar um firewall para essa finalidade.

5. **Reiniciar o servidor**

   Reinicie o servidor do Configuration Manager.

6. **Verificar a segurança do servidor**

   Para verificar se o Servidor do Configuration Manager está seguro, insira a seguinte URL no navegador da Web: **https://<nome do servidor do Configuration Manager ou endereço IP>:8143/cnc**.

7. No Configuration Manager, vá até **Configurações > Gerenciamento de Aplicativo > Configurações de Email** e altere o protocolo e a porta na **URL completa do Configuration Manager**, de acordo com os valores acima.

8. No UCMDB, vá até **Gerenciador de Configurações de Infraestrutura > Configurações Gerais** e altere o protocolo e a porta na **URL do Configuration Manager**, de acordo com os valores acima.

**Dica:** se você não conseguir estabelecer uma conexão, tente usar um navegador diferente

ou atualizar para uma versão mais nova do navegador.

# Habilitar o SSL no computador servidor com um certificado de uma Autoridade de Certificação - UCMDB

Para usar um certificado emitido por uma Autoridade de Certificação (CA), o repositório de chaves deve estar em formato Java. O exemplo a seguir explica como formatar o repositório de chaves para um computador com Windows.

1. **Pré-requisitos**

   Antes de iniciar o procedimento a seguir, remova o arquivo **server.keystore** antigo localizado em **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**.

2. **Gerar um repositório de chaves de servidor**

   a. Gere um certificado assinado CA e instale-o no Windows.

   b. Exporte o certificado para um arquivo ***.pfx** (incluindo chaves privadas) usando o Console de Gerenciamento Microsoft (**mmc.exe**).

      Insira qualquer cadeia de caracteres como senha do arquivo **pfx**. (Essa senha será pedida quando você converter o tipo de repositório de chaves em um repositório de chaves JAVA.) O arquivo **.pfx** agora contém um certificado público e uma chave privada, e é protegido por senha.

   c. Copie o arquivo **.pfx** que você criou para a seguinte pasta: **C:\hp\UCMDB\UCMDBServer\conf\security**.

   d. Abra o prompt de comando e altere o diretório para **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**.

      Altere o tipo de repositório de chaves de **PKCS12** para um repositório de chaves **JAVA** executando o seguinte comando:

      ```
      keytool -importkeystore -srckeystore c:\hp\UCMDB\UCMDBServer\conf\securit
      y\<nome do arquivo pfx> -srcstoretype PKCS12 -destkeystore server.keystor
      e
      ```

      Será pedida a senha do repositório de chaves (**.pfx**) de origem. Essa é a senha que você forneceu ao criar o arquivo **pfx** na etapa b).

   e. Insira a senha do repositório de chaves de destino. Essa senha deverá ser igual à definida anteriormente no método JMX **changeKeystorePassword**, em Security Services. Se a

senha não tiver sido alterada, use a senha **hppass** padrão.

> **Observação:** A senha do repositório de chaves de origem deve ser igual à senha do repositório de chaves de destino.

f. Após gerar o certificado, desabilite a porta HTTP 8080. Para ver detalhes, consulte "Habilitar ou desabilitar portas HTTP/HTTPS" Na página31.

g. Se você usou uma senha que não seja **hppass** ou a senha usada para o arquivo **.pfx**, execute o método JMX **changeKeystorePassword** e verifique se a chave tem a mesma senha.

> **Observação:** verifique se a comunicação HTTPS funciona antes de fechar a porta HTTP.

3. **Reiniciar o servidor**

4. **Verificar a segurança do servidor**

   Para verificar se o Servidor do UCMDB está seguro, insira a seguinte URL no navegador da Web: **https://<nome do servidor UCMDB ou endereço IP>:8443/ucmdb-ui**.

> **Cuidado:** só pode haver um certificado de servidor no **server.keystore**.

# Habilitar o SSL no computador servidor com um certificado de uma Autoridade de Certificação - Configuration Manager

No Configuration Manager, para usar um certificado emitido por uma Autoridade de Certificação (CA), o repositório de chaves deve estar em formato Java. O exemplo a seguir explica como formatar o repositório de chaves para um computador com Windows.

1. **Pré-requisitos**

   Antes de iniciar o procedimento a seguir, remova o arquivo **tomcat.keystore** antigo localizado na pasta **<*Configuration_Manager_installation_directory*>\java\windows\x86_64\lib\security** ou no **<diretório de instalação do Configuration Manager>\java\linux\x86_64\lib\security** (o que for relevante), se existir.

2. **Gerar um repositório de chaves de servidor**

a. Gere um certificado assinado CA e instale-o no Windows.

b. Exporte o certificado para um arquivo ***.pfx** (incluindo chaves privadas) usando o Console de Gerenciamento Microsoft (**mmc.exe**).

   Insira qualquer cadeia de caracteres como senha do arquivo **pfx**. (Essa senha será pedida quando você converter o tipo de repositório de chaves em um repositório de chaves JAVA.)
   O arquivo **.pfx** agora contém um certificado público e uma chave privada, e é protegido por senha.

   Copie o arquivo **.pfx** que você criou para a seguinte pasta: **<*Configuration_Manager_installation_directory*>\java\lib\security**.

c. Abra o prompt de comando e altere o diretório para **<*Configuration_Manager_installation_directory*>\java\bin**.

   Altere o tipo de repositório de chaves de **PKCS12** para um repositório de chaves **JAVA** executando o seguinte comando:

   ```
   keytool -importkeystore -srckeystore <Configuration_Manager_installation_directory>\conf\security\<nome do arquivo pfx> -srcstoretype PKCS12 -dest keystore tomcat.keystore
   ```

   Será pedida a senha do repositório de chaves (**.pfx**) de origem. Esta é a senha fornecida na criação do arquivo pfx na etapa b.

3. **Modificar o arquivo server.xml**

   Abra o arquivo **server.xml**, localizado em **<*Configuration_Manager_installation_directory*>\servers\server-0\conf**. Localize a seção que começa com

   ```
   Connector port="8143"
   ```

   que aparece nos comentários. Ative o script removendo o caractere de comentário e adicione as seguintes duas linhas:

   ```
   keystoreFile="../../java/lib/security/tomcat.keystore"
   keystorePass="password" />
   ```

   Comente a seguinte linha:

   ```
   <Listener className="org.apache.catalina.core.AprLifecycleListener"
   SSLEngine="on" />
   ```

   **Observação:** você não deve bloquear a porta de conexão HTTP. Se você deseja bloquear a comunicação HTTP, pode usar um firewall para essa finalidade.

4. **Reiniciar o servidor**

   Reinicie o servidor do Configuration Manager.

5. **Verificar a segurança do servidor**

   Para verificar se o servidor do Configuration Manager está seguro, insira a seguinte URL no navegador da Web: **https://<nome do servidor do Configuration Manager ou endereço IP>:8143/cnc**.

6. No Configuration Manager, vá até **Configurações > Gerenciamento de Aplicativo > Configurações de Email** e altere o protocolo e a porta na **URL completa do Configuration Manager**, de acordo com os valores acima.

7. No UCMDB, vá até **Gerenciador de Configurações de Infraestrutura > Configurações Gerais** e altere o protocolo e a porta na **URL do Configuration Manager**, de acordo com os valores acima.

**Limitação**: só pode haver um certificado de servidor no **tomcat.keystore**.

# Habilitar SSL nos computadores cliente - UCMDB

Se o certificado usado pelo servidor Web do HP Universal CMDB for emitido por uma Autoridade de Certificação (CA) conhecida, é bem provável que seu navegador da Web possa validar o certificado sem nenhuma ação adicional.

Se o CA não for confiável para o navegador da Web, você deverá importar o caminho confiável do certificado inteiro ou importar o certificado usado pelo HP Universal CMDB explicitamente para o repositório confiável do navegador.

O exemplo a seguir demonstra como importar o certificado **hpcert** autoassinado para o repositório confiável do Windows para ser usado pelo Internet Explorer.

**Para importar um certificado para o repositório confiável do Windows:**

1. Localize e renomeie o certificado **hpcert** como **hpcert.cer**.

   No Windows Explorer, o ícone mostra que o arquivo é um certificado de segurança.

2. Clique duas vezes em **hpcert.cer** para abrir a caixa de diálogo Certificado do Internet Explorer .

3. Siga as instruções para habilitar a confiabilidade instalando o certificado com o Assistente de Importação de Certificado.

**Observação:** Outro método de importar o certificado emitido pelo Servidor do UCMDB para o navegador da Web é fazer logon no UCMDB e instalar o certificado quando o aviso de certificado não confiável é exibido.

# Habilitar o SSL com um certificado de cliente - Configuration Manager

Se o certificado usado pelo servidor Web do Configuration Manager for emitido por uma Autoridade de Certificação (CA) conhecida, é bem provável que seu navegador da Web possa validar o certificado sem nenhuma ação adicional.

Se o CA não for confiável no repositório confiável do servidor, importe o certificado CA para o repositório confiável do servidor.

O exemplo a seguir demonstra como importar o certificado **hpcert** autoassinado para o repositório confiável do servidor (cacerts).

Para importar um certificado para o repositório confiável do servidor:

1. No computador cliente, localize e renomeie o certificado **hpcert** como **hpcert.cer**.
2. Copie **hpcert.cer** para o computador servidor na pasta **<*Configuration_Manager_installation_directory*>\java\windows\x86_64bin**.
3. No computador servidor, importe o certificado CA para o repositório confiável (cacerts) usando o utilitário keytool com o seguinte comando:

   ```
   <Configuration_Manager_installation_directory>\java\bin\keytool.exe -import
   -alias hp -file hpcert.cer -keystore ..\lib\security\cacerts
   ```

4. Modifique o arquivo **server.xml** (localizado na pasta **<*Configuration_Manager_installation_directory*>\servers\server-0\conf**) como se segue:

   a. Faça as alterações descritas em "Modificar o arquivo server.xml" Na página23.

   b. Imediatamente após essas alterações, adicione os seguintes atributos ao conector HTTPS:

   ```
   truststoreFile="../../java/lib/security/cacerts"
   truststorePass="changeit" />
   ```

   c. Defina `clientAuth="true"`.

5. Verifique a segurança do servidor conforme descrito em "Verificar a segurança do servidor" Na página anterior.

# Habilitar SSL no SDK do cliente

Você pode utilizar transporte HTTPS entre o SDK do cliente e o SDK do servidor:

1. No computador cliente, no produto que incorpora o SDK do cliente, localize a configuração de transporte e verifique se ele está configurado para HTTPS e não HTTP.

2. Baixe o certificado CA/certificado público autoassinado no computador cliente e importe-o para o repositório confiável **cacerts** no JRE que vai se conectar ao servidor.

   Use o seguinte comando:

   ```
   Keytool -import -alias <nome do CA> -trustcacerts -file <caminho do certific
   ado público do servidor> -keystore <caminho para o repositório cacerts confi
   ável do jre cliente (ex. x:\arquivos de programas\java\jre\lib\security\cace
   rts)>
   ```

# Habilitar a autenticação de certificado mútua para o SDK

Este modo usa SSL e habilita tanto a autenticação do servidor pelo UCMDB quanto a autenticação do cliente pelo cliente UCMDB-API. Tanto o servidor quanto o cliente UCMDB-API enviam seus certificados para a outra entidade para autenticação.

**Observação:** o método a seguir de habilitar SSL no SDK com autenticação mútua é o mais seguro e é, portanto, o modo de comunicação recomendado.

1. Proteger o conector do cliente UCMDB-API no UCMDB:

   a. Acesse o console JMX do UCMDB: inicie um navegador da Web e insira o seguinte endereço: **http://<nome do computador com UCMDB ou endereço IP>:8080/jmx-console**. Você pode precisar fazer logon com um nome de usuário e senha (o padrão é sysadmin/sysadmin).

   b. Localize **UCMDB:service=Ports Management Services** e clique no link para abrir a página Operations.

   c. Localize a operação **PortsDetails** e clique em **Invoke**. Tome nota do HTTPS com número da porta de autenticação do cliente. O padrão é 8444 e deve estar habilitada.

   d. Retorne à página Operations.

   e. Para mapear o conector do ucmdb-api para o modo de autenticação mútua, invoque o método **mapComponentToConnectors** com os seguintes parâmetros:

      - **componentName**: ucmdb-api
      - **isHTTPSWithClientAuth**: true
      - Todos os outros sinalizadores: false

A seguinte mensagem será exibida:

**Operation succeeded. Component ucmdb-api is now mapped to: HTTPS_CLIENT_AUTH ports.**

f. Retorne à página Operations.

2. Verifique se o JRE que executa o cliente UCMDB-API tem um repositório de chaves contendo um certificado de cliente.

3. Exporte o certificado do cliente UCMDB-API de seu repositório de chaves.

Importe o certificado do cliente UCMDB-api exportado para o repositório confiável do Servidor do UCMDB.

4. (missing or bad snippet)

5. Exporte o certificado do servidor do UCMDB do repositório de chaves do servidor.

a. No computador com o UCMDB, execute o seguinte comando:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert
-keystore
C:\HP\UCMDB\UCMDBServer\conf\security\server.keystore
-file C:\HP\UCMDB\conf\security\server.cert
```

b. Insira a senha do repositório confiável do Servidor do UCMDB (o padrão é **hppass**).

c. Verifique se o certificado foi criado no seguinte diretório:

**C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

6. Importe o certificado do UCMDB exportado para o JRE do repositório confiável do cliente UCMDB-API.

7. Reinicie o Servidor do UCMDB e o cliente UCMDB-API.

8. Para conectar do cliente UCMDB-API para o servidor UCMDB-API, use o seguinte código:

```
UcmdbServiceProvider provider = UcmdbServiceFactory.getServiceProvider
("https", <SOME_HOST_NAME>, <HTTPS_WITH_CLIENT_AUTH_PORT_NUMBER
(default:8444>));
UcmdbService ucmdbService = provider.connect(provider.createCertificateCrede
ntials(<TheClientKeystore.
por exemplo: "c:\\client.keystore">, <KeystorePassword>), provider.createCli
entContext(<ClientIdentification>));
```

# Configurar suporte CAC no UCMDB

Esta seção descreve como configurar o suporte a CAC (Common Access Card) no UCMDB.

**Observação:** O suporte CAC só está disponível ao usar o Internet Explorer 8, 9 ou 10.

1. Importe o CA raiz e qualquer certificado intermediário para o repositório confiável do Servidor UCMDB como a seguir:

   a. No computador com o UCMDB, copie os arquivos do certificado para o seguinte diretório no UCMDB:

   **C:\HP\UCMDB\UCMDBServer\conf\security**

   **Observação:** Se seu certificado está em formato Microsoft p7b, você pode precisar convertê-lo em formato PEM.

   b. Para cada certificado, execute o seguinte comando:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore
   C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file
   <certificate> - alias <certificate alias>
   ```

   c. Insira a senha do repositório confiável do Servidor do UCMDB (o padrão é **hppass**).

   d. Quando for perguntado **Trust this certificate?**, pressione **y** e depois **Enter**.

   e. Certifique-se de que **Certificate** produzido tenha sido adicionado ao repositório de chaves.

2. Abra o console JMX iniciando o navegador da Web e insira o endereço do servidor, da seguinte maneira: http://<Nome de Host do Servidor do UCMDB ou IP>:8080/jmx-console.

   Você pode precisar fazer logon com um nome de usuário e senha.

3. Em UCMDB, clique em **UCMDB:service=Ports Management Services** para abrir a página Operations.

   - (opcional) Clique em **ComponentsConfigurations**. Siga este procedimento:
     - Defina **HTTPSSetPort** como **8444** e clique em **Invoke**.
     - Clique em **Back to MBean**.
   - Clique em **mapComponentToConnectors**. Siga este procedimento:
     - No serviço mapComponentToConnectors, defina **componentName** como **ucmdb-ui**.
     - Defina apenas **isHTTPSWithClientAuth** como **true** e clique em **Invoke**.
     - Clique em **Back to MBean**.

- No serviço mapComponentToConnectors, defina **componentName** como **root**.
- Defina apenas **isHTTPSWithClientAuth** como **true** e clique em **Invoke**.

4. Em UCMDB, clique em **UCMDB:service=Security Services** para abrir a página Operations. No serviço **loginWithCAC**, faça o seguinte:
   - Defina **loginWithCAC** como **true** e clique em **Invoke**.
   - Clique em **Back to MBean**.
   - (opcional) Clique em **usernameField** para especificar o campo do certificado que será usado pelo UCMDB para extrair um nome de usuário e clique em **Invoke**.

     **Observação:** Se você não especificar um campo, o padrão de PRINCIPAL_NAME_ FROM_SAN_FIELD será usado.

   - Clique em **Back to MBean**.
   - Clique em **pathToCRL** para definir um caminho para uma CRL (Lista de Revogação de Certificado) offline a ser usada se a lista online (do certificado) não estiver disponível e clique em **Invoke**.

     **Observação:** Quando você está trabalhando com uma CRL local e há uma conexão de Internet em funcionamento com o servidor do UCMDB, a CRL local é usada. A validação de qualquer certificado (mesmo se não for revogada) falha nas seguintes situações:

     - se o caminho da CRL estiver definido, mas o arquivo da CRL em si estiver faltando
     - se o CRL estiver expirado
     - se o CRL tem uma assinatura incorreta

     Se você não definir o caminho para uma CRL offline e o servidor do UCMDB não puder acessar a CRL online, todos os certificados que contêm uma CRL ou URL OCSP são rejeitados (pois a URL não pode ser acessada, a verificação de revogação falha). Para dar ao servidor do UCMDB acesso à Internet, retire o comentário das seguintes linhas no arquivo **wrapper.conf** e forneça uma porta e um proxy válido:

     ```
     #wrapper.java.additional.40=-Dhttp.proxyHost=<PROXY_ADDR>
     #wrapper.java.additional.41=-Dhttp.proxyPort=<PORT>
     #wrapper.java.additional.42=-Dhttps.proxyHost=<PROXY_ADDR>
     #wrapper.java.additional.43=-Dhttps.proxyPort=<PORT>
     ```

   - Clique em **Back to MBean**.

- (opcional) Defina **onlyCACCerts** como **true** e clique em **Invoke**.

  Defina essa operação como **true** para aceitar apenas certificados que acompanham um dispositivo CAC físico.

Agora você deve poder fazer logon no UCMDB com https://<IP ou Nome do Host do Servidor UCMDB>.<domainname>:8444.

5. Configure o UCMDB para usar autenticação LW-SSO e reinicie o servidor do UCMDB.

Para ver detalhes sobre autenticação LW-SSO, consulte "Habilitando logon no HP Universal CMDB com LW-SSO" Na página98.

# Alterar a senha do repositório de chaves do servidor

Após instalar o Servidor, a porta HTTPS é aberta e o repositório é protegido com uma senha fraca (o padrão é **hppass**). Se você pretende trabalhar somente com SSL, deve alterar a senha.

O procedimento a seguir explica como alterar apenas a senha do **server.keystore**. Entretanto, você deve executar o mesmo procedimento para alterar a senha do **server.truststore**.

**Observação:** Você deve executar todas as etapas deste procedimento.

1. Inicie o Servidor do UCMDB.
2. Execute a alteração de senha no console JMX:
   a. Inicie o navegador da Web e insira o endereço do Servidor, da seguinte maneira: **http://<Nome de Host do Servidor do UCMDB ou IP>:8080/jmx-console**.

      Você pode precisar fazer logon com um nome de usuário e senha.

   b. No UCMDB, clique em **UCMDB:service=Security Services** para abrir a página Operations.

   c. Localize e execute a operação **changeKeystorePassword**.

      Esse campo não deve ficar vazio e deve ter pelo menos seis caracteres. A senha é alterada apenas no banco de dados.
3. Pare o Servidor do UCMDB.
4. Execute os comandos.

   De **C:\hp\UCMDB\UCMBServer\bin\jre\bin**, execute os seguintes comandos:

a. Altere a senha do repositório:

**keytool -storepasswd -new <new_keystore_pass> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <current_ keystore_pass>**

b. O seguinte comando exibe a chave interna do repositório de chaves. O primeiro parâmetro é o alias. Salve esse parâmetro para o comando seguinte:

**keytool -list -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**

c. Altere a senha da chave (se o repositório não estiver vazio):

**keytool -keypasswd -alias <alias> -keypass <currentPass> -new <newPass> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**

d. Digite a nova senha.

5. Inicie o Servidor do UCMDB.

6. Repita o procedimento para o repositório confiável do Servidor.

# Habilitar ou desabilitar portas HTTP/HTTPS

Você pode habilitar ou desabilitar as portas HTTP e HTTPS a partir da interface do usuário ou do console JMX.

Para habilitar ou desabilitar as portas HTTP/HTTPS a partir da interface do usuário:

1. Faça logon no HP Universal CMDB.

2. Selecione **Administração > Configurações de Infraestrutura**.

3. Insira **http** ou **https** na caixa **Filtro** (por Nome) para exibir as configurações de HTTP.

   - **Habilitar conexões HTTPS**. **Verdadeiro**: a porta está habilitada. **Falso**: a porta está desabilitada.

4. Reinicie o servidor para aplicar a alteração.

**Cuidado:** a porta HTTPS fica aberta por padrão; fechá-la impede o funcionamento do **Server_Management.bat**.

**Para habilitar ou desabilitar as portas HTTP/HTTPS a partir do console JMX:**

1. inicie um navegador da Web e insira o seguinte endereço: http://localhost.<nome_ domínio>:8080/jmx-console.

2. Insira as credenciais de autenticação do console JMX. As credenciais padrão são:
   - Nome de logon = **sysadmin**
   - Senha = **sysadmin**
3. Localize **UCMDB:service=Ports Management Services** e clique no link para abrir a página Operations.
4. Para habilitar ou desabilitar a porta HTTP, localize a operação **HTTPSetEnable** e defina o valor.
   - **True:** a porta está habilitada.
   - **False:** a porta está desabilitada.
5. Para habilitar ou desabilitar a porta HTTPS, localize a operação **HTTPSSetEnable** e defina o valor.
   - **True:** a porta está habilitada.
   - **False:** a porta está desabilitada.
6. Para habilitar ou desabilitar a porta HTTPS com autenticação do cliente, localize a operação **HTTPSClientAuthSetEnable** e defina o valor.
   - **True:** a porta está habilitada.
   - **False:** a porta está desabilitada.

# Mapear os componentes da Web do UCMDB para as portas

Você pode configurar o mapeamento de cada componente do UCMDB para as portas disponíveis a partir do console JMX.

**Para exibir as configurações atuais dos componentes:**

1. inicie um navegador da Web e insira o seguinte endereço: **http://localhost.<nome_ domínio>:8080/jmx-console**.
2. Insira as credenciais de autenticação do console JMX. As credenciais padrão são:

   Nome de logon = **sysadmin**

   Senha = **sysadmin**

3. Localize **UCMDB:service=Ports Management Services** e clique no link para abrir a página Operations.

4. Localize o método **ComponentsConfigurations** e clique em **Invoke**.

5. Para cada componente, as portas válidas e as portas mapeadas atuais serão exibidas.

**Para mapear os componentes:**

1. Localize **UCMDB:service=Ports Management Services** e clique no link para abrir a página Operations.

2. Localize o método **mapComponentToConnectors**.

3. Insira o nome de um componente na caixa Value. Selecione **True** ou **False** para cada uma das portas correspondente à sua seleção. Clique em **Invoke**. O componente selecionado será mapeado para as portas selecionadas. Você pode encontrar os nomes dos componentes invocando o método **serverComponentsNames**.

4. Repita o processo para cada componente relevante.

**Observação:**

- Cada componente deve estar mapeado para pelo menos uma porta. Se você não mapear um componente para nenhuma porta, ele será mapeado para a porta HTTP.
- Se você mapear um componente para a porta HTTPS e para a porta HTTPS com autenticação do cliente, somente a opção de autenticação do cliente será mapeada (a outra opção será redundante nesse caso).
- Se você definir **isHTTPSWithClientAuth** como **Verdadeiro** para o componente de interface do usuário do UCMDB, você também deverá defini-lo como **Verdadeiro** para o componente raiz.

Você também pode alterar o valor atribuído para cada uma das portas.

**Para definir valores para as portas:**

1. Localize **UCMDB:service=Ports Management Services** e clique no link para abrir a página Operations.

2. Para definir um valor para a porta HTTP, localize o método **HTTPSetPort** e insira um valor na caixa **Value**. Clique em **Invoke**.

3. Para definir um valor para a porta HTTPS, localize o método **HTTPSSetPort** e insira um valor na caixa **Value**. Clique em **Invoke**.

4. Para definir um valor para a porta HTTPS com autenticação do cliente, localize o método **HTTPSClientAuthSetPort** e insira um valor na caixa **Value**. Clique em **Invoke**.

# Configurar o Configuration Manager para funcionar com o UCMDB usando SSL

Você pode configurar o Configuration Manager para funcionar com o UCMDB usando SSL (Secure Sockets Layer). O conector SSL na porta 8443 é habilitado por padrão no UCMDB.

1. Vá para **<diretório de instalação do UCMDB>\bin\jre\bin** e execute o seguinte comando:

   ```
   keytool -export -alias hpcert -keystore <UCMDB_server_directory>
   \conf\security\server.keystore -storepass hppass -file <certificatefile>
   ```

2. Copie o arquivo de certificado para um local temporário no computador local com Configuration Manager.

3. Realize uma nova instalação ou reconfigure uma instalação existente do Configuration Manager. Para obter instruções, consulte as seções relevantes no *Guia de Implantação do HP Universal CMDB* interativo.

   Na tela de configuração do UCMDB, defina o protocolo como HTTPS e escolha o arquivo de certificado que você copiou na etapa 2.

4. Copie **hpcert.cer** para o computador servidor na pasta **<*Configuration_Manager_installation_directory*>\java\windows\x86_64\bin**.

5. No computador servidor, importe o certificado para o repositório confiável (cacerts) usando o utilitário keytool com o seguinte comando:

   ```
   <Configuration_Manager_installation_directory>\java\bin\keytool.exe -import -
   alias hp -file hpcert.cer -keystore <Configuration_Manager_installation_
   directory>\java\windows\x86_64\lib\security\cacerts
   ```

6. Copie **hpcert.cer** para o computador servidor na pasta **<*Configuration_Manager_installation_directory*>\java\ windows\x86_64\lib\security**.

7. Crie um repositório de chaves de servidor (tipo JKS) com um certificado autoassinado e chave privada correspondente. **A partir da pasta <*Configuration_Manager_installation_directory*>\java\windows\x86_64\bin**, execute o seguinte comando:

   ```
   keytool –genkey –alias tomcat –keyalg RSA –keystore <Configuration_Manager_i
   nstallation_directory>\java\windows\x86_64\lib\security\tomcat.keystore
   ```

   a. Insira uma senha do repositório de chaves.

   b. Para a questão: `Qual o seu nome e sobrenome?`, insira o nome do servidor web do Configuration Manager e insira os outros parâmetros de acordo com a sua organização.

c. Insira uma senha de chave. Ela DEVE ser igual à senha do repositório de chaves. Um repositório de chaves JKS chamado **tomcat.keystore** será criado com um certificado de servidor chamado **hpcert**.

8. Modificar o arquivo **server.xml** como a seguir:

   a. Abra o arquivo server.xml, localizado na pasta ***<Configuration_Manager_installation_directory>*\servers\server-0\conf**. Localize a seção que começa com:

   ```
   Connector port="8143"
   ```

   exibido como comentário. Ative o script removendo o caractere de comentário e adicione as seguintes linhas:

   ```
   keystoreFile="<Configuration_Manager_installation_directory>\java\windows
   \x86_64\lib\security\tomcat.keystore"
   keystorePass="password"
   truststoreFile="<Configuration_Manager_installation_directory>\java\windo
   ws\x86_64\lib\security\cacerts"
   truststorePass="changeit" />
   ```

   b. Comente a seguinte linha:

   ```
   <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEn
   gine="on" />
   ```

9. Reinicie o servidor.

Para configurar o Configuration Manager para funcionar com outros produtos (como balanceadores de carga) usando SSL, importe o certificado de segurança do produto para o repositório confiável do Configuration Manager (repositório confiável jre padrão) executando o seguinte comando:

```
<CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias <alias> -keystore
<CM_JAVA_HOME>\lib\security\cacerts -storepass changeit -file <certificatefile>
```

# Habilitar o adaptador de KPI do UCMDB para ser usado com SSL

Você pode configurar as informações do adaptador de KPI do UCMDB para serem enviadas usando SSL (Secure Sockets Layer).

1. Exportar o certificado do Configuration Manager:

   ```
   <CM_JAVA_HOME>\bin\keytool -export -alias tomcat -keystore
   <CM_JAVA_HOME>\lib\security\tomcat.keystore -storepass
   <keystore pass> -file <nome do arquivo de certificado>
   ```

2. Importe o certificado que você exportou do Configuration Manager para o repositório confiável

do UCMDB como a seguir:

```
<diretório do servidor UCMDB>\bin\jre\bin keytool -import -trustcacerts
-alias tomcat -keystore <diretório do servidor UCMDB>\bin\jre\lib
\security\cacerts -storepass changeit -file <certificatefile>
```

3. Importe o certificado que você exportou do Configuration Manager para o repositório confiável da sonda como a seguir:

   a. Abra o prompt de comando e execute o comando:

   ```
   <DataFlowProbe dir>\bin\jre\bin\keytool.exe -import -v -keystore
   <DataFlowProbe dir>\conf\security\hpprobeTrustStore.jks -file
   <certificatefile> -alias tomcat
   ```

   b. Insira a senha do repositório de chaves: logomania

   c. Quando for perguntado **Trust this certificate?**, pressione **y** e depois **Enter**.

   A seguinte mensagem será exibida:

   **Certificado adicionado ao repositório de chaves.**

   Para ver detalhes sobre a proteção do Data Flow Probe, consulte "Proteção do Data Flow Probe" Na página71.

4. Reiniciar o UCMDB, o Data Flow Probe e o Configuration Manager.

# Configurar o suporte SSL para o navegador do UCMDB

**Observação:** As instruções fornecidas aqui são relevantes para o Navegador do UCMDB versão 1.95. Se estiver usando uma versão posterior do Navegador do UCMDB que recebeu upgrade separadamente do resto do conjunto do produto UCMDB, consulte a seção sobre como configurar o suporte a SSL no *Guia de Instalação e Configuração do Navegador do HP Universal CMDB* daquela versão.

**Para instalar e configurar o suporte SSL no Tomcat:**

1. Crie um arquivo do repositório de chaves para armazenar a chave privada do servidor e o certificado autoassinado executando um dos seguintes comandos:

- Para o Windows: **%JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA**
- Para Unix: **$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA**

Para os dois comandos, use o valor de senha **changeit** (para todos os outros campos da caixa de diálogo do console aberta, você pode usar qualquer valor).

2. Remova comentários da entrada **SSL HTTP/1.1 Connector** em **$CATALINA_BASE/conf/server.xml**, onde **$CATALINA_BASE** é o diretório no qual você instalou o Tomcat.

   **Observação:** Para uma descrição completa de como configurar **server.xml** para usar SSL, consulte o site oficial do Apache Tomcat: http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html

3. Reinicie o servidor Tomcat.

**Para usar o protocolo HTTPS para conexão ao servidor UCMDB:**

1. Em **ucmdb_browser_config.xml**, atribua o valor **https** à tag **<protocol>** e atribua o valor da porta HTTPS do servidor do UCMDB (8443 por padrão) à tag **<port>.**

2. Baixe o certificado público do Servidor UCMDB à máquina do Navegador do UCMDB (se usar SSL no Servidor UCMDB, o administrador do UCMDB poderá fornecer a você esse certificado) e importe-o para o repositório confiável **cacerts** no JRE que vai se conectar ao servidor, executando o seguinte comando:

   **"%JAVA_HOME%\bin\keytool" -import -alias ucmdb -trustcacerts -file <UCMDB-Server-certificate-file> -keystore "%JAVA_HOME%\jre\lib\security\cacerts"**

   onde **<UCMDB-Server-certificate-file>** é o caminho completo para o arquivo do certificado público do Servidor UCMDB.

3. Reinicie o servidor Tomcat.

# Capítulo 3: Usando um proxy reverso

Esta seção descreve as ramificações de segurança dos proxies reversos e contém instruções para usar um proxy reverso com o HP Universal CMDB e o Configuration Manager. Os aspectos de segurança de um proxy reverso são discutidos, mas não outros aspectos como armazenamento em cache e balanceamento de carga.

Este capítulo inclui:



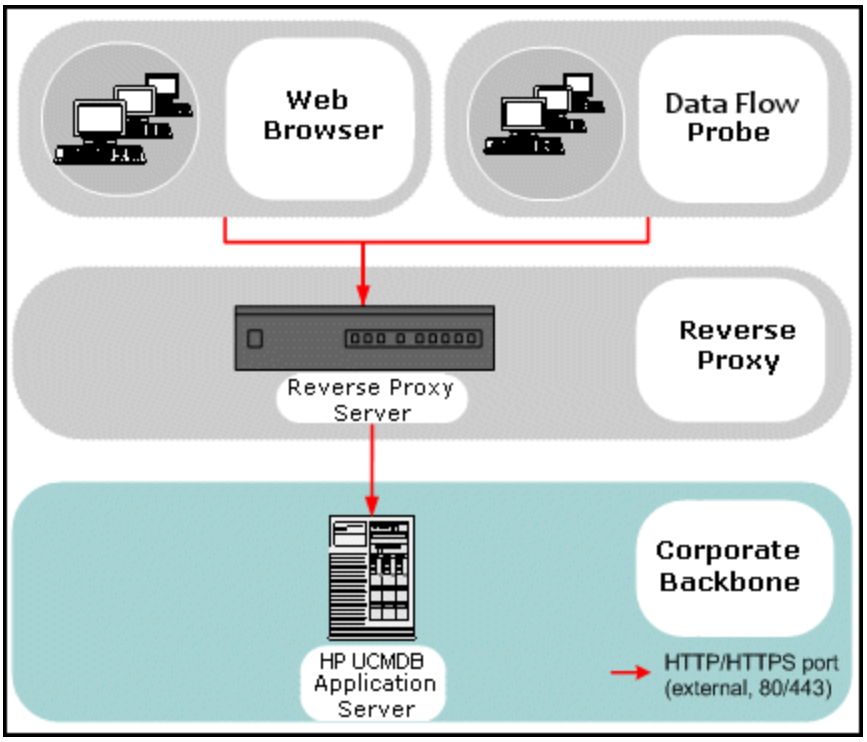
# Visão geral do proxy reverso

Um proxy reverso é um servidor intermediário que fica posicionado entre o computador cliente e os servidores Web. Para o computador cliente, o proxy reverso parece ser um servidor Web padrão que atende às solicitações de protocolo HTTP do computador cliente.

O computador cliente envia solicitações comuns de conteúdo da Web, usando o nome do proxy reverso em vez do nome de um servidor Web. O proxy reverso envia a solicitação para um dos servidores Web. Embora a resposta seja enviada de volta ao computador cliente pelo proxy reverso, ela aparece para o computador cliente como se estivesse sendo enviada pelo servidor Web.

É possível ter vários proxies reversos com diferentes URLs, representando a mesma instância do UCMDB/CM. Como alternativa, um único servidor de proxy reverso podpe ser usado para acessar vários servidores do UCMDB/CM, definindo contextos-raízes diferentes para cada servidor UCMDB/CM.

O HP Universal CMDB e o Configuration Manager suportam um proxy reverso em uma arquitetura DMZ. O proxy reverso é um mediador de HTTP entre o Data Flow Probe e o cliente Web e o servidor do HP Universal CMDB/CM.




**Observação:**

- Tipos diferentes de proxies reversos exigem sintaxes de configuração diferentes. Para ver um exemplo de configuração de proxy reverso do Apache 2.0.x, consulte "Exemplo: Configuração do Apache 2.0.x" Na página41.
- Somente é necessário definir a configuração da URL front-end ao criar um vínculo direto para um relatório usando o programador.

# Aspectos de segurança do uso de um servidor proxy reverso

Um servidor proxy reverso funciona como um bastion host. O proxy é configurado para ser o único computador endereçado diretamente pelos clientes externos, obscurecendo assim o resto da rede interna. O uso de um proxy reverso permite que o servidor de aplicativos seja colocado em um computador separado na rede interna.

Esta seção discute o uso de um DMZ e um proxy reverso em um ambiente de topologia back-to-back.

Estas são as principais vantagens relacionadas à segurança de usar um proxy reverso em tal ambiente:

- Não ocorre conversão de protocolo DMZ. O protocolo de entrada e o de saída são idênticos (ocorre apenas uma alteração de cabeçalho).
- Somente o acesso HTTP ao proxy reverso é permitido, o que significa que os firewalls de inspeção de pacotes com estado podem proteger melhor a comunicação.
- Um conjunto estático e restrito de requisições de redirecionamento pode ser definido no proxy reverso.
- A maioria dos recursos de segurança do servidor Web estão disponíveis no proxy reverso (métodos de autenticação, criptografia etc.).
- O proxy reverso faz uma triagem dos endereços IP dos servidores reais, bem como da arquitetura da rede interna.
- O único cliente acessível do servidor Web é o proxy reverso.
- Essa configuração fornece suporte para firewalls NAT (ao contrário das demais soluções).
- O proxy reverso requer um número mínimo de portas abertas no firewall.
- O proxy reverso oferece um bom desempenho em comparação com outras soluções de bastion.

# Configurar um proxy reverso

Esta seção descreve como configurar um proxy reverso. Desde o UCMDB versão 10.01, nenhuma configuração é necessária no UCMDB. No lado do proxy reverso, edite o arquivo de configuração de acordo com a documentação do proxy reverso. Para ver um exemplo, consulte "Exemplo: Configuração do Apache 2.0.x" Na página seguinte.

Para trabalhos agendados criados antes do UCMDB versão 10.01, você também precisa definir a configuração do UCMDB como a seguir:

## Configurar um proxy reverso usando configurações de infraestrutura

O procedimento a seguir explica como acessar as Configurações de Infraestrutura para configurar um proxy reverso. Essa configuração somente é necessária ao criar um vínculo direto para um relatório usando o programador.

**Para configurar um proxy reverso:**

1. Selecione **Administração > Configurações de Infraestrutura > categoria Configurações Gerais**.
2. Altere a configuração de **URL Frontend**. Insira o endereço, por exemplo, **https://my_proxy_server:443/**.

**Observação:** Depois de fazer essa alteração, você não poderá acessar o servidor do HP Universal CMDB diretamente através de um cliente. Para alterar a configuração do proxy reverso, use o console JMX no computador servidor. Para obter detalhes, consulte “Configurar

um proxy reverso usando o console JMX" abaixo.

## Configurar um proxy reverso usando o console JMX

Você pode fazer alterações na configuração do proxy reverso usando o console JMX na máquina do servidor do HP Universal CMDB. Essa configuração somente é necessária ao criar um vínculo direto para um relatório usando o programador.

**Para alterar uma configuração de proxy reverso:**

1. No computador servidor do HP Universal CMDB, abra o navegador da Web e insira o seguinte endereço:

   **http://<nome do computador ou endereço IP>.<nome_do_domínio>:8080/jmx-console**

   onde **<nome do computador ou endereço IP>** é o computador no qual o HP Universal CMDB está instalado. Você pode precisar fazer logon com o nome de usuário e senha.

2. Clique no link **UCMDB-UI > UCMDB-UI:name=UI Server frontend settings**.

   No campo **setUseFrontendURLBySettings**, insira a URL do proxy do servidor, por exemplo, `https://my_proxy_server:443/`.

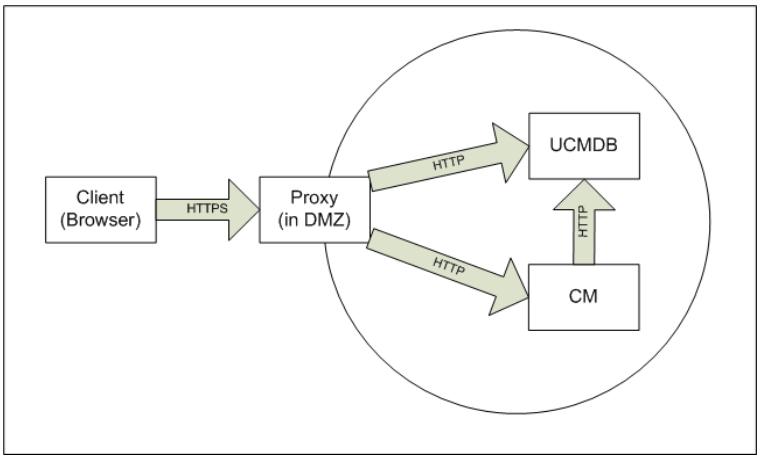
3. Clique em **Invoke**.

4. Para ver o valor dessa configuração, use o método **showFrontendURLInSettings**.

## Exemplo: Configuração do Apache 2.0.x

Esta seção descreve um arquivo de configuração de amostra que oferece suporte para o uso de um proxy reverso do Apache 2.0.x em um caso onde tanto as Sondas de Fluxo de Dados quanto os usuários do aplicativo se conectam ao HP Universal CMDB.

O diagrama a seguir ilustra o processo de configuração de um proxy reverso para o Configuration Manager e o UCMDB.



**Observação:**

- Neste exemplo, o nome DNS e a porta do computador do HP Universal CMDB são UCMDB_server.
- Neste exemplo, o nome DNS e a porta do computador do Configuration Manager são UCMDB_CM_server.
- Somente usuários com conhecimento sobre a administração do Apache devem fazer esta alteração.

1. Abra o arquivo **<diretório raiz do computador com Apache>\Webserver\conf\httpd.conf**.
2. Habilite os seguintes módulos:
   - **LoadModule proxy_module modules/mod_proxy.so**
   - **LoadModule proxy_http_module modules/mod_proxy_http.so**
3. Adicione as seguintes linhas ao arquivo **httpd.conf**:

```
ProxyRequests off
<Proxy *>
     Order deny,allow
     Deny from all
     Allow from all
</Proxy>

ProxyPass /mam http://UCMDB_server/mam
ProxyPassReverse /mam http://UCMDB_server/mam
ProxyPass /mam_images http://UCMDB_server/mam_images
ProxyPassReverse /mam_images http://UCMDB_server/mam_images
ProxyPass /mam-collectors http://UCMDB_server/mam-collectors
ProxyPassReverse /mam-collectors http://UCMDB_server/mam-collectors
ProxyPass /ucmdb http://UCMDB_server/ucmdb
ProxyPassReverse /ucmdb http://UCMDB_server/ucmdb
ProxyPass /site http://UCMDB_server/site
ProxyPassReverse /site http://UCMDB_server/site
ProxyPass /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPass /status http://UCMDB_server/status
ProxyPassReverse /status http://UCMDB_server/status
ProxyPass /jmx-console http://UCMDB_server/jmx-console
ProxyPassReverse /jmx-console http://UCMDB_server/jmx-console
ProxyPass /axis2 http://UCMDB_server/axis2
ProxyPassReverse /axis2 http://UCMDB_server/axis2
ProxyPass /icons http://UCMDB_server/icons
ProxyPassReverse /icons http://UCMDB_server/icons
ProxyPass /ucmdb-api http://UCMDB_server/ucmdb-api
```

```
ProxyPassReverse /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPass /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPassReverse /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPass /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPassReverse /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPass /cm http://UCMDB_Server/cm
ProxyPassReverse /cm http://UCMDB_Server /cm
ProxyPass /cnc http://UCMDB_CM_server/cnc
ProxyPassReverse /cnc http://UCMDB_CM_server/cnc
ProxyPass /docs http://UCMDB_CM_server/docs
ProxyPassReverse /docs http://UCMDB_CM_server/docs
ProxyPass /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
ProxyPassReverse /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
```

4. Salve suas alterações.

# Conectar o Data Flow Probe por proxy reverso ou o balanceador de carga usando autenticação mútua

Realize o seguinte procedimento para conectar o Data Flow Probe por um proxy reverso ou um balanceador de carga usando autenticação mútua. Esse procedimento se aplica à seguinte configuração:

- A autenticação SSL mútua entre a sonda e um proxy reverso ou balanceador de carga com base em um certificado cliente fornecido pela sonda e necessário pelo proxy reverso ou pelo balanceador de carga.
- Uma conexão SSL regular entre o proxy reverso ou o balanceador de carga e o Servidor do UCMDB.

**Observação:** as instruções a seguir usam o repositório de chaves **cKeyStoreFile** como repositório de chaves da Sonda. Esse é um repositório predefinido de chaves do cliente que é parte da instalação do do Data Flow Probe e contém certificados autoassinados. Para obter detalhes, consulte "Repositório de chaves e repositório confiável padrão do servidor e do Data Flow Probe" Na página87.

É recomendável criar um novo repositório de chaves exclusivo contendo uma nova chave privada recém-gerada. Para obter detalhes, consulte "Criar um repositório de chaves para o Data Flow Probe" Na página86.

## Obter um certificado de uma Autoridade de Certificação

Obter o certificado raiz do CA e importá-lo para os seguintes locais:

- o repositório confiável do Data Flow Probe
- o cacerts de JVM do Data Flow Probe

- o repositório confiável do servidor do UCMDB
- o repositório confiável do proxy reverso

1. Importe o certificado raiz do CA no repositório confiável do Data Flow Probe.

   a. Coloque o certificado raiz do CA no diretório a seguir: <Diretório de instalação do Data Flow Probe>\conf\security<nome do arquivo de certificado>.

   b. Importe o certificado raiz do CA no repositório confiável do Data Flow Probe executando o script a seguir:

   ```
   <Diretório de instalação do Data Flow Probe>\bin\jre\bin\keytool.exe -imp
   ort -trustcacerts -alias <YourAlias> -file C:\hp\UCMDB\DataFlowProbe\conf
   \security\<nome do arquivo de certificado> -keystore <diretório de instal
   ação do Data Flow Probe>\conf\security\hpprobeTrustStore.jks
   ```

   A senha padrão é: **logomania**.

2. Importe o certificado raiz do CA no cacerts de JVM do Data Flow Probe executando o script a seguir:

   ```
   <Diretório de instalação do Data Flow Probe>\bin\jre\bin\keytool.exe -import
   -trustcacerts -alias <YourAlias> -file <diretório de instalação do Data Flow
   Probe>\conf\security\<nome do arquivo de certificado> -keystore <diretório de
   instalação do Data Flow Probe>\bin\jre\lib\security\cacerts
   ```

   A senha padrão é: **changeit**.

3. Importe o certificado raiz do CA no repositório confiável do UCMDB.

   a. Coloque o certificado raiz do CA no diretório a seguir: <Diretório de instalação do UCMDB>\conf\security<nome do arquivo de certificado>.

   b. Importe o certificado raiz do CA no repositório confiável do UCMDB executando o script a seguir:

   ```
   <diretório de instalação do UCMDB>\bin\jre\bin\keytool.exe -import -trust
   cacerts -alias <YourAlias> -file <diretório de instalação do UCMDB>\conf\
   security\<nome do arquivo de certificado> -keystore <diretório de instala
   ção do UCMDB>\conf\security\sever.truststore
   ```

   A senha padrão é: **hppass**.

4. Importe o certificado raiz do CA no repositório confiável do proxy reverso. Essa etapa depende do fornecedor.

## Converter o certificado para um repositório de chaves Java

Obtenha o certificado do cliente (e a chave privada) para o Data Flow Probe da sua Autoridade de Certificado (CA) no formato PFX/PKCS12 e converta-o para um repositório de chaves Java executando o seguinte script:

```
<diretório de instalação do Data Flow Probe>\bin\jre\bin\keytool.exe -importkeys
tore -srckeystore <caminho completo do repositório de chaves PFX> -destkeystore
<caminho completo do novo repositório de chaves de destino> -srcstoretype PKCS12
```

Será solicitado que você indique as senhas do repositório de chaves de origem e de destino.

Para a senha do repositório de chaves de origem, use a mesma senha usada ao exportar o repositório de chaves PFX.

A senha do repositório de chaves de destino padrão para o repositório de chaves do Data Flow Probe é: **logomania**.

**Observação:** Se você inseriu uma senha diferente do repositório de chaves de destino da senha do repositório de chaves padrão do Data Flow Probe (logomania), precisará fornecer a nova senha em formato criptografado para o arquivo do **<diretório de instalação do Data Flow Probe>\conf\ssl.properties** (javax.net.ssl.keyStorePassword). Para obter detalhes, consulte "Criptografar as senhas do repositório de chaves e do repositório confiável da Sonda" Na página86.

Coloque o novo repositório de chaves no seguinte diretório: **<diretório de instalação do Data Flow Probe>\conf\security**.

**Cuidado:** Não substitua o arquivo **hpprobeKeyStore.jks**.

## Altere o arquivo de propriedades SSL para usar o repositório de chaves recém-criado

Defina o repositório de chaves contendo o certificado cliente no arquivo do **<diretório de instalação do Data Flow Probe>\conf\ssl.properties** como **javax.net.ssl.keyStore**.

Se a senha para seu repositório de chaves não for a senha padrão do repositório de chaves do Data Flow Probe (logomania), atualize **javax.net.ssl.keyStorePassword** após criptografá-la. Para obter detalhes sobre a criptografia da senha, consulte "Criptografar as senhas do repositório de chaves e do repositório confiável da Sonda" Na página86.

## Revisar a Configuração do Data Flow Probe

Edite o arquivo do **<diretório de instalação do Data Flow Probe>\conf\DataFlowProbe.properties** como a seguir:

```
appilog.agent.probe.protocol = HTTPS

serverName = <endereço do servidor proxy reverso>

serverPortHttps = <a porta HTTPS que o proxy reverso ouve para redirecionar soli
citações ao UCMDB>
```

## Configurar o UCMDB para funcionar usando SSL

Para obter detalhes, consulte "Habilitando comunicação SSL" Na página17.

Se o certificado do servidor do UCMDB for criado pelo mesmo CA que criou o restante dos certificados nesse procedimento, o proxy reverso ou balanceador de carga confia no certificado do UCMDB.

# Configurar o suporte CAC para o UCMDB por proxy reverso

Esta seção descreve como configurar o suporte a CAC (Common Access Card) no UCMDB usando um proxy reverso.

1. Abra o console JMX iniciando o navegador da Web e insira o endereço do servidor, da seguinte maneira: http://<Nome de Host do Servidor do UCMDB ou IP>:8080/jmx-console.

   Você pode precisar fazer logon com um nome de usuário e senha.

2. Em UCMDB, clique em **UCMDB:service=Ports Management Services** para abrir a página Operations.

   - (opcional) Clique em **ComponentsConfigurations**. Siga este procedimento:
     - Defina **HTTPSetPort** como **8080** e clique em **Invoke**.
     - Clique em **Back to MBean**.
   - Clique em **mapComponentToConnectors**. Siga este procedimento:
     - No serviço mapComponentToConnectors, defina **componentName** como **ucmdb-ui**.
     - Defina apenas **isHTTP** como **true** e clique em **Invoke**.
     - Clique em **Back to MBean**.
     - No serviço mapComponentToConnectors, defina **componentName** como **root**.
     - Defina apenas **isHTTP** como **true** e clique em **Invoke**.

3. No UCMDB, clique em **UCMDB:service=Security Services** para abrir a página Operations.

   - Defina **loginWithCAC** como **true** e clique em **Invoke**.
   - Clique em **Back to MBean**.
   - Defina **withReverseProxy** como **true** e clique em **Invoke**.

     Essa configuração instrui o servidor do UCMDB a extrair do cabeçalho UCMDB_SSL_CLIENT_CERT o nome de usuário a ser usado no UCMDB e o certificado a ser usado para autenticação.

- Clique em **Back to MBean**.
- (opcional) Defina **onlyCACCerts** como **true** e clique em **Invoke**.

  Defina essa operação como **true** para aceitar apenas certificados que acompanham um dispositivo CAC físico.

4. Reinicie o Servidor do UCMDB.

## Exemplo: Configuração do Apache 2.4.4

Esta seção descreve um arquivo de configuração de amostra para o Apache 2.4.4 (no arquivo do **<diretório raiz do computador com Apache>\Webserver\conf\httpd.conf**):

```
LoadModule headers_module modules/mod_headers.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_html_module modules/mod_proxy_html.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
LoadModule ssl_module modules/mod_ssl.so
ServerName Apache_Server_Name:80
Incluir conf/extra/httpd-ssl.conf
```

Esta seção descreve um arquivo de configuração de amostra para o Apache 2.4.4 com SSL (no arquivo do **<diretório raiz do computador com Apache>\Webserver\conf\extra\httpd-ssl.conf**:

```
Listen 8443<VirtualHost _default_:8443>
ServerName Apache_Server_Name:8443
SSLCACertificateFile "c:/Apache24/conf/ssl.crt"
SSLCARevocationFile "c:/Apache24/conf/ssl.crl"
#SSLCARevocationCheck chain|leaf|none
SSLCARevocationCheck leaf
RequestHeader set UCMDB_SSL_CLIENT_CERT %{SSL_CLIENT_CERT}e


ProxyRequests off
<Proxy *>
     Order deny,allow
     Deny from all
     Allow from all
</Proxy>

ProxyPass /mam http://UCMDB_server/mam
ProxyPassReverse /mam http://UCMDB_server/mam
ProxyPass /mam_images http://UCMDB_server/mam_images
ProxyPassReverse /mam_images http://UCMDB_server/mam_images
ProxyPass /mam-collectors http://UCMDB_server/mam-collectors
ProxyPassReverse /mam-collectors http://UCMDB_server/mam-collectors
ProxyPass /ucmdb http://UCMDB_server/ucmdb
ProxyPassReverse /ucmdb http://UCMDB_server/ucmdb
ProxyPass /site http://UCMDB_server/site
```

```
ProxyPassReverse /site http://UCMDB_server/site
ProxyPass /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPass /status http://UCMDB_server/status
ProxyPassReverse /status http://UCMDB_server/status
ProxyPass /jmx-console http://UCMDB_server/jmx-console
ProxyPassReverse /jmx-console http://UCMDB_server/jmx-console
ProxyPass /axis2 http://UCMDB_server/axis2
ProxyPassReverse /axis2 http://UCMDB_server/axis2
ProxyPass /icons http://UCMDB_server/icons
ProxyPassReverse /icons http://UCMDB_server/icons
ProxyPass /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPassReverse /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPass /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPassReverse /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPass /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPassReverse /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPass /cm http://UCMDB_Server/cm
ProxyPassReverse /cm http://UCMDB_Server /cm
ProxyPass /cnc http://UCMDB_CM_server/cnc
ProxyPassReverse /cnc http://UCMDB_CM_server/cnc
ProxyPass /docs http://UCMDB_CM_server/docs
ProxyPassReverse /docs http://UCMDB_CM_server/docs
ProxyPass /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
ProxyPassReverse /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
SSLVerifyClient requer
SSLVerifyDepth  10
SSLOptions+ExportCertData
```

# Capítulo 4: Gerenciamento de credenciais do fluxo de dados

Este capítulo inclui:

# Visão geral do gerenciamento de credenciais do fluxo de dados

Para realizar a descoberta ou executar a integração, você deve configurar as credenciais para acessar o sistema remoto. As credenciais são configuradas na janela Configuração do Data Flow Probe e salvas no Servidor do UCMDB. Para ver detalhes, consulte a seção que descreve a instalação do Data Flow Probe no *Guia de Gerenciamento de Fluxo de Dados do HP Universal CMDB*.

O armazenamento de credenciais é gerenciado pelo componente Confidential Manager. Para obter detalhes, consulte "Gerenciador Confidencial" Na página106.

O Data Flow Probe pode acessar as credenciais usando o cliente do Confidential Manager. O cliente do Confidential Manager reside no Data Flow Probe e se comunica com o servidor do Confidential Manager, que reside no Servidor do UCMDB. A comunicação entre o cliente do Confidential Manager e o servidor do Confidential Manager é criptografada, exigindo autenticação pelo cliente do Confidential Manager quando ele se conecta ao servidor do Confidential Manager.

A autenticação do cliente do Confidential Manager no servidor do Confidential Manager é baseada em um componente de LW-SSO. Antes de se conectar ao servidor do Confidential Manager, o cliente do Confidential Manager envia um cookie de LW-SSO. O servidor do Confidential Manager verifica o cookie e, se a verificação é bem-sucedida, a comunicação com o cliente do Confidential Manager se estabelece. Para ver detalhes sobre LW-SSO, consulte "Definir configurações de LW-SSO" Na página54.

A comunicação entre o cliente do Confidential Manager e o servidor do Confidential Manager é criptografada. Para ver detalhes sobre a atualização da configuração de criptografia, consulte "Configurar criptografia de comunicação do Confidential Manager " Na página55.

**Cuidado:** A autenticação do Confidential Manager usa o fuso horário universal definido no computador (UTC). Para que a autenticação seja bem-sucedida, verifique se o horário universal no Data Flow Probe e no servidor do UCMDB são iguais. O servidor e a sonda podem estar localizados em fusos horários diferentes, uma vez que o UTC é independente de fuso horário ou do horário de verão.

O cliente do Confidential Manager mantém um cache local das credenciais. O cliente do Confidential Manager é configurado para baixar todas as credenciais do servidor do Confidential Manager e armazená-las em um cache. As alterações nas credenciais são sincronizadas automaticamente do servidor do Confidential Manager de forma contínua. O cache pode ser um

cache de sistema de arquivos ou na memória, dependendo das configurações predefinidas. Além disso, o cache é criptografado e não pode ser acessado externamente. Para ver detalhes sobre a atualização das configurações do cache, consulte "Configurar o modo de cache do cliente do Confidential Manager na Sonda" Na página59. Para ver detalhes sobre a atualização da criptografia do cache, consulte "Definir as configurações de criptografia de cache do cliente do Confidential Manager na sonda" Na página60.

Para ver detalhes sobre como solucionar problemas, consulte "Alterar o nível da mensagem do arquivo de log do cliente do Confidentiality Manager" Na página63.

Você pode copiar informações de credenciais de um servidor do UCMDB para outro. Para obter detalhes, consulte "Exportar e importar informações de credencial e intervalo em formato criptografado" Na página61.

**Observação:** O **DomainScopeDocument** (DSD) que era usado para armazenamento de credenciais na Sonda (no UCMDB versão 9.01 ou anterior) não contém mais informações relacionadas a credenciais. O arquivo agora contém uma lista de Sondas e informações sobre intervalo da rede. Contém também uma lista de entradas de credencial para cada domínio, onde cada entrada inclui apenas o ID da credencial e um intervalo da rede (definido para essa entrada de credencial).

Esta seção inclui os seguintes tópicos:



# Premissas básicas de segurança

Observe a seguinte premissa de segurança:

Você protegeu o Servidor do UCMDB e o console JMX da Sonda para possibilitar acesso ao UCMDB somente por administradores do sistema, preferivelmente apenas por meio de acesso localhost.

# Data Flow Probe executado em modo separado

Quando o Probe Gateway e o Manager são executados como processos separados, o componente cliente do Confidential Manager torna-se parte do processo do Manager. As informações de credenciais são armazenadas em cache e usadas apenas pelo Probe Manager. Para acessar o servidor do Confidential Manager no sistema do UCMDB, a solicitação do cliente do Confidential Manager é atendida pelo processo do Gateway e de lá é encaminhada para o sistema do UCMDB.

Essa configuração é automática quando a Sonda é configurada em modo separado.

# Mantendo o cache de credenciais atualizado

Em sua primeira conexão bem-sucedida com o servidor do Confidential Manager, o cliente do Confidential Manager baixa todas as credenciais relevantes (todas as credenciais que estão configuradas no domínio da sonda). Após a primeira comunicação bem-sucedida, o cliente do Confidential Manager mantém sincronização contínua com o servidor do Confidential Manager. Uma sincronização diferencial é realizada a intervalos de um minuto, durante os quais apenas as diferenças entre o servidor do Confidential Manager e o cliente do Confidential Manager são sincronizadas. Se as credenciais são alteradas no servidor do UCMDB (como adição de novas credenciais, ou atualização ou exclusão de existentes), o cliente do Confidential Manager recebe uma notificação imediata do servidor do UCMDB e realiza uma sincronização adicional.

# Sincronizando todas as sondas com alterações de configuração

Para uma comunicação bem-sucedida, o cliente do Confidential Manager deve ser atualizado com a configuração de autenticação do servidor do Confidential Manager (cadeia init do LW-SSO) e configuração de criptografia (criptografia de comunicação do Confidential Manager). Por exemplo, quando a cadeia init é alterada no servidor, a sonda deve conhecer a nova cadeia init para autenticar.

O servidor do UCMDB monitora constantemente a configuração da criptografia de comunicação do Confidential Manager e a configuração de autenticação do Confidential Manager em busca de alterações. Esse monitoramento é feito a cada 15 segundos; caso uma alteração tenha ocorrido, a configuração atualizada é enviada para as sondas. A configuração é passada para as sondas em formato criptografado e armazenada no lado da sonda no armazenamento seguro. A criptografia da configuração que está sendo enviada é feita usando uma chave de criptografia simétrica. Por padrão, o servidor do UCMDB e o Data Flow Probe são instalados com a mesma chave de criptografia simétrica padrão. Para mais segurança, é altamente recomendável alterar essa chave antes de adicionar credenciais ao sistema. Para obter detalhes, consulte "Gerar ou atualizar a chave de criptografia" Na página64.

**Observação:** Devido ao intervalo de monitoramento de 15 segundos, é possível que o cliente do Confidential Manager, no lado da Sonda, possa não estar atualizado com a configuração mais recente por um período de 15 segundos.

Se você optar por desabilitar a sincronização automática da configuração de comunicação e autenticação do Confidential Manager entre o servidor do UCMDB e o Data Flow Probe, cada vez que você atualizar a configuração de comunicação e autenticação do Confidential Manager no lado do servidor do UCMDB, deverá atualizar todas as Sondas com a nova configuração também. Para obter detalhes, consulte "Desabilitar a sincronização automática das configurações de autenticação e criptografia do cliente do Confidential Manager entre o servidor e as sondas" Na página56.

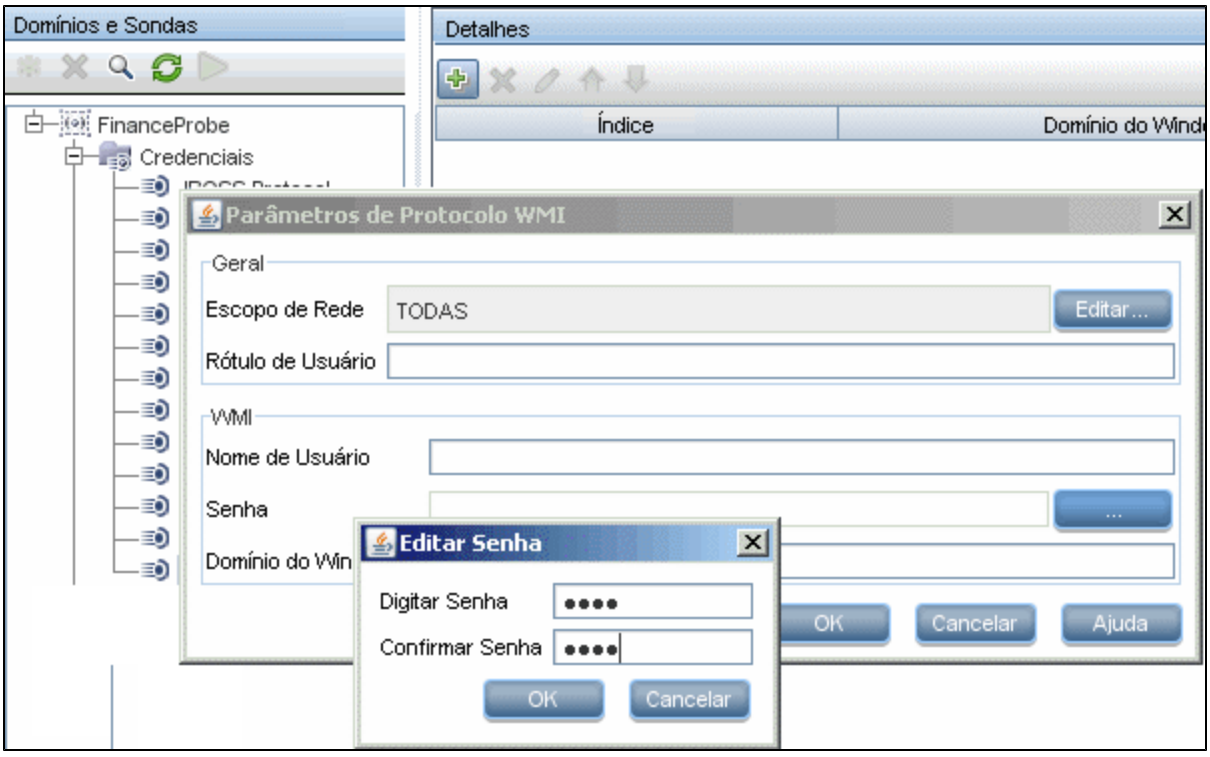
# Armazenamento protegido na Sonda

Todas as informações confidenciais (como a configuração de comunicação e autenticação do Confidential Manager e a chave de criptografia) são armazenadas na sonda em um armazenamento seguro no arquivo **secured_storage.bin**, localizado em **C:\hp\UCMDB\DataFlowProbe\conf\security**. Esse armazenamento protegido é criptografado usando DPAPI, que depende da senha do usuário do Windows no processo de criptografia. DPAPI é um método padrão usado para proteger dados confidenciais, como certificados e chaves privadas, em sistemas Windows. A Sonda sempre deve ser executada com o mesmo usuário do Windows, para que, mesmo se a senha for alterada, a Sonda ainda possa ler as informações do armazenamento seguro.

# Exibindo informações de credenciais

**Observação:** Esta seção trata da visualização de informações de credenciais quando a direção dos dados é do CMDB ao HP Universal CMDB

Senhas não são enviadas do CMDB para o aplicativo. Ou seja, o HP Universal CMDB exibe asteriscos (*) no campo da senha, independentemente do conteúdo:



# Atualizando credenciais

**Observação:** Esta seção trata de atualização de credenciais quando a direção dos dados é do HP Universal CMDB ao CMDB.

- A comunicação nesse sentido não é criptografada; portanto, você deve se conectar ao Servidor do UCMDB usando https\SSL ou garantir a conexão através de uma rede confiável.

  Embora a comunicação não seja criptografada, as senhas não são enviadas como texto claro na rede. Elas são criptografadas usando uma chave padrão e, portanto, é altamente recomendável usar SSL para obter uma confidencialidade eficaz em trânsito.

- Você pode usar caracteres especiais e caracteres não presentes no idioma português nas senhas.

# Definir configurações de autenticação e criptografia do cliente do Confidential Manager

Essa tarefa descreve as configurações de criptografia e de autenticação de cliente do Confidential Manager no servidor UCMDB e inclui as seguintes etapas:

- "Definir configurações de LW-SSO" abaixo
- "Configurar criptografia de comunicação do Confidential Manager " Na página seguinte

## Definir configurações de LW-SSO

Este procedimento descreve como alterar a cadeia init do LW-SSO no servidor do UCMDB. Essa alteração é enviada automaticamente para as Sondas (como uma cadeia criptografada), a menos que o servidor do UCMDB esteja configurado para não fazê-lo automaticamente. Para obter detalhes, consulte "Desabilitar a sincronização automática das configurações de autenticação e criptografia do cliente do Confidential Manager entre o servidor e as sondas" Na página56.

1. No Servidor do UCMDB, abra o navegador da Web e insira o seguinte endereço: **http://localhost:8080/jmx-console**.
2. Clique em **UCMDB-UI:name=LW-SSO Configuration** para abrir a página JMX MBEAN View.
3. Localize o método **setInitString**.
4. Insira uma nova cadeia init do LW-SSO.
5. Clique em Invoke.

# Configurar criptografia de comunicação do Confidential Manager

Este procedimento descreve como alterar as configurações de comunicação do Confidential Manager no servidor do UCMDB. Essas configurações especificam como a comunicação entre o cliente do Confidential Manager e o servidor do Confidential Manager é criptografada. Essa alteração é enviada automaticamente para as Sondas (como uma cadeia criptografada), a menos que o servidor do UCMDB esteja configurado para não fazê-lo automaticamente. Para obter detalhes, consulte "Desabilitar a sincronização automática das configurações de autenticação e criptografia do cliente do Confidential Manager entre o servidor e as sondas" Na página seguinte.

1. No Servidor do UCMDB, abra o navegador da Web e insira o seguinte endereço: **http://localhost:8080/jmx-console.**
2. Clique em **UCMDB:service=Security Services** para abrir a página JMX MBEAN View.
3. Clique no método **CMGetConfiguration**.
4. Clique em **Invoke**.

   O XML da configuração do Confidential Manager atual é exibido.
5. Copie o conteúdo do XML exibido.
6. Navegue de volta a **Security Services** na página JMX MBean View.
7. Clique no método **CMSetConfiguration**.
8. Cole o XML copiado no campo **Value**.
9. Atualize as configurações relacionadas a transporte relevantes e clique em **Invoke**.

   **Exemplo:**

```
<transport>
      <encryptTransportMode>true</encryptTransportMode>
      <CMEncryptionDecryption>
            <encryptDecryptInitString>radiohead</encryptDecryptInitStrin
            g>
            <cryptoSource>lw</cryptoSource>
            <lwJCEPBECompatibilityMode>true</lwJCEPBECompatibilityMode>
            <cipherType>symmetricBlockCipher</cipherType>
            <engineName>AES</engineName>
```

```
            <algorithmModeName>CBC</algorithmModeName>
            <algorithmPaddingName>PKCS7Padding</algorithmPaddingName>
            <keySize>256</keySize>
            <pbeCount>20</pbeCount>
            <pbeDigestAlgorithm>SHA1</pbeDigestAlgorithm>
            <encodingMode>Base64Url</encodingMode>
            <useMacWithCrypto>false</useMacWithCrypto>
            <macType>hmac</macType>
            <macKeySize>256</macKeySize>
            <macHashName>SHA256</macHashName>
      </CMEncryptionDecryption>
</transport>
```

Para ver detalhes sobre os valores que podem ser atualizados, consulte "Configurações de criptografia do Confidential Manager" Na página69.

# Definir configurações de autenticação e criptografia do cliente do Confidential Manager manualmente na sonda

**Esta tarefa inclui as seguintes etapas:**

- "Desabilitar a sincronização automática das configurações de autenticação e criptografia do cliente do Confidential Manager entre o servidor e as sondas" abaixo
- "Definir configurações de autenticação e criptografia do cliente do Confidential Manager na sonda" Na página seguinte
- "Configurar criptografia de comunicação do Confidential Manager na sonda" Na página seguinte

# Desabilitar a sincronização automática das configurações de autenticação e criptografia do cliente do Confidential Manager entre o servidor e as sondas

Por padrão, o Servidor do UCMDB está configurado para enviar automaticamente as configurações do Confidential Manager/LW-SSO para todas as Sondas. Essas informações são enviadas como uma cadeia de caracteres criptografada para as Sondas, que a descriptografa na recuperação. Você pode configurar o Servidor do UCMDB para não enviar os arquivos de configuração do

Confidential Manager/LW-SSO automaticamente para todas as Sondas. Nesse caso, é sua responsabilidade atualizar manualmente todas as Sondas com as novas configurações do Confidential Manager/LW-SSO.

Para desabilitar a sincronização automática das configurações do Confidential Manager/LW-SSO:

1. No UCMDB, clique em **Administração > Gerenciador de Configurações de Infraestrutura > Configurações Gerais**.
2. Selecione **Habilitar sincronização automática de configuração de CM/LW-SSO e cadeia init com sonda**.
3. Clique no campo **Valor** e mude **Verdadeiro** para **Falso**.
4. Clique no botão **Save**.
5. Reinicie o servidor UCMDB.

# Definir configurações de autenticação e criptografia do cliente do Confidential Manager na sonda

Este procedimento é relevante se o Servidor do UCMDB foi configurado para não enviar configurações do LW-SSO/Confidential Manager automaticamente para as Sondas. Para obter detalhes, consulte "Desabilitar a sincronização automática das configurações de autenticação e criptografia do cliente do Confidential Manager entre o servidor e as sondas" Na página anterior.

1. No computador da Sonda, abra o navegador da Web e insira o seguinte endereço: **http://localhost:1977**.

   **Observação:** Se o Probe Manager e o Probe Gateway estiverem sendo executados como processos separados, o endereço deverá será inserido no computador que estiver executando o Probe Manager da seguinte forma: **http://localhost:1978**.

2. Clique em **type=CMClient** para abrir a página JMX MBEAN View.
3. Localize o método **setLWSSOInitString** e forneça a mesma cadeia init que foi fornecida para a configuração de LW-SSO do UCMDB.
4. Clique no botão **setLWSSOInitString**.

# Configurar criptografia de comunicação do Confidential Manager na sonda

Este procedimento é relevante se o Servidor do UCMDB foi configurado para não enviar configurações do LW-SSO/Confidential Manager automaticamente para as Sondas. Para obter detalhes, consulte "Desabilitar a sincronização automática das configurações de autenticação e criptografia do cliente do Confidential Manager entre o servidor e as sondas" Na página anterior.

1. No computador da Sonda, abra o navegador da Web e insira o seguinte endereço: **http://localhost:1977**.

   **Observação:** Se o Probe Manager e o Probe Gateway estiverem sendo executados como processos separados, o endereço deverá será inserido no computador que estiver executando o Probe Manager da seguinte forma: **http://localhost:1978**.

2. Clique em **type=CMClient** para abrir a página JMX MBEAN View.

3. Atualize as seguintes configurações relacionadas a transporte:

   **Observação:** Você deve atualizar as mesmas configurações que atualizou no servidor do UCMDB. Para fazer isso, alguns dos métodos que você atualiza na Sonda podem exigir mais de um parâmetro. Para ver a configuração da sonda atual, clique em **displayTransportConfiguration** na página JMX MBEAN View. Para obter detalhes, consulte "Configurar criptografia de comunicação do Confidential Manager " Na página55. Para ver detalhes sobre os valores que podem ser atualizados, consulte "Configurações de criptografia do Confidential Manager" Na página69.

   a. **setTransportInitString** altera a configuração de **encryptDecryptInitString**.

   b. **setTransportEncryptionAlgorithm** altera as configurações do Confidential Manager na Sonda de acordo com o seguinte mapa:

      - **Engine name** refere-se à entrada <engineName>
      - **Key size** refere-se à entrada <keySize>
      - **Algorithm padding name** refere-se à entrada <algorithmPaddingName>
      - **PBE count** refere-se à entrada <pbeCount>
      - **PBE digest algorithm** refere-se à entrada <pbeDigestAlgorithm>

   c. **setTransportEncryptionLibrary** altera as configurações do Confidential Manager na Sonda de acordo com o seguinte mapa:

      - **Encryption Library name** refere-se à entrada <cryptoSource>
      - **Support previous lightweight cryptography versions** refere-se à entrada <lwJCEPBECompatibilityMode>

   d. **setTransportMacDetails** altera as configurações do Confidential Manager na Sonda de acordo com o seguinte mapa:

- **Use MAC with cryptography** refere-se à entrada <useMacWithCrypto>
- **MAC key size** refere-se à entrada <macKeySize>

4. Clique no botão **reloadTransportConfiguration** para tornar as alterações efetivas na Sonda.

Para ver detalhes sobre as diferentes configurações e seus possíveis valores, consulte "Configurações de criptografia do Confidential Manager" Na página69.

# Configurar o cache do cliente do Confidentiality Manager

Esta tarefa inclui as seguintes etapas:

- "Configurar o modo de cache do cliente do Confidential Manager na Sonda" abaixo
- "Definir as configurações de criptografia de cache do cliente do Confidential Manager na sonda" Na página seguinte

# Configurar o modo de cache do cliente do Confidential Manager na Sonda

O cliente do Confidential Manager armazena informações de credenciais no cache e as atualiza quando elas são alteradas no Servidor. O cache pode então ser armazenado no sistema de arquivos ou na memória:

- **Quando são armazenadas no sistema de arquivos**, as informações de credenciais ainda ficam disponíveis mesmo se a Sonda é reiniciada e não pode se conectar ao Servidor.
- **Quando são armazenadas na memória**, se a Sonda é reiniciada, o cache é limpo e todas as informações são recuperadas novamente do Servidor. Se o Servidor não está disponível, a Sonda não inclui nenhuma credencial, então nenhuma descoberta ou integração pode ser executada.

**Para alterar essa configuração:**

1. Abra o arquivo **DataFlowProbe.properties** em um editor de texto. Esse arquivo fica localizado no diretório **c:\hp\UCMDB\DataFlowProbe\conf**.
2. Localize o seguinte atributo:
   **com.hp.ucmdb.discovery.common.security.storeCMData=true**
   - Para armazenar as informações no sistema de arquivos, deixe o padrão (**true**).
   - Para armazenar as informações na memória, insira **false**.

3. Salve o arquivo **DataFlowProbe.properties**.

4. Reinicie a Sonda.

# Definir as configurações de criptografia de cache do cliente do Confidential Manager na sonda

Este procedimento descreve como alterar as configurações de criptografia do arquivo de cache do sistema de arquivos do cliente do Confidential Manager. Observe que alterar as configurações de criptografia do cache do sistema de arquivos do cliente do Confidential Manager faz com que o arquivo de cache do sistema de arquivos seja recriado. Esse processo de recriação requer a reinicialização da Sonda e uma sincronização completa com o Servidor do UCMDB.

1. No computador da Sonda, abra o navegador da Web e insira o seguinte endereço: **http://localhost:1977**.

   **Observação:** Se o Probe Manager e o Probe Gateway estiverem sendo executados como processos separados, o endereço deverá será inserido no computador que estiver executando o Probe Manager da seguinte forma: **http://localhost:1978**.

2. Clique em **type=CMClient** para abrir a página JMX MBEAN View.

3. Atualize as seguintes configurações relacionadas ao cache:

   **Observação:** Alguns dos métodos que você atualiza na Sonda podem exigir mais de um parâmetro. Para ver a configuração da sonda atual, clique em **displayCacheConfiguration** na página JMX MBEAN View.

   a. **setCacheInitString** altera a configuração <encryptDecryptInitString> do cache do sistema de arquivos.

   b. **setCacheEncryptionAlgorithm** altera as configurações do cache do sistema de arquivos de acordo com o seguinte mapa:

      - **Engine name** refere-se à entrada <engineName>
      - **Key size** refere-se à entrada <keySize>
      - **Algorithm padding name** refere-se à entrada <algorithmPaddingName>
      - **PBE count** refere-se à entrada <pbeCount>
      - **PBE digest algorithm** refere-se à entrada <pbeDigestAlgorithm>

   c. **setCacheEncryptionLibrary** altera as configurações do sistema de arquivos do cache de

acordo com o seguinte mapa:

- **Encryption Library name** refere-se à entrada <cryptoSource>
- **Support previous lightweight cryptography versions** refere-se à entrada <lwJCEPBECompatibilityMode>

d. **setCacheMacDetails** altera as configurações do sistema de arquivos do cache de acordo com o seguinte mapa:

- **Use MAC with cryptography** refere-se à entrada <useMacWithCrypto>
- **MAC key size** refere-se à entrada <macKeySize>

4. Clique no botão **reloadCacheConfiguration** para tornar as alterações efetivas na Sonda. Isso faz a Sonda ser reiniciada.

> **Observação:** Verifique se não há nenhum trabalho sendo executado na Sonda durante essa ação.

Para ver detalhes sobre as diferentes configurações e seus possíveis valores, consulte "Configurações de criptografia do Confidential Manager" Na página69.

# Exportar e importar informações de credencial e intervalo em formato criptografado

Você pode exportar e importar informações de credenciais e intervalos de rede em formato criptografado para copiar as informações de credenciais de um Servidor do UCMDB para outro. Por exemplo, você pode realizar essa operação durante a recuperação após uma falha do sistema ou durante a atualização.

- **Ao exportar informações de credenciais,** você deve inserir uma senha (à sua escolha). As informações são criptografadas com essa senha.
- **Ao importar informações de credenciais,** você deve usar a mesma senha que foi definida quando o arquivo DSD foi exportado.

> **Observação:** O documento de credenciais exportado também contém informações de intervalos que são definidas no sistema do qual o documento foi exportado. Durante a importação do documento de credenciais, as informações de intervalos também são importadas.

**Para exportar as informações de credenciais do Servidor do UCMDB:**

1. No Servidor do UCMDB, abra o navegador da Web e insira o seguinte endereço: **http://localhost:8080/jmx-console**. Você pode precisar fazer logon com um nome de usuário e senha.

2. Clique em **UCMDB:service=DiscoveryManager** para abrir a página Visualização do JMX MBEAN.

3. Localize a operação **exportCredentialsAndRangesInformation**. Siga este procedimento:

   - Insira seu ID de cliente (o padrão é 1).
   - Insira um nome para o arquivo exportado.
   - Digite a senha.
   - Defina **isEncrypted=True** se quiser que o arquivo exportado seja criptografado com a senha fornecida ou **isEncrypted=False** se quiser que o arquivo exportado não seja criptografado (nesse caso, senhas e outras informações confidenciais não serão exportadas).

4. Clique em **Invoke** para exportar.

   Quando o processo de exportação for concluído com êxito, o arquivo será salvo no seguinte local: **C:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>**.

**Para importar as informações de credenciais do Servidor do UCMDB:**

1. No Servidor do UCMDB, abra o navegador da Web e insira o seguinte endereço: **http://localhost:8080/jmx-console**.

   Você pode precisar fazer logon com um nome de usuário e senha.

2. Clique em **UCMDB:service=DiscoveryManager** para abrir a página Visualização do JMX MBEAN.

3. Localize a operação **importCredentialsAndRangesInformation**.

4. Insira seu ID de cliente (o padrão é 1).

5. Insira o nome do arquivo a ser importado. Esse arquivo deve estar localizado em **c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>**.

6. Insira a senha. Ela deve usar a mesma senha que foi usada quando o arquivo foi exportado.

7. Clique em **Invoke** para importar as credenciais.

# Alterar o nível da mensagem do arquivo de log do cliente do Confidentiality Manager

A Sonda fornece dois arquivos de log que contêm informações sobre comunicação relacionada ao Confidential Manager entre o cliente do Confidential Manager e o servidor do Confidential Manager. Os arquivos são:

- "Arquivo de log do cliente do Confidential Manager" abaixo
- "Arquivo de log do LW-SSO" abaixo

## Arquivo de log do cliente do Confidential Manager

O arquivo **security.cm.log** fica localizado na pasta **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

O log contém mensagens de informação trocadas entre o servidor do Confidential Manager e o cliente do Confidential Manager. Por padrão, o nível de log dessas mensagens está definido como INFO.

**Para alterar o nível de log das mensagens para DEBUG:**

1. No servidor do Gerenciador de Data Flow Probe, navegue até **c:\hp\UCMDB\DataFlowProbe\conf\log**.
2. Abra o arquivo **security.properties** em um editor de texto.
3. Mude a linha:

   ```
   loglevel.cm=INFO
   ```

   para:

   ```
   loglevel.cm=DEBUG
   ```

4. Salve o arquivo.

## Arquivo de log do LW-SSO

O arquivo **security.lwsso.log** file fica localizado na pasta **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

O log contém mensagens de informações relacionadas ao LW-SSO. Por padrão, o nível de log dessas mensagens está definido como INFO.

Para alterar o nível de log das mensagens para DEBUG:

1. No servidor do Gerenciador de Data Flow Probe, navegue até **c:\hp\UCMDB\DataFlowProbe\conf\log**.

2. Abra o arquivo security.properties em um editor de texto.
3. Mude a linha:

   ```
   loglevel.lwsso=INFO
   ```

   para:

   ```
   loglevel.lwsso=DEBUG
   ```

4. Salve o arquivo.

# Gerar ou atualizar a chave de criptografia

Você pode gerar ou atualizar uma chave de criptografia para ser usada para criptografia ou descriptografia das configurações de comunicação e autenticação do Confidential Manager trocadas entre o Servidor do UCMDB e o Data Flow Probe. Em cada caso (gerar ou atualizar), o Servidor do UCMDB cria uma nova chave de criptografia baseada em parâmetros que você fornece (por exemplo, comprimento da chave, ciclos extras de PBE, fornecedor de JCE) e a distribui às Sondas.

O resultado de executar o método **generateEncryptionKey** é uma nova chave de criptografia gerada. Essa chave é guardada somente em armazenamento protegido e seu nome e detalhes não são conhecidos. Se você reinstalar umo Data Flow Probe existente ou conectar uma nova Sonda ao Servidor do UCMDB, essa nova chave gerada não será reconhecida pela nova Sonda. Nesses casos, é preferível usar o método **changeEncryptionKey** para alterar as chaves de criptografia. Dessa forma, quando você reinstalar uma Sonda ou instalar uma nova, poderá importar a chave existente (cujo nome e local você conhece) executando o método **importEncryptionKey** no console JMX da Sonda.

**Observação:**

- A diferença entre os métodos usados para criar uma chave (**generateEncryptionKey**) e atualizar uma chave (**changeEncryptionKey**) é que **generateEncryptionKey** cria uma nova chave de criptografia aleatória, enquanto **changeEncryptionKey** importa uma chave de criptografia cujo nome você fornece.
- Só pode existir uma chave de criptografia em um sistema, independentemente da quantidade de Sondas instaladas.

Esta tarefa inclui as seguintes etapas:

- "Gerar uma nova chave de criptografia" Na página seguinte
- "Atualizar uma chave de criptografia em um Servidor do UCMDB" Na página66
- "Atualizar uma chave de criptografia em uma Sonda" Na página67

- "Alterar manualmente a chave de criptografia quando o Probe Manager e o Probe Gateway são instalados em computadores separados" Na página68
- "Definir diversos provedores de JCE" Na página68

# Gerar uma nova chave de criptografia

Você pode gerar uma nova chave para ser usada pelo Servidor do UCMDB e pelo Data Flow Probe para criptografia ou descriptografia. O Servidor do UCMDB substitui a chave antiga pela nova gerada e distribui essa chave entre as Sondas.

**Para gerar uma nova chave de criptografia através do console JMX:**

1. No Servidor do UCMDB, abra o navegador da Web e insira o seguinte endereço: **http://localhost:8080/jmx-console**.

   Você pode precisar fazer logon com um nome de usuário e senha.

2. Clique em **UCMDB:service=DiscoveryManager** para abrir a página Visualização do JMX MBEAN.

3. Localize a operação generateEncryptionKey.

   a. Na caixa de parâmetro **customerId**, insira 1 (o padrão).

   b. Para **keySize**, especifique o comprimento da chave de criptografia. Os valores válidos são 128, 192 ou 256.

   c. Para **usePBE**, especifique **True** ou **False**:

      - **Verdadeiro:** usar ciclos de hash PBE adicionais.
      - **False:**não usar ciclos de hash PBE adicionais.

   d. Para **jceVendor**, você pode escolher usar um provedor de JCE não padrão. Se a caixa ficar vazia, o provedor padrão será usado.

   e. Para **autoUpdateProbe**, especifique **True** ou **False**:

      - **Verdadeiro:** o servidor distribui a nova chave às Sondas automaticamente.
      - **False:** a nova chave deve ser colocada nas Sondas manualmente.

   f. Para **exportEncryptionKey**, especifique **True** ou **False**.

      - **Verdadeiro:** Além de criar a nova senha e guardá-la em armazenamento protegido, o Servidor exporta a nova senha para o sistema de arquivos (**c:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin**). Essa opção permite atualizar Sondas manualmente com a nova senha.

- **False:** A nova senha não é exportada para o sistema de arquivos. Para atualizar Sondas manualmente, defina **autoUpdateProbe** como False e **exportEncryptionKey** como True.

> **Observação:** Verifique se a Sonda está ativa e conectada ao servidor. Se a Sonda ficar inativa, a chave não conseguirá atingi-la. Se você alterar a chave antes da Sonda ficar inativa, quando ela voltar a ficar ativa, a chave será enviada novamente para ela. Porém, se você tiver alterado a chave mais de uma vez antes da Sonda ficar inativa, deverá alterar a chave manualmente através do console JMX. (Selecione **False** para **exportEncryptionKey**).

4. Clique em **Invoke** para gerar a chave de criptografia.

# Atualizar uma chave de criptografia em um Servidor do UCMDB

Você usa o método **changeEncryptionKey** para importar sua própria chave de criptografia para o servidor do UCMDB e distribuí-la entre todas as Sondas.

**Para atualizar uma chave de criptografia através do console JMX:**

1. No Servidor do UCMDB, abra o navegador da Web e insira o seguinte endereço: **http://localhost:8080/jmx-console.**

   Você pode precisar fazer logon com um nome de usuário e senha.

2. Clique em **UCMDB:service=DiscoveryManager** para abrir a página Visualização do JMX MBEAN.

3. Localize a operação **changeEncryptionKey**.

   a. Na caixa de parâmetro **customerId**, insira **1** (o padrão).

   b. Para **newKeyFileName**, insira o nome da nova chave.

   c. Para **keySizeInBits**, especifique o comprimento da chave de criptografia. Os valores válidos são 128, 192 ou 256.

   d. Para **usePBE**, especifique **True** ou **False**:

      - **Verdadeiro:** usar ciclos de hash PBE adicionais.
      - **False:**não usar ciclos de hash PBE adicionais.

   e. Para **jceVendor**, você pode escolher usar um provedor de JCE não padrão. Se a caixa

ficar vazia, o provedor padrão será usado.

f. Para **autoUpdateProbe**, especifique **True** ou **False**:

- **Verdadeiro:** o servidor distribui a nova chave às Sondas automaticamente.
- **False:** a nova chave deve ser distribuída manualmente usando o console JMX da Sonda.

> **Observação:** Verifique se a Sonda está ativa e conectada ao servidor. Se a Sonda ficar inativa, a chave não conseguirá atingi-la. Se você alterar a chave antes da Sonda ficar inativa, quando ela voltar a ficar ativa, a chave será enviada novamente para ela. Porém, se você tiver alterado a chave mais de uma vez antes da Sonda ficar inativa, deverá alterar a chave manualmente através do console JMX. (Selecione **False** para **autoUpdateProbe**).

4. Clique em **Invoke** para gerar e atualizar a chave de criptografia.

# Atualizar uma chave de criptografia em uma Sonda

Se você optar por não distribuir uma chave de criptografia do Servidor do UCMDB para todas as Sondas automaticamente (devido a questões de segurança), você deverá baixar a nova chave de criptografia em todas as Sondas e executar o método **importEncryptionKey** na Sonda:

1. Coloque a chave de criptografia no diretório **C:\hp\UCMDB\DataFlowProbe\conf\security**.
2. No computador da Sonda, abra o navegador da Web e insira o seguinte endereço: **http://localhost:1977**.

   Você pode precisar fazer logon com um nome de usuário e senha.

   > **Observação:** Se o Probe Manager e o Probe Gateway estiverem sendo executados como processos separados, o endereço deverá será inserido no computador que estiver executando o Probe Manager da seguinte forma: **http://localhost:1978**.

3. No domínio da Sonda, clique em **type=SecurityManagerService**.
4. Localize o método **importEncryptionKey**.
5. Insira o nome do arquivo da chave de criptografia que reside em **C:\hp\UCMDB\DataFlowProbe\conf\security**. Esse arquivo contém a chave a ser importada.

6. Clique no botão **importEncryptionKey**.

7. Reiniciar a sonda.

# Alterar manualmente a chave de criptografia quando o Probe Manager e o Probe Gateway são instalados em computadores separados

1. No computador do Probe Manager, inicie o serviço do Probe Manager (**Iniciar > Programas > HP UCMDB > Probe Manager**).

2. Importe a chave do servidor, usando o JMX do Probe Gateway. Para obter detalhes, consulte "Gerar uma nova chave de criptografia" Na página65.

3. Após a chave de criptografia ser importada com êxito, reinicie os serviços do Probe Manager e do Probe Gateway.

# Definir diversos provedores de JCE

Quando você gera uma chave de criptografia através do console JMX, pode definir diversos provedores de JCE, usando os métodos **changeEncryptionKey** e **generateEncryptionKey**.

**Para alterar o provedor de JCE padrão:**

1. Registre os arquivos jar do provedor de JCE em **$JRE_HOME/lib/ext**.

2. Copie os arquivos jar para a pasta $JRE_HOME:

   - Para o servidor UCMDB: o $JRE_HOME reside em: **c:\hp\UCMDB\UCMDBServer\bin\jre**

   - Para o Data Flow Probe: o $JRE_HOME reside em: **c:\hp\UCMDB\DataFlowProbe\bin\jre**

3. Adicione a classe do provedor ao final da lista de provedores no arquivo **$JRE_HOME\lib\security\java.security**.

4. Atualize os arquivos **local_policy.jar** e **US_export_policy.jar** para incluir políticas JCE ilimitadas. Você pode baixar esses arquivos jar do site da Sun.

5. Reinicie o Servidor do UCMDB e o Data Flow Probe.

6. Localize o campo do fornecedor de JCE para o método **changeEncryptionKey** ou **generateEncryptionKey** e adicione o nome do provedor de JCE.

# Configurações de criptografia do Confidential Manager

Esta tabela lista as configurações de criptografia que podem ser alteradas usando vários métodos JMX. Essas configurações de criptografia são relevantes para a criptografia da comunicação entre o cliente do Confidential Manager e o servidor do Confidential Manager, bem como para a criptografia do cache do cliente do Confidential Manager.

| Nome da Configuração do Confidential Manager | Nome da Configuração do Confidential Manager da Sonda | Descrição da configuração | Valores possíveis | Valor padrão |
|---|---|---|---|---|
| cryptoSource | Encryption Library name | Esta configuração define qual biblioteca de criptografia usar. | lw, jce, windowsDPAPI, lwJCECompatible | lw |
| lwJCEPBE CompatibilidadeModo | Support previous lightweight cryptography versions | Esta configuração define se há ou não suporte para a criptografia leve anterior. | true, false | true |
| engineName | Engine name | Nome do mecanismo de criptografia | AES, DES, 3DES, Blowfish | AES |
| keySize | Key size | Comprimento da chave de criptografia em bits | Para AES - 128, 192 ou 256;<br>Para DES - 64;<br>Para 3DES - 192;<br>Para Blowfish - qualquer número entre 32 e 448 | 256 |
| algoritmo Padding Nome | Algorithm padding name | Padrões de preenchimento | PKCS7Padding, PKCS5Padding | PKCS7Padding |
| pbeCount | PBE count | O número de vezes para executar o hash para criar a chave a partir da senha (cadeia init) | Qualquer número positivo | 20 |

| Nome da Configuração do Confidential Manager | Nome da Configuração do Confidential Manager da Sonda | Descrição da configuração | Valores possíveis | Valor padrão |
|---|---|---|---|---|
| pbeDigest Algoritmo | PBE digest algorithm | Tipo de hash | SHA1, SHA256, MD5 | SHA1 |
| useMacWith Crypto | Use MAC with cryptography | Indicação se se deve usar MAC com a criptografia | true, false | false |
| macKeySize | MAC key size | Depende do algoritmo de MAC | 256 | 256 |

# Solução de problemas e limitações

Se você alterar o nome de domínio padrão no servidor do UCMDB, primeiramente deverá verificar se o Data Flow Probe não está em execução. Depois que o nome de domínio padrão for aplicado, você precisará executar o script **DataFlowProbe\tools\clearProbeData.bat** no lado do Data Flow Probe.

**Observação:** A execução do script clearProbeData.bat ocasionará um ciclo de descoberta no lado da Sonda depois que ela estiver em operação.

# Capítulo 5: Proteção do Data Flow Probe

Este capítulo inclui:



# Modificar a senha criptografada do banco de dados PostgreSQL

Esta seção explica como modificar a senha criptografada para o usuário do banco de dados PostgreSQL.

1. Criar a forma criptografada de uma senha (AES, chave de 192 bits)

   a. Acesse o console JMX do Data Flow Probe. inicie um navegador da Web e insira o seguinte endereço: **http://<nome da máquina ou endereço IP do Data Flow Probe>:1977**. Se estiver executando o Data Flow Probe localmente, insira **http://localhost:1977**.

   Você pode precisar fazer logon com um nome de usuário e senha.

> **Observação:** Se não tiver criado um usuário, use o nome de usuário padrão sysadmin e a senha sysadmin para fazer logon.

b. Localize o serviço **Type=MainProbe** e clique no link para abrir a página Operations.

c. Localize a operação **getEncryptedDBPassword**.

d. No campo **DB Password**, insira a senha a ser criptografada.

e. Invoque a operação clicando no botão **getEncryptedDBPassword**.

O resultado da invocação é uma cadeia de senha criptografada, por exemplo:

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61
,61
```

2. Parar o Data Flow Probe

Iniciar > Todos os Programas > HP UCMDB > Parar Data Flow Probe

3. Executar o script set_dbuser_password.cmd

Esse script está localizado na seguinte pasta:
**C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\set_dbuser_password.cmd**

Execute o script **set_dbuser_password.cmd** com a nova senha como o primeiro argumento e a senha da conta raiz do PostgreSQL como o segundo argumento.

Por exemplo:

**set_dbuser_password <my_password><root_password>**.

A senha deve ser inserida em sua forma não criptografada (como texto simples).

4. Atualizar a senha nos arquivos de configuração do Data Flow Probe

a. A senha deve residir criptografada nos arquivos de configuração. Para recuperar a forma criptografada da senha, use o método JMX **getEncryptedDBPassword**, conforme explicado na etapa 1.

b. Adicione a senha criptografada às seguintes propriedades no arquivo **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

- **appilog.agent.probe.jdbc.pwd**

Por exemplo:

```
appilog.agent.probe.jdbc.user = mamprobe
appilog.agent.probe.jdbc.pwd =
```

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,
61,61
```

- **appilog.agent.local.jdbc.pwd**
- **appilog.agent.normalization.jdbc.pwd**

5. Iniciar o Data Flow Probe

   **Iniciar > Todos os Programas > HP UCMDB > Iniciar Data Flow Probe**

# O script clearProbeData: uso

Para recriar o usuário do banco de dados sem alterar sua senha atual, execute o script **clearProbeData.bat** para Windows ou o script **clearProbeData.sh** para Linux.

**Após executar o script:**

- Examine o seguinte arquivo em busca de erros: **C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log** para Windows, **/opt/hp/UCMDB/DataFlowProbe/runtime/log/probe_setup.log** para Linux.
- Exclua o arquivo, pois ele contém a senha do banco de dados.

**Observação:** Não execute esse script a menos que você seja instruído a fazê-lo pela equipe de Suporte ao Software HP.

# Definir a senha criptografada do console JMX

Esta seção explica como criptografar a senha para o usuário do banco do JMX. A senha criptografada é armazenada no arquivo DataFlowProbe.properties. Os usuários devem fazer logon para acessar o console JMX.

1. **Criar a forma criptografada de uma senha (AES, chave de 192 bits)**
   a. Acesse o console JMX do Data Flow Probe. inicie um navegador da Web e insira o seguinte endereço: **http://<nome da máquina ou endereço IP do Data Flow Probe>:1977**. Se estiver executando o Data Flow Probe localmente, insira **http://localhost:1977**.

      Você pode precisar fazer logon com um nome de usuário e senha.

      **Observação:** Se não tiver criado um usuário, use o nome de usuário padrão sysadmin e a senha sysadmin para fazer logon.

   b. Localize o serviço **Type=MainProbe** e clique no link para abrir a página Operations.

c. Localize a operação **getEncryptedKeyPassword**.

d. No campo **Key Password**, insira a senha a ser criptografada.

e. Invoque a operação clicando no botão **getEncryptedKeyPassword**.

O resultado da invocação é uma cadeia de senha criptografada, por exemplo:

```
85,-9,-61,11,105,-93,-81,118
```

### 2. Parar o Data Flow Probe

**Iniciar > Todos os Programas > HP UCMDB > Parar Data Flow Probe**

### 3. Adicionar a senha criptografada

Adicione a senha criptografada à seguinte propriedade no arquivo **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

**appilog.agent.Probe.JMX.BasicAuth.Pwd**

Por exemplo:

```
appilog.agent.Probe.JMX.BasicAuth.User=sysadmin
appilog.agent.Probe.JMX.BasicAuth.Pwd=12,-35,-37,82,-2,20,57,-40,38,80,-111,-99,-64,-5,35,-122
```

**Observação:** para desabilitar a autenticação, deixe esses campos vazios. Se você fizer isso, os usuários poderão abrir a página principal do console JMX da Sonda sem inserir uma autenticação.

### 4. Iniciar o Data Flow Probe

**Iniciar > Todos os Programas > HP UCMDB > Iniciar Data Flow Probe**

Teste o resultado em um navegador da Web.

# Definir a senha de UpLoadScanFile

Esta seção explica como definir a senha para **UpLoadScanFile**, usado para gravação de varredura fora do local. A senha criptografada é armazenada no arquivo **DataFlowProbe.properties**. Os usuários devem fazer logon para acessar o console JMX.

1. **Criar a forma criptografada de uma senha (AES, chave de 192 bits)**

   a. Acesse o console JMX do Data Flow Probe. inicie um navegador da Web e insira o seguinte endereço: **http://<nome da máquina ou endereço IP do Data Flow Probe>:1977**. Se estiver executando o Data Flow Probe localmente, insira

**http://localhost:1977**.

Você pode precisar fazer logon com um nome de usuário e senha.

> **Observação:** Se não tiver criado um usuário, use o nome de usuário padrão sysadmin e a senha sysadmin para fazer logon.

b. Localize o serviço **Type=MainProbe** e clique no link para abrir a página Operations.

c. Localize a operação **getEncryptedKeyPassword**.

d. No campo **Key Password**, insira a senha a ser criptografada.

e. Invoque a operação clicando no botão **getEncryptedKeyPassword**.

O resultado da invocação é uma cadeia de senha criptografada, por exemplo:

```
85,-9,-61,11,105,-93,-81,118
```

2. **Parar o Data Flow Probe**

**Iniciar > Todos os Programas > HP UCMDB > Parar Data Flow Probe**

3. **Adicionar a senha criptografada**

Adicione a senha criptografada à seguinte propriedade no arquivo **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

**com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd**

Por exemplo:

```
com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.User=UploadScanFile
com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd=116,116,21,34,-59,77,-
108,14,127,4,-89,101,-33,-31,116,53
```

4. **Iniciar o Data Flow Probe**

**Iniciar > Todos os Programas > HP UCMDB > Iniciar Data Flow Probe**

Teste o resultado em um navegador da Web.

# Acesso Remoto ao PostgreSQL Server

Esta seção explica como permitir/restringir o acesso à conta do Data Flow Probe PostgreSQL a partir de máquinas remotas.

> **Observação:**

- Por padrão, o acesso é restrito.
- Não é possível acessar a conta raiz do PostgreSQL a partir de máquinas remotas.

Para permitir acesso ao PostgreSQL:

- Execute o script a seguir em uma janela do prompt de comando:

  **C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\enable_remote_user_access.cmd**

**Para restringir acesso ao PostgreSQL:**

- Execute o script a seguir em uma janela do prompt de comando:

  **C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\remove_remote_user_access.cmd**

# Habilitar SSL entre o Servidor do UCMDB e o Data Flow Probe

Você pode configurar a autenticação para o Data Flow Probe e o Servidor do UCMDB com certificados. O certificado para cada componente é enviado e autenticado antes da conexão ser estabelecida.

**Observação:** O método a seguir de habilitar SSL no Data Flow Probe é o mais seguro e é, portanto, o modo de comunicação recomendado. Esse método substitui o procedimento de autenticação básica.

Esta seção inclui os seguintes tópicos:



## Visão geral

O UCMDB fornece suporte para os seguintes modos de comunicação entre o Servidor do UCMDB e o Data Flow Probe:

- **Autenticação do servidor.** Este modo usa SSL, e a Sonda autentica o certificado do Servidor do UCMDB. Para obter detalhes, consulte "Habilitar SSL com autenticação do servidor (unidirecional)" Na página seguinte.

- **Autenticação mútua.** Este modo usa SSL e habilita tanto a autenticação do Servidor pela Sonda quanto a autenticação do cliente pelo Servidor. Para obter detalhes, consulte "Ativar autenticação mútua de certificado (bidirecional)" Na página80.
- **HTTP padrão.** Sem comunicação SSL. Este é o modo padrão, e o componente de Data Flow Probe no UCMDB não requer nenhum certificado. O Data Flow Probe se comunica com o servidor através do protocolo HTTP padrão.

**Observação:** A descoberta não pode usar cadeias de certificado ao trabalhar com SSL. Portanto, se estiver usando cadeias de certificados, você deve gerar um certificado autoassinado para o Data Flow Probe poder se comunicar com o Servidor UCMDB.

# Repositórios de chaves e repositórios confiáveis

O Servidor do UCMDB e o Data Flow Probe trabalham com repositórios de chaves e repositórios confiáveis:

- **Repositório de chave.** Um arquivo contendo entradas de chave (um certificado e uma chave privada correspondente).
- **Repositório confiável.** Um arquivo contendo certificados que são usados para verificar um host remoto (por exemplo, ao usar autenticação do servidor, o repositório confiável do Data Flow Probe deve incluir o certificado do Servidor do UCMDB).

**Limitação da autenticação mútua**

O repositório de chaves do Data Flow Probe (conforme definido em **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**) deve conter apenas 1 (uma) entrada de chave.

# Habilitar SSL com autenticação do servidor (unidirecional)

Isso usa SSL e a sonda autentica o certificado do Servidor.

Esta tarefa inclui:

- "Pré-requisitos" abaixo
- "Configuração do Servidor do UCMDB" Na página seguinte
- "Configuração do Data Flow Probe" Na página79
- "Reinicie os computadores" Na página80

**Pré-requisitos**

1. Verifique se o UCMDB e o Data Flow Probe estão em execução.

   **Observação:** Se a Sonda estiver instalada em modo separado, estas instruções referem-se ao Probe Gateway.

2. Se o UCMDB ou o Data Flow Probe não estiverem instalados nas pastas padrão, anote o local correto e altere os comandos de acordo.

**Configuração do Servidor do UCMDB**

1. **Exporte o certificado do UCMDB**

   a. Abra o prompt de comando e execute o comando:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias <alias do repositório de chaves> -keystore <caminho do arquivo do repositório de chaves> -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   onde:

   - **keystore alias** é o nome dado ao repositório de chaves.
   - **Caminho do arquivo do repositório de chaves** é o caminho completo do local do arquivo do repositório de chaves.

   Por exemplo, para o server.keystore integrado, use o seguinte comando:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -keystore C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   b. Insira a senha do repositório de chaves. Por exemplo, a senha do repositório de chaves incorporada é **hppass**.

   c. Verifique se o certificado foi criado no seguinte diretório: **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **Proteger o conector do Data Flow Probe no UCMDB**

   a. Acesse o console JMX do UCMDB: No seu navegador da Web, insira a seguinte URL: **http://<nome do computador com UCMDB ou endereço IP>:8080/jmx-console**. Você pode precisar fazer logon com um nome de usuário e senha.

   b. Selecione o serviço: **Serviços de gerenciamento de portas**.

   c. Chame o método **PortsDetails** e anote o número da porta para HTPPS. (Padrão: 8443) Verifique se o valor na coluna **Is Enabled** é **True**.

d. Retornar a **Serviços de gerenciamento de portas**.

e. Para mapear o conector do Data Flow Probe para o modo de autenticação de servidor, invoque o método **mapComponentToConnectors** com os seguintes parâmetros:

- **componentName**: mam-collectors
- **isHTTPS**: true
- **Todos os outros sinalizadores**: false

A seguinte mensagem será exibida:

> **Operação bem-sucedida. Component mam-collectors is now mapped to: HTTPS ports.**

f. Retornar a **Serviços de gerenciamento de portas**.

g. Para mapear o conector do Confidential Manager para o modo de autenticação de servidor, invoque o método **mapComponentToConnectors** com os seguintes parâmetros:

- **componentName**: cm
- **isHTTPS**: true
- **Todos os outros sinalizadores**: false

A seguinte mensagem será exibida:

> **Operation succeeded. Component cm is now mapped to: HTTPS ports.**

3. **Copiar o certificado do UCMDB para cada máquina de sonda**

Copie o arquivo do certificado, **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**, na máquina do servidor UCMDB para a seguinte pasta em cada máquina do Data Flow Probe **C:\HP\UCMDB\DataFlowProbe\conf\security**

**Configuração do Data Flow Probe**

> **Observação:** Você deve configurar cada máquina do Data Flow Probe.

1. **Importe o arquivo server.cert, criado em** "Exporte o certificado do UCMDB" Na página anterior**, para o repositório confiável da sonda.**

a. Abra o prompt de comando e execute o comando:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore C:
\HP\UCMDB\DataFlowProbe\conf\security\hpprobeTrustStore.jks -file C:\HP\U
CMDB\DataFlowProbe\conf\security\server.cert -alias hpcert
```

b. Insira a senha do repositório de chaves: logomania

c. Quando for perguntado **Trust this certificate?**, pressione **y** e depois **Enter**.

A seguinte mensagem será exibida:

**Certificado adicionado ao repositório de chaves.**

2. **Abra o arquivo DataFlowProbe.properties localizado em: C:\HP\UCMDB\DataFlowProbe\conf**

a. Atualize a propriedade **appilog.agent.probe.protocol** para **HTTPS**.

b. Atualize a propriedade **serverPortHttps** para o número da porta relevante. (Usar o número da porta da etapa 2c de "Configuração do Servidor do UCMDB" Na página78.)

**Reinicie os computadores**

Reinicie o Servidor do UCMDB e as máquinas de sonda.

# Ativar autenticação mútua de certificado (bidirecional)

Este modo usa SSL e habilita tanto a autenticação do Servidor pela Sonda quanto a autenticação do cliente pelo Servidor. Tanto o Servidor quanto a Sonda enviam seus certificados para a outra entidade para autenticação.

Esta tarefa inclui:

- "Pré-requisitos" abaixo
- "Configuração inicial do Servidor do UCMDB" Na página seguinte
- "Configuração do Data Flow Probe" Na página82
- "Configuração adicional do Servidor do UCMDB" Na página85
- "Reinicie os computadores" Na página85

**Pré-requisitos**

1. Verifique se o UCMDB e o Data Flow Probe estão em execução.

   **Observação:** Se a Sonda estiver instalada em modo separado, estas instruções referem-se ao Probe Gateway.

2. Se o UCMDB ou o Data Flow Probe não estiverem instalados nas pastas padrão, anote o local correto e altere os comandos de acordo.

**Configuração inicial do Servidor do UCMDB**

1. **Exporte o certificado do UCMDB**

   a. Abra o prompt de comando e execute o comando:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias <alias do repositório de chaves> -keystore <caminho do arquivo do repositório de chaves> -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   onde:

   - **keystore alias** é o nome dado ao repositório de chaves.
   - **Caminho do arquivo do repositório de chaves** é o caminho completo do local do arquivo do repositório de chaves.

   Por exemplo, para o server.keystore integrado, use o seguinte comando:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -keystore C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   b. Insira a senha do repositório de chaves. Por exemplo, a senha do repositório de chaves incorporada é **hppass**.

   c. Verifique se o certificado foi criado no seguinte diretório: **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **Proteger o conector do Data Flow Probe no UCMDB**

   a. Acesse o console JMX do UCMDB: No seu navegador da Web, insira a seguinte URL: **http://<nome do computador com UCMDB ou endereço IP>:8080/jmx-console**. Você pode precisar fazer logon com um nome de usuário e senha.

   b. Selecione o serviço: **Serviços de gerenciamento de portas**.

   c. Chame o método **PortsDetails** e anote o número da porta para HTPPS com autenticação de cliente. (Padrão: 8444) Verifique se o valor na coluna **Is Enabled** é **True**.

d. Retornar a **Serviços de gerenciamento de portas**.

e. Para mapear o conector do Data Flow Probe para o modo de autenticação mútua, invoque o método **mapComponentToConnectors** com os seguintes parâmetros:

- **componentName**: mam-collectors
- **isHTTPSWithClientAuth**: true
- **Todos os outros sinalizadores**: false

A seguinte mensagem será exibida:

**Operation succeeded. Component mam-collectors is now mapped to: HTTPS_CLIENT_AUTH ports.**

f. Retornar a **Serviços de gerenciamento de portas**.

g. Para mapear o conector do Gerenciador Confidencial para o modo de autenticação mútua, invoque o método **mapComponentToConnectors** com os seguintes parâmetros:

- **componentName**: cm
- **isHTTPSWithClientAuth**: true
- **Todos os outros sinalizadores**: false

A seguinte mensagem será exibida:

**Operation succeeded. Component cm is now mapped to: HTTPS_CLIENT_AUTH ports.**

3. **Copiar o certificado do UCMDB para cada máquina de sonda**

Copie o arquivo do certificado, **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**, na máquina do servidor UCMDB para a seguinte pasta em cada máquina do Data Flow Probe: **C:\HP\UCMDB\DataFlowProbe\conf\security**

**Configuração do Data Flow Probe**

**Observação:** Você deve configurar cada máquina do Data Flow Probe.

1. **Importe o arquivo server.cert, criado em** "Exporte o certificado do UCMDB" Na página anterior**, para o repositório confiável da sonda.**

a. Abra o prompt de comando e execute o comando:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore C:
\HP\UCMDB\DataFlowProbe\conf\security\hpprobeTrustStore.jks -file C:\HP\U
CMDB\DataFlowProbe\conf\security\server.cert -alias hpcert
```

b. Insira a senha do repositório de chaves: logomania

c. Quando for perguntado **Trust this certificate?**, pressione **y** e depois **Enter**.

A seguinte mensagem será exibida:

**Certificado adicionado ao repositório de chaves.**

2. **Criar um novo arquivo client.keystore**

a. Abra o prompt de comando e execute o comando:

```
c:\HP\UCMDB\DataFlowProbe\bin\jre\keytool –genkey –alias <ProbeName> -key
alg RSA –sigalg SHA256withRSA –keysize 2048 –keystore c:\HP\UCMDB\DataFlo
wProbe\conf\security\client.keystore
```

onde **ProbeName** é o alias exclusivo do Data Flow Probe.

> **Observação:** Para garantir que esse alias seja exclusivo, use o identificador do Nome da Sonda fornecido à Sonda ao definir a Sonda.

b. Insira a senha para o repositório de chaves, de pelo menos 6 caracteres, e anote-a.

c. Insira a senha de novo para confirmar.

d. Pressione **Enter** após responder cada uma das perguntas a seguir:

**Qual o seu nome e sobrenome? [Desconhecido]:**

**Qual é o nome da sua unidade organizacional?[Desconhecido]:**

**Qual é o nome da sua organização?[Desconhecido]:**

**Qual é o nome da sua cidade ou localidade?[Desconhecido]:**

**Qual é o nome do seu estado ou província?[Desconhecido]:**

**Qual o código de país de duas letras para essa unidade?[Descohecido]:**

e. Digite **yes** quando for perguntado **Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?**

f. Pressione **Enter** após responder a pergunta a seguir:

**Insira a senha da chave para <probekey> (RETURN se for igual à senha do repositório de chaves):**

g. Verifique se o arquivo foi criado na pasta a seguir e garanta que o tamanho do arquivo seja maior que 0: **C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore**

3. **Exportar o novo Certificado de Cliente**

   a. Abra o prompt de comando e execute o comando:

   ```
   C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -export -alias <ProbeName> -keystore C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore -file C:\hp\UCMDB\DataFlowProbe\conf\security\<ProbeName>.cert
   ```

   b. Quando solicitado, insira a senha do repositório de chaves. (A senha da Etapa 2b acima.)

   A seguinte mensagem será exibida:

   **Certificado armazenado no arquivo <C:\hp\UCMDB\DataFlowProbe\conf\security\<ProbeName>.cert>**

4. **Abra o arquivo DataFlowProbe.properties localizado em: C:\HP\UCMDB\DataFlowProbe\conf**

   a. Atualize a propriedade **appilog.agent.probe.protocol** para **HTTPS**.

   b. Atualize a propriedade **serverPortHttps** para o número da porta relevante. (Usar o número da porta da etapa 2c de "Configuração inicial do Servidor do UCMDB" Na página81.)

5. **Abra o arquivo ssl.properties localizado em: C:\HP\UCMDB\DataFlowProbe\conf\security**

   a. Atualize a propriedade **javax.net.ssl.keyStore** para **client.keystore**.

   b. Criptografar a senha da Etapa 2b acima:

      i. Inicie o Data Flow Probe (ou verifique se ela já está em execução).

      ii. Acesse o JMX da Sonda. Procurar em: **http://<probe_hostname>:1977**

      Por exemplo, se estiver executando a sonda localmente, vá até: **http://localhost:1977**.

      iii. Pressione o link **type=MainProbe**.

      iv. Role para baixo até a operação **getEncryptedKeyPassword**.

      v. Insira a senha no campo **Senha da Chave**.

      vi. Pressione o botão **getEncryptedKeyPassword**.

c. Copie e cole a senha criptografada para atualizar a propriedade **javax.net.ssl.keyStorePassword**.

> **Observação:** Os números são separados por vírgulas. Por exemplo: -20,50,34,-40,-50.)

6. **Copiar o certificado da Sonda para o computador do UCMDB**

Copie o arquivo **C:\HP\UCMDB\DataFlowProbe\conf\security\client.cert** da máquina do Data Flow Probe para a máquina do UCMDB em **C:\HP\UCMDB\UCMDBServer\conf\security\<ProbeName>.cert**.

**Configuração adicional do Servidor do UCMDB**

1. **Adicionar cada certificado de sonda ao repositório confiável do UCMDB**

> **Observação:** Você deve concluir as seguintes etapas para cada certificado de Sonda.

a. Abra o prompt de comando e execute o comando:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore C:\hp
\UCMDB\UCMDBServer\conf\security\server.truststore -file C:\hp\UCMDB\UCMDB
Server\conf\security\<ProbeName>.cert -alias <ProbeName>
```

b. Insira a senha do repositório de chaves. Por exemplo, a senha do repositório de chaves incorporada é **hppass**.

c. Quando for perguntado **Trust this certificate?**, pressione **y** e depois **Enter**.

A seguinte mensagem será exibida:

**Certificado adicionado ao repositório de chaves**

**Reinicie os computadores**

Reinicie o Servidor do UCMDB e as máquinas de sonda.

# Controlar o local do arquivo domainScopeDocument

O sistema de arquivos da Sonda contém (por padrão) tanto a chave de criptografia quanto o arquivo **domainScopeDocument**. Toda vez que a Sonda é iniciada, recupera o arquivo **domainScopeDocument** do servidor e o armazena em seu sistema de arquivos. Para impedir usuários não autorizados de obter essas credenciais, você pode configurar a Sonda para que o arquivo **domainScopeDocument** seja mantido na memória e não seja armazenado no sistema de arquivos da Sonda.

**Para controlar a localização do arquivo domainScopeDocument:**

1. Abra **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** e altere:

   ```
   appilog.collectors.storeDomainScopeDocument=true
   ```

   para:

   ```
   appilog.collectors.storeDomainScopeDocument=false
   ```

   As pastas serverData do Probe Gateway e do Probe Manager não contêm mais o arquivo **domainScopeDocument**.

   Para ver detalhes sobre como usar o arquivo **domainScopeDocument** para proteger o DFM, consulte "Gerenciamento de credenciais do fluxo de dados" Na página49.

2. Reinicie a Sonda.

# Criar um repositório de chaves para o Data Flow Probe

1. No computador da Sonda, execute o seguinte comando:

   ```
   c:\HP\UCMDB\DataFlowProbe\bin\jre\keytool –genkey –alias <ProbeName> -keyalg
   RSA –sigalg SHA256withRSA –keysize 2048 –keystore c:\HP\UCMDB\DataFlowProbe\
   conf\security\client.keystore
   ```

2. Insira uma senha para o novo repositório de chaves.

3. Insira suas informações quando solicitado.

4. Quando for perguntado **Is CN=… C=… Correct?** insira **yes** e pressione **Enter**.

5. Pressione **Enter** novamente para aceitar a senha do repositório de chaves como senha da chave.

6. Verifique se **client.keystore** foi criado no seguinte diretório: **C:\HP\UCMDB\DataFlowProbe\conf\security**.

# Criptografar as senhas do repositório de chaves e do repositório confiável da Sonda

As senhas do repositório de chaves e do repositório confiável da Sonda são armazenadas criptografadas em **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**. Este procedimento explica como criptografar a senha.

1. Inicie o Data Flow Probe (ou verifique se ela já está em execução).
2. Acesse o console JMX do Data Flow Probe: inicie um navegador da Web e insira o seguinte endereço: http://<nome da máquina do Data Flow Probe ou endereço IP>:1977. Se estiver executando o Data Flow Probe localmente, insira http://localhost:1977.

   **Observação:** Você pode precisar fazer logon com um nome de usuário e senha. Se não tiver criado um usuário, use o nome de usuário padrão sysadmin e a senha sysadmin para fazer logon.
3. Localize o serviço **Type=MainProbe** e clique no link para abrir a página Operations.
4. Localize a operação **getEncryptedKeyPassword**.
5. Insira a senha do repositório de chaves ou do repositório confiável no campo **Key Password** e invoque a operação clicando em **getEncryptedKeyPassword**.
6. O resultado da invocação é uma cadeia de senha criptografada, por exemplo:

   ```
   66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61
   ```
7. Copie e cole a senha criptografada na linha relevante para o repositório de chaves ou o repositório confiável no seguinte arquivo: **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties.**

# Repositório de chaves e repositório confiável padrão do servidor e do Data Flow Probe

Esta seção inclui os seguintes tópicos:


- "Servidor do UCMDB" abaixo
- "Data Flow Probe" Na página seguinte


## Servidor do UCMDB

Os arquivos ficam localizados no seguinte diretório: **C:\HP\UCMDB\UCMDBServer\conf\security.**

| Entidade | Nome do arquivo/termo | Senha/termo | Alias |
|---|---|---|---|
| Repositório de chaves do servidor | server.keystore (sKeyStoreFile) | hppass (sKeyStorePass) | hpcert |

| Entidade | Nome do arquivo/termo | Senha/termo | Alias |
|---|---|---|---|
| Repositório confiável do servidor | server.truststore (sTrustStoreFile) | hppass (sTrustStorePass) | hpcert (entrada confiável padrão) |
| Repositório de chaves do cliente | client.keystore (cKeyStoreFile) | clientpass (cKeyStorePass) | clientcert |

# Data Flow Probe

Os arquivos ficam localizados no seguinte diretório:
**C:\HP\UCMDB\DataFlowProbe\conf\security.**

| Entidade | Nome do arquivo/termo | Senha/termo | Alias |
|---|---|---|---|
| Repositório de chaves da Sonda | hpprobeKeyStore.jks (pKeyStoreFile) | logomania (pKeyStorePass) | hpprobe |
| O Data Flow Probe usa o repositório de chaves **cKeyStoreFile** como repositório de chaves padrão durante o procedimento de autenticação mútua. Esse é um repositório de chaves do cliente que é parte da instalação do UCMDB. | | | |
| Repositório confiável da Sonda | hpprobeTrustStore.jks (pTrustStoreFile) | logomania (pTrustStorePass) | hpprobe (entrada confiável padrão) |
| A senha **cKeyStorePass** é a senha padrão do **cKeyStoreFile**. | | | |

# Capítulo 6: Autenticação LW-SSO (Lightweight Single Sign-On) – Referência geral

Este capítulo inclui:



## Visão geral da autenticação LW-SSO

LW-SSO é um método de controle de acesso que permite ao usuário fazer logon uma vez e obter acesso aos recursos de vários sistemas de software sem que ele precise fazer logon novamente. Os aplicativos dentro do grupo configurado de sistemas de software confiam na autenticação e não há necessidade de autenticação adicional quando o usuário se desloca de um aplicativo para outro.

As informações nesta seção se aplicam ao LW-SSO versão 2.2 e 2.3.

- **Expiração do token do LW-SSO**

  O valor de expiração do token do LW-SSO determina a validade da sessão do aplicativo. Portanto, seu valor de expiração deve ser no mínimo igual ao valor de expiração da sessão do aplicativo.

- **Configuração recomendada da expiração do token do LW-SSO**

  Cada aplicativo que usa o LW-SSO deve configurar a expiração do token. O valor recomendado é de 60 minutos. Para um aplicativo que não requer um nível alto de segurança, é possível configurar um valor de 300 minutos.

- **Hora GMT**

  Todos os aplicativos que participam de uma integração do LW-SSO devem usar a mesma hora GMT, com diferença máxima de 15 minutos.

- **Funcionalidade multidomínio**

A funcionalidade multidomínio requer que todos os aplicativos participantes da integração do LW-SSO definam as configurações de trustedHosts (ou as configurações de **protectedDomains**), se for necessário integrar com aplicativos em diferentes domínios DNS. Além disso, eles também devem adicionar o domínio correto no elemento **lwsso** da configuração.

- **Funcionalidade de obtenção de SecurityToken para URL**

  Para receber informações enviadas como um **SecurityToken para URL** de outros aplicativos, o aplicativo host deve configurar o domínio correto no elemento **lwsso** da configuração.

# Requisitos do LW-SSO

| Aplicativo | Versão | Comentários |
|---|---|---|
| Java | 1.5 e posterior | |
| API de Servlets HTTP | 2.1 e posterior | |
| Internet Explorer | 6.0 e posterior | O navegador deve habilitar cookie de sessão HTTP e a funcionalidade de Redirecionamento HTTP 302. |
| Firefox | 2.0 e posterior | O navegador deve habilitar cookie de sessão HTTP e a funcionalidade de Redirecionamento HTTP 302. |
| Autenticações do JBoss | JBoss 4.0.3<br>JBoss 4.3.0 | |
| Autenticações do Tomcat | Tomcat 5.0.28 autônomo<br>Tomcat 5.5.20 autônomo | |
| Autenticações do Acegi | Acegi 0.9.0<br>Acegi 1.0.4 | |
| Mecanismos de serviços Web | Axis 1 - 1.4<br>Axis 2 - 1.2<br>JAX-WS-RI 2.1.1 | |

# Avisos de segurança do LW-SSO

Esta seção descreve os avisos de segurança que são relevantes para a configuração do LW-SSO:

- **Parâmetro InitString confidencial no LW-SSO.**O LW-SSO usa Criptografia Simétrica para validar e criar um token do LW-SSO. O parâmetro **initString** na configuração é usado para inicialização da chave secreta. Um aplicativo cria um token e cada aplicativo que usa o mesmo parâmetro initString valida o token.

  **Cuidado:**

  - Não é possível usar o LW-SSO sem definir o parâmetro **initString**.
  - O parâmetro **initString** é uma informação confidencial e deve ser tratado como tal em termos de publicação, transporte e persistência.
  - O parâmetro **initString** deve ser compartilhado somente entre aplicativos que se integram entre si usando o LW-SSO.
  - O parâmetro **initString** deve ter um comprimento mínimo de 12 caracteres.

- **Habilite o LW-SSO somente se necessário.**O LWSSO deve ficar desabilitado, a menos que seja especificamente necessário.

- **Nível de segurança da autenticação**. O aplicativo que usa a estrutura de autenticação mais fraca e emite um token do LW-SSO que é considerado confiável por outros aplicativos integrados determina o nível de segurança da autenticação para todos os aplicativos.

  É recomendável que somente aplicativos que usam estruturas de autenticação fortes e seguras emitam um token do LW-SSO.

- **Implicações da criptografia simétrica.**O LW-SSO usa criptografia simétrica para emitir e validar tokens do LW-SSO. Portanto, qualquer aplicativo que usa LW-SSO pode emitir um token para ser confiado por todos os demais aplicativos que compartilham o mesmo parâmetro initString. Esse risco potencial é relevante quando um aplicativo que compartilha um initString reside em um local não confiável ou pode ser acessado a partir dele.

- **Mapeamento de usuários (sincronização).**A estrutura do LW-SSO não assegura o mapeamento de usuários entre os aplicativos integrados. Portanto, o aplicativo integrado deve monitorar o mapeamento de usuários. É recomendável que você compartilhe o mesmo registro de usuários (como LDAP/AD) entre todos os aplicativos integrados.

  Se os usuários não forem mapeados, poderão ocorrer violações de segurança e comportamento negativo dos aplicativos. Por exemplo, o mesmo nome de usuário pode ser atribuído a diferentes usuários reais nos vários aplicativos.

Além disso, em casos onde um usuário faz logon em um aplicativo (AplA) e depois acessa um segundo aplicativo (AplB) que usa autenticação de contêiner ou aplicativo, se o usuário não for mapeado, ele terá de fazer logon manualmente no AplB e inserir um nome de usuário. Se o usuário inserir um nome diferente do usado para fazer logon no AplA, pode surgir o seguinte comportamento: se o usuário subsequentemente acessar um terceiro aplicativo (AplC) do AplA ou AplB, ele o acessará usando os nomes de usuário que foram usados para fazer logon no AplA ou AplB, respectivamente.

- **Gerenciador de Identidade**. Usado para fins de autenticação, todos os recursos não protegidos no Gerenciador de Identidade devem ser definidos com a configuração **nonsecureURLs** no arquivo de configuração do LW-SSO.
- **Modo de demonstração LW-SSO.**
  - O modo de demonstração deve ser usado somente para fins demonstrativos.
  - O modo de demonstração deve ser usado somente em redes não protegidas.
  - O modo de demonstração não deve ser usado em produção. Nenhuma combinação do modo de demonstração com o de produção deve ser usada.

# Solução de problemas e limitações

Esta seção descreve problemas conhecidos e limitações ao trabalhar com a autenticação LW-SSO.

# Problemas conhecidos

Esta seção descreve problemas conhecidos na autenticação LW-SSO.

- **Contexto de segurança.**O contexto de segurança do LW-SSO fornece suporte para apenas um valor de atributo por nome de atributo.

  Portanto, quando o token do SAML2 envia mais de um valor para o mesmo nome de atributo, somente um valor é aceito pela estrutura do LW-SSO.

  Da mesma forma, se o token do IdM é configurado para enviar mais de um valor para o mesmo nome de atributo, somente um valor é aceito pela estrutura do LW-SSO.

- **Funcionalidade de logoff multidomínio ao usar o Internet Explorer 7.** A funcionalidade de logoff multidomínio pode falhar sob as seguintes condições:
  - O navegador usado é o Internet Explorer 7 e o aplicativo está chamando mais de três verbos de redirecionamento HTTP 302 consecutivos no procedimento de logoff.

  Nesse caso, o Internet Explorer 7 pode lidar incorretamente com a resposta de redirecionamento HTTP 302 e exibir uma página de erro **O Internet Explorer não pode exibir a página da Web**.

Como solução alternativa, recomenda-se reduzir, se possível, o número de comandos de redirecionamento de aplicativos na sequência de logoff.

# Limitações

Observe as seguintes limitações ao trabalhar com autenticação LW-SSO:

- **Acesso do cliente ao aplicativo.**

  **Se um domínio está definido na configuração do LW-SSO:**

  - Os clientes do aplicativo devem acessar o aplicativo com um Nome de Domínio Totalmente Qualificado (FQDN) na URL de logon. Exemplo: http://meuservidor.**domíniodaempresa**.com/WebApp.
  - O LW-SSO não dá suporte para URLs com endereço IP. Exemplo: http://192.168.12.13/WebApp..
  - O LW-SSO não dá suporte para URLs sem domínio. Exemplo: http://meuservidor/WebApp.

  **Se um domínio não está definido na configuração do LW-SSO:** O cliente pode acessar o aplicativo sem um FQDN na URL de logon. Nesse caso, um cookie de sessão do LW-SSO é criado especificamente para um único computador sem informações de domínio. Portanto, o cookie não é delegado pelo navegador a outro computador, nem é passado a outros computadores localizados no mesmo domínio DNS. Isso significa que o LW-SSO não funciona no mesmo domínio.

- **Integração de estrutura LW-SSO.**Os aplicativos poderão aproveitar e usar os recursos do LW-SSO somente se forem integrados na estrutura LW-SSO antecipadamente.

- **Suporte para multidomínio.**

  - A funcionalidade multidomínio baseia-se no referenciador HTTP. Portanto, o LW-SSO dá suporte para links de um aplicativo para outro e não dá suporte para a digitação de uma URL em uma janela do navegador, exceto quando ambos os aplicativos estão no mesmo domínio.
  - O primeiro link entre domínios usando **HTTP POST** não tem suporte.

    A funcionalidade multidomínio não dá suporte para a primeira solicitação **HTTP POST** para um segundo aplicativo (somente a solicitação **HTTP GET** tem suporte). Por exemplo, se seu aplicativo tem um link HTTP para um segundo aplicativo, há suporte para uma solicitação **HTTP GET**, mas não para uma solicitação **HTTP FORM**. Todas as solicitações após a primeira podem ser **HTTP POST** ou **HTTP GET**.
  - Tamanho do token do LW-SSO:

O tamanho das informações que o LW-SSO pode transferir de um aplicativo em um domínio para outro aplicativo em outro domínio está limitado a 15 Grupos/Funções/Atributos (observe que cada elemento pode ter em média 15 caracteres de comprimento).

- Vinculando de uma página protegida (HTTPS) para uma não protegida (HTTP) em um cenário multidomínio:

  A funcionalidade multidomínio não funciona quando se vincula de uma página protegida (HTTPS) para uma não protegida (HTTP). Essa é uma limitação do navegador onde o cabeçalho do referenciador não é enviado quando se vincula de um recurso protegido para um não protegido. Para ver um exemplo, consulte: `http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP`

- Comportamento de cookie de terceiros no Internet Explorer:

  O Microsoft Internet Explorer 6 contém um módulo que oferece suporte ao "Projeto Platform for Privacy Preferences (P3P)", o que significa que cookies provenientes de um domínio de terceiros são bloqueados por padrão na zona de segurança da Internet. Cookies de sessão também são considerados cookies de terceiros pelo IE e, portanto, são bloqueados, fazendo com que o LW-SSO pare de funcionar. Para obter detalhes, consulte: `http://support.microsoft.com/kb/323752/en-us`.

  Para resolver esse problema, adicione o aplicativo iniciado (ou um subconjunto do domínio de DNS como *.meudominio.com) à intranet/zona confiável do seu computador (ou no Microsoft Internet Explorer, selecione **Menu > Ferramentas > Opções da Internet > Segurança > Intranet local > Sites > Avançado**), que fará os cookies serem aceitos.

  > **Cuidado:** O cookie de sessão LW-SSO é apenas um dos cookies usados pelo aplicativo de terceiros que é bloqueado.

- **Token do SAML2**

  - A funcionalidade de logoff não tem suporte quando o token do SAML2 é usado.

    Portanto, se o token do SAML2 é usado para acessar um segundo aplicativo, um usuário que faz logoff do primeiro aplicativo não é desconectado do segundo aplicativo.

  - **A expiração do token do SAML2 não é refletida no gerenciamento de sessão do aplicativo.**

    Portanto, se o token do SAML2 é usado para acessar um segundo aplicativo, o gerenciamento de sessão de cada aplicativo é tratado independentemente.

- **JAAS Realm.**O JAAS Realm no Tomcat não tem suporte.

- **Uso de espaços em diretórios do Tomcat.**Não há suporte para o uso de espaços em

diretórios do Tomcat.

Não é possível usar o LW-SSO quando um caminho de instalação do Tomcat (pastas) inclui espaços (por exemplo, Arquivos de Programas) e o arquivo de configuração do LW-SSO está localizado na pasta **common\classes** do Tomcat.

- **Configuração do balanceador de carga.**Um balanceador de carga implantado com o LW-SSO deve ser configurado para usar sticky sessions.
- **Modo de demonstração.** No modo de demonstração, o LW-SSO dá suporte para links de um aplicativo para outro, mas não dá suporte para a digitação de uma URL em uma janela do navegador, devido à ausência de um cabeçalho do referenciador HTTP nesse caso.

# Capítulo 7: Autenticação de logon do HP Universal CMDB

Este capítulo inclui:



# Configurando um método de autenticação

Para realizar a autenticação, você pode trabalhar:

- **Em relação ao serviço interno do HP Universal CMDB.**
- **Através do LDAP (Lightweight Directory Access Protocol).** Você pode usar um servidor LDAP externo dedicado para armazenar informações de autenticação em vez de usar o serviço interno do HP Universal CMDB. O servidor LDAP deve residir na mesma sub-rede que todos os demais servidores do HP Universal CMDB.

  Para ver detalhes sobre LDAP, consulte a seção sobre Mapeamento LDAP no *Guia de Administração do HP Universal CMDB*.

  O método de autenticação padrão usa o serviço interno do HP Universal CMDB. Se você usar o método padrão, não precisará fazer nenhuma alteração no sistema.

  Estas opções aplicam-se aos logons executados através de serviços Web, bem como da interface do usuário.

- **Por LW-SSO.** O HP Universal CMDB está configurado com LW-SSO. O LW-SSO permite fazer logon no HP Universal CMDB ter acesso automaticamente aos outros aplicativos configurados executados no mesmo domínio, sem a necessidade de fazer logon nesses aplicativos.

  Quando o Suporte para Autenticação LW-SSO está habilitado (fica desabilitado por padrão), você deve garantir que os outros aplicativos no ambiente de logon único tenham o LW-SSO habilitado e estejam trabalhando com o mesmo parâmetro initString.

# Habilitando logon no HP Universal CMDB com LW-SSO

**Para habilitar o LW-SSO para o HP Universal CMDB, use o seguinte procedimento:**

1. Acesse o console JMX inserindo o seguinte endereço no navegador da Web: **http://<nome_servidor>:8080/jmx-console**, em que **<nome_servidor>** é o nome do computador em que o HP Universal CMDB está instalado.
2. Em **UCMDB-UI**, selecione **name=LW-SSO configuration** para abrir a página Operations.
3. Defina a cadeia init usando o método **setInitString**.
4. Defina o nome de domínio do computador no qual o UCMDB está instalado usando o método **setDomain**.
5. Invoque o método **setEnabledForUI**, com o parâmetro definido como **True**.
6. **Opcional**. Se desejar trabalhar usando a funcionalidade de vários domínios, selecione o método **addTrustedDomains**, insira os valores do domínio e clique em **Invoke**.
7. **Opcional.** Se desejar trabalhar usando um proxy reverso, selecione o método **updateReverseProxy**, defina o parâmetro **Is reverse proxy enabled** como **True**, insira a URL para o parâmetro **Reverse proxy full server URL** e clique em Chamar. Se desejar acessar o UCMDB diretamente e usando um proxy reverso, defina a seguinte configuração adicional: selecione o método **setReverseProxyIPs**, insira o endereço IP para o parâmetro ip/s do proxy reverso e clique em **Chamar.**
8. **Opcional**. Se desejar acessar o UCMDB usando um ponto de autenticação externo, selecione o método **setValidationPointHandlerEnable**, defina o parâmetro **Is validation point handler enabled** como **True**, insira a URL para o ponto de autenticação no parâmetro **Authentication point server** e clique em **Invoke**.
9. Para visualizar a configuração do LW-SSO como está salva no mecanismo de configurações, invoque o método **retrieveConfigurationFromSettings**.
10. Para visualizar a configuração do LW-SSO efetivamente carregada, invoque o método **retrieveConfiguration**.

**Observação:** Não é possível ativar o LW-SSO pela interface do usuário.

# Definindo uma conexão segura com o protocolo SSL (Secure Sockets Layer)

Como o processo de logon envolve passar informações confidenciais entre o HP Universal CMDB e o servidor LDAP, você pode aplicar um determinado nível de segurança ao conteúdo. Isso é feito habilitando a comunicação SSL no servidor LDAP e configurando o HP Universal CMDB para operar usando SSL.

O HP Universal CMDB aceita SSL que usa um certificado emitido por uma Autoridade de Certificação (CA).

A maioria dos servidores LDAP, inclusive o Active Directory, pode expor uma porta segura para uma conexão baseada em SSL. Se você estiver usando o Active Directory com um CA privado, deverá adicionar seu CA aos CAs confiáveis no JRE.

Para ver detalhes sobre a configuração da plataforma do HP Universal CMDB para suporte à comunicação usando SSL, consulte "Habilitando comunicação SSL" Na página17.

**Para adicionar um CA aos CAs seguros para expor uma porta segura para uma conexão baseada em SSL:**

1. Exporte um certificado do seu CA e importe-o para o JVM que é usado pelo HP Universal CMDB, usando as seguintes etapas:

   a. No computador do Servidor do UCMDB, acesse a pasta **UCMDBServer\bin\JRE\bin** .

   b. Execute o seguinte comando:

   ```
   Keytool -import -file <arquivo do seu certificado> -keystore C:\hp\UCMDB\
   UCMDBServer\bin\JRE\lib\security\cacerts
   ```

   Por exemplo:

   ```
   Keytool -import -file c:\ca2ss_ie.cer -keystore C:\hp\UCMDB\UCMDBServer\b
   in\JRE\lib\security\cacerts
   ```

2. Selecione **Administração > Configurações de Infraestrutura > categoria LDAP Geral**.

   **Observação:** Também é possível definir essas configurações usando o console JMX. Para obter detalhes, consulte "Como habilitar e definir o método de autenticação LDAP usando o console JMX" Na página102.

3. Localize **URL do Servidor LDAP** e insira um valor, usando o formato:

   ```
   ldaps://<hostLdap>[:<porta>]/[<DNbase>][??scope]
   ```

   Por exemplo:

```
ldaps://my.ldap.server:389/ou=People,o=myOrg.com??sub
```

Observe o **s** em **ldaps**.

4. Clique em **Salvar** para salvar o novo valor ou em **Restaurar Padrão** para substituir a entrada pelo valor padrão (uma URL em branco).

# Usando o console JMX para testar conexões LDAP

Esta seção descreve um método para testar a configuração da autenticação LDAP usando o console JMX.

1. Inicie o navegador da Web e insira o seguinte endereço: **http://<nome_servidor>:8080/jmx-console**, em que **<nome_servidor>** é o nome do computador em que o HP Universal CMDB está instalado.

   Você pode precisar fazer logon com um nome de usuário e senha.

2. No **UCMDB**, clique em **UCMDB:service=LDAP Services** para abrir a página Operations.

3. Localize **testLDAPConnection**.

4. Na caixa **Value** do parâmetro **customer id**, insira o ID do cliente.

5. Clique em **Invoke**.

   A página JMX MBEAN Operation Result indicará se a conexão LDAP foi bem-sucedida. Se a conexão for bem-sucedida, a página também mostrará os grupos raiz do LDAP.

# Como habilitar e definir o método de autenticação LDAP

Você pode habilitar e definir o método de autenticação LDAP para um sistema do HP Universal CMDB.

**Observação:**

- Você também pode definir as configurações de autenticação LDAP usando o console JMX. Para obter detalhes, consulte "Como habilitar e definir o método de autenticação LDAP usando o console JMX" Na página102.
- Para ver um exemplo de configurações de autenticação LDAP, consulte "Configurações de autenticação LDAP - exemplo" Na página103.

**Para habilitar e definir o método de autenticação LDAP na interface do usuário do UCMDB:**

1. Selecione **Administração > Configurações de Infraestrutura > categoria LDAP Geral**.
2. Selecione **URL de servidor LDAP** e digite o valor da URL do LDAP, usando o formato:

   ```
   ldap://<ldapHost>[:<port>]/[<baseDN>][??scope]
   ```

   Por exemplo:

   ```
   ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub
   ```

3. Selecione a categoria **Definição de Grupo LDAP**, localize **DN de base de Grupos** e insira o nome diferenciado do grupo geral.
4. Localize **DN de base de grupos raiz** e insira o nome diferenciado do grupo raiz.
5. Selecione a categoria **LDAP Geral**, localize **Habilitar Sincronização de Permissões de Usuário** e verifique se o valor está definido como **Verdadeiro**.
6. Selecione a categoria **Autenticação Geral LDAP**, localize **Senha de Usuário Qualificado para Pesquisa** e preencha a senha.
7. Selecione a categoria **Opções de LDAP para Classes e Atributos**, localize **Objeto de classe de grupo** e preencha o nome da classe do objeto (**group** para Microsoft Active Directory e **groupOfUniqueNames** para Oracle Directory Server).
8. Localize **Atributo de membro dos grupos** e preencha o nome do atributo (**member** para Microsoft Active Directory e **uniqueMember** para Oracle Directory Server).
9. Localize **Classe de objeto de usuários** e preencha o nome da classe do objeto (**user** para Microsoft Active Directory e **inetOrgPerson** para Oracle Directory Server).
10. Localize **Atributo UUID** e preencha o atributo de identificação exclusivo para um usuário no seu servidor de diretórios. Selecione um atributo exclusivo no servidor de diretório. Por exemplo, ao usar SunOne/Oracle Directory Server, o atributo UID não é exclusivo. Nesse caso, use o atributo de endereço de email ou o nome diferenciado. Usar um atributo não exclusivo como o atributo de identificação exclusivo no UCMDB pode causar um comportamento inconsistente durante o logon.
11. Salve os novos valores. Para substituir uma entrada pelo valor padrão, clique em **Restaurar Padrão**.
12. Se a configuração de infraestrutura **A diferenciação de maiúsculas e minúsculas é imposta ao autenticar com LDAP**, em **LDAP Geral**, é definida como **Verdadeira**, a autenticação diferencia maiúsculas de minúsculas.

**Cuidado:** Quando o valor dessa configuração de infraestrutura é alterada, todos os usuários externos devem ser excluídos manualmente pelo administrador do UCMDB.

13. Mapeie grupos de usuários LDAP para grupos de usuários do UCMDB. Para obter detalhes, consulte "Autenticação de logon do HP Universal CMDB" Na página97.

14. Se desejar definir um conjunto padrão de permissões para usuários em um grupo LDAP que não tem um mapeamento de grupo, selecione a categoria **LDAP Geral**, localize **Grupo de Usuários Atribuído Automaticamente** e insira o nome do grupo.

15. **Importante:** Se estiver configurando o LDAP em um ambiente de alta disponibilidade, você deve reiniciar o cluster para que as alterações entrem em vigor.

**Observação:** Cada usuário do LDAP tem um nome, sobrenome e endereço de email salvos no repositório local. Se o valor de qualquer um desses parâmetros armazenado no servidor LDAP for diferente do valor no repositório local, os valores do servidor LDAP substituirão os valores locais em cada logon.

# Como habilitar e definir o método de autenticação LDAP usando o console JMX

Esta tarefa descreve como definir configurações de autenticação LDAP usando o console JMX.

**Observação:**

- Em um ambiente de alta disponibilidade, faça logon no console JMX do servidor de gravação.
- Você também pode definir as configurações de autenticação LDAP no UCMDB. Para obter detalhes, consulte "Como habilitar e definir o método de autenticação LDAP" Na página100.
- Para ver um exemplo de configurações de autenticação LDAP, consulte "Configurações de autenticação LDAP - exemplo" Na página seguinte.

**Para definir as configurações de autenticação LDAP:**

1. Inicie o navegador da Web e insira o seguinte endereço: **http://<nome_servidor>:8080/jmx-console**, em que **<nome_servidor>** é o nome do computador em que o HP Universal CMDB está instalado.

   Você pode precisar fazer logon com um nome de usuário e senha.

2. No **UCMDB**, clique em **UCMDB:service=LDAP Services** para abrir a página Operations.

3. Para exibir as configurações de autenticação LDAP atuais, localize o método **getLDAPSettings**. Clique em **Invoke**. Uma tabela exibirá todas as configurações de LDAP e seus valores.

4. Para alterar os valores das configurações de autenticação LDAP, localize o método **configureLDAP**. Insira os valores das configurações relevantes e clique em **Invoke**. A página JMX MBEAN Operation Result indicará se as configurações de autenticação LDAP foram atualizadas com êxito.

   **Observação:** Se você não inserir um valor para uma configuração, ela preservará seu valor atual.

5. Após definir as configurações de LDAP, você pode verificar as credenciais de usuário LDAP:

   a. Localize o método **verifyLDAPCredentials**.

   b. Insira a ID do cliente, o nome do usuário e a senha.

   c. Clique em **Invoke**.

      A página JMX MBEAN Operation Result indicará se o usuário passou na autenticação LDAP.

6. **Importante:** Se estiver configurando o LDAP em um ambiente de alta disponibilidade, você deve reiniciar o cluster para que as alterações entrem em vigor.

**Observação:** Cada usuário do LDAP tem um nome, sobrenome e endereço de email salvos no repositório local. Se o valor de qualquer um desses parâmetros armazenado no servidor LDAP for diferente do valor no repositório local, os valores do servidor LDAP substituirão os valores locais em cada logon.

# Configurações de autenticação LDAP - exemplo

A tabela a seguir contém um exemplo de valores de configuração para autenticação LDAP:

| Configuração | Valor |
|---|---|
| Classe de objeto de usuários | user |
| distingue entre maiúsculas e minúsculas na autenticação LDAP | false |
| Atributo de membro dos grupos | member |
| Resolução de DN (Nome Diferenciado) | true |

| Configuração | Valor |
|---|---|
| Filtro de grupos raiz | (objectCategory=group) |
| Cadeia da conexão LDAP | ldap://myldap.example.com:389/OU=Users,OU=Dept,OU=US,DC=example,DC=com??sub |
| Usuário de pesquisa LDAP | CN=John Doe,OU=Users,OU=Dept,OU=US,DC=example,DC=com |
| Objeto de classe de grupo | group |
| Usar algoritmo de baixo para cima para encontrar grupos de pais. | true |
| Atributo UUID | sAMAccountName |
| Atributo de nome dos grupos | cn |
| Filtro de Base de Grupo | (objectclass=group) |
| Filtro do usuário | (&(sAMAccountName=*)(objectclass=user)) |
| Contagem de Repetições de Pesquisa | 3 |
| Atributo de nome de exibição dos grupos | cn |
| Escopo de grupos raiz | sub |
| Atributo de nome de exibição do usuário | cn |
| Escopo para pesquisa de grupos | sub |
| Habilitar autenticação LDAP | false |
| Habilitar sincronização LDAP | true |
| Grupo raiz | OU=Users,OU=Security Groups,DC=example,DC=com |
| Base do grupo | OU=AMRND,OU=Security Groups,DC=example,DC=com |
| Grupo padrão | AdminsGroup |
| Atributo de descrição dos grupos | description |

# Recuperando a configuração atual do LW-SSO em um ambiente distribuído

Quando o UCMDB estiver inserido em um ambiente distribuído, por exemplo, em uma implantação do BSM, execute o procedimento a seguir para recuperar a configuração atual do LW-SSO no computador de processamento.

**Para recuperar a configuração atual do LW-SSO:**

1. Inicie um navegador da Web e insira o seguinte endereço: `http://localhost.<nome_domínio>:8080/jmx-console.`

   Seu nome de usuário e senha poderão ser solicitados.

2. Localize **UCMDB:service=Security Services** e clique no link para abrir a página Operations.

3. Localize a operação **retrieveLWSSOConfiguration**.

4. Clique em **Invoke** para recuperar a configuração.

# Capítulo 8: Gerenciador Confidencial

Este capítulo inclui:



# Visão Geral do Gerenciador Confidencial

A estrutura do Confidential Manager resolve o problema de gerenciar e distribuir dados confidenciais para o HP Universal CMDB e outros produtos da HP Software.

O Confidential Manager consiste em dois componentes principais: o cliente e o servidor. Esses dois componentes são responsáveis por transferir dados de maneira segura.

- O cliente do Confidential Manager é uma biblioteca usada pelos aplicativos para acessar dados confidenciais.
- O servidor do Confidential Manager recebe solicitações de clientes do Confidential Manager ou de clientes de terceiros e executa as tarefas necessárias. O servidor do Confidential Manager é responsável por salvar os dados de maneira segura.

O Confidential Manager criptografa credenciais no transporte, no cache do cliente, na persistência e na memória. O Confidential Manager usa criptografia simétrica para transportar credenciais entre o cliente do Confidential Manager e o servidor do Confidential Manager, usando um segredo compartilhado. O Confidential Manager usa vários segredos para criptografia do cache, persistência e transporte de acordo com a configuração.

Para ver diretrizes detalhadas de gerenciamento da criptografia de credenciais no Data Flow Probe, consulte "Gerenciamento de credenciais do fluxo de dados" Na página49.

# Considerações sobre segurança

- Você pode usar os seguintes tamanhos de chave para o algoritmo de segurança: 128, 192 e 256 bits. O algoritmo é executado mais rápido com a chave menor, mas é menos seguro. O tamanho de 128 bits é suficientemente seguro na maioria dos casos.
- Para tornar o sistema mais seguro, use MAC: definir **useMacWithCrypto** como **true.** Para obter detalhes, consulte "Propriedades de criptografia" Na página109.
- Para usar fornecedores de segurança forte para o cliente, você pode usar o modo JCE.

# Configurar o Servidor do HP Universal CMDB

Ao trabalhar com o HP Universal CMDB, você deve configurar as propriedades de segredo e criptográficas da criptografia, usando os seguintes métodos JMX:

1. No computador com o Servidor do HP Universal CMDB, inicie o navegador da Web e insira o endereço do servidor, da seguinte maneira: **http://<Nome de Host do Servidor do UCMDB ou IP>:8080/jmx-console**.

   Você pode precisar fazer logon com um nome de usuário e senha.

2. No UCMDB, clique em **UCMDB:service=Security Services** para abrir a página Operations.

3. Para recuperar a configuração atual, localize a operação **CMGetConfiguration**.

   Clique em **Invoke** para exibir o arquivo XML de configuração do servidor do Confidential Manager.

4. Para fazer alterações na configuração, copie o XML que você invocou na etapa anterior para um editor de texto. Faça alterações de acordo com a tabela em "Propriedades de criptografia" Na página109.

   Localize a operação **CMSetConfiguration**. Copie a configuração atualizada para a caixa **Value** e clique em **Invoke**. A nova configuração será gravada no Servidor do UCMDB.

5. Para adicionar usuários ao Gerenciador Confidencial para autorização e replicação, localize a operação **CMAddUser**. Esse processo também é útil no processo de replicação. Na replicação, o escravo deve se comunicar com o mestre do servidor, usando um usuário privilegiado.

   - **username**. O nome de usuário.
   - **customer.** O padrão é ALL_CUSTOMERS.
   - **resource.** O nome do recurso. O padrão é ROOT_FOLDER.
   - **permission.** Escolha entre ALL_PERMISSIONS, CREATE, READ, UPDATE e DELETE. O padrão é ALL_PERMISSIONS.

   Clique em **Invoke**.

6. Se necessário, reinicie o HP Universal CMDB.

   Na maioria dos casos, não há necessidade de reiniciar o Servidor. Você pode precisar reiniciar o Servidor quando alterar um dos seguintes recursos:

   - Tipo de armazenamento
   - Nome de tabela ou nomes de colunas do banco de dados

- O criador da conexão do banco de dados
- As propriedades de conexão com o banco de dados (ou seja, URL, usuário, senha, nome de classe do driver)
- Tipo de banco de dados

**Observação:**

- É importante que o Servidor do UCMDB e seus clientes tenham as mesmas propriedades de criptografia do transporte. Se essas propriedades forem alteradas no Servidor do UCMDB, você deverá alterá-las em todos os clientes. (Isso não é relevante para o Data Flow Probe, porque ela é executada no mesmo processo com o Servidor do UCMDB; ou seja, não há necessidade de configuração de criptografia do transporte.)
- A Replicação do Confidential Manager não é configurada por padrão e pode ser configurada, se necessário.
- Se a Replicação do Confidential Manager estiver habilitada e o **initString** ou do transporte ou qualquer outra propriedade de criptografia do mestre for alterada, todos os escravos deverão adotar as alterações.

# Definições

**Propriedades de criptografia do armazenamento.** A configuração que define como o servidor armazena e criptografa os dados (no banco de dados ou arquivo, quais propriedades de criptografia devem criptografar ou descriptografar os dados e assim por diante), como as credenciais são armazenadas de maneira segura, como a criptografia é processada e de acordo com qual configuração.

**Propriedades de criptografia do transporte.** A configuração do transporte define como o servidor e os clientes criptografam o transporte entre eles, qual configuração é usada, como as credenciais são transferidas de maneira segura, como a criptografia é processada e de acordo com qual configuração. Você deve usar as mesmas propriedades para criptografia e descriptografia do transporte, tanto no servidor quanto no cliente.

**Replicações e propriedades de criptografia da replicação.** Dados armazenados de forma segura pelo Confidential Manager são replicados com segurança entre diversos servidores. Essas propriedades definem como os dados devem ser transferidos entre o servidor escravo e o mestre.

**Observação:**

- A tabela de banco de dados que armazena a configuração do servidor do Confidential Manager chama-se: **CM_CONFIGURATION.**
- O arquivo de configuração padrão do Servidor do Confidential Manager fica localizado em app-infra.jar e chama-se **defaultCMServerConfig.xml**.

# Propriedades de criptografia

A tabela a seguir descreve as propriedades de criptografia. Para ver detalhes sobre o uso desses parâmetros, consulte "Configurar o Servidor do HP Universal CMDB" Na página107.

| Parâmetro | Descrição | Valor recomendado |
|---|---|---|
| encryptTransportMode | Criptografar os dados transportados:<br>true false | true |
| encryptDecrypt InitString | Senha para criptografia | Maior que 8 caracteres |
| cryptoSource | Biblioteca de implementação de criptografia a ser usada:<br>• lw<br>• jce<br>• windowsDPAPI<br>• lwJCECompatible | lw |
| lwJCEPBE CompatibilityMode | Suporte para versões anteriores de criptografia leve:<br>• true<br>• false | true |
| cipherType | O tipo de codificação que o Confidential Manager usa. O Confidential Manager aceita apenas um valor:<br>**symmetricBlockCipher** | simétrico BlockCipher |
| engineName | • AES<br>• Blowfish<br>• DES<br>• 3DES<br>• Nulo (sem criptografia) | AES |
| algorithmModeName | Algoritmo do modo de criptografia de bloco:<br>• CBC | CBC |

| Parâmetro | Descrição | Valor recomendado |
|---|---|---|
| algorithmPaddingName | Padrões de preenchimento:<br>• PKCS7Padding<br>• PKCS5Padding | PKCS7Padding |
| keySize | Depende do algoritmo (o que **engineName** aceita) | 256 |
| pbeCount | O número de vezes para executar o hash para criar a chave de **encryptDecryptInitString**.<br>Qualquer número positivo. | 1000 |
| pbeDigestAlgorithm | Tipo de hash:<br>• SHA1<br>• SHA256<br>• MD5 | SHA256 |
| encodingMode | Representação ASCII do objeto criptografado:<br>• Base64<br>• Base64Url | Base64Url |
| useMacWithCrypto | Define se MAC é usado com a criptografia:<br>• true<br>• false | false |
| macType | Tipo de código de autenticação de mensagem (MAC):<br>• hmac | hmac |
| macKeySize SHA256 | Depende do algoritmo de Mac | 256 |
| macHashName | O algoritmo de Mac do hash:<br>• SHA256 | SHA256 |

# Capítulo 9: Proteção da alta disponibilidade

Este capítulo inclui:



# Autenticação de Cluster

**Para habilitar a autenticação de cluster:**

1. No UCMDB, vá até **Administração > Gerenciador de Configurações de Infraestrutura**.
2. Localize a configuração **Habilitar autenticação ao entrar em um cluster de alta disponibilidade** e defina-a como **verdadeiro**.
3. Forneça um repositório de chaves de autenticação de servidor único (certificado + chaves privadas e públicas) em formato JKS. Esse repositório de chaves será colocado em todos os servidores e usado para autenticação ao conectar a um cluster de alta disponibilidade.

   Coloque o repositório de chaves no seguinte local: **<pasta de instalação do UCMDB >\conf\security** e nomeie-o como **cluster.authentication.keystore.**

   > **Observação:** O UCMDB traz esse repositório de chaves pré-configurado pronto para o uso. Esse repositório de chaves é o mesmo para todas as instalações limpas do UCMDB e, portanto, não é seguro. Se desejar autenticar de modo seguro solicitações de associação, exclua esse arquivo e crie um novo.

4. Gere um repositório de chaves de autenticação de cluster como a seguir:

   a. De C:\hp\UCMDB\UCMDBServer\bin\jre\bin, execute o seguinte comando:

   ```
   keytool -genkey -alias hpcert –keystore <UCMDB installation folder>\conf\
   security\cluster.authentication.keystore -keyalg RSA
   ```

   A caixa de diálogo do console é aberta e solicita a você uma nova senha do repositório de chaves.

   b. A senha padrão é **hppass**. Se desejar usar uma senha diferente, atualize o servidor executando o seguinte método JMX: **UCMDB:service=High Availability Services: changeClusterAuthenticationKeystorePassword**

c. Na caixa de diálogo do console, responda a pergunta **What is your first and last name?** (Qual seu nome e sobrenome?) inserindo o nome do cluster.

d. Insira os outros parâmetros de acordo com os detalhes da sua organização.

e. Insira uma senha de chave. Ela deve ser igual à senha do repositório de chaves.

Um repositório de chaves JKS é criado na **<pasta de instalação do UCMDB>\conf\security\cluster.authentication.keystore**

5. Substitua a antiga **<pasta de instalação do UCMDB>\conf\security\cluster.authentication.keystore** em todos os servidores do cluster pelo novo repositório de chaves.

6. Reinicie todos os servidores no cluster.

# Criptografia de Mensagem de Cluster

Use a criptografia de mensagem do cluster para criptografar todas as mensagens do cluster.

**Para habilitar a criptografia de mensagem de cluster:**

1. No UCMDB, vá até **Administração > Gerenciador de Configurações de Infraestrutura**.

2. Localize a configuração **Habilitar criptografia de comunicação de cluster de alta disponibilidade** e defina-a como **verdadeiro**.

3. Forneça uma chave secreta para criptografia simétrica em todos os servidores. A chave deve ser colocada em um repositório de chaves de tipo JCEKS no seguinte local **<pasta de instalação do UCMDB>\conf\security\cluster.encryption.keystore**.

**Observação:** O UCMDB traz esse repositório de chaves pré-configurado pronto para o uso. Esse repositório de chaves é o mesmo para todas as instalações limpas do UCMDB e, portanto, não é seguro. Se desejar criptografar de modo seguro mensagens de cluster, exclua esse arquivo e crie um novo seguindo este procedimento.

4. A partir da **<pasta de instalação do UCMDB>\bin\jre\bin**, execute o seguinte comando:

**Keytool –genseckey –alias hpcert –keystore <UCMDB installation folder>\conf\security\cluster.encryption.keystore –storetype JCEKS**

5. A nova senha do repositório de chaves será solicitada a você. A senha padrão é "hppass". Se desejar usar uma senha diferente, atualize o servidor executando o seguinte método JMX:

**UCMDB:service=High Availability Services: changeClusterEncryptionKeystorePassword**

6. Substitua a antiga **<pasta de instalação do UCMDB>\conf\security\cluster.encryption.keystore** em todos os servidores do cluster por esse novo repositório de chaves.

7. Reinicie os servidores.

# Solução de problemas

Mediante cada inicialização do servidor, o servidor envia uma mensagem de teste ao cluster para verificar se ele se conectou com êxito ao cluster. Se houver um problema com a conexão, a mensagem falha e o servidor é interrompido para evitar que todo o cluster fique travado.

Alguns exemplos de configuração de criptografia de cluster incorreta são:

- Criptografia desabilitada em um nó quando outro nó a habilitou.
- cluster.encryption.keystore incorreto ou ausente
- Chave incorreta ou ausente no repositório de chaves

Se o servidor fica travado devido a um problema de configuração, a mensagem de erro é:

```
2012-09-11 17:48:23,584 [Thread-14] FATAL - Servidor falhou ao conectar corretam
ente ao cluster e seu serviço foi interrompido! Corrija o problema e comece de n
ovo

2012-09-11 17:48:23,586 [Thread-14] FATAL -       Possíveis problemas podem ser:
configuração de segurança incorreta (cluster.encryption.keystore incorreto ou au
sente, chave incorreta, criptografia desabilitada em um cluster com criptografia
habilitada)
```

# Alterando a Chave em key.bin

Em um ambiente de alta disponibilidade com vários servidores, altere a **chave** em **key.bin** como a seguir:

1. Vá para a máquina do gravador no JMX. Você pode escolher qualquer máquina do cluster e clicar no link **gravador (writer)** na parte superior de cada página.

2. Na seção do UCMDB do console, clique em **UCMDB:service=Discovery Manager**.

3. Altere a chave de uma das seguintes maneiras:

   - Clique em **changeEncryptionKey** (isso importa a chave de criptografia existente)
   - Clique em **generateEncryptionKey** (isso gera uma chave de criptografia aleatória)

4. Na máquina gravadora, vá para o sistema de arquivos e localize **key.bin** em: **C:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin**

5. Copie o **key.bin** do local na máquina gravadora para cada uma das outras máquinas no cluster para a pasta: **C:\hp\UCMDB\UCMDBServer\conf\discovery\customer_1** e renomeie o arquivo de destino (por exemplo, **key_new.bin**).

6. Para cada um dos outros servidores (leitores), faça o seguinte:

   a. Mude o leitor para ser um gravador (você pode fazer isso a partir do JMX de alta disponibilidade) e aguarde até que ele mude.

   b. Conecte-se ao JMX do gravador atual e clique em **UCMDB:service=Discovery Manager**.

   c. Clique e chame **changeEncryptionKey**, use os mesmos detalhes inseridos na etapa 3 (para **newKeyFileName**, use o novo nome atribuído na etapa 5).

   d. Verifique se você recebe a seguinte mensagem: **Chave foi criada com êxito**.

# Agradecemos seu feedback!

Se tiver comentários sobre este documento, entre em contato com a equipe de documentação por e-mail. Se um cliente de e-mail estiver configurado nesse sistema, clique no link acima e uma janela de e-mail será aberta com as seguintes informações na linha de assunto:

**Feedback sobre Guia de proteção (Universal CMDB Configuration Manager 10.10)**

Adicione seu feedback ao e-mail e clique em Enviar.

Se nenhum cliente de e-mail estiver disponível, copie as informações acima para uma nova mensagem em um cliente de e-mail da Web e envie seu feedback para SW-Doc@hp.com.