HP Universal CMDB 9.10 Configuration Manager

para o sistema operacional Windows

Guia de Implantação

Data de lançamento do documento: novembro de 2010
Data de lançamento do software: novembro de 2010

Avisos Legais

Garantia

As únicas garantias para produtos e serviços HP estão estipuladas nas declarações de garantia que acompanham tais produtos e serviços. Nada neste documento deve ser interpretado como constituindo garantia adicional. A HP não se responsabiliza por erros técnicos ou editoriais, nem omissões contidas neste documento.

As informações aqui contidas estão sujeitas a alteração sem prévio aviso.

Legenda de Direitos Restritos

Software de computador confidencial. Licença válida da HP necessária para posse, uso ou reprodução. Em conformidade com as cláusulas 12.211 e 12.212 da FAR, Software de Computação Comercial, Documentação de Software de Computador e Dados Técnicos para Itens Comerciais são licenciados ao Governo dos EUA sob uma licença comercial padrão do fabricante.

Avisos de Direitos Autorais

Atualizações da documentação

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

- Data de lançamento do documento, alterada toda 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 confirmar se você está usando a edição mais recente de um documento, vá para:

http://h20230.www2.hp.com/selfsolve/manuals

Esse site exige que você se cadastre para obter um HP Passport e faça logon. Para se cadastrar, vá para:

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

Ou clique no link para **cadastro de novos usuários** (em inglês) na página de logon do HP Passport.

Você também receberá edições novas ou atualizadas se assinar o serviço apropriado de suporte ao produto. Contate seu representante de vendas HP para obter detalhes.

Suporte

Visite o site de suporte da HP Software em:

http://www.hp.com/go/hpsoftwaresupport

Esse site fornece informações de contato e detalhes sobre os produtos, serviços e suporte que a HP Software oferece.

O suporte online da HP Software apresenta recursos para o cliente resolver problemas por conta própria. Ele oferece uma maneira rápida e eficiente de acessar as ferramentas de suporte técnico interativo necessárias para você administrar seus negócios. Sendo um cliente de suporte, você pode se beneficiar usando o site de suporte para:

- Procurar documentos contendo conhecimento de seu interesse
- Enviar e acompanhar casos de suporte e solicitações de aprimoramento
- Baixar patches de software
- Gerenciar contratos de suporte
- Pesquisar contatos de suporte HP
- Examinar informações sobre os serviços disponíveis
- Participar de discussões com outros clientes de software
- Pesquisar e se inscrever para treinamento de software

A maioria das áreas de suporte exige que você se cadastre como um usuário do HP Passport e faça logon. Muitas também exigem um contrato de suporte. Para se cadastrar e obter um ID de usuário do HP Passport, vá para:

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

Para encontrar mais informações sobre níveis de acesso, vá para:

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

Sumário

1

Instalação e configuração

Este capítulo inclui:

Visão geral do Configuration Manager

O HP Universal CMDB Configuration Manager (Configuration Manager) possibilita que você analise e controle os dados no seu CMS, fornecendo um ambiente para controlar a infraestrutura do CMS, a qual abrange muitas fontes de dados e serve vários produtos e aplicativos.

A implantação do Configuration Manager em um ambiente de rede empresarial é um processo que requer planejamento de recursos e o projeto de uma arquitetura de sistema. Antes de instalar o Configuration Manager, examine as informações desta seção, incluindo os requisitos do sistema.

Requisitos do sistema do Configuration Manager

Requisitos do sistema do servidor

A tabela a seguir descreve os requisitos do sistema para o servidor do Configuration Manager:

CPU	Intel Pentium 4, mínimo de 4 processadores
Memória (RAM)	Mínimo de 4 GB
Plataforma	x64
Sistema operacional	Os seguintes sistemas operacionais Windows de 64 bits são compatíveis: ➤ Windows 2003 Enterprise SP2 e R2 SP2 ➤ Windows 2008 Enterprise SP2 e R2

Banco de dados	➤ Microsoft SQL Server 2005 SP2; 2005 Modo de Compatibilidade 80; (Enterprise Editions para todos) ➤ Oracle 11.1.x
HP Universal CMDB	➤ HP Universal CMDB versão 9.03 (Instalação Típica do CMDB) Para ver uma lista completa de requisitos do sistema para essa versão, consulte a documentação do HP Universal CMDB.

Requisitos do cliente

A tabela a seguir descreve os requisitos do cliente para exibir o Configuration Manager:

Navegador	➤ Microsoft Internet Explorer 7.0, 8.0. ➤ Mozilla Firefox 3.x
Plug-in Flash Player do navegador	Flash Player 9 ou superior
Resolução da tela	➤ Mínima de 1024x768 ➤ 1280x1024 recomendada
Qualidade das cores	Mínimo de 16 bits

Diretrizes recomendadas para instalação

A tabela a seguir lista as diretrizes para as opções de instalação do Configuration Manager.

LDAP	Os seguintes ambientes LDAP são compatíveis: ➤ Active Directory ➤ SunONE 6.x
Tamanho mínimo recomendado para o esquema do banco de dados	2 GB

Limites de capacidade do Configuration Manager

A tabela a seguir lista os limites de capacidade do Configuration Manager.

Número máximo de visualizações recomendado	100
Número máximo de políticas recomendado	300
Número máximo de ECs compostos recomendado por visualização	5000
Número máximo de usuários simultâneos recomendado	50

Configurar o esquema de banco de dados ou de usuário

Para trabalhar com o Configuration Manager, é necessário fornecer um esquema de banco de dados. O Configuration Manager fornece suporte para o Microsoft SQL Server e o Oracle Database Server. Esta tarefa descreve como configurar propriedades de conexão para o esquema de banco de dados ou usuário do Configuration Manager usando o assistente de instalação.

Observação: para ver os requisitos do sistema do Microsoft SQL Server e do Oracle Server, consulte "Requisitos do sistema do servidor" na página 8.

Para configurar seu banco de dados:

1 Aloque um esquema de banco de dados do Microsoft SQL Server ou um esquema de usuário do Oracle Server.

➤ Para o **Microsoft SQL Server 2005**: ative o isolamento de instantâneo.

Execute o seguinte comando uma vez após criar o banco de dados:

```
alter database <ccm_database_name> set read_committed_snapshot on
```

Para obter mais informações sobre o recurso de isolamento de instantâneo do SQL Server, consulte http://msdn.microsoft.com/en-us/library/tcbchxcb(VS.80).aspx.

➤ Para o **Oracle**: conceda as funções **Conectar** e **Recurso** somente para usuário do Oracle.
(A concessão do privilégio **Selecionar qualquer tabela** provoca uma falha no procedimento de população do esquema.)

2 Verifique as seguintes informações, que serão necessárias durante este processo de configuração:

✔	**Informações necessárias**
	Nome e porta do host do banco de dados
	Nome de usuário e senha do banco de dados

✔	**Informações necessárias**
	Para o MS SQL: nome do banco de dados
	Para o Oracle: SID

3 Execute o Assistente de Instalação do Configuration Manager. Para ver detalhes, consulte "Instalar o Configuration Manager" na página 12.

Instalar o Configuration Manager

Esta tarefa descreve como instalar o Configuration Manager no seu servidor, bem como configurar a conexão do banco de dados e a integração do UCMDB. Você pode clicar em **Ajuda** em qualquer uma das páginas do assistente para obter ajuda com a instalação. Para ver descrições detalhadas das páginas do assistente, consulte "Assistente de Configuração Pós-instalação do Configuration Manager" na página 23.

Para instalar o Configuration Manager:

1 No diretório raiz do DVD do Configuration Manager, localize o arquivo **install.bat**.

2 Clique duas vezes no arquivo para executar o Assistente de Instalação do Configuration Manager.

3 Clique em **Next** para abrir a página do Contrato de Licença do Usuário Final.

4 Aceite os termos da licença e clique em **Next** para abrir a página de Instalação do Produto.

5 Selecione os produtos a serem instalados (UCMDB e Configuration Manager) e especifique o local da instalação. Se você tem uma licença do UCMDB personalizada, marque a caixa de seleção. Clique em **Next** para iniciar a instalação do UCMDB. Para ver detalhes sobre a instalação do UCMDB, consulte o O PDF do *Guia de Implantação do HP Universal CMDB*.

6 Quando a instalação e a pós-instalação do UCMDB estiverem concluídas, o Assistente de Configuração Pós-instalação do Configuration Manager será iniciado automaticamente.

7. Clique em **Next** na página de boas-vindas para abrir a página Database Connection Configuration (Configuração da Conexão de Banco de Dados).
8. Selecione o tipo de banco de dados (Oracle ou Microsoft SQL Server) e insira o nome de usuário e a senha. É recomendável testar a conexão clicando no botão **Test**. Se o teste de conexão for bem-sucedido, clique em **Next** para abrir a página Application Server Configuration (Configuração do Servidor de Aplicativos).

Observação: você pode configurar opções mais avançadas de conexão de banco de dados após a conclusão do assistente. Para ver detalhes, consulte "Configurando opções avançadas de conexão de banco de dados" na página 15.

---

9. Insira o nome do host e clique em **Next** para abrir a página Windows Service Configuration (Configuração do Serviço do Windows).
10. Se desejar instalar o Configuration Manager como um serviço do Windows, marque a caixa de seleção. Clique em **Next** para abrir a página Users Credentials (Credenciais de Usuários).
11. Insira o nome de usuário e a senha do usuário Administrativo e de Integração. Clique em **Next** para abrir a página HP UCMDB Connection Configuration (Configuração da Conexão com o HP UCMDB).
12. Se o UCMDB já estiver instalado neste computador ou em um computador diferente, certifique-se de que o servidor do UCMDB esteja ativo antes de prosseguir.

    Se você estiver instalando o UCMDB em um computador diferente, verifique se a caixa de seleção está marcada e insira os parâmetros necessários. É recomendável testar a conexão clicando no botão **Test**. Se o teste de conexão for bem-sucedido, clique em **Next** para abrir a página Post Installation Actions Summary (Resumo das Ações Pós-instalação).
13. Examine as informações da página Post Installation Actions Summary (Resumo das Ações Pós-instalação). Se estiverem corretas, clique em **Next** para prosseguir com a pós-instalação.
14. Clique em **Finish** na página Finish (Concluir) para terminar a pós-instalação.

15 Se esta não for a primeira inicialização do UCMDB, será necessário alterar o tamanho da coluna no UCMDB da seguinte maneira:

a Vá para **Administração** > **Gerenciador de Configurações de Infraestrutura**. Localize a configuração **Raiz do Objeto** e mude-a para **dados**. Faça logoff no UCMDB e logon novamente para que a alteração tenha efeito.

b Vá para **Modelagem** > **Gerenciador de Tipo de EC**. Selecione o tipo de EC **dados** na árvore e selecione a guia Atributos. Edite o atributo **Rótulo de Usuário** mudando o **Tamanho do Valor** para 900.

c Volte para o **Gerenciador de Configurações de Infraestrutura** e mude a configuração **Raiz do Objeto** de volta ao seu valor original. Faça logoff e logon novamente para que a alteração tenha efeito.

16 Se o Gerenciamento de Fluxo de Dados já foi executado no UCMDB, os dados do histórico podem estar corrompidos. Para corrigir esse problema, execute o seguinte procedimento:

a Inicie um navegador da Web e insira o seguinte endereço: http://<endereço do servidor do UCMDB>.<nome_domínio>:8080/jmx-console.

Insira as credenciais de autenticação do console JMX, que são, por padrão:

- Nome de logon = **sysadmin**
- Senha = **sysadmin**

b Em **UCMDB**, selecione **Serviços do Banco de Dados de Histórico**.

c Selecione o método **Fix902EndTimeRecords**.

d Para o cliente do estado real, insira **1** como valor do ID do Cliente e clique em **Invocar**.

e Se a operação for bem-sucedida, uma mensagem será exibida informando que "O Banco de Dados de Histórico foi atualizado com êxito”.

f Para o cliente do estado autorizado, insira **100001** como valor do ID do Cliente e clique em **Invocar**.

g Se a operação for bem-sucedida, uma mensagem será exibida informando que "O Banco de Dados de Histórico foi atualizado com êxito”.

Configurando opções avançadas de conexão de banco de dados

Se você precisa de propriedades mais avançadas de conexão de banco de dados para suporte à sua implantação do banco de dados, pode fazer isso depois que a execução do Assistente Pós-instalação for concluída. O Configuration Manager fornece suporte para todas as opções de conexão de banco de dados compatíveis com o driver JDBC do fornecedor e pode ser configurado com a URL de conexão de banco de dados. Para configurar conexões mais avançadas, edite a propriedade **jdbc.url** no arquivo **<Diretório de instalação do Configuration Manager>\conf\database.properties**.

Veja alguns exemplos de opções mais avançadas para o Microsoft SQL Server:

- **Autenticação do Windows (NTLM).** Para aplicar a autenticação do Windows, adicione a propriedade de domínio à sua URL de conexão JTDS no arquivo database.properties. Especifique o domínio do Windows a ser autenticado.

  Por exemplo:

  ```
  jdbc:jtds:sqlserver://myServer:1433/myDatabase;sendStringParametersAsUnicode=false;domain=myDomain
  ```

- **SSL.** Para ver detalhes sobre a proteção da conexão do MS SQL Server usando SSL, consulte http://jtds.sourceforge.net/faq.html.

Veja alguns exemplos de opções mais avançadas para o Oracle Database Server:

- **URL do Oracle.** Especifique a URL de conexão do driver nativo do Oracle. Inclua um nome de servidor Oracle e SID válidos. Alternativamente, se você estiver usando **Oracle RAC**, especifique os detalhes de configuração do Oracle RAC.

  Observação: para ver detalhes sobre a configuração do formato nativo da URL do Oracle JDBC, consulte http://www.orafaq.com/wiki/JDBC#Thin_driver. Para ver detalhes sobre a configuração da URL para o Oracle RAC, consulte http://download.oracle.com/docs/cd/B28359_01/java.111/e10788/rac.htm.

- **SSL.** Para ver detalhes sobre a proteção da conexão do Oracle usando SSL, consulte as seguintes explicações:
  - http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/asojbdc.htm#ASOAG9604
  - http://download.oracle.com/docs/cd/E11882_01/java.112/e16548/clntsec.htm#insertedID6

Configuração de banco de dados - suporte para MLU (Multi-Lingual Unit ou Unidade Multilíngue)

Esta seção descreve as configurações do banco de dados necessárias para suporte à localização.

Configurações do Oracle Server

A tabela a seguir lista as configurações necessárias para o Oracle Server:

Opção	Com suporte	Recomendado	Observações
Conjunto de caracteres	WE8ISO8859P1; UTF8,AL32UTF8	AL32UTF8	

Configurações do Microsoft SQL Server

A tabela a seguir lista as configurações necessárias para o Microsoft SQL Server:

Opção	Com suporte	Recomendado	Observações
Agrupamento	Não diferencia maiúsculas de minúsculas. Não oferece suporte para ordem de classificação binária e diferenciação de maiúsculas e minúsculas. Há suporte apenas para ordem sem diferenciação de maiúsculas e minúsculas com uma combinação de configurações de largura, acento ou kana.	Use a caixa de diálogo Configurações de Agrupamento para selecionar o agrupamento. Não marque a caixa de diálogo binária. A diferenciação de acento, kana e largura deve ser selecionada de acordo com os requisitos de idioma dos dados relevantes. O idioma selecionado deve ser o mesmo das configurações regionais do Windows.	Limitado à localidade do Agrupamento e às definições padrão do inglês.
Propriedade do Banco de Dados de Agrupamento	Padrão do servidor		

Observação:

Para todos os idiomas: **<Idioma>_CI_AS** é a opção mínima necessária. Por exemplo, em japonês, se você desejar selecionar as opções que distinguem kana e largura, a opção recomendada é: **Japanese_CI_AS_KS_WS** ou **Japanese_90_CI_AS_KS_WS**. Essa recomendação indica que os caracteres japoneses diferenciam acentos, kana e largura.

- **Diferenciação de acento (_AS).** Distingue entre caracteres acentuados e não acentuados. Por exemplo, **a** não é igual a **á**. Se essa opção não é selecionada, o Microsoft SQL Server considera as versões acentuadas e não acentuadas das letras como idênticas para fins de classificação.
- **Diferenciação de kana (_KS).** Distingue entre os dois tipos de caracteres kana japoneses: Hiragana e Katakana. Se essa opção não é selecionada, o Microsoft SQL Server considera caracteres Hiragana e Katakana iguais para fins de classificação.
- **Diferenciação de largura (_WS).** Distingue entre um caractere de byte único e o mesmo caractere quando representado como um caractere de byte duplo. Se essa opção não é selecionada, o Microsoft SQL Server considera as representações de byte único e de byte duplo do mesmo caractere como idênticas para fins de classificação.

Habilitar LW-SSO (Lightweight Single Sign-On)

Alguns usuários do Configuration Manager também têm permissão para fazer logon no UCMDB. Para conveniência, o Configuration Manager fornece um link direto para a interface do usuário do UCMDB (selecione **Administração** > **Abrir UCMDB**). Para usar o logon único (que isenta da necessidade de fazer logon no UCMDB após o logon no Configuration Manager), você deve habilitar o LW-SSO para o Configuration Manager e para o UCMDB e se certificar de que ambos estejam trabalhando com o mesmo initString. Esta tarefa descreve como habilitar o LW-SSO no Configuration Manager e no UCMDB.

Para habilitar o LW-SSO:

1 Abra o seguinte arquivo no diretório de instalação do Configuration Manager: **\servers\server-0\webapps\cnc\WEB-INF\classes\cnclwssofmconf.xml**.

Observação: esse arquivo não existe antes de iniciar o Configuration Manager.

---

2 Localize a seguinte seção:

```
enableLWSSO enableLWSSOFramework="true"
```

e verifique se o valor é **true**.

3 Localize a seguinte seção:

```
lwssoValidation  id="ID000001">
<domain> </domínio>
```

e insira o domínio do servidor do Configuration Manager após <**domain**>.

4 Localize a seguinte seção:

```
<initString="This string should be replaced"></crypto>
```

e substitua "This string should be replaced" por uma cadeia de caracteres compartilhada que seja usada por todos os aplicativos confiáveis que se integram com o LW-SSO.

5 Localize a seguinte seção:

```
<!--multiDomain>
<trustedHosts>
<DNSDomain>This value should be replaced by your application
domain</DNSDomain>
<DNSDomain>This value should be replaced by domain of other
application</DNSDomain>
</trustedHosts>
</multiDomain-->
```

Remova o caractere de comentário no início e insira os domínios do servidor do Configuration Manager nos elementos DNSDomain (no lugar de This value should be replaced by your application domain). A lista deve incluir o domínio do servidor inserido na etapa 3 na página 20.

6 Salve o arquivo com suas alterações e reinicie o servidor.

7 Inicie um navegador da Web e insira o seguinte endereço: http://<endereço do servidor do UCMDB>.<nome_domínio>:8080/jmx-console.

Insira as credenciais de autenticação do console JMX, que são, por padrão:

- Nome de logon = **sysadmin**
- Senha = **sysadmin**

8 Em **UCMDB-UI**, selecione **Configuração do LW-SSO** para abrir a página Visualização do JMX MBEAN.

9 Selecione o método **setEnabledForUI**, defina o valor como **true** e clique em **Invocar**.

10 Selecione o método **setDomain**. Insira o nome do domínio do servidor do UCMDB e clique em **Invocar**.

11 Selecione o método **setInitString**. Insira o mesmo initString que você inseriu para o Configuration Manager na etapa 4 na página 21 e clique em **Invocar**.

12 Se o Configuration Manager e o UCMDB estiverem localizados em domínios separados, selecione o método **addTrustedDomains** e insira os nomes de domínio dos servidores do UCMDB e do Configuration Manager. Clique em **Invocar**.

13 Para visualizar a configuração do LW-SSO como está salva no mecanismo de configurações, selecione o método **retrieveConfigurationFromSettings** e clique em **Invocar**.

14 Para visualizar a configuração do LW-SSO efetivamente carregada, selecione o método **retrieveConfiguration** e clique em **Invocar**.

Suporte para IPv6

O Configuration Manager fornece suporte apenas para URLs IPv6 voltadas para o cliente.

Para trabalhar com o Configuration Manager usando um endereço IPv6:

1 Verifique se o seu sistema operacional oferece suporte para IPv6. Consulte detalhes na documentação relevante do sistema operacional.

2 Abra o arquivo **client-config.properties**, localizado no diretório **conf** do <**Diretório de instalação do Configuration Manager**>. Mude o valor do parâmetro **bsf.server.url** para o endereço IPv6 inserido entre colchetes. Por exemplo:

```
bsf.server.url=http://[2620:0:a17:e008:d840:5b0f:2040:519c]:8080/bsf
```

2

Assistente de Configuração Pós-instalação do Configuration Manager

Este capítulo inclui:

Visão geral da Configuração Pós-instalação do Configuration Manager

Este capítulo apresenta descrições detalhadas das páginas do Assistente Pós-instalação do Configuration Manager e as tarefas de configuração associadas. Esse é o conteúdo que é aberto quando você clica em **Ajuda** em qualquer uma das páginas do assistente.

Página Database Connection (Conexão de Banco de Dados)

Esta seção inclui:

Geral

Uma conexão de banco de dados deve ser configurada associada a uma conexão de URL padrão. Se recursos mais avançados forem necessários, como o Oracle Real Application Cluster, configure uma conexão padrão e edite manualmente o arquivo **database.properties** para configurar os recursos avançados.

O Configuration Manager usa drivers nativos para Oracle e Microsoft SQL Server. Isso significa que, em geral, todos os recursos dos drivers nativos têm suporte, contanto que possam ser configurados usando a URL do banco de dados. A URL fica localizada no arquivo **database.properties**.

Observação: a configuração dos recursos avançados deve ser feita depois que o processo pós-instalação é concluído e depois que uma configuração de trabalho é estabelecida.

Parâmetros

Para configurar a conexão do banco de dados, defina os seguintes parâmetros:

Parâmetro	Valor recomendado	Descrição
Vendor (Fornecedor)	<definido pelo usuário>	Fornecedor do banco de dados Valores possíveis: **Oracle** ou **Microsoft** O HP Universal CMDB pode ser instalado usando o mesmo instalador do Configuration Manager — ou separadamente. Se o Configuration Manager e o UCMDB estão sendo instalados no mesmo computador usando o mesmo instalador, o valor padrão para este parâmetro é o fornecedor do banco de dados já selecionado no assistente pós-instalação do UCMDB. Somente quando se instalam ambos os aplicativos usando os mesmos instaladores é que os valores padrão são definidos. Se você estiver instalando usando pacotes de instalação separados, mesmo quando o UCMDB estiver instalado no mesmo computador que o Configuration Manager, os valores padrão NÃO aparecerão neste assistente pós-instalação.
Hostname (Nome do host)	<definido pelo usuário>	Nome do host do servidor de banco de dados Se o Configuration Manager e o UCMDB estão sendo instalados no mesmo computador, o padrão para este parâmetro é o servidor de banco de dados já selecionado no assistente pós-instalação do UCMDB. **Este valor é obrigatório.**

Parâmetro	Valor recomendado	Descrição
Port (Porta)	<definido pelo usuário>	Porta do ouvinte do banco de dados Se o Configuration Manager e o UCMDB estão sendo instalados no mesmo computador, o padrão para este parâmetro é a porta do banco de dados já selecionada no assistente pós-instalação do UCMDB. Para o Oracle, o valor padrão é **1521**. Para o Microsoft SQL Server, o valor padrão é **1433**. **Este valor é obrigatório.**
SID/DB	<definido pelo usuário>	Nome do Oracle SID ou nome do banco de dados Microsoft SQL Server Se o Configuration Manager e o UCMDB estão sendo instalados no mesmo computador, o padrão para este parâmetro é o db/sid do banco de dados já selecionado no assistente pós-instalação do UCMDB. **Este valor é obrigatório.**
Username (Nome de usuário)	<definido pelo usuário>	Nome de usuário usado para fazer logon no banco de dados. **Este valor é obrigatório.**
Password (Senha)	<definido pelo usuário>	Senha usada para fazer logon no banco de dados.

Opções

As seguintes opções também estão disponíveis:

Parâmetro	Valor recomendado	Descrição
Encrypt password (Criptografar senha)	<definido pelo usuário>	Se selecionada, esta opção criptografa a senha no arquivo **database.properties**. Por motivos de segurança, é recomendável criptografar senhas armazenadas em arquivos de texto.
Create schema objects (Criar objetos de esquema)	<definido pelo usuário>	Se selecionada, esta opção cria os objetos de esquema necessários para executar o Configuration Manager. Desmarque esta opção somente quando a instalação usar um esquema existente que foi criado e preenchido anteriormente com Objetos do Configuration Manager.

Testar

Observação: é altamente recomendável testar as propriedades da conexão antes de continuar.

Para testar as propriedades da conexão, clique em **Test** (Testar). O assistente tentará acessar o banco de dados e verificará a conexão. Os resultados do teste aparecem à direita do botão **Test**.

O banco de dados gera várias mensagens de erro. Elas são autoexplicativas, geralmente relacionadas à inserção de um nome de usuário ou senha incorreto(a). O erro deve ser corrigido, seguido de um resultado de teste bem-sucedido, antes que se possa continuar.

Página Application Server (Servidor de Aplicativos)

Esta seção inclui:

Geral

Configure o Servidor de Aplicativos do Configuration Manager usando os números de porta padrão mostrados abaixo.

Parâmetros

Para configurar o Servidor de Aplicativos do Configuration Manager, defina os seguintes parâmetros:

Parâmetro	Valor recomendado	Descrição
Hostname (Nome do host)	<definido pelo usuário>	Nome externo do servidor de aplicativos Por padrão, este valor é o nome do host totalmente qualificado do computador que está executando o assistente (e o Configuration Manager). Em algumas implantações, este nome deve ser diferente, como quando se implanta um servidor Web na frente do Servidor de Aplicativos do Configuration Manager.
Customize ports (Personalizar portas)	<definido pelo usuário>	Por padrão, esta opção não fica selecionada. Quando selecionada, você pode personalizar os números das portas padrão do servidor de aplicativos.

Parâmetro	Valor recomendado	Descrição
HTTP port (Porta HTTP)	<definido pelo usuário>	Porta HTTP do Servidor de Aplicativos do Configuration Manager Valor padrão: **8080** Valor padrão quando instalado no mesmo computador que o HP Universal CMDB: **8180**
HTTPS port (Porta HTTPS)	<definido pelo usuário>	Porta HTTPS do Servidor de Aplicativos do Configuration Manager Valor padrão: **8443** Valor padrão quando instalado no mesmo computador que o UCMDB: **8143**
Tomcat port (Porta do Tomcat)	<definido pelo usuário>	Porta de gerenciamento do Servidor de Aplicativos do Configuration Manager Valor padrão: **8005**
AJP port (Porta AJP)	<definido pelo usuário>	Porta AJP (Apache Java Protocol) do Servidor de Aplicativos do Configuration Manager Valor padrão: **8009**
JMX HTTP port (Porta HTTP JMX)	<definido pelo usuário>	Porta HTTP JMX do Servidor de Aplicativos do Configuration Manager Valor padrão: **39900**
JMX remote port (Porta remota JMX)	<definido pelo usuário>	Porta remota JMX do Servidor de Aplicativos do Configuration Manager Valor padrão: **39600**

Página Windows Service Configuration (Configuração do Serviço do Windows)

Selecione se o Configuration Manager será ou não instalado como um serviço do Windows. Esta opção só está disponível quando a instalação é feita em um computador com Windows.

O serviço do Windows pode ser configurado manualmente usando o utilitário **create-windows-service.bat** localizado no diretório **cnc-home/bin**.

Página Users Credentials (Credenciais de Usuários)

Esta seção inclui:

➤ "Geral" na página 30

Geral

Configure os seguintes usuários iniciais do Configuration Manager:

Parâmetro	Valor recomendado	Descrição
Admin user (Usuário admin)	<definido pelo usuário>	Usuário administrativo do Configuration Manager — o "superusuário"
Integration user (Usuário de integração)	<definido pelo usuário>	Usuário criado pelo Configuration Manager no HP Universal CMDB para fins de integração

Observação: você deve fornecer as credenciais de nome de usuário e senha para os usuários Administrativo e de Integração.

Página HP Universal CMDB Connection (Conexão do HP Universal CMDB)

Esta seção inclui:

Geral

A configuração da conexão ao HP Universal CMDB é opcional.

Ao instalar o Configuration Manager no mesmo computador que o UCMDB em uma instalação combinada, você não precisa fornecer nenhum dado nesta página.

Quando você não instala o UCMDB em uma instalação combinada ou quando instala o UCMDB em um computador diferente — mesmo quando se conecta ao UCMDB no host local — ou quando instala o UCMDB antes de instalar o Configuration Manager, o UCMDB deve estar ativo e você deve fornecer estas propriedades da conexão.

Observação: quando a instalação é feita usando uma instância remota do UCMDB, a instância deve estar ativa e em execução. Quando o Configuration Manager e o UCMDB são instalados no mesmo computador, o UCMDB deve ficar inativo durante a execução deste assistente.

Parâmetros

Para configurar a conexão do UCMDB, defina os seguintes parâmetros:

Parâmetro	Valor recomendado	Descrição
Use HP UCMDB on a different host (Usar o HP UCMDB em um host diferente)	<definido pelo usuário>	Selecione esta opção para habilitar todas as demais propriedades ao instalar o Configuration Manager e o UCMDB em computadores diferentes.
Hostname (Nome do host)	<definido pelo usuário>	Nome do host no qual o UCMDB está instalado
Port (Porta)	<definido pelo usuário>	Porta no qual o UCMDB está ouvindo
Protocol (Protocolo)	<definido pelo usuário>	HTTP ou HTTPS
Customer (Cliente)	<definido pelo usuário>	Cliente do UCMDB
Administrative username (Nome do usuário administrativo)	<definido pelo usuário>	Nome do usuário de administração do sistema do UCMDB
Administrative password (Senha administrativa)	<definido pelo usuário>	Senha de administração do sistema do UCMDB

Testar

Observação: é altamente recomendável testar as propriedades da conexão antes de continuar.

Para testar as propriedades da conexão, clique em **Test** (Testar). O assistente tentará acessar o UCMDB e verificará a conexão. Os resultados do teste aparecem à direita do botão **Test**.

O UCMDB gera várias mensagens de erro. Elas são autoexplicativas, geralmente relacionadas à inserção de um nome de usuário ou senha incorreto(a). O erro deve ser corrigido, seguido de um resultado de teste bem-sucedido, antes que se possa continuar.

Página Summary (Resumo)

Todas as seleções feitas nas páginas anteriores do assistente são exibidas. Confirme se todas as seleções estão certas e faça as alterações necessárias. Quando todas as seleções estiverem corretas, clique em **Avançar** e o assistente concluirá as tarefas de configuração.

Página Finish (Concluir)

Esta é a página final do **Assistente de Configuração Pós-instalação do Configuration Manager**. As tarefas de configuração pós-instalação foram concluídas. Clique em **Concluir** para fechar o assistente.

Observação: mesmo quando todas as tarefas foram concluídas com êxito, é recomendável verificar os logs localizados em **cnc-home/tmp/chp/app.log**.

3

Configurando o LDAP

O HP UCMDB Configuration Manager usa LDAP para gerenciar usuários, funções e permissões. Este capítulo descreve as etapas para configurar e resolver problemas no LDAP.

Este capítulo inclui:

Visão geral do LDAP

O Configuration Manager vem com um servidor LDAP interno (identificado na interface do usuário como **Compartilhado**) e também pode se conectar a um servidor LDAP organizacional. O Configuration Manager usa esses servidores para localizar usuários, grupos e funções; para armazenar dados de personalização; e para autenticar usuários. Você pode escolher qual desses usará o servidor LDAP e qual usará o servidor LDAP interno.

Uma implantação típica usa o servidor LDAP interno (compartilhado) para armazenar funções e o externo (organizacional) para o resto.

Escolhendo provedores

1. Faça logon no **Configuration Manager** como usuário administrador.
2. Vá para **Administração** > **Administração de Servidor** > **Gerenciamento de Usuários** > **Configuração do Gerenciamento de Usuários** e selecione COMPARTILHADO ou EXTERNO para cada um dos atributos a seguir, de acordo com a sua preferência de provedor (COMPARTILHADO é a seleção padrão):
   - Provedor de autenticação
   - Provedor de grupos
   - Provedor de personalização
   - Provedor de funções
   - Provedor de Relações de Funções
3. Salve o conjunto de configurações.

Conectando ao seu LDAP organizacional

O HP UCMDB Configuration Manager é inicialmente configurado com um LDAP interno (compartilhado). Esta seção descreve as etapas para se conectar ao seu servidor LDAP organizacional.

Esta seção inclui:

Configurar a conexão LDAP

Esta seção explica como conectar o Configuration Manager a um servidor LDAP externo. O servidor LDAP externo é o LDAP organizacional e contém os usuários organizacionais.

1. Faça logon no **Configuration Manager** como usuário administrador.
2. Vá para **Administração** > **Administração de Servidor** > **Gerenciamento de Usuários** > **Configuração do Gerenciamento de Usuários** > **Repositório de Usuários Externo** e atualize os atributos a seguir, de acordo com as suas propriedades de LDAP organizacional:

   Conexão LDAP geral

   ldapHost: <nome do host LDAP>

   ldapPort: <número da porta LDAP>

   enableSSL: <true/false - use a conexão SSL ao LDAP>

   useAdministrator: <true/false - use o usuário para se conectar ao LDAP>

   ldapAdministrator: <nome do usuário LDAP (deve ser definido se **useAdministrator=true)**>

   ldapAdministratorPassword: <senha do usuário LDAP (deve ser definida se **useAdministrator=true**)>
3. Salve o conjunto de configurações.

Configurar os provedores de grupos e usuários

Este procedimento define o LDAP organizacional (repositório externo) como provedor para os grupos e usuários. O LDAP interno (repositório compartilhado) ainda é usado para autenticação, mas os usuários e grupos são recuperados do LDAP externo. Este modo é usado para testar a configuração do LDAP externo e para atribuir permissões aos usuários organizacionais.

Para definir os provedores de grupos e usuários:

1. Se você ainda não estiver nessa página, vá para **Administração** > **Administração de Servidor** > **Gerenciamento de Usuários** > **Configuração do Gerenciamento de Usuários** > **Repositório de Usuários Externo**. Verifique se você está usando o mesmo rascunho de conjunto de configurações que salvou na seção "Configurar a conexão LDAP" na página 37.
2. Atualize os atributos a seguir de acordo com as suas propriedades de LDAP organizacional:
   a. **Pesquisa de usuários**

      usersBase: <DN de base para pesquisa de usuários>

      usersScope: <escopo para pesquisa de usuários>

      usersFilter: <filtro para pesquisa de usuários>

   b. **Classe de objeto dos usuários** (dependente do fornecedor LDAP)

      usersObjectClass: <classe de objeto LDAP dos usuários>

      usersUniqueIDAttribute: <atributo LDAP de ID exclusivo dos usuários>

      Os seguintes atributos são opcionais:

      usersDisplayNameAttribute: <atributo LDAP de nome de exibição dos usuários>

      usersLoginNameAttribute: <atributo LDAP de nome de logon dos usuários>

      usersFirstNameAttribute: <atributo LDAP de nome dos usuários>

      usersLastNameAttribute: <atributo LDAP de sobrenome dos usuários>

      usersEmailAttribute: <atributo LDAP de email dos usuários>

      usersPreferredLanguageAttribute: <atributo LDAP de idioma de preferência dos usuários>

      usersPreferredLocationAttribute: <atributo LDAP de local de preferência dos usuários>

      usersTimeZoneAttribute: <atributo LDAP de fuso horário dos usuários>

usersDateFormatAttribute: <atributo LDAP de formato de data dos usuários>

usersNumberFormatAttribute: <atributo LDAP de formato de número dos usuários>

usersWorkWeekAttribute: <atributo LDAP de semana de trabalho dos usuários>

usersTenantIDAttribute: <atributo LDAP de ID de locatário dos usuários>

usersPasswordAttribute: <atributo LDAP de senha dos usuários>

c **Pesquisa de grupos**

groupsBase: <DN de base para pesquisa de grupos>

groupsScope: <escopo LDAP para pesquisa de grupos>

groupsFilter: <filtro para pesquisa de grupos>

rootGroupsBase: <DN de base para pesquisa de grupos raiz>

rootGroupsScope: <escopo LDAP para pesquisa de grupos raiz>

rootGroupsFilter: <filtro para pesquisa de grupos>

d **Classe de objeto dos grupos** (dependente do fornecedor LDAP)

groupsObjectClass: <classe de objeto LDAP dos grupos>

groupsMembersAttribute: <atributo LDAP dos membros dos grupos>

Os seguintes atributos são opcionais:

groupsNameAttribute: <atributo LDAP de nome exclusivo dos grupos>

groupsDisplayNameAttribute: <atributo LDAP de nome de exibição dos grupos>

groupsDescriptionAttribute: <atributo LDAP de descrição dos grupos>

enableDynamicGroups: <habilitar grupos dinâmicos>

dynamicGroupsClass: <classe de objeto LDAP dos grupos dinâmicos>

dynamicGroupsMemberAttribute: <atributo LDAP dos membros dos grupos dinâmicos>

dynamicGroupsNameAttribute: <atributo LDAP de nome exclusivo dos grupos dinâmicos>

dynamicGroupsDisplayNameAttribute: <atributo LDAP de nome de exibição dos grupos dinâmicos>

dynamicGroupsDescriptionAttribute: <atributo LDAP de descrição dos grupos dinâmicos>

e **Hierarquia dos grupos** (se seu LDAP organizacional usar hierarquia de grupos)

enableNestedGroups: <habilitar suporte de grupos aninhados>

maximalAllowedGroupsHierarchyDepth: <profundidade máxima permitida da hierarquia de grupos>

f **Configuração avançada**

ldapVersion: <versão do LDAP>

baseDistinguishNameDelimiter: <delimitador do DN de base>

scopeDelimiter: <delimitador do escopo>

attributeValuesDelimiter: <delimitador dos valores de atributos do LDAP>

3 Salve o rascunho do conjunto de configurações.

Ativar o conjunto de configurações

1 Vá para **Administração** > **Administração de Servidor** > **Gerenciamento de Usuários** > **Configuração do Gerenciamento de Usuários** e atualize o seguinte:

Origem do UUM Externo: Verdadeiro

Provedor de Grupos: EXTERNO

Provedor de Usuários: EXTERNO

2 Salve o novo conjunto de configurações e ative-o.

3 Faça logoff e reinicie o servidor do **Configuration Manager**.

Atribuir permissões a usuários

Este procedimento atribui a função **Administrador do Sistema** ao(s) usuário(s) organizacional(is). Um usuário com a função **Administrador do Sistema** terá permissões para atribuir as funções relevantes aos demais usuários organizacionais.

1. Faça logon no **Configuration Manager** como usuário administrador.
2. Abra o módulo **Gerenciamento de Usuários** (**Administração** > **Gerenciamento de Usuários**).
3. Confirme se você vê os grupos e usuários do seu LDAP organizacional.
4. Vá para **Gerenciamento de Usuários** > **painel Pesquisar Usuários** e pesquise o(s) usuário(s) que atuarão como administrador(es). Exemplo: Nome = j*, Sobrenome = Silva.
5. Adicione a função **Administrador do Sistema** ao(s) usuário(s).

Definir o Provedor de Autenticação para o LDAP externo

Este procedimento define o LDAP organizacional externo para o Provedor de Autenticação, para que os usuários organizacionais sejam usados para autenticação.

1. Vá para **Administração** > **Administração de Servidor** > **Gerenciamento de Usuários** > **Configuração do Gerenciamento de Usuários** e atualize o seguinte:

   Provedor de Autenticação: EXTERNO
2. Salve o novo conjunto de configurações e ative-o.
3. Faça logoff e reinicie o servidor do **Configuration Manager**.
4. Faça logon com um dos usuários organizacionais que receberam a função **Administrador do Sistema**.

Importar o certificado LDAP

Se for necessário um certificado para se conectar ao seu LDAP organizacional, execute as seguintes etapas:

1. Exporte o certificado para um arquivo.
2. Pare o serviço do Windows do Configuration Manager.
3. Execute o seguinte comando:

   <instalação do Configuration Manager>\java\windows\x86_64\bin\keytool.exe -import -trustcacerts -alias <alias do certificado> -keystore <instalação do Configuration Manager>\java\windows\x86_64\lib\security\cacerts -storepass changeit -file <caminho do arquivo do certificado>

4. Inicie o serviço do Windows do Configuration Manager.

Configurando o LDAP interno (compartilhado)

Alterando a senha do servidor LDAP interno (compartilhado) (opcional)

Você pode alterar a senha do servidor LDAP interno (compartilhado) por motivos de segurança.

1. Faça logon no **HP Universal CMDB Configuration Manager**.
2. Abra uma linha de comando e navegue até a pasta **<instalação do Configuration Manager>\ldap\serverRoot\bat** .
3. Execute **ldappasswordmodify -h localhost -p <porta ldap> -D "cn=Directory Manager" -w <senha de admin do ldap> -c <senha de admin do ldap> -n <nova senha de admin do ldap>**.
   a. A senha de admin do ldap padrão é **ldapadmin**.
   b. A porta padrão é **2389**.
   c. Confirme se o comando foi executado com êxito e só então continue com as etapas a seguir.

4 No **UCMDB Configuration Manager**, selecione **Administração** > **Administração de Servidor** > **Gerenciamento de Usuários** > **Configuração do Gerenciamento de Usuários** > **Repositório de Usuários Compartilhado**.

5 Atualize a senha no atributo **ldapAdministratorPassword**.

6 Salve o novo conjunto de configurações e ative-o.

7 Faça logoff no **UCMDB Configuration Manager**.

8 Reinicie o servidor do **UCMDB Configuration Manager**.

Configurando a porta LDAP interna (compartilhada)

A porta padrão, 2389, pode já estar em uso por outro aplicativo. Para mudar essa porta padrão, use o procedimento a seguir.

Para configurar a porta LDAP interna:

1 Abra uma linha de comando e navegue até a pasta **<instalação do Configuration Manager>\ldap\serverRoot\bat** .

2 Execute o seguinte comando:
dsconfig -h localhost -p 2444 -D "cn=directory manager" -w <senha do admin do ldap> --trustAll -X -n set-connection-handler-prop --handler-name "LDAP Connection Handler" --set listen-port:<nova porta>

A <senha de admin do ldap> padrão é **ldapadmin**.

3 Confirme se nenhuma mensagem de erro foi exibida e só então continue com as etapas a seguir.

4 Faça logon no HP Universal CMDB Configuration Manager.

5 No UCMDB Configuration Manager, selecione **Administração** > **Administração de Servidor** > **Gerenciamento de Usuários** > **Configuração do Gerenciamento de Usuários** > **Repositório de Usuários Compartilhado** e atualize o número da porta no atributo **ldapPort**.

6 Salve o novo conjunto de configurações e ative-o.

7 Faça logoff no UCMDB Configuration Manager.

8 Reinicie o servidor do UCMDB Configuration Manager.

Solucionando problemas no LDAP

Problema: não é possível estabelecer a comunicação com o servidor LDAP. Aparece uma exceção de comunicação nos logs.

Solução: verifique as configurações do host e porta LDAP e do modo SSL:

a Verifique se o host e a porta LDAP estão configurados corretamente: Selecione **Administração** > **Administração de Servidor** > **Gerenciamento de Usuários** > **Configuração do Gerenciamento de Usuários** > **Repositório de Usuários Externo** e verifique as configurações de **ldapHost, ldapPort**.

b Verifique se o modo SSL está configurado corretamente. Verifique com seu administrador do LDAP organizacional se o usuário administrador é necessário para conexão LDAP. Selecione **Administração** > **Administração de Servidor** > **Gerenciamento de Usuários** > **Configuração do Gerenciamento de Usuários** > **Repositório de Usuários Externo** e verifique a configuração **enableSSL**.

c Verifique se o certificado de servidor apropriado está instalado. Execute o seguinte comando:

```
<instalação do Configuration Manager>\java\windows\x86_64\bin\keytool.exe -list -trustcacerts [-alias <alias do certificado>] -keystore <instalação do Configuration Manager>\java\windows\x86_64\lib\security\cacerts -storepass changeit
```

d Verifique com seu administrador do LDAP organizacional se o administrador é necessário para conexão LDAP. Selecione **Administração** > **Administração de Servidor** > **Gerenciamento de Usuários** > **Configuração do Gerenciamento de Usuários** > **Repositório de Usuários Externo** e verifique as seguintes configurações: **useAdministrator, ldapAdministrator, ldapAdministratorPassword**.

Problema: nenhum grupo aparece na tela de gerenciamento de usuários ou grupos. Nenhuma exceção aparece nos logs.

Solução: verifique o seguinte:

a Verifique se os filtros de pesquisa de Usuários e Grupos estão configurados corretamente: selecione **Administração** > **Administração de Servidor** > **Gerenciamento de Usuários** > **Configuração do Gerenciamento de Usuários** > **Repositório de Usuários Externo** e modifique as seguintes propriedades: **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope, rootGroupsFilter**.

b Abra o navegador do cliente LDAP e procure os usuários sob o DNS de base.

Problema: a interface do usuário está muito lenta.

Solução: geralmente isso acontece porque há muitos grupos ou usuários configurados no seu LDAP. Configure o DNS de base e os filtros e reduza o número de grupos para o subconjunto relevante da seguinte forma:

a Selecione **Administração** > **Administração de Servidor** > **Gerenciamento de Usuários**> **Configuração do Gerenciamento de Usuários** > **Repositório de Usuários Externo**.

b Modifique as seguintes configurações: **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope, rootGroupsFilter**.

Problema: alguns usuários conhecidos não aparecem na tela de gerenciamento de grupos ou usuários.

Solução: a tela de gerenciamento de Usuários e Grupos mostra apenas usuários que pertencem a algum grupo. Coloque os usuários nos grupos apropriados no LDAP a fim de vê-los na tela principal.

Problema: o logon demora muito.

Solução: talvez o usuário pertença a grupos demais. Você pode otimizar o tempo de inicialização alterando o filtro de pesquisa de grupos para que retorne menos grupos, da seguinte maneira:

a Selecione **Administração** > **Administração de Servidor** > **Gerenciamento de Usuários**> **Configuração do Gerenciamento de Usuários** > **Repositório de Usuários Externo**.

b Modifique a configuração **groupsFilter**.

4

Autenticação LW-SSO (Lightweight Single Sign-On) – referência geral

Esta seção do 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.

Esta seção inclui os seguintes tópicos:

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.

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 LW-SSO 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. 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.

Solução de problemas e limitações

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 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

- **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.

5

Autenticação do Gerenciador de Identidade

Esta seção do capítulo inclui:

Aceitar a autenticação do Gerenciador de Identidade

Se você usa um Gerenciador de Identidade e pretende adicionar o HP Universal CMDB Configuration Manager, deve executar esta tarefa.

Esta tarefa descreve como configurar o HP Universal CMDB Configuration Manager para aceitar a autenticação do Gerenciador de Identidade.

Esta tarefa inclui as seguintes etapas:

Pré-requisitos

O servidor Tomcat do Configuration Manager deve estar conectado ao seu Servidor Web (IIS ou Apache) protegido pelo seu Gerenciador de Identidade por meio de um conector Tomcat Java (AJP13).

Para ver instruções sobre o uso de um conector Tomcat Java (AJP13), consulte a documentação do Tomcat Java (AJP13).

Configurar o HP Universal CMDB Configuration Manager para aceitar o Gerenciador de Identidade

Para configurar o Tomcat Java (AJP13) com IIS6:

1. Configure o Gerenciador de Identidade para enviar um retorno de chamada/cabeçalho de personalização que contenha o nome de usuário e solicitar o nome do cabeçalho.
2. Abra o arquivo <**Diretório de instalação do Configuration Manager**>**conf****lwssofmconf.xml** e localize a seção que começa com **in-ui-identity-management**.

   Por exemplo:

   ```
   <in-ui-identity-management enabled="false">
       <identity-management>
         <userNameHeaderName>sm-user</userNameHeaderName>
       </identity-management>
   </in-ui-identity-management>
   ```

   a. Ative a funcionalidade removendo o caractere de comentário.

   b. Substitua **enabled**="**false**" por **enabled**="**true**".

   c. Substitua **sm-user** pelo nome do cabeçalho que você solicitou na etapa 1.
3. Abra o arquivo <**Diretório de instalação do Configuration Manager**>**conf****client-config.properties** e edite as seguintes propriedades:

   a. Mude **bsf.server.url** para a URL do Gerenciador de Identidade e mude a porta para a porta do Gerenciador de Identidade:

   ```
   bsf.server.url=http://<URL do Gerenciador de Identidade>:<porta do Gerenciador de Identidade>/bsf
   ```

   b. Mude **bsf.server.services.url** para o protocolo HTTP e mude a porta para a porta original do Configuration Manager:

   ```
   bsf.server.services.url=http://<URL do Configuration Manager>:<Porta do Configuration Manager>/bsf
   ```

Exemplo de uso do Conector Java para configurar o gerenciamento de identidade para o Configuration Manager com IIS6 em um sistema operacional Windows 2003

Esta tarefa de exemplo descreve como instalar e configurar o Conector Java para ser usado para configurar o gerenciamento de identidade para uso com o Configuration Manager com o IIS6 executado em um sistema operacional Windows 2003.

Para instalar o Conector Java e configurá-lo para o IIS6 no Windows 2003:

1. Baixe a versão mais recente do Conector Java (por exemplo: **djk-1.2.21**) do site da Apache.
   a. Clique em **http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/**.
   b. Selecione a versão mais recente.
   c. Baixe o arquivo **isapi_redirect.dll** do diretório **amd64**.
2. Armazene esse arquivo em <**Diretório de instalação do Configuration Manager**>**tomcat****bin****win32**.
3. Crie um novo arquivo de texto chamado **isapi_redirect.properties** no mesmo diretório em que está o arquivo isapi_redirect.dll.

   O conteúdo desse arquivo é o seguinte:

   ```
   # Configuration file for the Jakarta ISAPI Redirector

   # The path to the ISAPI Redirector Extension, relative to the website

   # This must be in a virtual directory with execute privileges

   extension_uri=/jakarta/isapi_redirect.dll

   # Full path to the log file for the ISAPI Redirector

   log_file=<Configuration Manager Install Directory>\servers\server-0\logs\isapi.log

   # Log level (debug, info, warn, error or trace)

   log_level=info
   ```

```
# Full path to the workers.properties file

worker_file==<Configuration Manager Install
Directory>\tomcat\conf\workers.properties.minimal

# Full path to the uriworkermap.properties file

worker_mount_file==<Configuration Manager Install
Directory>\tomcat\conf\uriworkermap.properties
```

4 Crie um novo arquivo de texto chamado **workers.properties.minimal** em <**Diretório de instalação do Configuration Manager**>**\tomcat\conf**.

O conteúdo desse arquivo é o seguinte:

```
# workers.properties.minimal -

#

# This file provides minimal jk configuration

# properties needed to

# connect to Tomcat.

#

# Defining a worker named ajp13w and of type ajp13

# Note that the name and the type do not have to

# match.

        worker.list=ajp13w

        worker.ajp13w.type=ajp13

        worker.ajp13w.host=localhost

        worker.ajp13w.port=8009

#END
```

5 Crie um novo arquivo de texto chamado **uriworkermap.properties** em <**Diretório de instalação do Configuration Manager**>**\tomcat\conf**.

O conteúdo desse arquivo é o seguinte:

```
# uriworkermap.properties - IIS

#
```

```
# This file provides sample mappings for example:
# ajp13w worker defined in workermap.properties.minimal
# The general syntax for this file is:
# [URL]=[Worker name]

/cnc=ajp13w
/cnc/*=ajp13w
/bsf=ajp13w
/bsf/*=ajp13w
#END
```

Importante: note que o Configuration Manager deve ter duas regras. A nova sintaxe permite que elas sejam unidas em uma só, como:

/cnc|/*=ajp13w

---

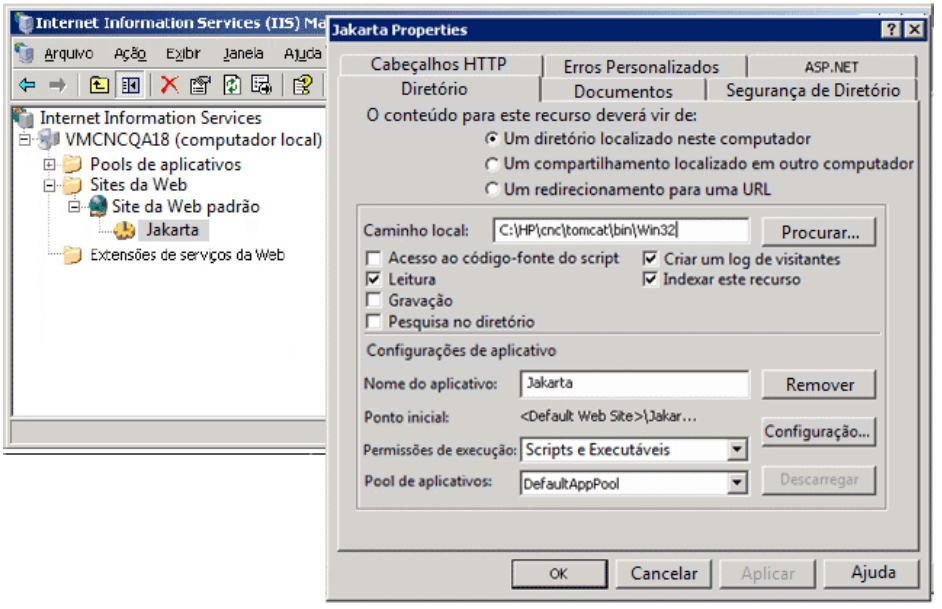
6 Crie o diretório virtual no objeto do site correspondente na configuração do IIS.

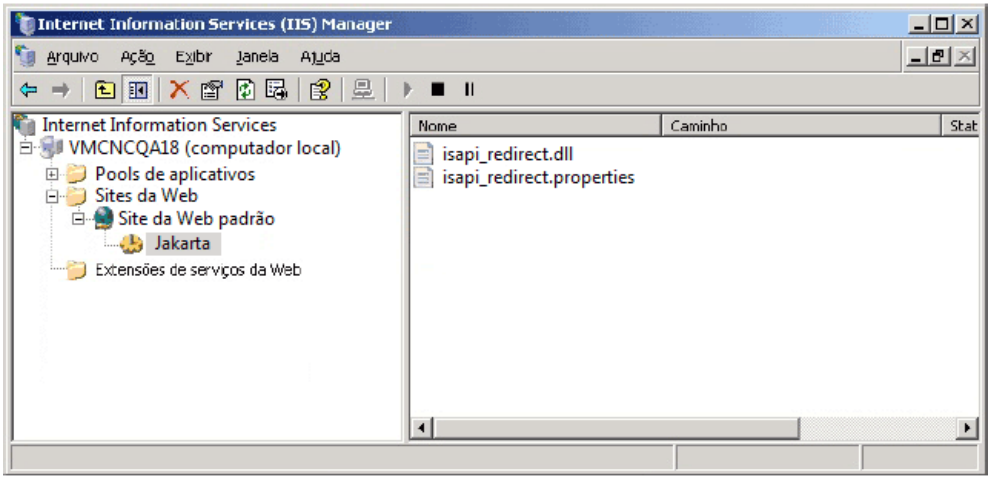
a No menu Iniciar do Windows, abra **Configurações\Painel de Controle\Ferramentas Administrativas\Gerenciador do Serviços de Informações da Internet (IIS)**.

b No painel direito, clique com o botão direito do mouse em **<Nome do Computador Local>\Web Sites\<Nome do seu site>** e selecione **Novo\Diretório Virtual**.

c Nomeie o diretório com o alias **Jakarta** e defina o caminho local para o diretório que contém o arquivo isapi_redirect.dll.

A janela do Gerenciador parecerá com esta:





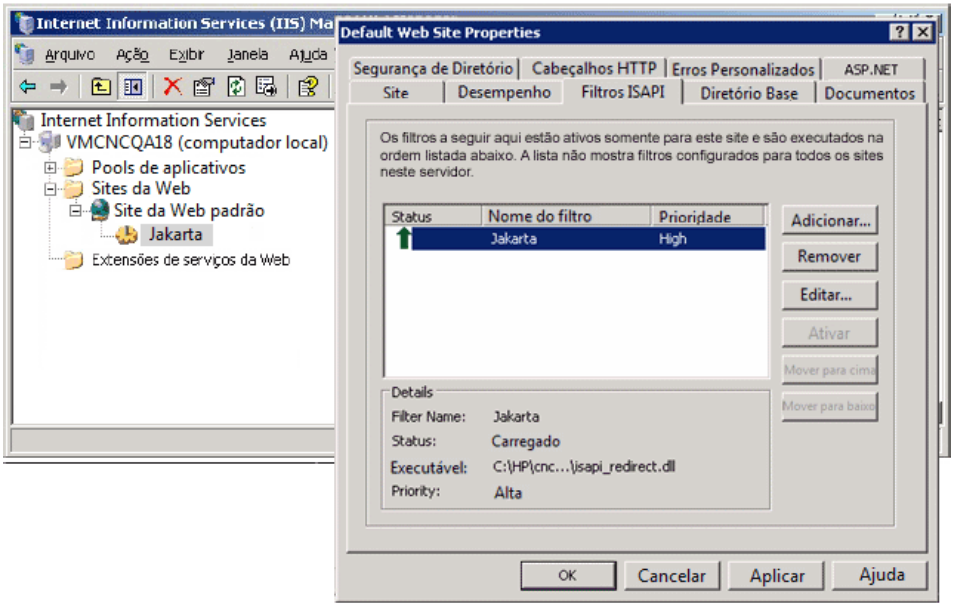
7 Adicione **isapi_redirect.dll** como um filtro ISAPI.

a Clique com o botão direito do mouse em **<Nome do seu site>** e selecione **Propriedades**.

b Selecione a guia **Filtros ISAPI** e clique no botão **Adicionar…**.

c Selecione o Nome do Filtro **Jakarta** e navegue até o arquivo **isapi_redirect.dll**. O filtro será adicionado, mas ainda estará inativo.

A janela de configuração parecerá com esta:



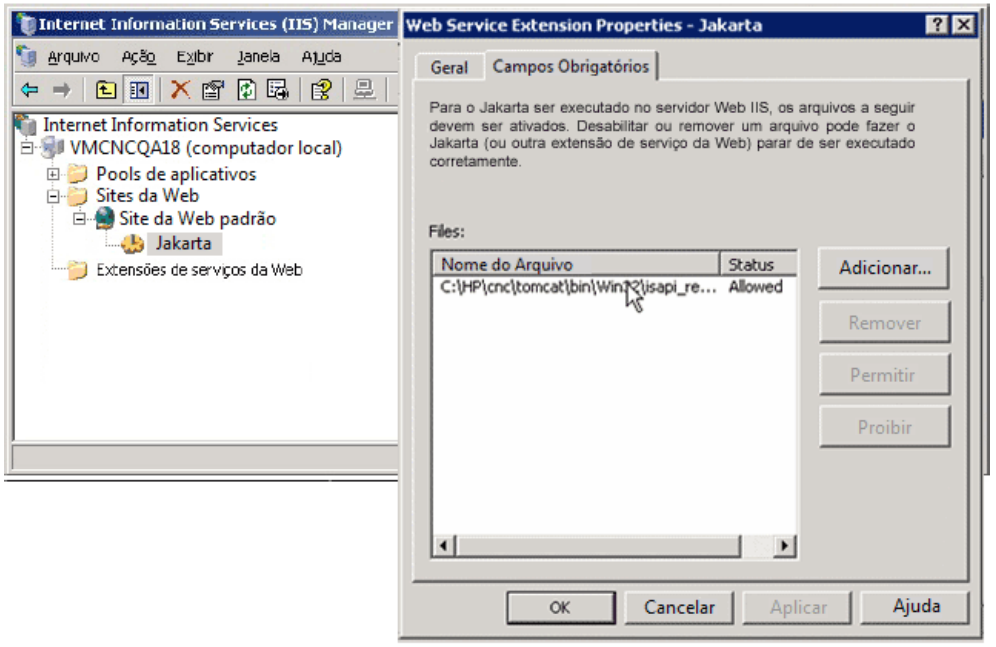
d Clique no botão **Aplicar**.

8 Defina e permita a nova extensão do Serviço Web.

a Clique com o botão direito do mouse na entrada **<Nome do Computador Local>\Extensões de Serviços Web** e selecione o item do menu **Adicionar nova Extensão do Serviço Web…**.

b Nomeie a nova extensão do Serviço Web como **Jakarta** e navegue até o arquivo **isapi_redirect.dll**.

Observação: Antes de clicar no botão **OK**, marque a caixa de seleção **Definir status da extensão como permitido**.



9 Reinicie o Servidor Web do IIS e acesse o aplicativo através do Serviço Web.

6

Fazendo logon no Configuration Manager

Este capítulo inclui:

Acessando o Configuration Manager

O acesso ao Configuration Manager é feito usando um navegador da Web compatível, de qualquer computador com uma conexão de rede (intranet ou Internet) ao servidor do Configuration Manager. O nível de acesso concedido a um usuário depende das permissões desse usuário. Para ver detalhes sobre a concessão de permissões ao usuário, consulte "Gerenciamento de Usuários" no *Guia do Usuário do HP Universal CMDB Configuration Manager*.

Para ver detalhes sobre os requisitos do navegador da Web, bem como requisitos mínimos para visualizar o Configuration Manager, consulte "Requisitos do sistema do Configuration Manager" na página 8.

Para ver detalhes sobre como acessar o Configuration Manager de forma segura, consulte "Proteção" na página 73.

Como acessar o Configuration Manager

No navegador da Web, insira a URL do Servidor do Configuration Manager, por exemplo, **http://<nome do servidor ou endereço IP>.<nome do domínio>:<porta>** onde **<nome do servidor ou endereço IP>.<nome do domínio>** representa o nome de domínio totalmente qualificado (FQDN) do servidor do Configuration Manager, e **<porta>** representa a porta selecionada durante a instalação.

Fazer logon no Configuration Manager

1. Insira o nome de usuário e a senha que você definiu no Assistente Pós-instalação do Configuration Manager.
2. Clique em **Logon**. Após o logon, o nome do usuário aparece no canto superior direito da tela.
3. (Recomendável) Conecte-se ao servidor LDAP organizacional e atribua funções administrativas a usuários LDAP para habilitar administradores do Configuration Manager a acessar o sistema. Para ver detalhes sobre a atribuição de funções a usuários no sistema do Configuration Manager, consulte "Gerenciamento de Usuários" no *Guia do Usuário do HP Universal CMDB Configuration Manager*.

Fazer logoff

Quando tiver concluído sua sessão, é recomendável que você faça logoff e saia do site, a fim de impedir a entrada não autorizada.

Para fazer logoff:

Clique em **Logoff** no topo da página.

Observação: Há um tempo padrão de expiração da sessão de 30 minutos.

Acessando o console JMX do Configuration Manager

Para fins de solução de problemas ou para modificar determinadas configurações, pode ser necessário acessar o console JMX.

Para acessar o console JMX:

1. Abra o console JMX em http://<nome do servidor ou endereço IP>:<porta>/cnc/jmx-console. A porta é a porta configurada durante a instalação do Configuration Manager.
2. Insira as credenciais de usuário padrão, que são as mesmas que as credenciais de usuário para logon no Configuration Manager.

Solução de problemas e limitações

Problema. Após mudar o conjunto de configurações no Administrador de Servidor, o servidor não é iniciado.

Solução. Reverter para o conjunto de configurações anterior. Proceda da seguinte maneira:

1. Execute o seguinte comando para localizar o ID do último conjunto de configurações ativado:

   ```
   <HP Universal CMDB Configuration Manager>\bin\export-cs.bat
   <propriedades do banco de dados> --history
   ```

   onde <**propriedades do banco de dados**> pode ser especificado apontando para o local do arquivo <**diretório de instalação do Configuration Manager**>**conf****database.properties** ou especificando cada propriedade do banco de dados. Por exemplo:

   ```
   cd <HP Universal CMDB Configuration Manager>\bin export-cs.bat -p
   ..\conf\database.properties --history
   ```

2. Execute o seguinte comando para exportar o último conjunto de configurações:

   ```
   <HP Universal CMDB Configuration Manager>\bin\export-cs.bat
   <propriedades do banco de dados> <ID do conjunto de configurações>
   <nome do arquivo de despejo>
   ```

onde <**ID do conjunto de configurações**> é o ID do conjunto de configurações da etapa anterior e <**arquivo de despejo**> é o nome de um arquivo temporário usado para armazenar o conjunto de configurações. Por exemplo, para exportar um conjunto de configurações com um ID de **491520** para o arquivo **mydump.zip**, insira o seguinte:

```
cd <início da instalação do HP Universal CMDB Configuration Manager>\bin export-cs.bat -p ..\conf\database.properties -i 491520 -f mydump.zip
```

3 Pare o serviço do HP Universal CMDB Configuration Manager.

4 Execute o seguinte comando para importar e ativar o conjunto de configurações anterior:

```
<HP Universal CMDB Configuration Manager>\bin\import-cs.bat <propriedades do banco de dados> <nome do arquivo de despejo> --activate
```

Problema. Ocorreu um erro na conexão do UCMDB.

Solução. A causa pode ser uma das seguintes:

- O servidor do UCMDB está inativo. Reinicie o Configuration Manager após o UCMDB ficar totalmente ativo (verifique se o status do servidor do UCMDB é **Ativo**).
- O servidor do UCMDB está ativo, mas a URL ou as credenciais da conexão do Configuration Manager estão incorretas. Inicie o Configuration Manager. Vá para Administração de Servidor, altere as configurações de conexão do UCMDB e salve o novo conjunto de configurações. Ative o conjunto de configurações e reinicie o servidor.

Problema. As configurações da conexão LDAP estão incorretas.

Solução. Reverter para o conjunto de configurações anterior. Defina as configurações corretas da conexão LDAP e ative o novo conjunto de configurações.

Problema. Mudanças no modelo de classe do UCMDB não são detectadas no Configuration Manager.

Solução. Reiniciar o servidor do Configuration Manager.

Problema. O log do Configuration Manager contém um erro de **Tempo limite de execução expirado** do **UCMDB**.

Solução. Isso ocorre quando o banco de dados do UCMDB está sobrecarregado. Para corrigir, aumente o tempo limite da conexão da seguinte maneira:

1. Crie um arquivo jdbc.properties na pasta **UCMDBServer\conf**.
2. Insira o seguinte texto: QueryTimeout=<número em segundos>.
3. Reinicie o servidor do UCMDB.

Problema. O Configuration Manager não permite adicionar uma visualização para ser gerenciada.

Solução. Quando uma visualização é adicionada para ser gerenciada, um novo TQL é criado no UCMDB. Se o limite máximo de TQLs ativos é atingido, a visualização não pode ser adicionada. Aumente o limite de TQLs ativos no UCMDB alterando as seguintes configurações no Gerenciador de Configurações de Infraestrutura:

- Número Máx de TQLs Ativos no Servidor
- Número Máx de TQLs Ativos do Cliente

Problema. O certificado do Servidor HTTPS não é válido.

Solução. A causa pode ser uma das seguintes:

- A data de validação do certificado passou. Você precisa obter um novo certificado.
- A autoridade de certificação do certificado não é uma autoridade confiável. Adicione uma autoridade de certificação à sua lista de Autoridades de Certificação Raiz Confiáveis.

Problema. Ao fazer o logon na página de logon do Configuration Manager, você obtém um erro de logon ou uma página de acesso negado.

Solução. A causa pode ser uma das seguintes:

- O nome de usuário pode não estar definido no provedor de autenticação (LDAP externo/compartilhado). Adicione o usuário no sistema provedor de autenticação.
- O usuário está definido, mas não tem permissão de logon para o Configuration Manager. Conceda a permissão de logon ao usuário. Como prática recomendada, atribua a permissão de logon ao grupo raiz de todos os usuários do Configuration Manager.
- Essas soluções também se aplicam nos casos em que o logon falha ao vir de um sistema IDM.

Problema. O servidor do Configuration Manager não é iniciado devido à inserção de credenciais de banco de dados incorretas.

Solução. Se você fez uma alteração nas credenciais do banco de dados e o servidor falha na inicialização, as credenciais podem estar incorretas. (**Observação**: o Assistente Pós-instalação não testa automaticamente as credenciais inseridas. É necessário clicar no botão **Testar** no assistente.) Você precisa recriptografar a senha do banco de dados e inserir novas credenciais no arquivo de configuração. Proceda da seguinte maneira:

1. De uma linha de comando, execute o seguinte comando para criptografar a senha do banco de dados atualizada:

   <pasta de instalação do Configuration Manager (CnC)>\bin\encrypt-password.bat –p <senha>

   que retorna uma senha criptografada.

2. Copie a senha criptografada (inclusive o prefixo {ENCRYPTED}) para o parâmetro **db.password** em **<pasta de instalação do CnC>\conf\database.properties**.

Problema. Se o DNS não está configurado corretamente, pode ser necessário fazer logon usando o endereço IP do servidor. Quando o endereço IP é inserido, um segundo erro de DNS ocorre.

Solução. Substituir o nome do computador pelo endereço IP novamente. Por exemplo:

Se você faz logon usando o seguinte endereço IP:
http://16.55.245.240:8180/cnc/

e obtém um endereço com o nome do computador mostrando um erro de DNS como
http://meu.exemplo.com:8180/bsf/secure/authenicationPointURL.jsp...

substitua-o por http://10.0.0.1:8180/bsf/secure/authenicationPointURL.jsp...

e inicie o aplicativo novamente no navegador.

Problema. O servidor tomcat do Configuration Manager não é iniciado.

Solução. Tente uma das opções a seguir:

- Execute o Assistente Pós-instalação e substitua as portas do servidor do Configuration Manager.
- Anule o outro processo que ocupa as portas do Configuration Manager.
- Altere manualmente as portas nos arquivos de configuração do Configuration Manager editando o seguinte arquivo: **<pasta de instalação do CnC>\servers\server-0\conf\server.xml** e atualizando as portas relevantes:
  - HTTP (8080): linha 69
  - HTTPS (8443): linhas 71, 90

Problema. Um erro de memória insuficiente é encontrado no log do Configuration Manager.

Solução. Aumentar o máximo de memória do Java conforme a necessidade.

Para alterar o tamanho da memória no serviço do Configuration Manager:

1. Vá para o diretório **<pasta de instalação do CnC>\cnc\bin** e execute o seguinte comando: edit-server-0.bat.
2. Selecione a guia **Java**.
3. Atualize os parâmetros **Pool de memória inicial** e **Pool de memória máximo**.

Para alterar o tamanho da memória no arquivo em lotes:

1. Vá para o diretório <**pasta de instalação do CnC**>**cnc** e abra o arquivo **start-server-0.bat** para edição
2. Localize a linha que começa com **SET JAVA_OPTS=-Dcnc.home**.
3. Localize os comandos **-Xms** e **-Xmx** e altere-os de acordo com os seus requisitos:

   -Xms<tamanho do pool de memória inicial> -Xmx<tamanho do pool de memória máximo>

   Por exemplo: para definir o pool de memória inicial como 100 MB e o pool de memória máximo como 800 MB, insira:

   -Xms100m -Xmx800m

Problema. O Assistente Pós-instalação demora muito depois que se clica em **Concluir**.

Solução. Para um sistema UCMDB que não foi pré-configurado com o modo consolidado, a operação de consolidar o esquema pode demorar bastante (dependendo da quantidade de dados). Aguarde 15 minutos. Se nenhum progresso for detectado, anule o Assistente Pós-instalação e reinicie o processo.

Problema. Modificações nos ECs no UCMDB não são refletidas no Configuration Manager.

Solução. O Configuration Manager executa um processo de análise assíncrona offline. O processo pode não ter processado ainda as modificações mais recentes no UCMDB. Para resolver isso, tente uma das seguintes opções:

- Aguarde alguns minutos. O intervalo padrão entre as execuções do processo de análise é de 10 minutos e é configurável no módulo Administração de Servidor.
- Execute uma chamada JMX para executar o cálculo de análise offline na visualização relevante.

➤ Vá para a Administração de Política. Clique no botão **Recalcular Análise da Política**. Isso chama o processo de análise offline para todas as visualizações (o que pode levar algum tempo). Talvez você também precise fazer uma modificação artificial em uma política e salvá-la.

Problema. Quando você clica em **Administração** > **Abrir UCMDB**, a página de logon do UCMDB é exibida.

Solução. Para acessar o UCMDB sem fazer logon novamente, é necessário habilitar o logon único. Para ver detalhes, consulte "Habilitar LW-SSO (Lightweight Single Sign-On)" na página 20. Além disso, verifique se o usuário do Configuration Manager conectado está definido no sistema de gerenciamento de usuários do UCMDB.

Problema. Quando se configura uma conexão do UCMDB no Assistente Pós-instalação com um endereço IPv6, o item do menu **Administração** > **Abrir UCMDB** não funciona.

Solução. Proceda da seguinte maneira:

1. Vá para **Administração** > **Administração de Servidor** > **Configuration Manager** > **Conexão do UCMDB**.
2. Adicione colchetes ao endereço IP na URL do endereço do UCMDB. A URL deve ficar assim: http://[x:x:x:x:x:x:x:x]:8080/.
3. Salve o conjunto de configurações e ative-o.
4. Reinicie o Configuration Manager.

As seguintes limitações aplicam-se ao trabalhar com o Configuration Manager:

➤ Sempre que a hora é alterada no servidor tomcat do Configuration Manager, o servidor precisa ser reiniciado para atualizar a hora.

7

Proteção

Este capítulo inclui:

Proteção do Configuration Manager

Esta seção apresenta o conceito de um aplicativo seguro do Configuration Manager 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 Configuration Manager 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 Configuration Manager mais seguro (protegido).

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

As preparações recomendadas para proteger seu sistema são as seguintes:

- Avaliar o risco/estado de segurança da sua rede geral e usar as conclusões ao decidir como integrar o Configuration Manager à rede da melhor forma.
- Desenvolver uma boa compreensão da estrutura técnica do Configuration Manager e de seus recursos de segurança.
- Examinar todas as diretrizes de proteção.
- Verificar se o Configuration Manager está totalmente funcional antes de iniciar os procedimentos de proteção.
- Seguir as etapas do procedimento de proteção cronologicamente em cada seção.

Importante:

- Os procedimentos de proteção baseiam-se na premissa de que você esteja implementando somente as instruções fornecidas nestas seções 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 nas seções a seguir sejam executados em computadores dedicados ao Configuration Manager. O uso dos computadores para outras finalidades além do Configuration Manager 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.

Criptografar a senha do banco de dados

A senha do banco de dados fica armazenada em **<Diretório de instalação do Configuration Manager>\conf\database.properties**. Se desejar criptografar a senha, nosso algoritmo de criptografia padrão é compatível com os padrões de FIPS 140-2. Para criptografar a senha do banco de dados, marque a caixa de seleção **Encrypt password** (Criptografar senha) na página Database Configuration (Configuração do Banco de Dados) do Assistente Pós-instalação do Configuration Manager.

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 obter detalhes sobre os parâmetros usados no processo de criptografia, consulte "Parâmetros de criptografia" na página 83.

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 **<Diretório de instalação do Configuration Manager>\conf\encryption.properties** e edite os seguintes campos:
   - **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 seguinte diretório: **cnc\security\encrypt_repository** e gera a chave de criptografia.
3. Execute o Assistente Pós-instalação novamente.

Habilitar o SSL no computador servidor com um certificado autoassinado

Estas seções explicam como configurar o Configuration Manager para suporte a autenticação e criptografia usando o canal SSL (Secure Sockets Layer).

O Configuration Manager usa o Tomcat 6.0 como servidor de aplicativos.

Observação: todos os locais de diretórios e arquivos dependem das suas preferências específicas de plataforma, sistema operacional e instalação.

---

1 Pré-requisitos

Antes de iniciar o procedimento a seguir, remova o arquivo **tomcat.keystore** antigo localizado em **<Diretório de instalação do Configuration Manager>\java\lib\security\tomcat.keystore**.

2 Gerar um repositório de chave de servidor

Crie um keystore (tipo JKS) com um certificado autoassinado e chave privada correspondente:

➤ No diretório bin da instalação Java em **<Diretório de instalação do Configuration Manager>**, execute o seguinte comando:

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

A caixa de diálogo do console será aberta.

➤ Insira a chave do keystore. Se a senha tiver sido alterada, altere-a manualmente no arquivo.

➤ Responda a pergunta "**Qual é o seu nome e sobrenome?**". 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 keystore.

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

3 Colocar o certificado no repositório confiável do cliente

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

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

---

4 Verificar as definições da configuração do cliente

Abra o arquivo **client-config.properties**, localizado no diretório **conf** do <**Diretório de instalação do Configuration Manager**>. Defina o protocolo como **https** e a porta como **8443**.

5 Modificar o arquivo server.xml

Abra o arquivo **server.xml**, localizado no diretório **conf** do <**Diretório de instalação do Configuration Manager**>. Localize a seção que começa com

Connector port="8443"

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

keystoreFile="<local do arquivo tomcat.keystore>" (consulte a etapa 2 na página 76)

keystorePass="<senha>"

6 Reiniciar o servidor

7 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>:8443/cnc**.

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

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

1 Pré-requisitos

Antes de iniciar o procedimento a seguir, remova o arquivo **tomcat.keystore** antigo localizado em **<Diretório de instalação do Configuration Manager>\java\lib\security\tomcat.keystore**.

2 Gerar um keystore 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 keystore em um keystore 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: <**Diretório de instalação do Configuration Manager**>**java****lib****security**.

d Abra o prompt de comando e altere o diretório para <**Diretório de instalação do Configuration Manager**>**bin****jre****bin**.

➤ Altere o tipo de keystore de **PKCS12** para um keystore **JAVA** executando o seguinte comando:

```
keytool -importkeystore -srckeystore <Diretório de instalação do Configuration Manager>\conf\security\<nome do arquivo pfx> -srcstoretype PKCS12 -destkeystore tomcat.keystore
```

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

3 Verificar as definições da configuração do cliente

Abra o seguinte arquivo: <**Diretório de instalação do Configuration Manager**>**cnc****conf****client-config.properties** e verifique se a propriedade **bsf.server.url** está definida como **https** e a porta é **8443**.

4 Modificar o arquivo server.xml

Abra o seguinte arquivo: <**Diretório de instalação do Configuration Manager**>**conf****server.xml**. Localize a seção que começa com

```
Connector port="8443"
```

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="senha" />
```

5 Reiniciar o servidor

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>:8443/cnc**.

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

Habilitar o SSL com um certificado de cliente

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**.

   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 e importar o arquivo.

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

   ```
   keytool.exe -import -alias hp -file hp.cer -keystore ..\lib\security\cacerts
   ```

4. Modifique o arquivo server.xml da seguinte maneira:
   a. Faça as alterações descritas na etapa 5 na página 77.
   b. Imediatamente após essas alterações, adicione as seguintes linhas:

      truststoreFile="../../java/lib/security/cacerts"

      truststorePass="changeit" />

   c. Defina clientAuth="true".
5. Verifique a segurança do servidor conforme descrito na etapa 7 na página 78.

Habilitar o SSL somente para autenticação

Esta tarefa descreve como configurar o Configuration Manager para suporte apenas à autenticação. Esse é o nível mínimo de segurança necessário para trabalhar com o Configuration Manager.

Para habilitar o SSL para autenticação:

1. Siga um dos procedimentos para habilitar o SSL no computador servidor conforme descrito em "Habilitar o SSL no computador servidor com um certificado autoassinado" na página 76 até a etapa 6 na página 78 ou em "Habilitar o SSL no computador servidor com um certificado de uma Autoridade de Certificação" na página 78 até a etapa 5 na página 80.
2. Insira a seguinte URL no navegador da Web: **http://<Nome do servidor do Configuration Manager ou endereço IP>:8080/cnc**.

Habilitar a autenticação do certificado do cliente

Esta tarefa descreve como configurar o Configuration Manager para aceitar a autenticação do certificado no cliente.

Para habilitar a autenticação do certificado do cliente:

1. Siga o procedimento para habilitar o SSL no computador servidor conforme descrito em "Habilitar o SSL no computador servidor com um certificado autoassinado" na página 76.
2. Abra o seguinte arquivo: **<Diretório de instalação do Configuration Manager>\conf\lwssofmconf.xml.** Localize a seção que começa com in-client certificate. Por exemplo:

   ```
   <in-clientCertificate userIdentifierRetrieveField="SubjectDN"
   userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="e" />
   ```

   Ative a funcionalidade de certificado do cliente removendo o caractere de comentário.
3. Extraia o nome de usuário do certificado de acordo com o seguinte procedimento:
   a. O parâmetro **userIdentifierRetrieveField** indica qual campo do certificado contém o nome de usuário. As opções são:
      - **SubjectDN**
      - **SubjectAlternativeName**

   b. O parâmetro **userIdentifierRetrieveMode** indica se o nome de usuário consiste no conteúdo inteiro do campo relevante ou apenas parte dele. As opções são:
      - **EntireField**
      - **FieldPart**

   c. Se o valor de **userIdentifierRetrieveMode** for **FieldPart**, o parâmetro **userIdentifierRetrieveFieldPart** indicará qual parte do campo relevante constitui o nome de usuário. O valor é uma letra de código baseada em uma legenda definida no próprio certificado.

4 Abra o arquivo <**Diretório de instalação do Configuration Manager**>**conf****client-config.properties** e edite as seguintes propriedades:

- Altere **bsf.server.url** para usar o protocolo HTTPS e mude a porta HTTPS para a porta descrita em "Habilitar o SSL no computador servidor com um certificado autoassinado" na página 76.
- Altere **bsf.server.services.url** para usar o protocolo HTTP e mude a porta HTTPS para a porta HTTP original.

Parâmetros de criptografia

A tabela a seguir lista os parâmetros incluídos no arquivo **encryption.properties** usado para a criptografia da senha do banco de dados. Para ver detalhes sobre a criptografia da senha do banco de dados, consulte "Criptografar a senha do banco de dados" na página 75.

Parâmetro	Descrição
cryptoSource	Indica a infraestrutura que implementa o algoritmo de criptografia. As opções disponíveis são: ➤ **lw.** Usa implementação leve da Bouncy Castle (opção padrão) ➤ **jce.** Aprimoramento da Criptografia Java (infraestrutura de criptografia Java padrão)
storageType	Indica o tipo do armazenamento de chave. 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 somente há suporte para **symmetricBlockCipher**.

Parâmetro	Descrição
engineName	O nome do algoritmo de criptografia. As seguintes opções estão disponíveis: ➤ **AES.** American Encryption Standard. Esta criptografia é compatível com FIPS 140-2 (opção padrão). ➤ **Blowfish** ➤ **DES** ➤ **3DES.** (compatível com FIPS 140-2) ➤ **Null**. Sem criptografia
keySize	O tamanho da chave mestra. O tamanho é determinado pelo algoritmo: ➤ **AES.** 128, 192 ou 256 (a opção padrão é 256) ➤ **Blowfish.** 0-400 ➤ **DES.** 56 ➤ **3DES.** 156
encodingMode	A codificação ASCII dos resultados da criptografia binária. As seguintes opções estão disponíveis: ➤ **Base64** (opção padrão) ➤ **Base64Url** ➤ **Hex (Hexadecimal)**
algorithmModeName	O modo do algoritmo. Atualmente somente há suporte para **CBC**.
algorithmPaddingName	O algoritmo de preenchimento utilizado. As seguintes opções estão disponíveis: ➤ **PKCS7Padding** (opção padrão) ➤ **PKCS5Padding**
jceProviderName	O nome do algoritmo de criptografia JCE. **Observação:** relevante apenas quando crytpSource é **jce**. Para **lw**, é usado engineName.