



Servidor de Configuração

Manual de Instalação

Sumário

1. Controle de Revisão	3
2. Introdução.....	4
3. Informações Gerais e Requisitos para Instalação.....	5
4. Instalação	6
4.1. Configuração do Controle de Acesso e Permissões – Keycloak.....	6
4.2. Configuração do <i>datasource</i> da Aplicação	6
4.2.1. Criando um Domínio de Segurança para a Aplicação.....	6
4.2.2. Criando um <i>datasource</i> para a Aplicação.....	8
4.3. Distribuição do pacote da Aplicação	9
5. Atualização.....	10
5.1. Redistribuição do pacote da Aplicação (Atualização).....	10
6. Remoção	11
6.1. Remoção da distribuição da Aplicação.....	11
6.1.1. Remoção do <i>datasource</i> da Aplicação	11
6.1.2. Remoção do domínio de Segurança.....	12
7. Informações Adicionais	12
7.1.1. Criptografando senha de acesso	12

1. Controle de Revisão

Revisão	Data	Histórico das revisões	Autor
01.00	17/04/2017	Criação do documento	Igor C. Ramos
01.01	20/04/2017	Revisão do documento	Marcelo Mello
01.02	25/05/2017	Correção de referência cruzada	Igor C. Ramos
01.03	05/072017	Adicionando informações do Linx-SSO	Igor C. Ramos

2. Introdução

Este documento tem como objetivo fornecer as informações necessárias para instalação e configuração do Servidor de Configuração (SC) em ambientes Windows e Unix.

Use os procedimentos indicados a seguir para realizar a instalação.

3. Informações Gerais e Requisitos para Instalação

A máquina onde será instalado o SC, deve possuir o servidor do WildFly versão 10.0 distribuído pela Linx instalado e executando. É de responsabilidade do usuário verificar se já existe uma instalação do SC antes de prosseguir com os passos deste manual.

Apenas o suporte aos bancos de dados Oracle 10g e 11g é fornecido. A estrutura do banco de dados usada pela aplicação deve estar disponível e pronta antes da execução dos passos deste manual. A configuração estrutural (tabelas, constraints, etc.) deve ser fornecida pela Linx.

Neste documento, "diretório raiz" é o diretório onde o Servidor de Aplicação Linx-Wildfly foi instalado. O exemplo utilizado neste documento utilizará como diretório raiz o caminho "/opt/linx-wildfly" para Sistema Operacional UNIX e "c:\program files\linx-wildfly" para SO Windows.

4. Instalação

Para configurarmos uma aplicação precisamos configurar seu controle de acesso, usaremos o Linx-SSO, e sua fonte de dados no Servidor Linx-Wildfly, o *datasource*.

O pacote distribuído para instalação do SC possui os seguintes arquivos:

- Este manual (SERVIDOR-CONFIGURACAO-DI.pdf);
- Pacote de Instalação.

4.1. Configuração do Controle de Acesso e Permissões – Linx-SSO

Antes de iniciar o uso da aplicação, é necessário configurar o Servidor de Autenticação com os dados da aplicação.

Acesse a interface de administração do Linx-SSO. Ex: *http://localhost:8180/auth/*

Após o login na área de administração do Linx-SSO acessar o menu “Clientes” e clicar em “servidor-configuracao”. Nessa tela adicionar um novo valor para o campo “URIs de redirecionamento válidas” usando o endereço da aplicação. Por exemplo:

*http://192.168.16.240:8080/linx-servidor-configuracao/**

Se o Servidor da aplicação estiver no IP “192.168.16.240” e porta “8080”.

Após a primeira distribuição da aplicação, o arquivo "linx-sso.properties" é criado no diretório "*standalone\data\ConfigurationManager*" do Servidor. Esse arquivo deve ter a propriedade "*auth-server-url*" com a URL do Linx-SSO que deve ser usado pela aplicação para obtenção das autenticações. Após essa alteração o servidor deve ser reiniciado.

4.2. Configuração do *datasource* da Aplicação

O *datasource* é usado pela aplicação para ter acesso ao banco de dados, então para isto as informações devem estar disponíveis para configuração da conexão.

Durante a criação do *datasource* a senha de acesso ao banco de dados pode ser armazenada de dois modos: criptografada, que necessita a criação de um domínio de segurança ou em texto plano que não requer configuração adicional.

4.2.1. Criando um Domínio de Segurança para a Aplicação

Para criar *datasource* com senha criptografada é necessário criar um domínio de segurança para o mesmo. A criação desse domínio exige conhecimentos e linha de comando do Sistema Operacional onde o Linx-Wildfly está instalado.

Primeiro precisamos *do texto correspondente* da senha criptografada. Para conseguir a senha criptografada ver seção 7.1.1. Vamos assumir que o texto da senha criptografada é: "64c5fd2979a86168". Aos passos:

- i) Acesse o diretório "bin", dentro do diretório raiz do servidor.
- ii) Localize o arquivo "jboss-cli.bat" para Windows ou "jboss-cli.sh" para Linux e execute-o.
- iii) Ao iniciar digite:

```
connect localhost:PORTA_GERENCIAMENTO
```

Onde "PORTA_GERENCIAMENTO" é a porta da interface de gerenciamento do servidor.

- iv) Ao conectar execute o comando:

```
/subsystem=security/security-domain=ConfigurationManager-security-domain/:add(cache-type=default)
```

Se for executado com sucesso, teremos: {"outcome" => "success"}.

- v) A seguir os campos para "Login" e "Senha" de acesso ao banco Oracle deverão ser informados. Utilize o texto gerado da senha criptografada para o valor do campo "DB_PASSWORD". Você deve **MANTER** as aspas:

```
/subsystem=security/security-domain=ConfigurationManager-security-domain/authentication=classic:add(login-modules=[{"code"=>"org.picketbox.datasource.security.SecureIdentityLoginModule", "flag"=>"required", "module-options"=>[("username"=>"DB_USER"),("password"=>"DB_PASSWORD"),("managedConnectionFactoryName"=>"jboss.jca:service=LocalTxCM,name=ConfigurationManagerDS")] ] )
```

Se for executado com sucesso, teremos: {"outcome" => "success", "response-headers" => { "operation-requires-reload" => true, "process-state" => "reload-required"}}

- vi) O domínio de segurança ConfigurationManager-security-domain foi criado e pode ser usado para a configuração de datasource.

4.2.2. Criando um datasource para a Aplicação

- i) Acesse a Interface de administração do Linx-Wildfly. Por padrão deve estar acessível através do endereço ***http://localhost:9990***, caso a porta não tenha sido alterada no servidor. Esse acesso necessita de login e senha;
- ii) Acessar menu *Configuration* e navegar: ***Subsystems -> Datasources -> Non-XA***;
- iii) Clicar em ***"Add"*** e aguardar abertura de tela;
- iv) Escolha ***"Oracle Datasource"*** e clique em ***"Next"***;
- v) Na tela *Step 1/3: Datasource Attributes*, preencher o campo *Name* com ***"ConfigurationManagerDS"*** (sem aspas), preencher o campo *JNDI Name* com ***"java:jboss/datasources/ConfigurationManagerDS"*** (sem aspas) e clique em ***"Next"***;
- vi) Na tela *"Step 2/3: JDBC Drive"*, clique em ***"Detected driver"***, selecione ***"ojdbc6.jar"*** na tabela *"Name"* e clique em ***"Next"***;
- vii) Na tela *"Step 3/3: Connection Settings"* você deve informar os dados de conexão do banco de dados.

Para o campo *"URL"* Informe o valor:

"jdbc:oracle:thin:@DB_HOST_NAME:DB_PORT:DB_SID" (sem aspas), onde *"DB_HOST_NAME"*, *"DB_PORT"*, *"DB_SID"* são informações de conexão do banco. Exemplo: ***jdbc:oracle:thin:@192.168.16.232:1521:ORA11GD***.

Para os campos *"login"*, *"password"* e *"Security Domain"* você deve escolher o modo como essas informações serão armazenadas no Linx-Wildfly.

Se os campos de *"login"* e *"password"* forem informados, a senha será armazenada como texto plano no *datasource*. Se esse não for o resultado desejável, informe o nome de um domínio de segurança que pode ser criado com senha criptografada (ver *Criando um Domínio de Segurança para a Aplicação*).

- viii) Confirme as informações do *datasource* e clique em ***"Next"***;
- ix) Clique no botão ***"Reload server(s) now"***. Você será redirecionado para o menu ***"Runtime"*** para executar o ***"reload"*** do servidor. Clique em ***"Standalone Server"*** e depois em ***"Reload"***. Você será questionado se deseja prosseguir, clique em ***"Confirm"*** e aguarde.
- x) Feito.

4.3. Distribuição do pacote da Aplicação

A aplicação é distribuída através de um arquivo *“.war”*. Para iniciar sua distribuição, usando a interface de administração do servidor, acesse o menu *“Deployments”* e siga os seguintes procedimentos:

- i) Clique em *“Add”* e aguarde a tela;
- ii) Escolha a opção *“Upload a new deployment”* e clique em *“Next”*;
- iii) Clique no botão para indicar onde está o pacote de distribuição da aplicação. Nesse passo você deve selecionar o *.war* enviado no pacote de instalação e clique em *“Next”*;
- iv) A tela de verificação de informações de Upload não deve ser alterada. Clique em *“Finish”*;
- v) Aguarde a distribuição da aplicação e a mensagem de sucesso.
- vi) Verifique o acesso a aplicação, por exemplo:

localhost:8080/linx-servidor-configuracao

- vii) Feito.

5. Atualização

5.1. Redistribuição do pacote da Aplicação (Atualização)

Essa operação deve ser usada caso a aplicação tenha sido instalada anteriormente e agora precise ser atualizada. Siga os seguintes procedimentos:

- i) Para redistribuir a aplicação no servidor acesse o menu "**Deployments**" e clique na opção "**Replace**" do combo da aplicação já distribuída.
- ii) Escolha o caminho do pacote para redistribuição, clique em "**Finish**" e aguarde o processamento.
- iii) Aguarde a distribuição da aplicação e a mensagem de sucesso.
- iv) Verifique o acesso a aplicação, por exemplo:

localhost:8080/linx-servidor-configuracao

- v) Feito.

6. Remoção

6.1. Remoção da distribuição da Aplicação

Essa operação deve ser usada caso a aplicação tenha sido instalada anteriormente e agora deve ser removida. Primeiro vamos aos procedimentos para remoção da aplicação:

- i) Para remoção da aplicação no servidor acesse o menu "**Deployments**" e clique na opção "**Remove**" do combo da aplicação já distribuída.
- ii) Ao abrir a tela, clique em "**Confirm**" e aguarde a remoção.
- iii) Feito.

6.1.1. Remoção do *datasource* da Aplicação

O *datasource* da aplicação não é removido quando a distribuição da aplicação é removida. Para isso é necessário realizar essa remoção diretamente no seu registro:

- i) Acesse a Interface de administração do Linx-Wildfly.
- ii) Acessar menu **Configuration** e navegar: **Subsystems -> Datasources -> Non-XA**;
- iii) Selecionar a opção "**Remove**" no combo de opções do *datasource* da aplicação;
- iv) Ao abrir a tela, clique em "**Confirm**" e aguarde a remoção.
- v) Feito.

6.1.2. Remoção do domínio de Segurança

O domínio de segurança da aplicação, se criado, também pode ser removido:

- i) Acesse a Interface de administração do Linx-Wildfly.
- ii) Acessar menu **Configuration** e navegar: **Subsystems -> Security**;
- iii) Localizar o domínio de segurança "**ConfigurationManager-security-domain**" e selecionar "**Remove**" no combo de opção do mesmo.
- iv) Confirme remoção e aguarde.
- v) Feito.

7. Informações Adicionais

7.1.1. Criptografando senha de acesso

Usando a linha de comando do sistema operacional, navegue até o diretório raiz do Linx-Wildfly e digite:

- i) Para Windows:

```
jre\bin\java -cp modules\system\layers\base\org\picketbox\main\picketbox-4.9.6.Final.jar org.picketbox.datasource.security.SecureIdentityLoginModule "DB_PASSWORD"
```

- ii) Para Linux:

```
jre/bin/java -cp modules/system/layers/base/org/picketbox/main/picketbox-4.9.6.Final.jar org.picketbox.datasource.security.SecureIdentityLoginModule "DB_PASSWORD"
```

Onde "DB_PASSWORD" deve ser substituído pela senha a ser criptografada, sem as aspas. Por exemplo, executando-o para senha "123456" no Windows teremos:

```
jre\bin\java -cp modules\system\layers\base\org\picketbox\main\picketbox-4.9.6.Final.jar org.picketbox.datasource.security.SecureIdentityLoginModule 123456
```

Tendo como resultado:

Encoded password: 64c5fd2979a86168.

Onde a senha criptografada é "64c5fd2979a86168".