- `sqljdbc.dll` files to support either 32-bit or 64-bit SQL Server are in `win32` and `win64_amd64`
- `instjdbc.sql`

Messaging component setup
The Installation Startup Kit includes scripts that you can use to install the InfoSphere MDM messaging component when WebSphere MQ is on a machine that is different than the one where IBM Installation Manager is running, use the scripts `custSetupMQServer.mqsc` and `ChannelAuth.mqsc`.

Prerequisite checking tool
The prerequisite checking command line tool helps to prevent you from beginning an installation that will be unable to successfully complete due to missing prerequisites. This tool has the following capabilities:

- Runs prerequisite checks for InfoSphere MDM installation.
- Performs basic data collection – Collects logs and configuration files.
- Performs extended data collection – Collects logs, configuration files, and metadata stored in the database

The prerequisite checking tool's data collection capabilities can be useful after an InfoSphere MDM has completed or if you need to troubleshoot an installation. The results of these collections are stored in a compressed file.

Silent installation response files
The Installation Startup Kit includes sample response files (`.res`). These files are samples that can be used as templates for running silent installations. The sample response files are located in *STARTUPKIT_INSTALL_HOME* at the root level.

Related tasks:

"Installing silently by using a response file" on page 142

"Installing the Installation Startup Kit" on page 73

"Installing and setting up the database" on page 81

"Checking prerequisites using the command line tool" on page 112

Related reference:

"Silent installation" on page 132

Multiple instance support

Multiple instances of InfoSphere MDM is supported by installing the application in a clustered environment.

All InfoSphere MDM application instances in the clustered nodes within a WebSphere Application Server cell must be deployed with the same version of InfoSphere MDM product code and must have the same version of the InfoSphere MDM customization code.

If you want to use the same physical machine (or LPAR) to deploy a second InfoSphere MDM application instance that is running a different version of InfoSphere MDM product code, you must create a second WebSphere Application Server cell, deployment manager, and node profile.

If you want to configure a simple functional test environment, you can use the same WebSphere Application Server cell and node to deploy multiple instances of InfoSphere MDM with the same version of InfoSphere MDM product code and different version of the InfoSphere MDM customization code. However, some

Enabling user security for the operational server

Configuring users and user groups for virtual MDM

Password storage and exposure

During installation, passwords are encrypted by using WebSphere Application Server encryption.

All user interface applications and client applications have a user name and password to connect to the MDM operational server. These passwords are also encrypted by using the WebSphere Application Server encryption mechanism. If any of the passwords are changed on the application server, then you must also apply the change in the respective component properties file as well.

Be aware that when the installer generates response files that can be used for silent installations, these files contain user passwords in plain text. If plain text passwords stored in the files are against your organizational policies, use the graphical installation mode.

Related information:

Configuring secure MDM environments

Encrypting passwords with WebSphere Application Server

If you must change a user name and password in a properties file after installation, you can use this task to encrypt the new password.

About this task

To prevent the password from being stored in clear text in your properties file, you can use WebSphere Application Server to encrypt the password.

Procedure

1. Create a text file called `mypassword.txt`.
2. Add this line to the file: `mypassword=`*`user_password`* and save the file.
3. Run the following command to encode the password value:
   - For Microsoft Windows: `$NODE_HOME\bin\PropFilePasswordEncoder.bat` *`path`*`\mypassword.txt mypassword`
   - For Linux and UNIX: *`$NODE_HOME`*`/bin/PropFilePasswordEncoder.sh` *`path`*`/mypassword.txt mypassword`

   Where *`$NODE_HOME`* represents the home directory of the WebSphere Application Server node and *`path`* represents the directory location of the `mypassword.txt` file.
4. Open the `mypassword.txt` file and copy the encrypted password value to the password field in your properties file.

Related information:

Configuring secure MDM environments

Directory structures

There are three directories you want to understand when you install and use InfoSphere MDM: the installation directory, the shared directory, and the application server directory.