HITACHI
Inspire the Next

Secure LDAP Passwords for Pentaho Suite

HITACHI
Inspire the Next

Change log (if you want to use it):

Date	Version	Author	Changes

Contents

This page intentionally left blank.

Overview

The default Pentaho deployment requires the entry of the master-user's password in plain text within the LDAP properties configuration file. The usual recommendation is to secure this file by removing read permissions for all OS users except for the master-user, but your security regulations may specify that you are not able to use a plain text password in the file system.

If you are configuring the Pentaho BA server to use LDAP authentication, you will need to create a master-user that is able to query the LDAP server to get details about users, roles, and authenticate when a user is logging in.

The intention of this document is to speak about topics generally; however, these are the specific versions covered here:

Software	Version(s)
Pentaho	6.x, 7.x, 8.0

The Components Reference in Pentaho Documentation has a complete list of supported software and hardware.

Secure LDAP Passwords

Pentaho provides a service (`IPasswordService`) that allows the encryption and decryption of strings that have `Base64` as the default encoding/decoding scheme. Other schemes, such as AES or Triple DES, can be implemented.

You can use a Spring Expression Language (SpEL) query to access this service and use it to decode a string from a properties file, then assign it to the Spring variable that holds this password.

Solution

This section has steps that demonstrate how to implement the solution described above. We will be using `Base64` encoding in these steps, to use a different encoding/decoding scheme you will need to implement the `IPasswordService` with your desired method.

1. Stop the Pentaho BA Server.
2. Run your password through a Base64 encoder. An example password is `Password1`, which results in an encoded password of `UGFzc3dvcmQx`.
3. Open the `pentaho-solutions/system/applicationContext-security-ldap.properties` file with any text editor.
4. Edit to assign the encoded value to the `contextSource.password` property, then save and close the file:

```
contextSource.password=UGFzc3dvcmQx
```

5. Open the `pentaho-solutions/system/applicationContext-spring-security-ldap.xml`.
6. Change the password property value to use the SpEL query as shown below:

```
<bean id="contextSource"
class="org.springframework.security.ldap.DefaultSpringSecurityContextSource
">

    <constructor-arg value="${ldap.contextSource.providerUrl}"/>

    <property name="userDn" value="${ldap.contextSource.userDn}"/>

    <property name="password"
value="#{IPasswordService.decrypt('${ldap.contextSource.password}')}"/>

  </bean>
```

7. Save and close the file.
8. Start the Pentaho BA Server.

Related Information

Here are some links to information on advanced security for Pentaho, Spring Expression Language, and the Base64 Encoder website:

- Pentaho Documentation: Implement Advanced Security
- Spring Expression Language Example
- Base64 Encoder