Recover Decrypt WebLogic Server Admin Password

One of the most important WebLogic Server files in terms of security is *SerializedSystemIni.dat* which contains encrypted security data and is located in *$DOMAIN\_HOME/security*directory. Other file is *boot.properties* file located in *$DOMAIN\_HOME/servers/AdminServer/security* directory which contains an encrypted version of weblogic admin username and password.

 Below tutorial shows how to decrypt, recover username or password, having access to *SerializedSystemIni.dat* and *boot.properties* files. But not only, we can also use this method to:

* recover database username and password of JDBC Connection pool – encrypted password resides in $DOMAIN\_HOME/config/jdbc directory, in xml files
* recover password of a keystore where we store SSL certificates
* any encrypted password from config.xml  located in $DOMAIN\_HOME/config dir

**Let’s roll:**

**NOTE**: *SerializedSystemIni.dat*file exists in *$DOMAIN\_HOME/security*directory.

**1. Create a script *decrypt\_password.py*in*$DOMAIN\_HOME/security*directory and paste the following code into it:**



|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15 | from weblogic.security.internal import \*  from weblogic.security.internal.encryption import \*  encryptionService = SerializedSystemIni.getEncryptionService(".")  clearOrEncryptService = ClearOrEncryptedService(encryptionService)    # Take encrypt password from user  pwd = raw\_input("Paste encrypted password ({AES}fk9EK...): ")    # Delete unnecessary escape characters  preppwd = pwd.replace("\\", "")    # Display password  print "Decrypted string is: " + clearOrEncryptService.decrypt(preppwd) |

**2. Set domain environment variables**



|  |  |
| --- | --- |
| 1  2  3 | source $DOMAIN\_HOME/bin/setDomainEnv.sh |

**3. Get encrypted password, in this example from *boot.properties* file of AdminServer**



|  |  |
| --- | --- |
| 1  2  3  4  5  6  7 | #Username:  grep username $DOMAIN\_HOME/servers/AdminServer/security/boot.properties | sed -e "s/^username=\(.\*\)/\1/"    #Password:  grep password $DOMAIN\_HOME/servers/AdminServer/security/boot.properties | sed -e "s/^password=\(.\*\)/\1/" |

**4. Navigate to *$DOMAIN\_HOME/security* directory and run the following command to start decryption:**



|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15 | cd $DOMAIN\_HOME/security    java weblogic.WLST decrypt\_password.py      Initializing WebLogic Scripting Tool (WLST) ...    Welcome to WebLogic Server Administration Scripting Shell    Type help() for help on available commands    Please enter encrypted password (Eg. {AES}fk9EK...): {AES}jkIkkdh693dsyLt+DrKUfNcXryuHKLJD76\*SXnPqnl5oo\=  Decrypted string is: welcome01 |

Decrypted value will be displayed on the screen.

- See more at: http://emarcel.com/recover-decrypt-weblogic-server-admin-password/#sthash.lSWvbLHT.dpuf