Module Réglementaire DSN

DSN 4.1

Guide de Sécurité

HRa Suite 7 et 9

**F REGDSN 2017 1 GS 041 HRA** Edition : **1**

Date : **Mai 2017**

Le paragraphe qui suit ne s'applique pas au Royaume‑Uni ou à tout autre pays dans lequel ces dispositions sont incompatibles avec la législation en vigueur : LE PRÉSENT DOCUMENT EST LIVRÉ "EN L'ETAT". Sopra HR Software DÉCLINE TOUTE RESPONSABILITÉ, EXPRESSE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE QUALITÉ MARCHANDE OU D'ADAPTATION À VOS BESOINS. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Il n'est pas garanti que le contenu du présent document et les exemples de code source qui y figurent, pris individuellement ou en tant qu'ensemble, répondent à vos besoins, ni qu'ils soient exempts d'erreurs.

Ce document peut comporter des inexactitudes d'ordre technique ou des erreurs typographiques. Son contenu est périodiquement mis à jour et chaque nouvelle édition inclut les mises à jour. Sopra HR Software peut procéder à des améliorations et/ou des modifications du ou des produit(s) ou programme(s) décrits dans ce document, à tout moment.

Pour obtenir des exemplaires de documents ou pour toute demande d'ordre technique, adressez-vous à votre revendeur.

© 1996-2017 Sopra HR Software. Tous droits réservés.

Avertissement

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services HR Access non annoncés dans ce pays. Cela ne signifie pas que Sopra HR Software ait l'intention de les y annoncer. Sopra HR Software peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet.

Les logiciels tierce partie inclus dans HR Access ne peuvent être utilisés séparément de HR Access.

Marques

HRa Suite et HR Access sont des marques déposées de Sopra HR Software. Toute utilisation, reproduction ou représentation nécessite l'accord express et préalable de Sopra HR Software.

Les autres noms utilisés pour désigner des sociétés, des produits ou des services sont des marques ayant leur titulaire respectif.

Mise à jour de la documentation

Le contenu de la documentation HR Access est régulièrement mis à jour à travers les Delivery Pack

Remarques du lecteur

Vos commentaires et suggestions nous permettent d'améliorer la qualité de nos documentations. Ils jouent un rôle important lors de leur mise à jour. N'hésitez pas à en faire part à la hot-line HR Access.



www.soprahr.com

Le Triangle de l'Arche

8, cours du Triangle

92937 Paris La Défense Cedex

Table des matières

Introduction 4

Type d'accès 5

Exploitant Technique Paie 6

Exploitant Système Moteur Déclaratif 8

Accès JMX et SSH 8

Configuration des Services 8

Configuration JDBC de l'accès aux bases de données 10

Paramétrage 10

Chiffrement des mots de passe 12

# Introduction

Ce document traite des différents aspects Sécurité autour du module réglementaire DSN, pour les **composants mis en œuvre à travers ce module**, c'est-à-dire le ***Moteur Déclaratif*** et le ***Rechargeur***.

Ce document ne reprend pas les éléments de Sécurité décrits pour le Produit HR Access, disponibles dans un guide spécifique et qui restent inchangés avec la DSN.

La sécurité est évaluée ici sous l'angle des **accès utilisateur**, pour les différents types d'acteurs du module.

Ce document reprend également certains éléments décrits dans les Guides techniques et les rassemble ici pour donner une vue exhaustive du domaine.

# Type d'accès

Les accès utilisateur du Module Réglementaire sont des accès Exploitant qui regroupent des accès de type :

* **Exploitant Système Moteur Déclaratif** pour l'administration système de l'application regDSN (Moteur Déclaratif), incluant le pilotage et le monitoring de cette application.
* **Exploitant Technique Paie**, pour l'usage de l'application "Rechargeur".

# Exploitant Technique Paie

L'**Exploitant Technique Paie** utilise le Rechargeur (dsnReloader), qui est une application en ligne de commande. Elle nécessite un accès JDBC à la base de données HR Access. C'est ce **lien JDBC**, décrit dans le fichier 'propriétés' de l'application, qui contrôle l'usage de l'application. Ce fichier de propriétés contient les éléments utilisateur/mot de passe d'accès à la base. Cependant, si les règles de sécurité en place interdisent le stockage des utilisateurs / mot de passe en clair dans des fichiers, il est possible de ne pas les renseigner. Ils devront alors être **saisis** au lancement de l'application, via des paramètres spécifiques de la ligne de commande. Pour plus de détail, voir le document Rechargeur - Guide Technique.

La liste des tables HR Access accédées par ce Rechargeur est la suivante :

$CONFLUENCETABLE$

| **Table** | **Libellé** | **Versions**  **DSN (\*)** | **Spécifique DSN** | **Lecture/Ecriture** |
| --- | --- | --- | --- | --- |
| PP10 | Plate-forme physique |  | Non | Lecture |
| ZD00 | Identifiant dossiers réglementaires |  | Non | Lecture |
| ZD7O | Transcodification normalisée |  | Oui | Lecture |
| ZDAG | Renseignements pour édition TDS-DUCS | **>= 2.0** | Non | Lecture |
| ZDAO | Editions et contrôles | **>= 2.0** | Non | Lecture |
| DI30 | Domaines |  | Non | Lecture |
| ZD7P | Déversement DSN d'une rubrique |  | Oui | Lecture |
| ZD7Q | Attributs des compteurs DSN |  | Oui | Lecture |
| ZD7R | Attributs DSN | **>= 2.0** | Oui | Lecture |
| ZXMI | Identification contrat DSN |  | Oui | Lecture/Ecriture |
| ZX5V | Statut du dossier |  | Non | Lecture |
| ZXMJ | DSN : attributs historisés du contrat |  | Oui | Lecture/Ecriture |
| ZXMK | DSN : Bloc 60 (arrêts de travail) |  | Oui | Lecture/Ecriture |
| ZXML | DSN : Bloc 65  (suspensions tempo.) |  | Oui | Lecture/Ecriture |
| ZXMQ | DSN : Bloc 62 (fin de contrat) |  | Oui | Lecture/Ecriture |
| ZX8K | Eléments de rémunération |  | Non | Lecture |
| ZX8R | Compléments ZX8K |  | Oui | Lecture |
| ZXMM | DSN : Montants |  | Oui | Lecture/Ecriture |
| ZXTD11 | Table technique des informations | **>= 2.0** | Non | Lecture/Ecriture |
| ZXTD12 | Table technique des informations |  | Non | Lecture/Ecriture |

$CONFLUENCETABLE$

(\*) lorsque la version DSN n'est pas renseignée, cela signifie que la ligne est valable pour toutes les versions de la DSN.

# Exploitant Système Moteur Déclaratif

Pour les accès **Exploitant Système Moteur Déclaratif**, on considère :

* les accès **JMX** et **SSH**.
* l'accès **JDBC** aux bases de données.

## Accès JMX et SSH

Fichier user.properties

#### Comptes d'accès

L'accès aux services JMX et SSH nécessite une connexion : les utilisateurs de ces services JMX et SSH sont des **utilisateurs système spécifiques** qui sont déclarés dans le fichier **users.properties.**

#### Usage

Les usages de ces services sont précisés dans la partie "Exploitation" de ce document.

|  |
| --- |
| Authentification SSH par Clef en DSN 3.0 (et supérieure)  Dans le cadre d'usage du Moteur Déclaratif (et bien que référencé dans la documentation officielle Karaf), l'usage de **l'authentification par clef SSH n'est pas supporté** par l'Éditeur.  L'usage de la connexion SSH est d'ailleurs restreint à la **boucle locale**. |

### Configuration des Services

L'accès au service peut être contrôlé également via son paramétrage.

#### SSH

Dans le cas du SSH, le paramètre **sshHost** permet de contrôler les accès réseau à ce service.

Pour rappel, la configuration SSH comporte les éléments principaux suivants :

  Fichier org.apache.karaf.shell.cfg

#### Paramètres obligatoires

##### sshPort

Port du service SSH.

Valeur par défaut : 8101

##### sshHost

Adresse IP de l'interface réseau sur laquelle est ouvert le service SSH.

Indiquez 0.0.0.0 pour ouvrir le service sur toutes les interfaces réseaux.

#### Paramètre important

##### sshIdleTimeout

Timeout (en millisecondes) de la session SSH

Valeur par défaut : 1800000SHEDBLOCKWITHFORMAT$

#### JMX

Dans le cas du JMX, le paramètre **serviceUrl** permet de contrôler les accès réseau à ce service.

Pour rappel, la configuration JMX comporte les éléments principaux suivants :

  Fichier org.apache.karaf.management.cfg

#### Paramètres obligatoires

##### rmiRegistryPort

Numéro de port du service de registre RMI.

Valeur par défaut : 1099

##### rmiServerPort

Numéro de port du service JMX.

Valeur par défaut : 44444

##### serviceUrl

URL d'appel du service JMX. Remplacez "0.0.0.0" par le nom de la machine d'installation pour un accès distant.

Valeur par défaut :

serviceUrl = service:jmx:rmi://0.0.0.0:${rmiServerPort}/jndi/rmi://0.0.0.0:${rmiRegistryPort}/dsnASHEDBLOCKWITHFORMAT$

## Configuration JDBC de l'accès aux bases de données

Il s'agit ici des liens JDBC :

* avec la **base de données** HR Access (fichier com.soprahr.edsn.hraccess.datasource.cfg)
* avec la **BDSN** (fichier com.soprahr.edsn.datasource.cfg)

### Paramétrage

Pour rappel, les principaux paramètres intéressants pour la configuration des liens JDBC sont :

##### datasource.jdbc.driver

Nom de la classe driver JDBC permettant la connexion à la base de données.

##### datasource.jdbc.url

URL JDBC de la base de données.

##### datasource.user

Nom de l'utilisateur pour se connecter à la base de données.

##### datasource.password

Mot de passe pour se connecter à la base de données.

##### datasource.pool.validationQuery

Ordre SQL permettant de valider les connexions du pool.

|  |
| --- |
| Validation des pools de connexion  Ce paramètre n'est pas à proprement parler obligatoire pour le fonctionnement. **Cependant**, il est placé dans cette catégorie pour l'explication ci-dessous. |

Le Moteur Déclaratif utilise des  **pools de connexions JDBC**  pour l'accès aux bases de données (base HR Access et BDSN). Lorsque la base de données est  redémarrée , il se peut que des connexions présentes dans le pool deviennent invalides et engendrent des erreurs lors de leur utilisation.

Pour éviter cela il faut demander au pool de valider les connexions avec un ordre SQL SELECT renvoyant au moins une ligne.

Ce paramètre permet de spécifier l'ordre utilisé.

Il n'existe **pas de valeur par défaut** car l'ordre est dépendant de la base utilisée. Les valeurs proposées sont les suivantes :

|  |
| --- |
| Pour Oracle ...  datasource.pool.validationQuery=SELECT 1 FROM DUAL |

|  |
| --- |
| Pour DB2 ...  datasource.pool.validationQuery=SELECT 1 FROM SYSIBM.SYSDUMMY1 |

|  |
| --- |
| Pour MS SQL Server  datasource.pool.validationQuery=SELECT 1 |

|  |  |
| --- | --- |
| Valorisation de datasource.pool.validationQuery  La configuration de datasource.pool.vaidationQuery est considérée comme **optionnelle**...  Mais cela dépend de la **version du driver JDBC**.  Lorsque le paramètre n'est pas présent, c'est la méthode Connection.isValid() du JDK qui est appelée. Cette méthode est apparue en Java 1.6 : si le driver JDBC est ancien et qu'il a été développé avec un JDK < 1.6, cela peut provoquer une erreur du type :   |  | | --- | | 2015-04-30 18:07:23,194 | ERROR | FelixStartLevel | BlueprintContainerImpl | Unable to start blueprint container for bundle com.soprahr.edsn.hibernateloader  org.osgi.service.blueprint.container.ComponentDefinitionException: Unable to initialize bean hibernateStarter  Caused by: java.lang.AbstractMethodError: java/sql/Connection.isValid(I) |   La méthode la plus sûre consiste donc à renseigner le paramètre avec les valeurs données ci-dessus. |

$DASHEDBLOCKWITHFORMAT$

Pour plus de sécurité, il est possible d'utiliser le paramètre **datasource.cryptedPassword** à la place de ce paramètre si l'on souhaite chiffrer le mot de passe, comme décrit ci-dessous.

### Chiffrement des mots de passe

#### Principe

Sur les environnements de production, il est généralement proscrit de faire apparaître des mots de passe en clair dans les fichiers de configuration.

C'est le cas par exemple du paramètre datasource.password de la connexion JDBC. Dans ce cas, on peut remplacer le paramètre "datasource.password" par le paramètre "datasource.cryptedPassword" contenant une version chiffrée du mot de passe. Les étapes suivantes décrivent la manière de l'obtenir.

Il existe d'autres paramètres type mots de passe qui possèdent leur équivalent encrypté. Ils sont alors précisés dans les chapitres de configuration concernés.

#### Méthodologie

Avant de chiffrer les mots de passe, on commence par renseigner le paramètre "en clair" (ex : "datasource.password" pour le cas de la connexion JDBC) dans les fichiers de configuration concernés.

Après le démarrage de l'application DSN, on s'assure que tout fonctionne correctement.

Puis on utilise la commande interactive "encryption:encrypt-password" depuis le shell de l'application pour chiffrer chacun des mots de passe :

|  |
| --- |
| dsn>encryption:encrypt-password Password: t+zOLpMEeyoBTGMV+Rh8gw== |

Une fois le mot de passe entré, la version chiffrée s'affiche. Il suffit alors de la copier, puis de remplacer dans le fichier adéquat le paramètre en clair par le paramètre en version cryptée (Ex : "datasource.cryptedPassword") avec la valeur copiée.

Par exemple :

|  |
| --- |
| datasource.jdbc.driver=oracle.jdbc.driver.OracleDriver  datasource.jdbc.url=jdbc:oracle:thin:@ukx00684.ptx.fr.sopra:1521:DSN01  datasource.user=toto  datasource.cryptedPassword=t+zOLpMEeyoBTGMV+Rh8gw== |

 Lorsque tous les mots de passe ont été chiffrés, il est nécessaire de redémarrer l'application.