



**LSC : la nouvelle version qui
vous aide à maintenir vos
données à jour !**

Sommaire



Principes de gestion d'identité

Stratégies pour maintenir ses données à jour

Présentation de LSC

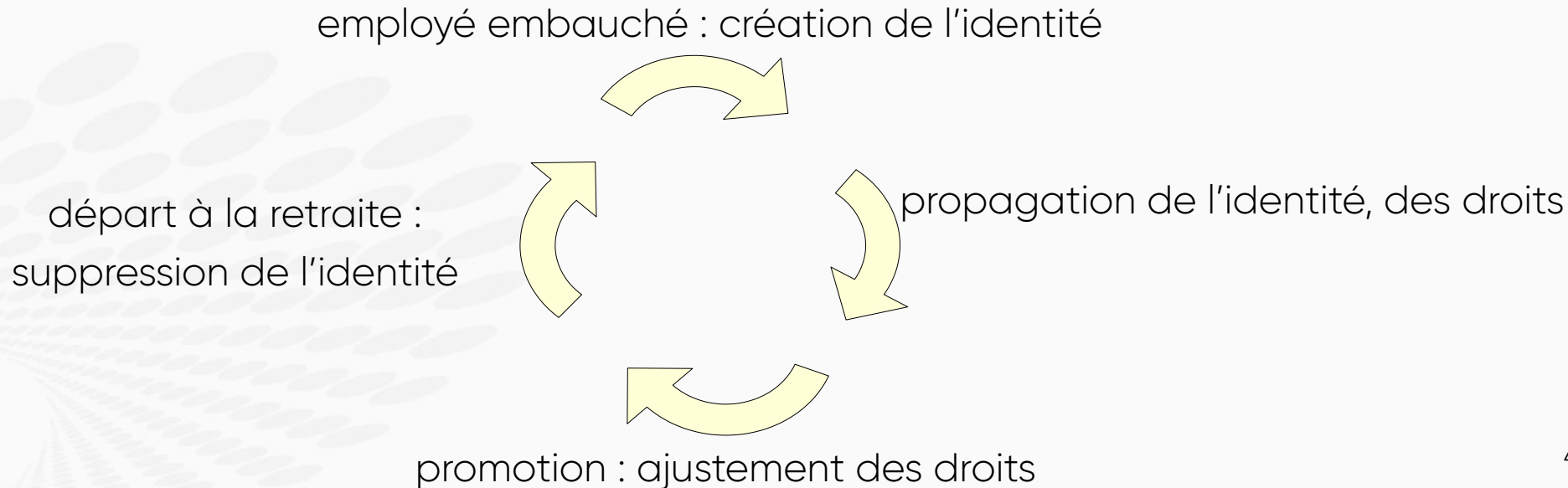
Présentation des nouveautés de LSC 2.2




Principes de gestion d'identité

Principes de gestion d'identité

- gestion du cycle de vie
- diffusion de l'identité au sein du SI et au-delà
- authentification
- autorisation

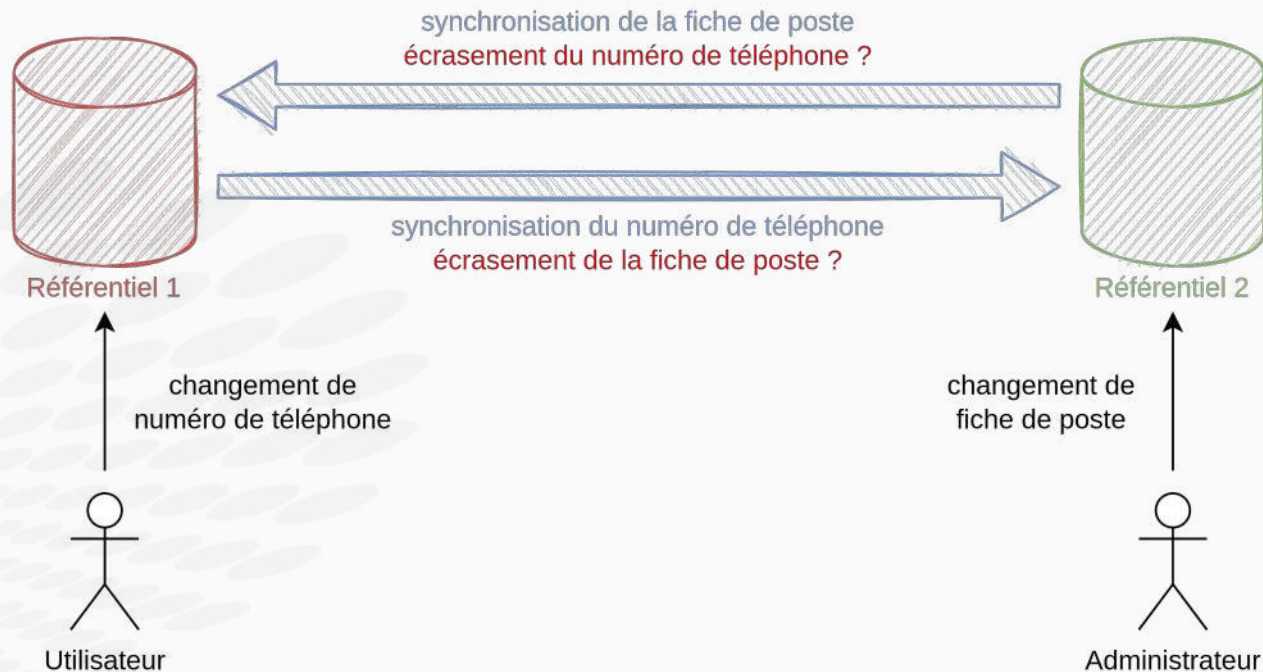




Stratégies pour maintenir ses données à jour

Stratégies pour maintenir ses données à jour

- Référentiel unique
- Référentiels multiples avec synchronisation unidirectionnelle
- Référentiels multiples avec synchronisation bidirectionnelle
 - écrasement : la dernière synchronisation « gagne » !





Présentation de LSC

Présentation de LSC

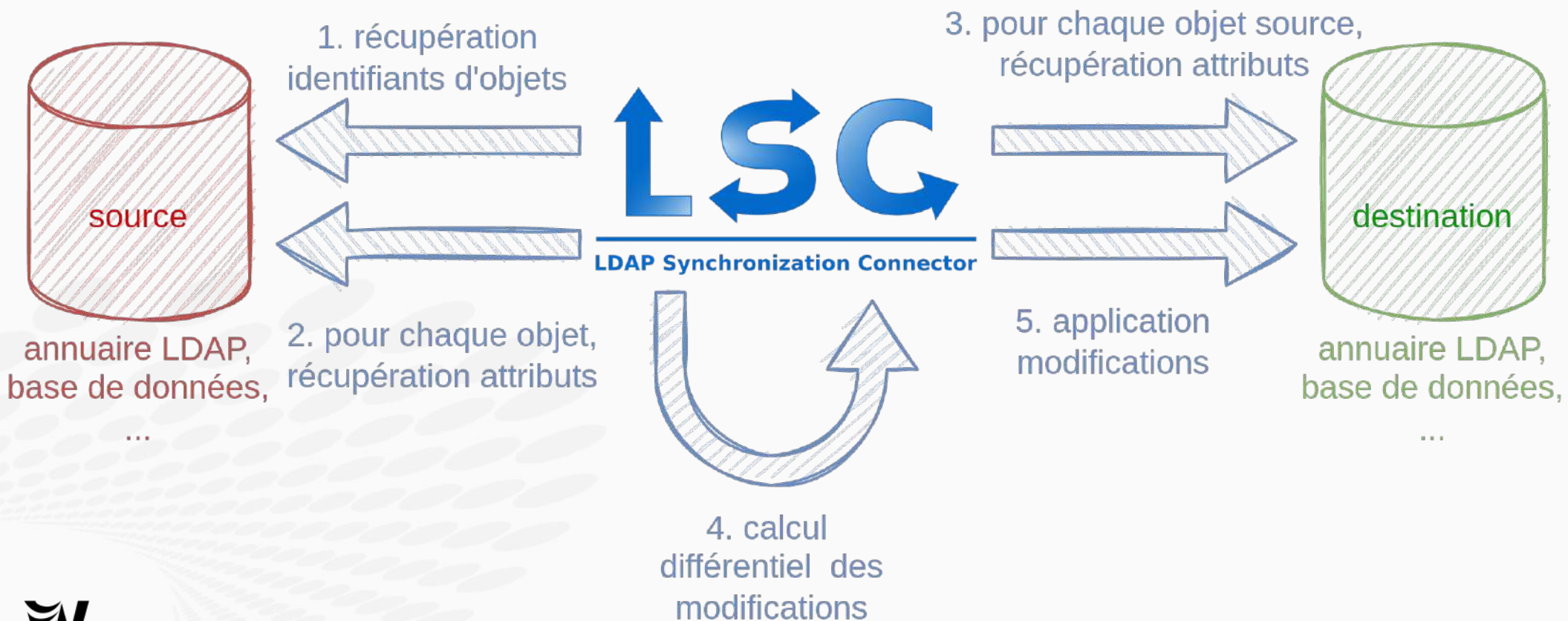
- **LDAP Synchronization Connector**
- lancé en 2008
- outil en ligne de commande
- développé en Java
- très grande modularité :
 - connecteurs BdD et LDAP (dont AD)
 - API REST
 - extensible avec système de plugins : executable, graphAPI,...



Architecture fonctionnelle



Architecture technique



Présentation

- Interface en ligne de commande
- tâches de nettoyage et d'ajout+modification séparées
- option de dry-run
- logs ldif ou csv
- ligne de statut final

```
Fichier  Édition  Affichage  Signets  Modules externes  Configuration  Aide
janv. 18 16:53:30 - INFO - Starting sync for MySyncTask
janv. 18 16:53:31 - INFO - # Adding new object mail=luke@starwars.com,ou=Sample,dc=lsc-project,dc=org for MySyncTask
janv. 18 16:53:31 - INFO - # Adding new object mail=darth@starwars.com,ou=Sample,dc=lsc-project,dc=org for MySyncTask
# Wed Jan 18 16:53:31 CET 2023
dn: mail=darth@starwars.com,ou=Sample,dc=lsc-project,dc=org
changetype: add
uid: dvader
userPassword: changethis
mail: darth@starwars.com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Darth Vader
sn: Vader

# Wed Jan 18 16:53:31 CET 2023
dn: mail=luke@starwars.com,ou=Sample,dc=lsc-project,dc=org
changetype: add
uid: lskywalker
userPassword: changethis
mail: luke@starwars.com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Luke Skywalker
sn: Skywalker

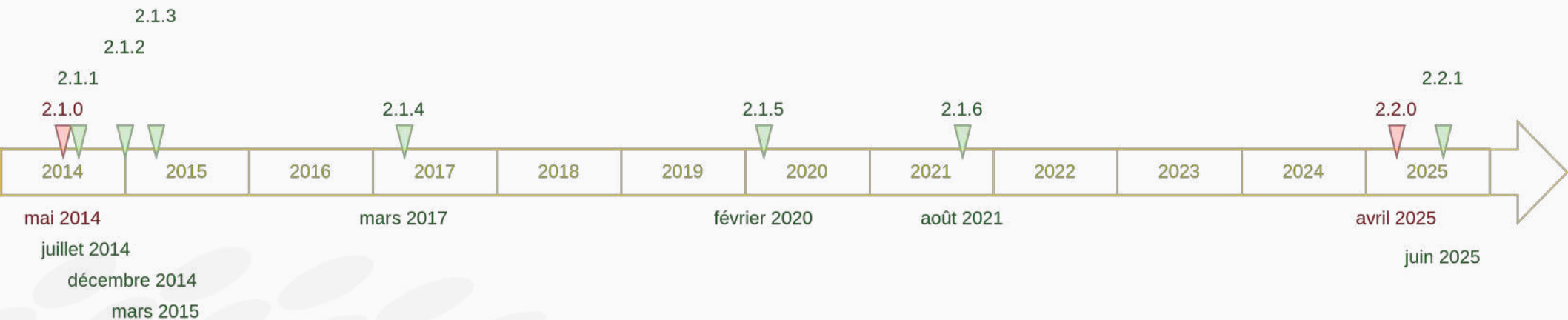
janv. 18 16:53:31 - INFO - # Adding new object mail=leia@starwars.com,ou=Sample,dc=lsc-project,dc=org for MySyncTask
# Wed Jan 18 16:53:31 CET 2023
dn: mail=leia@starwars.com,ou=Sample,dc=lsc-project,dc=org
changetype: add
uid: lorgana
userPassword: changethis
mail: leia@starwars.com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: Leia Organa
sn: Organa

janv. 18 16:53:31 - INFO - All entries: 3, to modify entries: 3, successfully modified entries: 3, errors: 0
janv. 18 16:53:31 - INFO - Starting clean for MySyncTask
janv. 18 16:53:31 - INFO - All entries: 3, to modify entries: 0, successfully modified entries: 0, errors: 0
clement@ader-worteks:~/Téléchargements/lsc-2.1.6/sample/hsqldb$
```



Présentation des nouveautés de LSC 2.2

LSC 2.2



- précédente version : la 2.1, apparue 10 ans auparavant
- préalable : montée de version de java et des dépendances de LSC

LSC 2.2

- **Principales nouveautés de la version 2.2 :**
 - placeholders dans la configuration
 - hooks
 - transformation de pivôts
 - support de Java 21
 - intégration de GraalVM comme moteur js par défaut
 - adaptation des tests unitaires pour utiliser l'API Apache Directory



LSC 2.2

- **Placeholders dans la configuration**
 - permet la variabilisation des secrets, des environnements,...

/etc/lsc/lsc.xml

...

```
<ldapConnection id="${LDAP_CONNECTION_ID}">
  <name>${LDAP_CONNECTION_NAME}</name>
  <url>ldap://${LDAP_HOST}:${LDAP_PORT}/dc=lsc,dc=org</url>
  <username>${LDAP_USERNAME}</username>
  <password>${LDAP_PASSWORD}</password>
```

...



LSC 2.2

- **Hooks**
 - déclenchement d'actions via l'appel de scripts externes
 - activable indépendamment pour les actions de :
 - création d'entrée
 - modification
 - suppression
 - renommage / déplacement
 - le DN et le type d'opération sont passés en argument
 - l'entrée au format Idif ou json est passée sur l'entrée standard du script (STDIN)



LSC 2.2

- **Transformation de pivots**

- pivot = attribut identifiant l'entrée de façon unique en src ou en dst
- quand ils diffèrent : mapping simple. sAMAccountName → uid
- avec LSC 2.2, introduction de règles de transformation de pivot

```
<pivotTransformation>
  <transformation fromAttribute="uid" toAttribute="name"><![CDATA[
    var result = value.replace(/^prefix:/, "");
    result;
  ]]></transformation>
  <transformation fromAttribute="name" toAttribute="uid"><![CDATA[
    var result = "prefix:" + value;
    result;
  ]]></transformation>
</pivotTransformation>
```



LSC 2.2

- **Support de Java 21**
 - LSC 2.1 supportait uniquement Java 8
 - paquets LSC 2.2 : Debian 11, 12, 13, et RHEL 8, 9 (10 à venir)
 - paquets LSC 2.2 supportent uniquement Java 21
 - Java 21 disponible nativement à partir de RHEL 8 et Debian 13
 - sinon, installable via <https://adoptium.net/>
 - LSC 2.2 compatible Java 17, mais recompilation nécessaire
 - toutes les dépendances de LSC ont été mises à jour



LSC 2.2

- **GraalVM comme moteur js par défaut**
 - Le moteur JS permet l'évaluation de règles de construction avancées d'attribut
 - GraalVM a beaucoup d'adhérence à la version de Java

| Version de Java | Moteur JS disponible |
|-----------------|--|
| Java 8 | Jscript evaluator (js), RhinoJS (rjs), Groovy (gr) |
| Java 11 | Jscript evaluator (js), RhinoJS (rjs) |
| Java 17 | RhinoJS |
| Java 21 | RhinoJS |

LSC 2.2

- **GraalVM comme moteur js par défaut**
 - Dans LSC 2.2, utilisation par priorité décroissante de :
 - GraalJS,
 - Jscript evaluator (js),
 - RhinoJS (rjs)
 - Possible de forcer un moteur en préfixant la règle par l'acronyme

```
<string>
  gjs:
    var givenName = srcBean.getDatasetFirstValueById("givenName");
    var sn = srcBean.getDatasetFirstValueById("sn");
    givenName + " " + sn
</string>
```



LSC 2.2

- **API Apache Directory**
 - Auparavant : lancement du serveur d'annuaire OpenDJ pour chaque test unitaire → **long** !
 - Désormais, passage par l'API Apache Directory
 - Annotations pour initialiser les données pour chaque test





www.worteks.com

✉ info@worteks.com

☎ +33 1 84 20 86 47

🌐 worteks.com

🌐 [in worteks](https://www.linkedin.com/company/worteks)

**Merci pour votre
attention**