RENFORCEZ LA SÉCURITÉ DE VOS DONNÉES SAS® GRÂCE AUX METADATA-BOUND LIBRARIES

Caractéristiques :

Catégories : OMA
OS : Windows, Unix, z/OS
Version : SAS® 9.3 TS1M2 et 9.4 M0
Vérifié en septembre 2013

A partir de SAS 9.3 TS1M2, un nouveau type de bibliothèque fait son apparition, et promet de bouleverser notre approche de la sécurité : les bibliothèques liées aux métadonnées (ou « metadata-bound libraries »). Lorsqu'une bibliothèque est liée aux métadonnées, alors l'utilisateur ne pourra accéder à ses tables qu'à condition d'avoir les droits suffisants physiquement mais aussi dans le référentiel, et cela qu'il utilise un outil client ou une simple instruction LIBNAME.
Cet article vous présente ce concept innovant et comment le mettre en œuvre.

Table des matières

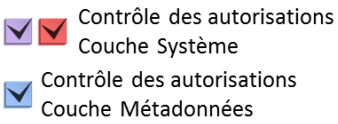
1. Présentation 2
   a. Concept 2
   b. Avantages 3
   c. Limites 3
2. Bibliothèque traditionnelle versus bibliothèque sécurisée 4
3. Le mécanisme de liaison 4
4. Permissions 6
5. Mise en oeuvre 7
   a. Etape 1 : Créer un répertoire dédié dans les dossiers partagés 7
   b. Etape 2 : Lier le répertoire physique aux métadonnées 8
   c. La procédure AUTHLIB 13
   d. Assigner une bibliothèque 14
6. Illustration 16
   a. Une bibliothèque traditionnelle 16
   b. Une bibliothèque sécurisée 17
7. Les erreurs les plus courantes 18
8. Liens utiles 19
9. En cas de problème 19
10. Conclusion 19

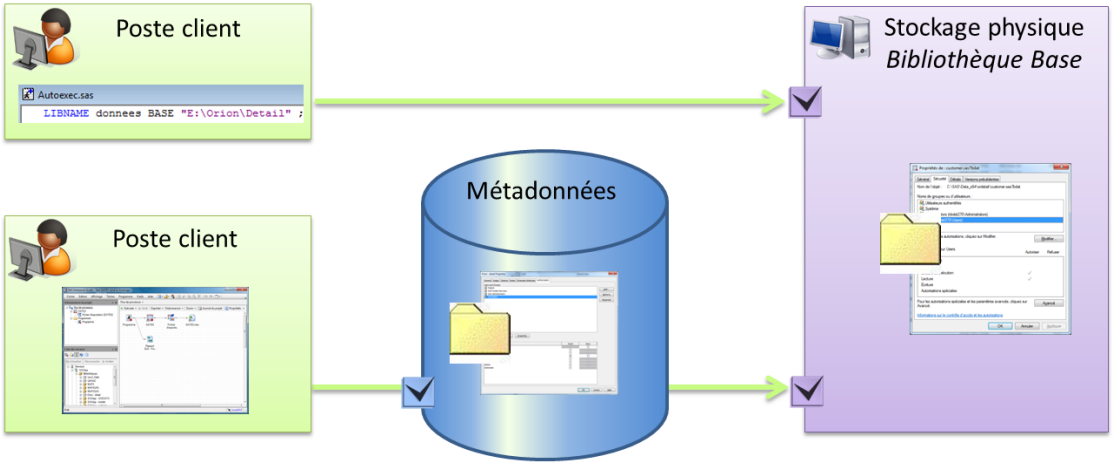
1. Présentation

a. Concept

La sécurité des données dans l'architecture OMA (« Open Metadata Architecture ») repose à la fois sur les droits affectés dans le référentiel et sur les droits physiques. Les utilisateurs sont déclarés dans le référentiel de métadonnées, et l'administrateur définit pour chacun (par personne ou par groupe) leurs droits d'accès aux objets (bibliothèques, tables, cubes, rapports, serveurs etc). Il accorde ou refuse notamment le droit de créer, de lire, de supprimer ces objets.
Cette sécurité n'est toutefois appliquée que lorsque l'utilisateur se connecte au serveur de métadonnées pour accéder aux données, via une bibliothèque de type META ou via un client tel que SAS© Enterprise Guide par exemple. S'il a les droits système suffisants, il peut également accéder aux données en déclarant une bibliothèque de type BASE, indépendamment des autorisations déclarées dans le référentiel (et qui ne seront donc pas appliquées).

Le schéma ci-dessous illustre cela.
Si un utilisateur accède aux données déclarées dans le référentiel en assignant une bibliothèque META ou via un client, alors les permissions META sont d'abord vérifiées, puis ce sont les autorisations système.
Il peut aussi accéder à la même table SAS en assignant une bibliothèque sur le répertoire directement. Dans ce cas, seuls les droits physiques sont contrôlés.





A partir de SAS 9.3 M2, un nouveau type de bibliothèque est possible. Les bibliothèques liées aux métadonnées (« Metadata-Bound Libraries » ou « MBL ») restreignent l'accès aux tables SAS aux utilisateurs identifiés sur le serveur de métadonnées, et ayant les droits physiques suffisants. Ces 2 conditions doivent être remplies pour lire, créer ou modifier le contenu de ces bibliothèques.

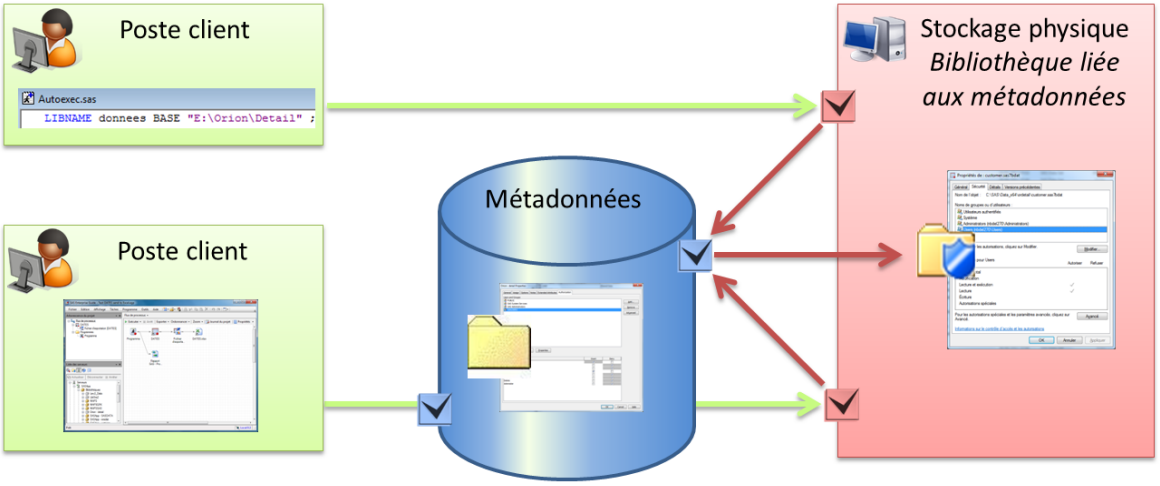
Si l'utilisateur déclare une bibliothèque BASE, alors :

1. Le droit de lecture est vérifié physiquement ;
2. Puis SAS contrôle dans le référentiel l'identité de l'utilisateur, puis ses droits sur la bibliothèque sécurisée.

S'il est inconnu ou n'a pas les permissions suffisantes, alors la table est inaccessible, même si les droits physiques lui sont favorables. S'il est connu, qu'il a les permissions adéquates sur les bibliothèques traditionnelles et sécurisées, et que le droit physique de lecture est accordé, alors il accède à la table.

Si l'utilisateur déclare une bibliothèque META, alors :

1. SAS contrôle son identité dans le référentiel, puis vérifie ses autorisations sur la bibliothèque traditionnelle (telles que déclarées dans le « Gestionnaire de bibliothèques ») ;
2. Puis SAS vérifie que le droit de lecture est accordé physiquement ;
3. Enfin, les droits sur la bibliothèque sécurisée sont contrôlés dans le référentiel.



Les tables contenues dans le répertoire sont appelées « tables sécurisées ». Leur en-tête (ou « header ») spécifie qu'elles sont liées aux métadonnées. De cette manière, si une table sécurisée venait à être déplacée dans un autre répertoire, tout utilisateur y accédant devrait être authentifié sur le référentiel, même si l'assignation de la bibliothèque ne l'y a pas déjà contraint.

b. Avantages

- L'avantage principal est le renforcement de la sécurité, car la même sécurité est appliquée quelle que soit l'application utilisée pour accéder aux données.
- La sécurité dépend totalement des métadonnées SAS et non plus du système.

c. Limites

- La création d'une bibliothèque liée aux métadonnées se fait :
  - par code et non par une interface utilisateur graphique ;
  - en sus de la définition d'une bibliothèque « traditionnelle » si l'on souhaite y accéder par les outils clients de la plateforme (Enterprise Guide, Web Report Studio…) ;
  - dans un dossier (ou « Folder ») défini (/System/Secured Libraries) qui n'est pas personnalisable.
- Seules les tables et vues SAS, créées à partir de la version SAS 9.3 TS1M2, sont éligibles.
- Ces bibliothèques n'acceptent pas les permissions au niveau des colonnes
- Les commandes systèmes (copier, supprimer, renommer…) sont toujours possibles.

2. Bibliothèque traditionnelle versus bibliothèque sécurisée

Désormais, le référentiel peut contenir 2 types de bibliothèques, dont voici les différences.

	Bibliothèque traditionnelle	Bibliothèque sécurisée
Moteur	SAS ou SGBD (Oracle, Teradata…)	SAS
Membres	Une sélection de tables et vues	Une sélection de tables et vues (« tout » étant le défaut).
Création / Gestion	SAS Management Console > Onglet « Plug-in » > Gestionnaire de bibliothèques de données 	SAS Management Console > Onglet « Folder » > /System/Secured Libraries/ Nécessite également la procédure AUTHLIB.
Type d'objet meta	SASLibrary Name / Type / Object ID Pegase - Detail / SASLibrary / A58XNXJR.AZ000005	SecuredLibrary Name / Type / Object ID Orion - Detail (MBL) / SecuredLibrary / A58XNXJR.BW000001
Accès	Depuis un outil client ou un libname META	Depuis un outil client, un libname META ou BASE
Contenu du dossier physique		SAS a ajouté un dossier .sassl contenant un fichier dont le nom est « loc ». Les tables de ce répertoire ont des en-têtes modifiées spécifiant qu'elles sont sécurisées.

3. Le mécanisme de liaison

La liaison entre un répertoire physique et une bibliothèque sécurisée repose sur la concordance :

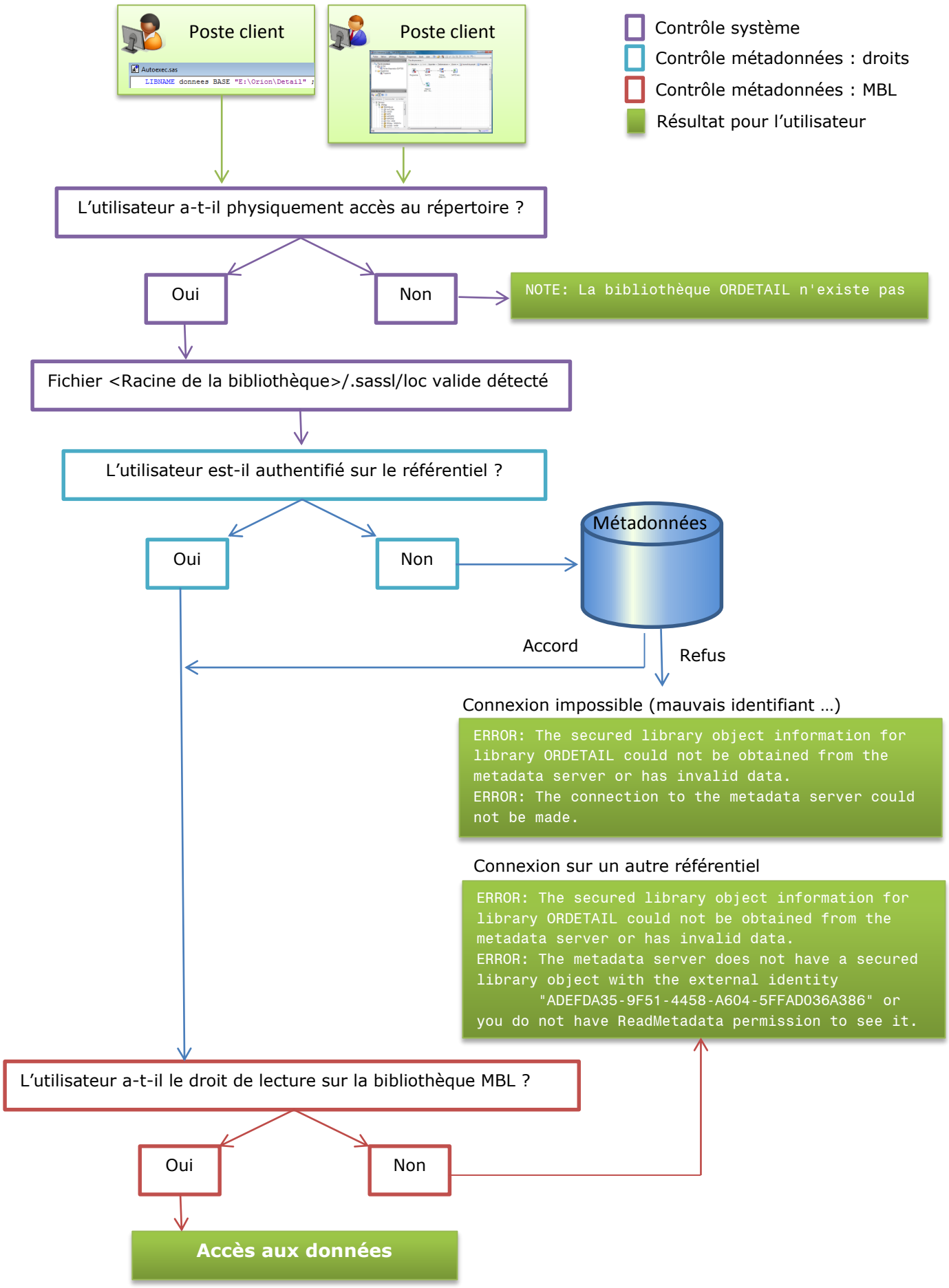
- du dossier référencé dans le fichier <Racine de la bibliothèque>\.sassl\loc
- du dossier existant dans les bibliothèques sécurisées du référentiel.

Ce lien est indépendant de l'existence de la bibliothèque traditionnelle dans le référentiel.

Le fichier loc ne doit en aucun cas être modifié manuellement.

Il en est de même pour les tables sécurisées : les informations de sécurité présentes dans l'en-tête de la table doivent concorder avec le contenu du référentiel.

Le schéma suivant montre pas-à-pas le cheminement réalisé lorsqu'une instruction LIBNAME est soumise depuis SAS Foundation ou qu'un utilisateur accède à une bibliothèque META référençant un répertoire sécurisé.


Poste client
Autoexec.sas
LIBNAME donnees BASE "E:\Orion\Detail" ;
Poste client
Contrôle système
Contrôle métadonnées : droits
Contrôle métadonnées : MBL
Résultat pour l'utilisateur
L'utilisateur a-t-il physiquement accès au répertoire ?
Oui
Non
NOTE: La bibliothèque ORDETAIL n'existe pas
Fichier <Racine de la bibliothèque>/.sassl/loc valide détecté
L'utilisateur est-il authentifié sur le référentiel ?
Oui
Non
Métadonnées
Accord
Refus
Connexion impossible (mauvais identifiant ...)
ERROR: The secured library object information for library ORDETAIL could not be obtained from the metadata server or has invalid data.
ERROR: The connection to the metadata server could not be made.
Connexion sur un autre référentiel
ERROR: The secured library object information for library ORDETAIL could not be obtained from the metadata server or has invalid data.
ERROR: The metadata server does not have a secured library object with the external identity "ADEFDA35-9F51-4458-A604-5FFAD036A386" or you do not have ReadMetadata permission to see it.
L'utilisateur a-t-il le droit de lecture sur la bibliothèque MBL ?
Oui
Non
Accès aux données

4. Permissions

Outre l'accès aux tables, les bibliothèques liées aux métadonnées permettent d'accorder des permissions fines sur chaque bibliothèque et table. L'administrateur peut par exemple indiquer qu'un utilisateur n'a pas le droit de créer des tables, mais que lui seul a le droit de mettre à jour les données.

Pour une bibliothèque sécurisée, les permissions nécessaires sont :

- Pour créer une bibliothèque liée aux métadonnées : Write Member Metadata sur le dossier Secured Libraries
- Pour supprimer la liaison entre un répertoire et les métadonnées : Write Member Metadata sur le dossier Secured Libraries, et Write Member sur la bibliothèque
- Pour ajouter des tables sécurisées dans une bibliothèque : Create Table sur la bibliothèque

Par défaut, seul les membres du groupe administrateurs ont le droit WMM sur les bibliothèques sécurisées. Par défaut, ce groupe ne contient qu'un membre : l'administrateur, qui peut être un compte interne (sasadm@saspw). Lors de la création d'une MBL, si sasadm pourra mettre à jour les métadonnées, en revanche il aura besoin d'un compte système ayant les droits suffisants pour créer le dossier .sassl et pour mettre à jour les en-têtes des tables. Il faut donc bien prévoir :

- Un compte ayant la permission WMM côté métadonnées
- Un compte système ayant le droit de modifier les tables. De plus, il devra être en mesure de démarrer une session SAS : soit pour lancer la procédure AUTHLIB manuellement, soit pour lancer un workspace server avec l'assistant de création de bibliothèque.

Pour une table sécurisée, les permissions disponibles sont :

- Delete : supprimer des observations
- Insert : ajouter des observations
- Update : mettre à jour des observations (nécessite également Select)
- Select : consulter les données
- Create table : créer une nouvelle table, renommer une table
- Drop Table : supprimer une table, copier une table sécurisée vers une bibliothèque traditionnelle par programme (nécessite également Select)
- Alter Table : renommer des variables, modifier leurs libellés, remplacer une table

Ces différentes permissions peuvent également être définies au niveau de la bibliothèque sécurisée, ainsi elle s'applique sur l'ensemble des tables.

5. Mise en oeuvre

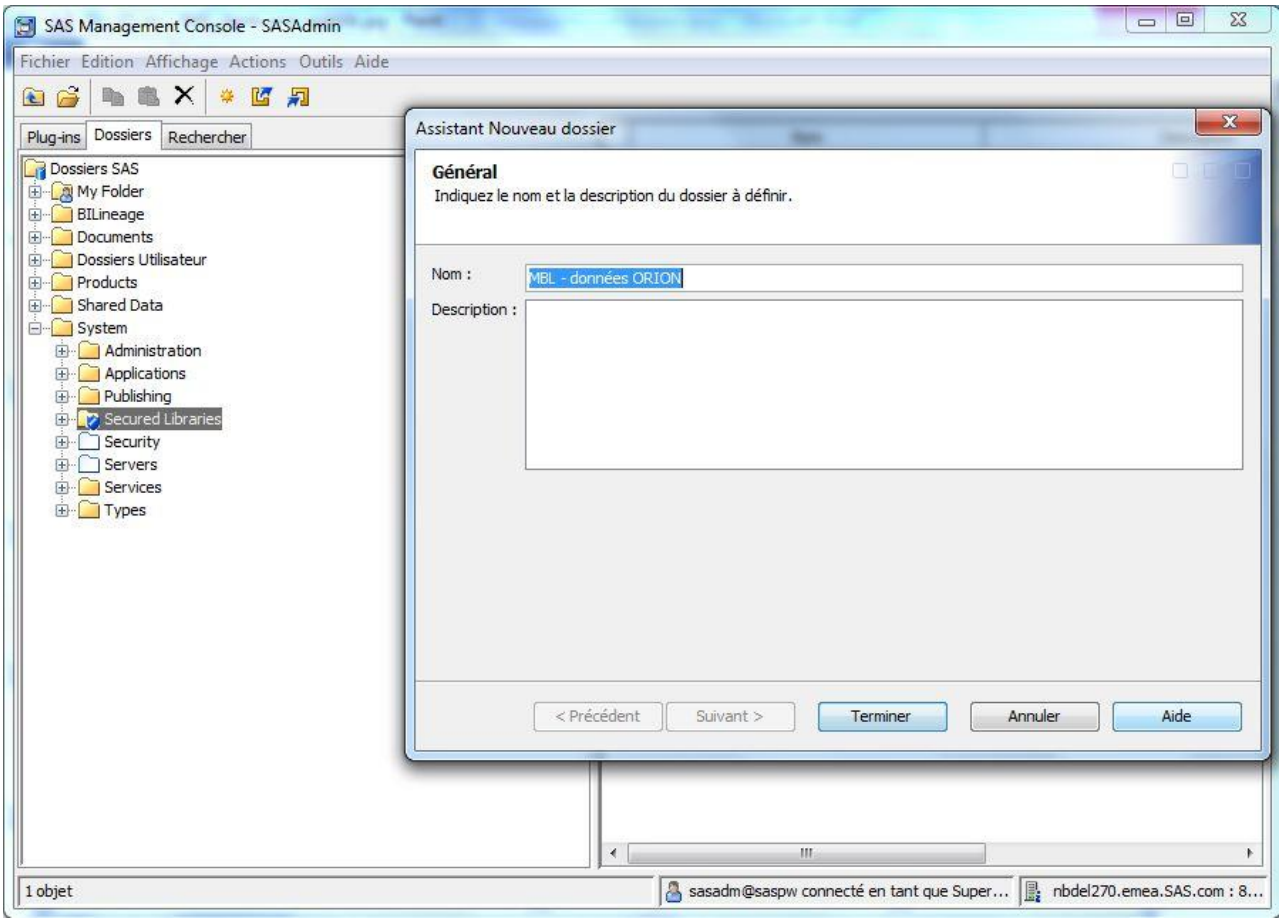
Elle se fait en deux étapes, la première pouvant être réalisée une seule et unique fois selon le cahier des charges :

1. Créer un dossier dédié dans le dossier System ;
2. Lier le répertoire physique à un dossier méta.

a. Etape 1 : Créer un répertoire dédié dans les dossiers partagés

Les objets du référentiel sont stockés dans les « dossiers » (ou « Folders »). Les bibliothèques liées aux métadonnées doivent être placées dans un dossier sous /System/Secured Libraries/.

1. Ouvrir SAS Management Console, et s'identifier. Par défaut, seuls les membres du groupe SAS Administrators et l'utilisateur non-restreint ont les permissions nécessaires sur le dossier « Secured Libaries », à savoir ReadMetadata et WriteMemberMetadata.
2. Aller dans l'onglet Dossiers, puis déplier System.
3. Faire un clic-droit sur « Secured Libaries », choisir Nouveau, puis Dossier
4. Donner un nom à ce dossier, puis cliquer sur Terminer
5. Par défaut, seul le groupe administrateur peut ajouter des tables. Si vous avez besoin de modifier les permissions, faire un clic-droit sur le nouveau dossier, et définir si nécessaire les permissions dans l'onglet Droits (cf. paragraphe précédent).



Ce dossier pourra contenir une ou plusieurs bibliothèques liées aux métadonnées, ainsi que leurs tables. Il ne contiendra pas de bibliothèque ou de table traditionnelle.

b. Etape 2 : Lier le répertoire physique aux métadonnées

Cette étape peut se réaliser :
- Soit depuis SAS Foundation avec la procédure AUTHLIB
- Soit depuis SAS Management Console à partir de SAS 9.4

Cette étape se fait depuis une session SAS. Elle va provoquer :
- la création d'un sous-répertoire dans le répertoire physique de la bibliothèque, qui contiendra un fichier définissant la liaison unissant les données et le référentiel (*bibliothèque*/.sassl/loc);
- l'ajout d'une information dans l'en-tête (ou « header ») de chaque table du répertoire, spécifiant qu'il s'agit désormais d'une table sécurisée.

i. En code SAS avec la procédure AUTHLIB

L'utilisateur, ayant le droit d'accéder à la bibliothèque en question, démarre une session SAS.

Le programme se découpe en 3 phases :
1. Assigner la bibliothèque, en spécifiant un libref, et le répertoire que l'on veut lier aux métadonnées
2. Spécifier les options définissant la connexion au référentiel, avec un utilisateur du groupe SAS Administrators, l'utilisateur non-restreint, ou encore un compte ayant la permission WMM sur le sous-dossier créé à l'étape précédente.
3. Soumettre la PROC AUTHLIB :
   a. LIBRARY : libref de la bibliothèque déclarée dans la session SAS en cours (celui donnée en phase 1)
   b. SECUREDFOLDER : nom du sous-dossier créé dans les dossiers partagés (cf. étape 1 « Créer un répertoire dédié dans les dossiers partagés »)
   c. SECUREDLIBRARY : nom de la bibliothèque MBL à créer
   d. PW : le mot de passe, qui devra être donné lorsque pour modifier la bibliothèque / la table sécurisée

```
LIBNAME ORDETAIL "E:\Orion\Detail" ;

OPTIONS metaserver=localhost
        metaport=8561
        metaprotocol=bridge
        metauser='sasadm@saspw'
        metapass=sasadm
        metarepository='Foundation' ;

PROC AUTHLIB library=ORDETAIL;
 create
   securedfolder='/System/Secured Libraries/MBL - données ORION'
   securedlibrary='Orion - Detail (MBL)'
   pw=Pwd123;
run; quit ;
```

Le journal liste les actions menées (mise à jour de la bibliothèque puis de chaque table et vue) et le statut de ces actions (succès ou échec). Extrait :

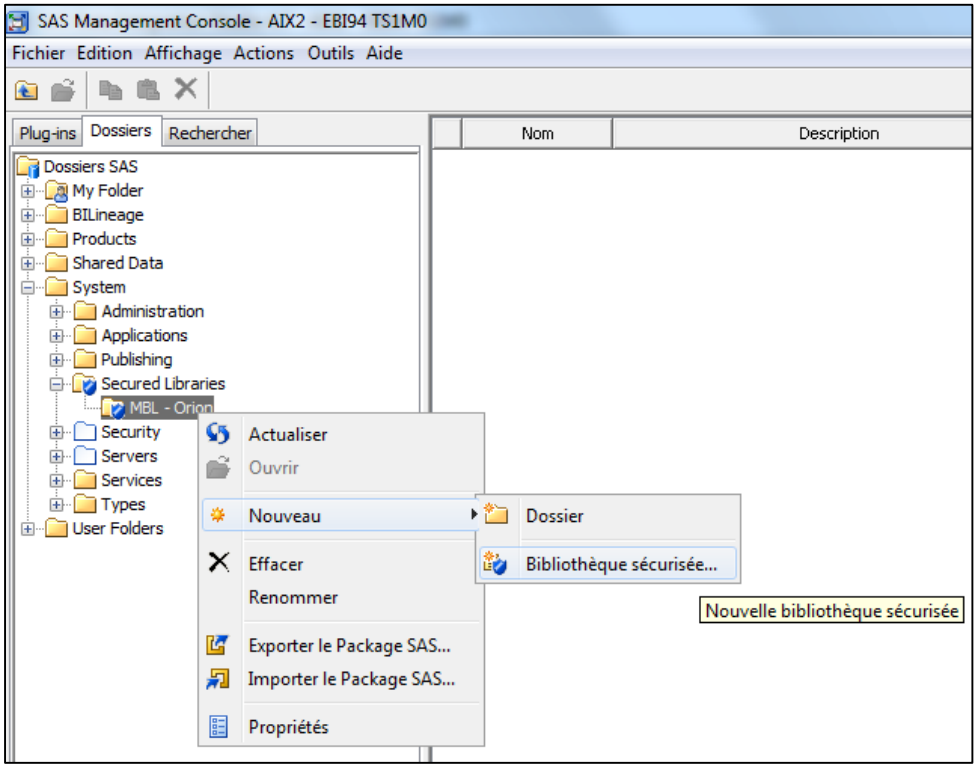
```
NOTE: Successfully created a secured library object for the physical library ORDETAIL and
recorded its location as:
           SecuredFolder:      /System/Secured Libraries/MBL - données ORION
           SecuredLibrary:     Orion - Detail (MBL)
           SecuredLibraryGUID: ADEFDA35-9F51-4458-A604-5FFAD036A386
NOTE: Successfully added new secured table object "CONTINENT.DATA" to the secured library
object at path "/System/Secured
      Libraries/MBL - données ORION/Orion - Detail (MBL)" for data set
ORDETAIL.CONTINENT.DATA.
```

ii. *En utilisant l'interface graphique*

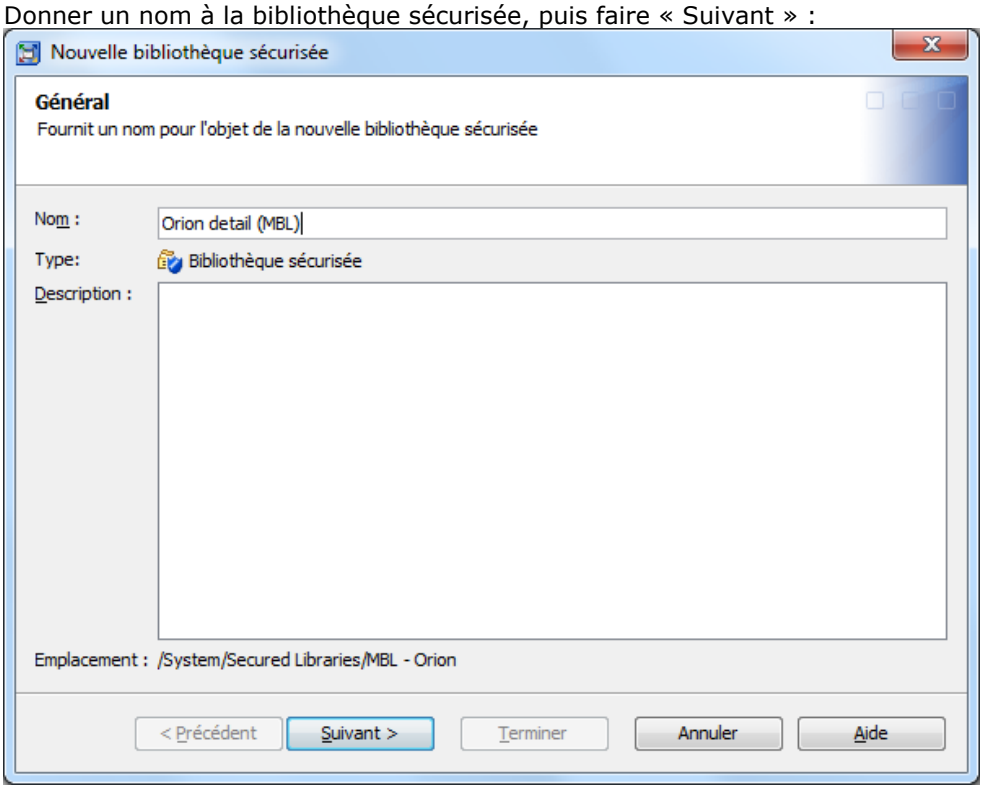
A partir de SAS 9.4 TS1M0, l'utilisateur peut créer la liaison depuis SAS Management Console. Il doit :

- Soit être membre du groupe SAS Administrators
- Soit être non-restreint
- Soit avoir la permission WMM sur le sous-dossier créé à l'étape précédente.

Faire un clic droit sur le dossier de données sécurisées :



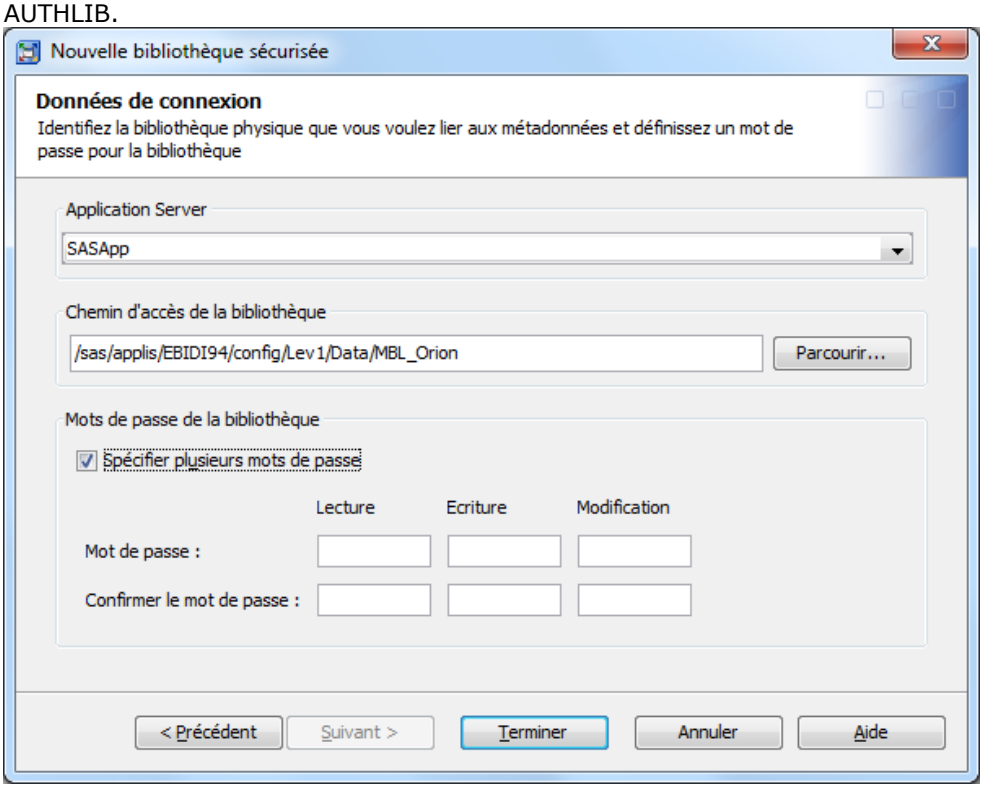
Donner un nom à la bibliothèque sécurisée, puis faire « Suivant » :



Renseigner les données de connexion :

- Le serveur d'application qui sera utilisé pour lancer une session workspace server
- Le chemin du répertoire où sont les tables à sécuriser
- Le mot de passe qui peut être unique (option PW) ou bien différent pour la lecture (READ), l'écriture (WRITE) et la modification (ALTER).

Ce sont les informations nécessaires au lancement d'une session SAS, qui exécutera la procédure AUTHLIB.

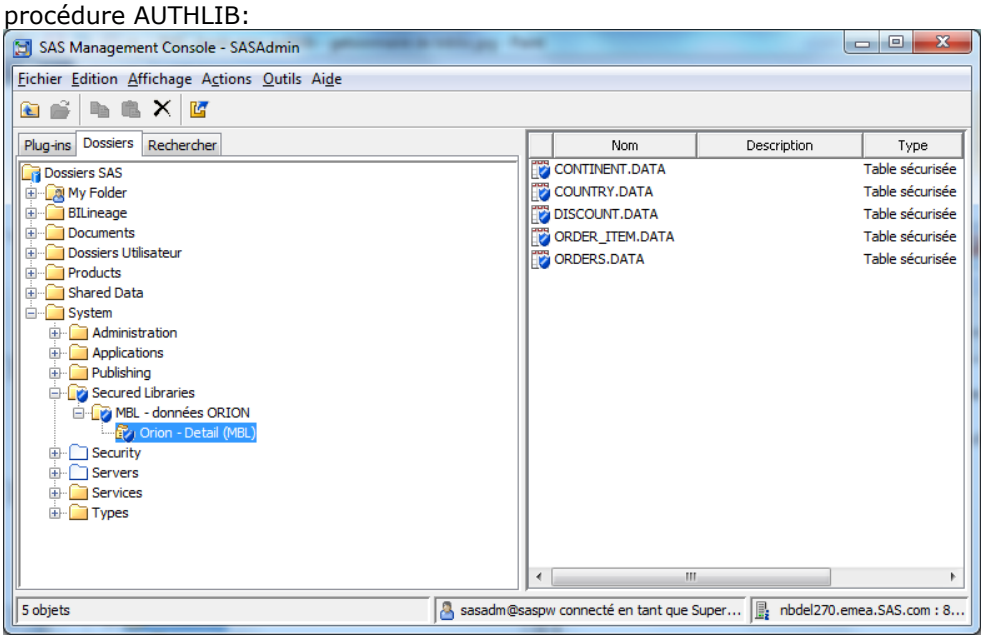


Cliquer sur « Terminer ».

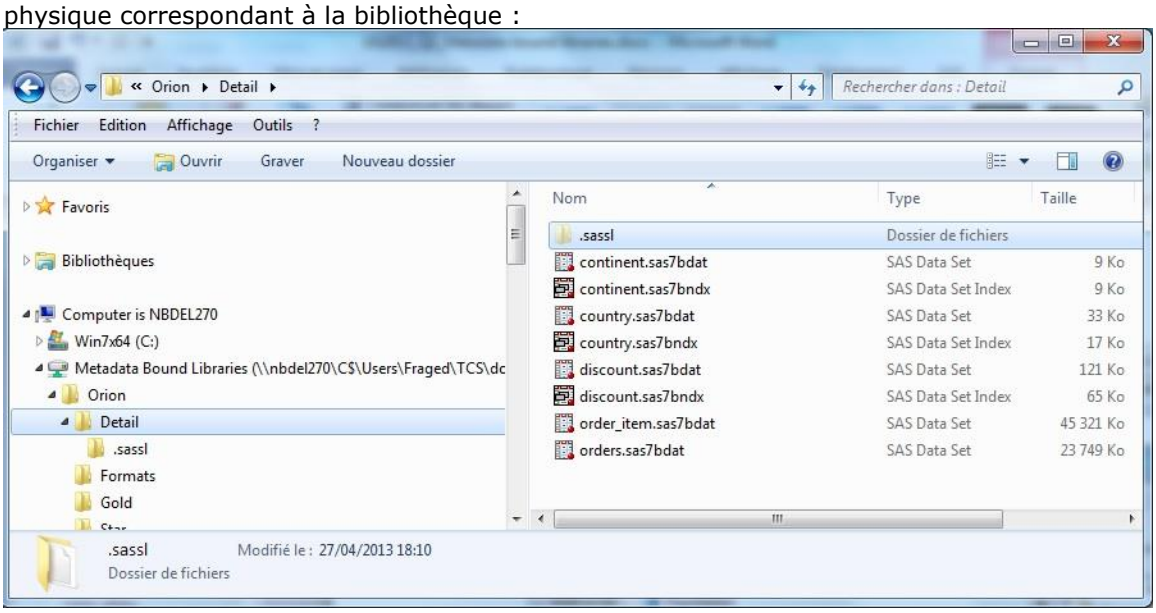
Vous serez alors prompté pour vous identifier au serveur d'application. Si l'identifiant et le mot de passe sont valides, un workspace server démarre et exécute la procédure AUTHLIB.

iii. Résultat de la liaison

Toutes les tables contenues dans le répertoire ont été modifiées au niveau de leurs en-têtes, et elles sont enregistrées dans le référentiel comme étant sécurisées, sous la bibliothèque ajoutée par la procédure AUTHLIB:



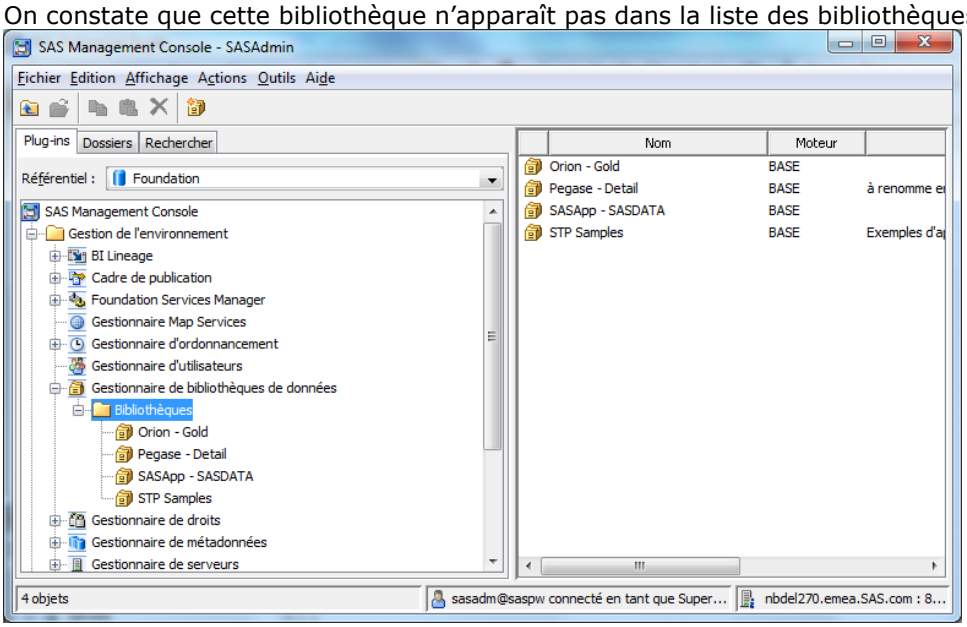
Physiquement, le répertoire caché « .sassl », contenant le fichier loc, a été ajouté dans le répertoire physique correspondant à la bibliothèque :



Exemple sur unix :

```
bash-3.2$ ls -al
80408 total
drwxrwxr-x    3 ebi94    staff          256 05 sep 16:53 .
drwxr-xr-x    3 ebi94    sas            256 05 sep 14:12 ..
-rwxrwxrwx    1 sasdemo  staff        40960 05 sep 16:53 country.sas7bdat
-rwxrwxrwx    1 sasdemo  staff        40960 05 sep 16:53 country.sas7bndx
-rwxrwxrwx    1 sasdemo  staff     16777216 05 sep 16:53 customer.sas7bdat
-rwxrwxrwx    1 sasdemo  staff     24322048 05 sep 16:53 orders.sas7bdat
drwxr-xr-x    2 ebi94    staff          256 05 sep 16:53 .sassl
```

On constate que cette bibliothèque n'apparaît pas dans la liste des bibliothèques du référentiel :



Les bibliothèques liées aux métadonnées ne sont pas automatiquement mises à disposition des utilisateurs de la plateforme. Si l'on souhaite intégrer cette bibliothèque dans le référentiel, alors il faut l'ajouter de la même façon que toute autre bibliothèque, via le « Gestionnaire de bibliothèque ». Cela illustre également ce principe : on peut lier aux métadonnées des répertoires qui ne sont pas définis dans le référentiel en tant que bibliothèque. L'administrateur des données souhaite s'assurer que les accès par bibliothèque BASE ne soient faits que par un groupe de personnes, sans pour autant mettre ces données à disposition des utilisateurs de la plateforme.

c. La procédure AUTHLIB

La procédure AUTHLIB est l'outil de gestion des bibliothèques et tables sécurisées. Elle est détaillée dans la documentation Base SAS® 9.4 Procedures Guide. Elle permet, pour une bibliothèque donnée :

- la création du lien entre la bibliothèque physique et le référentiel (CREATE)
- la modification (MODIFY) du mot de passe
- la suppression de la sécurité (REMOVE)
- la création d'un rapport (REPORT) indiquant la cohérence entre les définitions du référentiel et le répertoire physique

Exemples de rapports :

1er cas : le contenu du répertoire concorde avec les métadonnées. Le rapport liste les tables qu'il contient :

```
The OS library is properly registered to this SecuredLibrary. These data sets are
                    properly registered to SecuredTables in it.
SecuredLibrary Path: /System/Secured Libraries/MBL - données ORION/Orion - Detail
(MBL)
SecuredLibrary Guid: ADEFDA35-9F51-4458-A604-5FFAD036A386
Registered in OS Path: E:\Orion\Detail
Password Set: 0
```

Obs	MemberName	MemberType	SecuredTableName	SecuredTableGUID
1	CONTINENT	DATA	CONTINENT.DATA	0DBFD8B1-858B-42CB-8D90-2AEF0AE83644
2	COUNTRY	DATA	COUNTRY.DATA	B183C96F-1E44-4C18-A748-1A538BD2E6B5
3	DISCOUNT	DATA	DISCOUNT.DATA	4A1E75DA-67CD-41D1-92C4-289211854BCB
4	ORDERS	DATA	ORDERS.DATA	4D08B02D-D6E4-4680-B0F7-03DA073E38E9
5	ORDER_ITEM	DATA	ORDER_ITEM.DATA	04D131E8-DF8E-4393-A73B-DC3E145E0E6F

2ème cas : Le répertoire contient des tables qui ne sont pas sécurisées. Le rapport liste alors les différences :

```
The OS library is properly registered to this SecuredLibrary. These data sets have
                 no registered SecuredTable location information.
SecuredLibrary Path: /System/Secured Libraries/MBL - données ORION/Orion - Detail
(MBL)
SecuredLibrary Guid: ADEFDA35-9F51-4458-A604-5FFAD036A386
Registered in OS Path: E:\Orion\Detail
Password Set: 1
```

Obs	MemberName	MemberType	SecuredTableName	SecuredTableGUID
6	CUSTOMER_DIM	DATA		
7	GEOGRAPHY_DIM	DATA		
8	ORDER_FACT	DATA		
9	ORGANIZATION_DIM	DATA		

d. Assigner une bibliothèque

Depuis SAS Foundation

Lorsque l'instruction LIBNAME est soumise depuis SAS Foundation, tout d'abord SAS constate la présence du répertoire .sassl. Il recherche alors les informations de connexion au serveur de métadonnées :

- 1er cas : elles ont été déclarées au préalable via les options usuelles metaserver, metaport etc
- 2ème cas : les options ne sont pas définies, alors une fenêtre « Metadata Server Configuration » demande à l'utilisateur de renseigner ces informations. Les champs apparaissent soit vides, soit avec un profil précédemment enregistré. Ils ne sont pas pré-remplis avec les informations propres au référentiel auquel est liée la bibliothèque.

Si l'authentification réussit, le journal rappelle le moteur, le chemin physique, le dossier de métadonnées et l'identifiant authentifié :

```
1    libname ORDETAIL "E:\Orion\Detail" ;
NOTE: Libref ORDETAIL was successfully assigned as follows:
      Engine:           V9
      Physical Name:    E:\Orion\Detail
      Secured Library:  /System/Secured Libraries/MBL - données ORION/Orion -
Detail (MBL)
      Authenticated ID: SASDEMO@NBDEL270 as Utilisateur de démonstration SAS
```

On notera que le mot de passe donné lors de la procédure AUTHLIB n'est pas demandé : ce mot de passe sert à l'administration et non à l'accès aux données.

Depuis un client

Depuis un client tel que SAS Enterprise Guide par exemple, un serveur d'application exécute les requêtes : l'utilisateur est donc authentifié sur le référentiel.

Il accède à des bibliothèques traditionnelles déclarées dans le référentiel. Si l'une d'entre elle référence le même répertoire qu'une bibliothèque sécurisée (présence physique du répertoire .sassl), alors seront vérifiés :

- les droits sur la bibliothèque traditionnelle,
- les droits physiques,
- les droits sur la bibliothèque sécurisée.

La liaison sécurisée est totalement transparente pour l'utilisateur dans la mesure où il est déjà authentifié.

Si l'utilisateur soumet une instruction LIBNAME dans une fenêtre « programme », c'est le même serveur d'application qui va l'exécuter : il est déjà authentifié. Ses droits sont contrôlés en fonction de cet identifiant de manière transparente également.

6. Illustration

Soit un environnement OMA contenant ces définitions :

- Un groupe d'utilisateurs « Ressources Humaines » dont les membres sont RH1 et RH2
- Un groupe d'utilisateurs « Data Managers » dont les membres sont DM1, DM2, DM3 et DM4

Il y a par ailleurs un utilisateur DM5 qui n'est pas déclaré dans le référentiel.

a. Une bibliothèque traditionnelle

Il s'agit ici d'illustrer le schéma ci-contre : si les droits physiques ne sont pas restreints, alors un utilisateur peut accéder aux tables SAS en dehors du référentiel.

Soit la bibliothèque « Orion – Détail », déclarée dans le référentiel. Le tableau ci-dessous montre les différentes combinaisons de droits physiques et de droits déclarés dans les métadonnées, et leurs conséquences pour l'utilisateur.

	SYSTEME	BIBLIOTHEQUE TRADITIONNELLE	
	Droit « lecture »	**Droits Meta : « Read Metadata » et « Read »**	**Comportement pour un utilisateur**

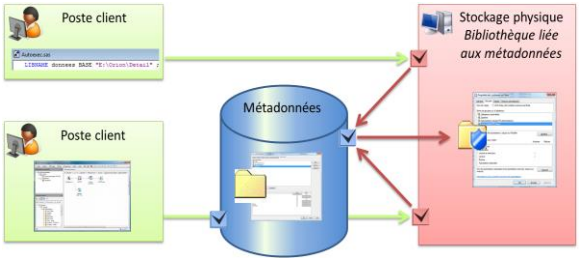
Groupe RH	Refuser	Accorder	L'utilisateur RH1 ne peut pas accéder aux données :
			- Ni par bibliothèque META :
			Bien que la bibliothèque soit assignée avec succès, les tables ne peuvent pas être ouvertes :
			`ERROR: L'utilisateur n'a pas le bon niveau d'autorisation pour la biblio. ORDETAIL.Ordetail.CAKE. ne peut être ouvert. Voulez-vous sélectionner un autre tableau à ouvrir ?`
			- Ni par bibliothèque BASE :
			`ERROR: L'utilisateur n'a pas le bon niveau d'autorisation pour la biblio. ORDETAIL`

Groupe DM	Accorder	Accorder	L'utilisateur DM1 peut accéder aux données : - par bibliothèque Meta - par bibliothèque Base
Utilisateur DM4	Accorder	Refuser	L'utilisateur DM4 - ne peut pas accéder aux données par bibliothèque Meta :

			ERROR: Aucun objet de métadonnées trouvé dans l'URI spécifiée. ERROR: Error in the LIBNAME statement. - mais il le peut par une bibliothèque Base.
Utilisateur DM5	Accorder	-	L'utilisateur DM5 peut accéder aux données par bibliothèque BASE uniquement.

b. Une bibliothèque sécurisée

A présent, en supplément de la bibliothèque traditionnelle, la bibliothèque « Orion – Détail » est liée aux métadonnées. Ceci est illustré dans le schéma ci-contre : une même bibliothèque/table est déclarée dans 2 types de bibliothèque différents avec chacun leurs propres droits.



	SYSTEME	BIBLIOTHEQUE TRADITIONNELLE	BIBLIOTHEQUE SECURISEE	
	Droit « lecture »	**Droits Meta : « Read Metadata » et « Read »**	**Droits Meta : « Read Metadata » et « Read »**	**Comportement pour un utilisateur**
Groupe RH	Refuser	Accorder	Accorder	Même comportement : l'utilisateur RH1 ne peut pas accéder aux données ni par bibliothèque META, ni par bibliothèque BASE. La restriction système l'emporte.
Groupe DM	Accorder	Accorder	Accorder	Même comportement : l'utilisateur DM1 peut accéder aux données par bibliothèque Meta et par bibliothèque Base. La différence est qu'il sera prompté pour saisir les informations du référentiel.
Utilisateur DM4	Accorder	Refuser	Refuser	Comportement différent : l'utilisateur DM4 ne peut accéder aux données ni par bibliothèque META, ni par bibliothèque BASE.
Utilisateur DM5	Accorder	-	Refuser	Comportement différent : l'utilisateur DM5 ne peut accéder aux données ni par bibliothèque META, ni par bibliothèque BASE.

7. Les erreurs les plus courantes

Ce paragraphe explique quelques messages d'erreurs possibles.

L'authentification au référentiel de métadonnées échoue car un paramètre est erroné (port faux par exemple) :

```
ERROR: The secured library object information for library ORDETAIL could not be
obtained from the metadata server or has invalid data.
ERROR: The connection to the metadata server could not be made.
ERROR: Un refus de connexion indique en général que le serveur cible n'est pas actif.
Ou alors, s'il l'est, cela signifie qu'il écoute sur un autre port ou avec un autre
service.
ERROR: La méthode Bridge Protocol Engine Socket Access Method n'a pas réussi à se
connecter à l'hôte localhost, port 8561.
ERROR: La routine de support TCP/IP tcpSockConnect() a échoué et généré l'erreur
10061 (La connexion a été refusée.).
ERROR: Error in the LIBNAME statement.
```

L'authentification au référentiel de métadonnées échoue car l'identifiant n'est pas reconnu :

```
ERROR: The secured library object information for library ORDETAIL could not be obtained from
the metadata server or has invalid data.
ERROR: The connection to the metadata server could not be made.
ERROR: Invalid credentials
ERROR: Accès refusé.
ERROR: Erreur lors de l'authentification de l'utilisateur sasdemo dans la fonction LogonUser.
Erreur   1326 (Échec d'ouverture de session : nom d'utilisateur inconnu ou mot de passe
incorrect.).
ERROR: Error in the LIBNAME statement.
```

Un référentiel est déjà déclaré, mais la bibliothèque est liée à un autre référentiel :

```
1    libname ORDETAIL "E:\Orion\Detail" ;
ERROR: The secured library object information for library ORDETAIL could not be obtained from
the metadata server or has invalid data.
ERROR: The metadata server does not have a secured library object with the external identity
"ADEFDA35-9F51-4458-A604-5FFAD036A386" or you do not have ReadMetadata permission to see it.
ERROR: Error in the LIBNAME statement.
```

Si une table traditionnelle a été copiée dans une bibliothèque sécurisée, sans ajout dans les métadonnées, alors l'utilisateur recevra cet avertissement :

```
WARNING: Data set GOLD.GEOGRAPHY_DIM.DATA is not bound to a secured table object, but it resides
in a directory that is bound to a secured library object. The data set might have existed in
this directory before the library was bound, or the data set might have been copied to this
directory with a host copy utility.
WARNING: Metadata permissions are not enabled.
```

Si l'utilisateur n'a pas les droits READ et READ METADATA dans le référentiel :

```
ERROR: L'utilisateur n'a pas le bon niveau d'autorisation pour la biblio. ORDETAIL.
ERROR: Error in the LIBNAME statement.
```

Si l'utilisateur ayant démarré la session SAS

- n'a pas les droits physiques pour créer/mettre à jour le dossier .sassl
- ou n'a pas le droit de lire le dossier .sassl pour vérifier ses informations d'authentification :

```
ERROR: sasdemo does not have sufficient host permission to the library SLIBREF to
administer it as a metadata-bound library.
```

8. Liens utiles

Pour plus de détails sur ce nouveau mode de sécurité, il faut consulter les documents suivants sur notre site http://support.sas.com/ :

- Documentation sur les bibliothèques liées aux métadonnées : SAS® 9.4 Guide to Metadata-Bound Libraries
- Documentation de la procédure AUTHLIB : Base SAS® 9.4 Procedures Guide - PROC AUTHLIB
- Les options de connexions au serveur de métadonnées : SAS® 9.4 Language Interfaces to Metadata - System Options for Metadata

9. En cas de problème

Si vous rencontrez des problèmes lors de la mise en place de ce type de bibliothèque, vous pouvez nous écrire à support@sas.com, en attachant à votre message l'erreur reçue, la procédure AUTHLIB, le fichier loc s'il existe.

10. Conclusion

Les bibliothèques liées aux métadonnées offrent de nouvelles possibilités dans votre stratégie de sécurité. Assez simple à définir, elles doivent être le résultat d'une réflexion sur la politique de sécurité.

Géraldine Cade-Deschamps
Consultante Support Clients SAS France