LE LOCKDOWN OU COMMENT RESTREINDRE L'ACCES A CERTAINES RESSOURCES

Caractéristiques :

Catégories : SAS Base
OS : Windows, Unix
Version : SAS® 9.4
Vérifié en mai 2014

Apparu avec SAS 9.4 M1, le LOCKDOWN a pour objectif de permettre aux administrateurs de restreindre l'accès à certaines ressources.

« *To be in lockdown* » peux être traduit par « *faire l'objet de mesures de confinement* ». La traduction prend tout son sens quand on sait que la mise en œuvre du LOCKDOWN permet d'interdire l'accès aux répertoires qui n'ont pas été explicitement autorisés ou encore de désactiver certaines options et fonctions SAS.

Cet article s'adresse donc aux administrateurs souhaitant limiter les possibilités offertes aux utilisateurs SAS intervenant sur leurs environnements.

1. INTRODUCTION

Les administrateurs SAS peuvent avoir besoin de bloquer l'accès à certaines ressources système afin de limiter les possibilités offertes aux développeurs.

Cette nouvelle option, LOCKDOWN, empêche ainsi l'exécution des fonctionnalités interagissant directement ou indirectement avec le système d'exploitation.

L'option permet également de mettre en place une « *whitelist* » de répertoires autorisés. Il est ainsi possible de limiter la création de bibliothèques à une liste clairement définie de répertoires.

Enfin, comme vous allez le voir, cette option impacte :

- Les utilisateurs de SAS® Enterprise Guide,
- Les utilisateurs exécutant leur programme SAS via SAS/CONNECT®.

Gardez à l'esprit qu'une option peut être limitée au niveau global (autrement dit pour toutes les sessions), par groupe ou par utilisateur. Cela peut être pratique si vous voulez activer LOCKDOWN selon l'utilisateur ou le groupe. Pour plus d'informations sur ce point, je vous invite à prendre connaissance de l'article Comment restreindre l'utilisation d'options SAS par groupe, par utilisateur ou globalement?

2. CONFIGURATION

La mise en œuvre du LOCKDOWN se fait en deux étapes. En effet, l'activation du LOCKDOWN implique le positionnement de **l'option LOCKDOWN** et l'utilisation de **LOCKDWON statement**, l'un ne fonctionnant pas sans l'autre.

Tout d'abord, il faut définir l'option LOCKDOWN.
Cette option peut être définie dans la configuration ou en argument au lancement de SAS.

Si vous souhaitez modifier le fichier de configuration, il faut éditer le fichier SASApp/WorkspaceServer/sasv9_usermods.cfg et ajouter la ligne suivante :

```
-lockdown
```

Si, au contraire, vous souhaitez passer l'option en argument du démarrage de SAS, il faut éditer le fichier SASApp/WorkspaceServer/WorkspaceServer_usermods.bat (ou WorkspaceServer_usermods.sh sous UNIX) et paramétrer comme suit :

```
Set USERMODS_OPTIONS=-LOCKDOWN
```

Il est possible de mixer l'option LOCKDOWN et l'option NOLOCKDOWN dans le fichier WorkspaceServer_usermods.bat :

```
if %USERNAME%==sasadmin(
  Set USERMODS_OPTIONS=
) else (
  Set USERMODS_OPTIONS=-LOCKDOWN
)
```

L'ajout de l'option dans le script de démarrage permet de personnaliser le LOCKDOWN en fonction des utilisateurs.

Une restriction tout de même, l'option LOCKDOWN ne doit pas être utilisée si l'option XCMD ou RLANG est positionnée.

Maintenant que l'option est correctement définie, il est nécessaire de positionner l'instruction LOCKDOWN. L'instruction permet de sécuriser SAS en limitant l'accès à certaines ressources. Si la définition de l'instruction LOCKDOWN semble similaire à la définition de l'option LOCKDOWN, leurs buts sont bien différents.

Dans l'exemple ci-dessous nous allons indiquer les seuls répertoires autorisés :

```
lockdown path='d:\data\marketing' 'd:\data\finance';
```

Quelques règles à avoir en tête :

- Chaque répertoire doit être spécifié entre guillemets (les guillemets simples sont préférables pour éviter les conflits avec les macro-variables SAS)
- L'argument PATH accepte plusieurs répertoires.
- Si vous spécifiez plusieurs répertoires, ils doivent être séparés par un espace.
- SAS ajoute automatiquement les sous-répertoires de tous les répertoires valides
- Un chemin peut être un chemin relatif ou un chemin absolu.
- Un chemin d'accès peut également inclure des variables d'environnement du système d'exploitation, les variables d'environnement SAS (par exemple, !SASROOT) ou le répertoire de travail courant (.)
- Sous Windows, un chemin d'accès n'est PAS case sensitive.

En plus de limiter l'accès aux répertoires définis via l'instruction PATH, les fonctionnalités présentées dans la liste ci-dessous sont désactivées :

- DATA step Java Object "javaobj"
- PROC JAVAINFO et PROC GROOVY
- Fonctions: ADDR, ADDRLONG, PEEK, PEEKLONG, PEEKC, PEEKCLONG, POKE, POKELONG et MODULE
- Certaines procédures Z/OS : PDS, PDSCOPY, RELEASE, SOURCE, TAPECOPY, et TAPELABEL

3. MISE EN PRATIQUE

Dans notre scenario d'exemple, nous souhaitons uniquement autoriser les bibliothèques sur les répertoires **/sas94/sasdata/public** et **/sas94/sasdata/secure.**

L'accès au répertoire **/sas94/sasdata/private** est interdit à tous les utilisateurs.

Pour faire simple, les répertoires pour lesquels une autorisation n'a pas été explicitement faite ne sont pas accessibles.

Pour mettre en place cette solution, il est nécessaire de modifier deux fichiers de configuration :

- SASApp/WorkspaceServer/autoexec_usermods.sas
- SASApp/WorkspaceServer/sasv9_usermods.cfg

```
[sasinst@sasserver01 WorkspaceServer]$ ls -l
total 52
-rw-r--r--. 1 sasinst sas  382 Jul 12 06:02 autoexec.sas
-rw-r--r--. 1 sasinst sas  208 Sep 27 05:09 autoexec_usermods.sas
drwxr-xr-x. 3 sasinst sas 4096 Jul 12 06:02 dtest
-rw-r--r--. 1 sasinst sas 3641 Jul 12 06:02 logconfig.apm.xml
-rw-r--r--. 1 sasinst sas 4044 Jul 12 06:02 logconfig.trace.xml
-rw-r--r--. 1 sasinst sas 3027 Jul 12 06:02 logconfig.xml
drwxrwx---. 2 sasinst sas 4096 Jul 12 06:02 Logs
drwxrwxr-x. 2 sasinst sas 4096 Sep 27 05:08 PerfLogs
-rw-r--r--. 1 sasinst sas  525 Jul 12 06:02 sasv9.cfg
-rw-r--r--. 1 sasinst sas  373 Sep 27 05:11 sasv9_usermods.cfg
-rw-r--r--. 1 sasinst sas  187 Jul 12 07:38 sev_logtracker_plugin.properties
-rwxr-xr-x. 1 sasinst sas  856 Jul 12 06:02 WorkspaceServer.sh
-rwxr-xr-x. 1 sasinst sas  185 Jul 12 06:02 WorkspaceServer_usermods.sh
```

La première étape est d'ajouter l'option lockdown dans le fichier de configuration du WorkSpaceServer SASApp/WorkspaceServer/sasv9_usermods.cfg :

```
/*
 * sasv9_usermods.cfg
 *
 *   This config file extends options set in sasv9.cfg.  Place your site-specific
 *   options in this file.  Any options included in this file are common across
 *   all server components in this application server.
 *
 *   Do NOT modify the sasv9.cfg file.
 *
 */

-logconfigloc /sas94/config/Lev1/SASApp/WorkspaceServer/logconfig.apm.xml

-lockdown
```

Maintenant que l'option est activée, nous pouvons définir les répertoires autorisés dans le fichier SASApp/WorkspaceServer/autoexec_usermods.cfg :

```
/*
 * autoexec_usermods.sas
 *
 *    This autoexec file extends autoexec.sas.  Place your site-specific include
 *    statements in this file.
 *
 *    Do NOT modify the autoexec.sas file.
 *
 */

lockdown path = "~" "/sas94/sasdata/public" "/sas94/sasdata/secure";
```

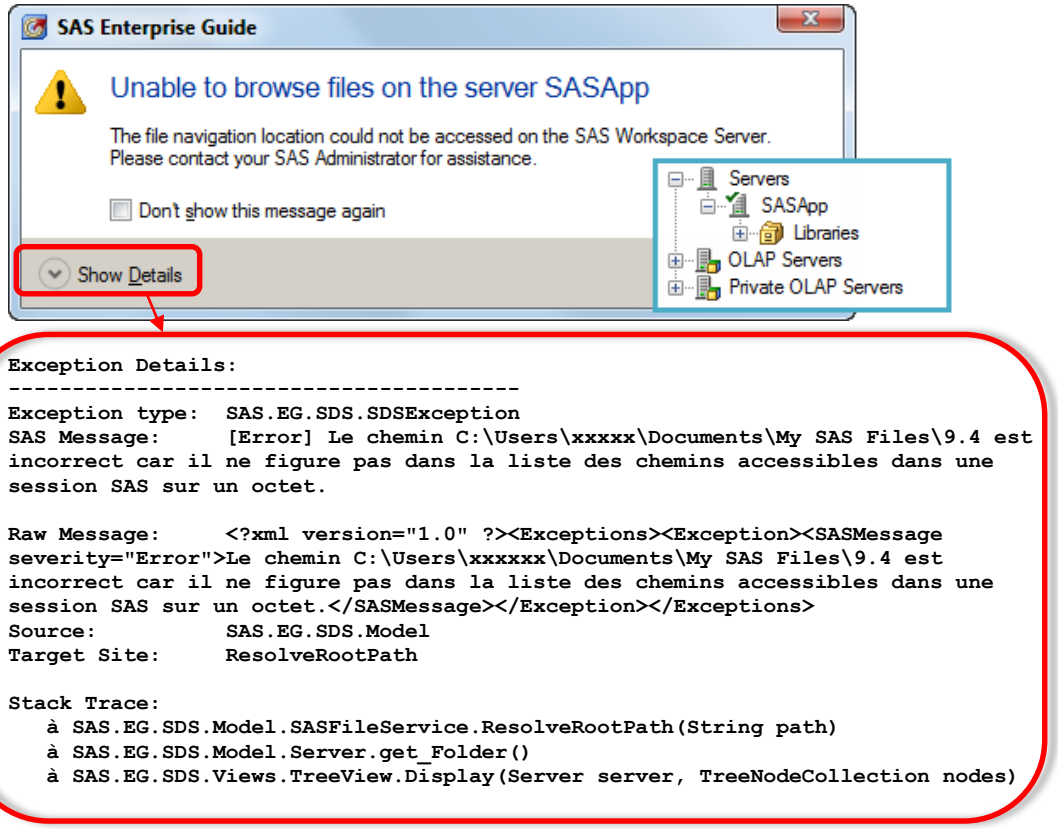
Nous avons donc explicitement ajouté les deux répertoires que nous souhaitons autoriser.

```
lockdown path = "~" "/sas94/sasdata/public/"
"/sas94/sasdata/secure/";
```

Nous avons également ajouté le répertoire ~. Sous environnement UNIX, ~ fait référence au répertoire personnel de l'utilisateur. Il s'agit du répertoire contenant les fichiers appartenant à un utilisateur. L'équivalent sous environnement Windows est ?FOLDERID_Profile

```
lockdown path="?FOLDERID_Profile";
```

Si vous n'ajoutez pas le répertoire personnel de l'utilisateur dans la « *whitelist* » vous obtiendrez le message d'erreur ci-dessous lors de toute tentative d'accès à SAS APP :



- Les ressources nécessaires au bon fonctionnement de SAS sont prises en compte automatiquement : WORK,SASHELP, SASUSER…
- Les librairies pré-assignées sont également non restreintes par l'option LOCKDOWN.

4. TESTS

Une fois la mise en œuvre réalisée, connectons-nous à SAS Enterprise Guide et vérifions si l'option lockdown est correctement prise en compte :

```
PROC Options group=EXECMODES;run;
…

LOCKDOWN          Specifies that access to files and certain SAS features will be
restricted. This feature is only applicable for a SAS session executing in a
batch or server processing mode
```

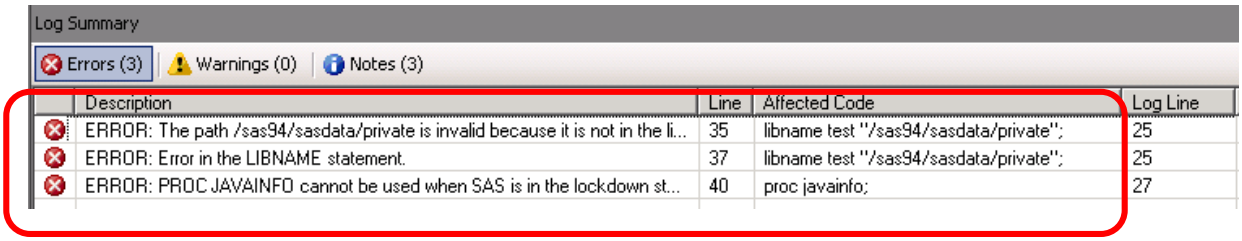
Soumettons maintenant le code suivant afin de vérifier notre paramétrage.
Ce code permet de valider la prise en compte de l'option, la bonne affectation des droits d'accès aux répertoire et la désactivation de certains proc. Dans l'exemple ci-dessous, nous testons avec la proc javainfo.

```
libname test "/sas94/sasdata/public";
libname test "/sas94/sasdata/secure";
libname test "/sas94/sasdata/private";

proc javainfo;
```

Logs d'exécution :

```
23 libname test "/sas94/sasdata/public";
NOTE: Libref TEST was successfully assigned as follows:
      Engine:        V9
      Physical Name: /sas94/sasdata/public

24 libname test "/sas94/sasdata/secure";
NOTE: Libref TEST was successfully assigned as follows:
      Engine:        V9
      Physical Name: /sas94/sasdata/secure

25 libname test "/sas94/sasdata/private";
ERROR: The path /sas94/sasdata/private is invalid because it is not in the list
of accessible paths when SAS is in the lockdown       state.
ERROR: Error in the LIBNAME statement.

27 proc javainfo;

ERROR: PROC JAVAINFO cannot be used when SAS is in the lockdown state.
```

Nous constatons que seul l'accès aux répertoires **public** et **secure** est possible. Nous constatons également que la **proc javainfo** est désactivée.



Supprimons maintenant l'option lockdown dans le fichier de configuration du workspace server SASApp/WorkspaceServer/sasv9_usermods.cfg.

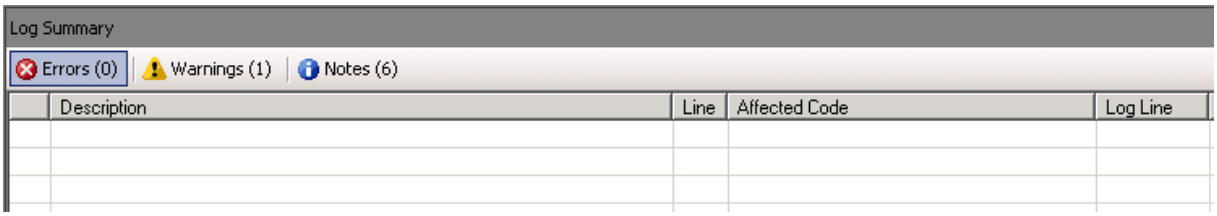
Après avoir relancé notre session SAS Enterprise Guide, vérifions l'option lockdown.
Nous constatons maintenant que l'option apparaît sous la forme de NOLOCKDOWN :

```
PROC Options group=EXECMODES;run;
…
LOCALEDATA=SASLOCALE  Specifies the location of the locale database.

NOLOCKDOWN        Specifies that access to files and certain SAS features will not
be restricted. This feature is only applicable for a SAS session executing in a
batch or server processing mode.
```

```
LOGAPPLNAME=      Specifies a SAS session name for SAS logging.

…
```

Il est maintenant possible d'accéder à l'ensemble des répertoires. La **proc javainfo** fonctionne également :

```
23 libname test "/sas94/sasdata/public";
NOTE: Libref TEST was successfully assigned as follows:
      Engine:        V9
      Physical Name: /sas94/sasdata/public

24 libname test "/sas94/sasdata/secure";
NOTE: Libref TEST was successfully assigned as follows:
      Engine:        V9
      Physical Name: /sas94/sasdata/secure

25 libname test "/sas94/sasdata/private";
NOTE: Libref TEST was successfully assigned as follows:
      Engine:        V9
      Physical Name: /sas94/sasdata/private
26
27 proc javainfo;

PFS_TEMPLATE = /sas94/sashome/SASFoundation/9.4/misc/tkjava/qrpfstpt.xml
java.class.path =
/sas94/sashome/SASVersionedJarRepository/eclipse/plugins/sas.launcher.jar
java.class.version = 51.0
java.runtime.name = Java(TM) SE Runtime Environment
java.runtime.version = 1.7.0_15-b03
java.security.auth.login.config =
/sas94/sashome/SASFoundation/9.4/misc/tkjava/sas.login.config
java.security.policy = /sas94/sashome/SASFoundation/9.4/misc/tkjava/sas.policy
java.specification.version = 1.7

…
```



5. ASTUCES

Plutôt que de définir la liste des répertoires autorisés dans l'autoexec.sas, il est possible de maintenir un fichier «whitelist ». L'idée est de créer un fichier texte dans lequel l'administrateur liste les répertoires accessibles par les utilisateurs. Si l'administrateur le souhaite, il peut cacher le contenu de cette « whitelist » en localisant le fichier dans un répertoire qui n'est pas accessible par les utilisateurs (c'est-à-dire un répertoire non défini dans la « whitelist), ni dans un répertoire de configuration du serveur d'application SAS (comme SASAPP).

Pour résumer :

- Créer un fichier texte pour y définir tous les chemins valides.
- Placer ce fichier dans un répertoire non accessible par les utilisateurs SAS.
- Modifier l'autoexec SAS du serveur pour la prise en compte de cette liste.

Par exemple, dans whitelist.txt, nous trouvons les répertoires suivants :

```
C:\DATA\PUBLIC1
C:\DATA\MARKETING
```

Ensuite, il suffit de modifier le fichier autoexec du serveur en ajoutant une instruction LOCKDOWN pointant vers ce fichier « whitelist » :

```
filename lkdn "C:\SAS\Config\Lev1\Lockdown\whitelist.txt";
lockdown file = lkdn;
```

6. LIENS UTILES ET REFERENCES

LOCKDOWN System Option

Access to SAS Data : Locked-Down Servers

SAS® 9.4 TS1M1 products and solutions that do not support the lockdown feature

Authorization > Access to SAS Data > Locked-Down Servers

7. CONCLUSION

Si vous décidez de mettre en œuvre le LOCKDOWN dans votre environnement, je vous conseille de prendre suffisamment de temps pour tester son fonctionnement et de bien avoir en tête les impacts que cela peut avoir.

Il est en effet très facile d'exclure accidentellement un répertoire nécessaire aux utilisateurs.

En outre, gardez en tête que certaines applications SAS ne sont pas compatibles avec le LOCKDOWN. La liste des applications non compatibles sont disponibles dans la note http://support.sas.com/kb/51/644.html

Nicolas Housset
Consultant Support Clients SAS France