CONFIGURATION DE L'AUTHENTIFICATION PAM POUR UNE UTILISATION AVEC SAS® 9.2 OU 9.3

Caractéristiques :

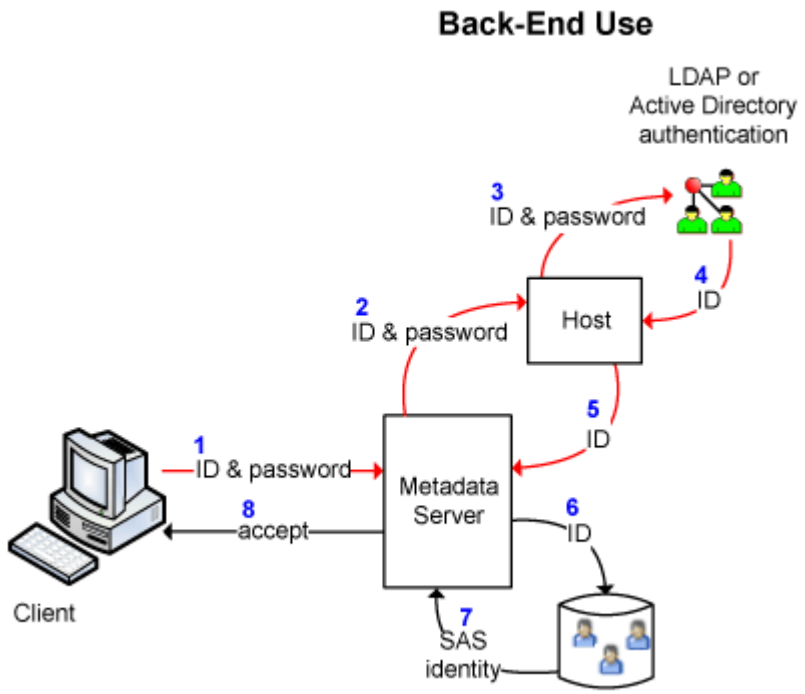
Catégorie : OMA
OS : Unix
Version : à partir de SAS 9.2
Vérifié en mars 2012

Active Directory est utilisé pour simplifier le processus d'authentification pour les utilisateurs professionnels afin de réduire le nombre de systèmes d'authentification requis dans une entreprise.
Sur Unix, les serveurs SAS peuvent être configurés pour authentifier les utilisateurs contre un annuaire LDAP en utilisant les modules PAM (des bibliothèques dynamiques) qui étend le processus d'authentification de l'hôte UNIX pour reconnaître un prestataire supplémentaire tel qu'Active Directory ou LDAP.

Configuration de l'authentification PAM pour une utilisation avec SAS® 9.2 ou 9.3 1
Introduction à Pluggable Authentication Modules (PAM) 1
Les étapes pour utiliser l'authentification PAM depuis SAS 2
Les points à retenir 3
Quelques références 3

Introduction à Pluggable Authentication Modules (PAM)

Cette méthode d'authentification fonctionne de façon similaire à *password* – la méthode classique sur unix. Les fichiers de configuration PAM doivent être édités avec les services « sasauth ». Quand le serveur SAS demande à son hôte UNIX de valider les informations d'identification d'un utilisateur, l'hôte renvoie l'identifiant de l'utilisateur et son mot de passe au fournisseur pour vérification. PAM ne modifie pas le comportement des serveurs SAS.
Voici un diagramme qui illustre l'authentification PAM :



D'une certaine façon, on peut dire que la configuration PAM/LDAP est transparente pour le serveur de Métadonnées SAS, c'est l'hôte UNIX qui gère la redirection avec les modules PAM.

Les étapes pour utiliser l'authentification PAM depuis SAS

1. Vérifier les autorisations pour les fichiers d'authentification suivants :

```
cd $SASROOT/utilities/bin
ls -l
-rwsr-xr-x  1 root sas   69042 Dec 04 2008  elssrv
-rwsr-xr-x  1 root sas   67048 Jan 16 2009  sasauth
-rwsr-xr-x  1 root sas   18634 Dec 04 2008  sasperm
```

   Si les permissions ne sont pas définies comme ci-dessus, il faut les modifier ainsi :

```
 su root
 cd $SASROOT/utilities/bin
 mv setuid/* .
 chown root elssrv sasauth sasperm
 chmod 4755 elssrv sasauth sasperm
exit
```

2. Dans le fichier $SASROOT/utilities/bin/sasauth.conf, il faut ajouter pam à "methods"

```
methods=pam pw
```

   Pour plus de détails, vous pouvez consulter la documentation « Configuration Guide for SAS® 9.2 Foundation for UNIX® Environments » au chapitre 3 « Post-Installation Configuration for User Authentication and Identification », paragraphe « Configuring sasauth » (page 7).

3. Configuration de l'authentification PAM pour une utilisation avec sasauth.

   Le fichier de configuration contient des entrées dans le formulaire ci-dessous : <module_type> <control_flag> <module_path> <options>
   Son contenu sera différent selon le système d'exploitation, le chemin étant propre à chacun.

   1er exemple : configurer PAM sur AIX.
   Il faut ajouter les lignes suivantes dans le fichier /etc/pam.conf :

```
sasauth auth required /usr/lib/security/64/pam_aix
sasauth account required /usr/lib/security/64/pam_aix
```

   2ème exemple : configurer WINBINDS sur Linux.
   Il faut ajouter les lignes suivantes dans le fichier /etc/pam.conf. Sur Linux, le répertoire /etc/pam.d contient un fichier pour chaque programme autorisé à utiliser PAM.

   Fichier /etc/pam.d/sasauth :

```
#%PAM-1.0
auth    required        pam_env.so
auth    sufficient      pam_unix.so nullok try_first_pass
auth    requisite       pam_succeed_if.so uid>=500 quiet
auth    sufficient      pam_winbind.so cached_login use_first_pass
auth    required        pam_deny.so

account required        pam_unix.so broken_shadow
account sufficient      pam_localuser.so
account sufficient      pam_succeed_if.so uid<500 quiet
account [default=bad success=ok user_unknown=ignore] pam_winbind.so
cached_login
account required        pam_permit.so
```

   Pour plus de détails, vous pouvez consulter la documentation « Configuration Guide for SAS® 9.2 Foundation for UNIX® Environments » chapitre 3 «Post-Installation Configuration for User Authentication and Identification », paragraphe « Configuring PAM Authentication for Use with sasauth » (page 11).

4. Tester depuis SAS avec la procédure PERMTEST

   L'exemple ci-dessous lance SAS en mode non fenêtré et la procédure :

   ```
   cd $SASROOT
   ./sas -path ./utilities/src/auth -nodms
   proc permtest;run;
   ```

   Pour plus de details,
   Usage Note 33751: Using PROC PERMTEST to diagnose UNIX host authentication issues

5. En cas d'erreur, il faut activer les journaux.

   Dans le fichier $SASROOT/utilities/bin/sasauth.conf, il convient de modifier les lignes suivantes:

   ```
   debugLog=/tmp/sasauth-debug.log
   accessLog=/tmp/sasauth-access.log
   errorLog=/tmp/sasauth-error.log
   ```

   Les journaux vont être générés dans /tmp : sasauth-access.log, sasauth-debug.log, sasauth-error.log. Ils vous guideront sur la cause de l'erreur.

Les points à retenir

1. Il est préférable de vérifier la connexion d'un utilisateur (authentifié via PAM) avec un autre outil (rlogin, ssh, telnet, etc) avant d'essayer de le configurer avec SAS.

2. Chaque module d'authentification SAS (sasauth) est une application 64-bit. De la même manière, les objets qui sont définis dans le fichier de configuration PAM doivent être des objets 64-bit.

3. Dans certains cas, c'est l'incohérence des politiques de sécurité d'utilisateur définies dans le fichier (/etc/security/utilisateur) qui pose des problèmes. Par exemple, si le paramètre MAXAGE est défini à 4 et UPW_LASTUPDATE à 0, cela signifie que le mot de passe est expiré. Dans ce cas, il faut essayer de définir le MAXAGE à 0 et réessayer.

4. La méthode « pw » n'est compatible qu'avec du type crypt ou SSHA, mais pas avec l'encryption SSHA256. Sur les nouveaux systèmes (par exemple Aix 6.1) qui supportent SSHA256 pour l'authentification, il faut aussi passer par « pam ».

5. L'utilitaire sasumgmt fait des vérifications sur les droits de l'utilisateur. Il peut être utile pour valider la connexion des utilisateurs au niveau de la machine Unix. Sa syntaxe :

   ```
   sasumgmt –u utilisateur –p motdepasse -v
   ```

   Exemple :

   ```
   cd $SASROOT/utilities/bin
   ./sasumgmt -u sasdemo -p saspw1 -v
   NOTE: [sasumgmt: SASUMGT_STATUS_OK]
   ./sasumgmt -u sasdemo -p saspw2 -v
   NOTE: [sasumgmt: SASUMGT_STATUS_ACCESS_DENIED]
   ```

Quelques références

- Dans SAS(R) 9.2 Intelligence Platform: Security Administration Guide, la section Pluggable Authentication Modules (PAM).
- Configuration Guide for SAS® 9.2 Foundation for UNIX® Environments

Anitha DATCHANAMOURTY
Consultant Support Clients SAS France