



IMPLEMENTATION D'UNE AUTHENTIFICATION LDAP DANS SAS

Par défaut, le serveur de métadonnées exploite le système d'authentification de la machine l'hébergeant pour valider les utilisateurs. Ce système d'authentification peut être modifié et il est possible de configurer le serveur de métadonnées pour exploiter un annuaire LDAP ou Active directory. Dans ce cas, les

utilisateurs se connecteront aux différentes applications clientes de l'architecture SAS® à l'aide de leur compte LDAP ou AD. Cet article présente la mise en place de ce mécanisme d'authentification.



Caractéristiques :

Catégories : Base SAS®

OS : Windows, Unix, z/OS

Version : SAS® 9.4

Vérifié en septembre 2016

Sommaire

Implémentation d'une authentification LDAP dans SAS.....	1
1. Présentation.....	2
1.1. Qu'est-ce qu'un annuaire ?	2
1.2. Les intérêts d'un annuaire.....	2
1.3. Le protocole LDAP.....	3
2. Implémentation dans SAS.....	3
2.1. Externaliser le processus d'authentification	3
2.1. SAS et LDAP, quelles solutions ?.....	4
2.1. Authentification ou Autorisation ?	5
2.2. Comment est déterminée l'identité d'un utilisateur SAS ?	5
2.3. Connecter SAS à un annuaire LDAP (metadata server use of LDAP)	7
2.4. Comprendre le routage de l'authentification en fonction du domaine d'authentification ...	9
2.5. Utiliser LDAP comme authentification par défaut.....	10
3. Configuration des utilisateurs dans SAS pour un usage dans SAS® Enterprise Guide®.....	11
4. Lier une identité externe à un compte physique	15
4.1. Présentation de la problématique.....	15
4.2. L'authentification de jeton pour le Workspace Server.	16
4.2.1. Configuration de l'authentification de jeton.....	16
4.3. Création d'un groupe d'utilisateurs.....	18
4.4. Modification de la configuration du Workspace Server.....	21
5. Tester et valider sa connexion	22
5.1. Valider la connexion au serveur LDAP, en dehors de SAS.....	22
5.2. Utilisation de la procédure METAOPERATE	23
5.3. Validation de son authentification via la proc permtest	25
5.4. Utilisation de l'outil SASUMGMT	25
5.5. Activation des traces SAS Enterprise Guide	26
5.6. Activer les traces SAS Metadataserver.....	27
5.6.1. Exemple de traces et analyse détaillée.....	29

5.7.	Visualiser les identités associées à votre compte.....	31
6.	Implémentation avancée.....	31
6.1.	Les nouveautés SAS 9.4	32
6.2.	Relier SAS à plusieurs annuaire LDAP	32
6.3.	Gérer le délai de connexion	33
6.4.	Se connecter à un serveur LDAP sécurisé via SSL	34
7.	En cas de problème.....	36
7.1.	Les problèmes les plus fréquents	36
7.1.1.	Messages d'erreurs	36
7.2.	Autres problèmes.....	38
7.3.	Éléments à transmettre au Support Clients	38
8.	Liens utiles.....	39
9.	Conclusion	39

1. PRESENTATION

1.1. Qu'est-ce qu'un annuaire ?

Un annuaire est avant tout une base de données. A la différence des bases de données relationnelles où les données sont stockées de manière tabulaire (ligne, colonne), l'annuaire classe les informations de manière hiérarchique. Toutes sortes de données peuvent figurer dans un annuaire électronique : répertoire téléphonique, liste des ressources matérielles de l'entreprise, identité du personnel,...

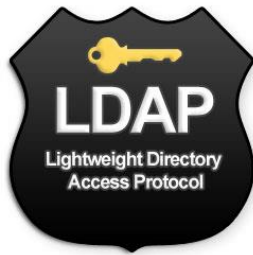
Autre différence, le mode d'utilisation : comparé aux bases de données relationnelles, un annuaire a vocation à être plus souvent consulté que mis à jour.

1.2. Les intérêts d'un annuaire

D'une façon générale, l'utilisation d'un annuaire présente plusieurs intérêts :

- **Administration centralisée et simplifiée** : la gestion des comptes utilisateurs est simplifiée. Tout est centralisé dans l'annuaire.
- **Authentification unifiée** : un utilisateur authentifié sur une machine, sous condition d'avoir les autorisations nécessaires, peut accéder aux ressources stockées sur d'autres serveurs ou ordinateurs enregistrés dans l'annuaire.
Un seul compte permet un accès à tout le système d'information.
- **Référencement de tous les utilisateurs** : l'annuaire s'apparente à une énorme base de données qui référence les utilisateurs, les groupes et les ordinateurs d'une entreprise. Les applications et systèmes d'exploitation s'appuient sur cette base de données pour réaliser de nombreuses opérations : authentification, identification, stratégie de groupe, déploiement de logiciels...

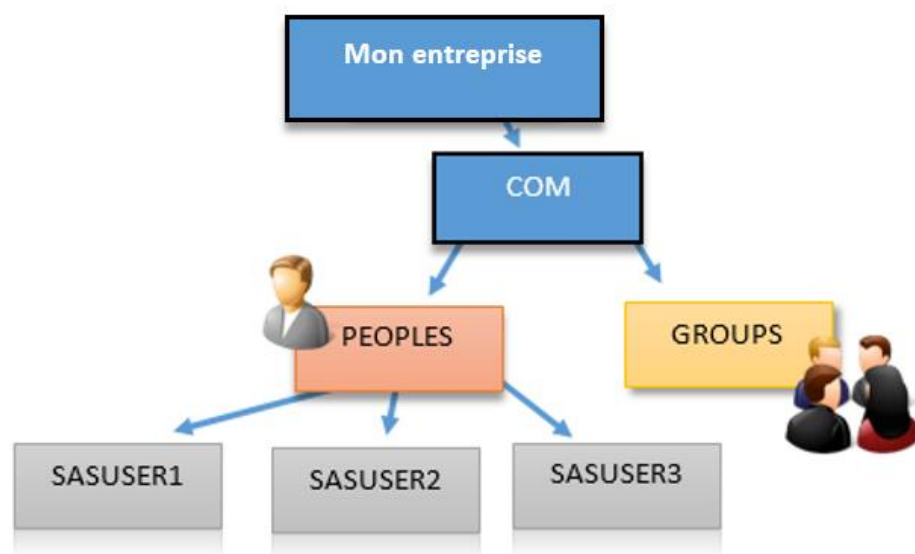
1.3. Le protocole LDAP



LDAP (*Lightweight Directory Access Protocol*) est un protocole pour l'accès à des services d'annuaire.

Ce protocole est une définition de la norme de communication client-serveur et propose un ensemble d'outils et de commandes pour se connecter, rechercher et administrer les entrées dans un annuaire.

Le schéma ci-dessous présente un exemple d'organisation logique d'un annuaire LDAP :



2. IMPLEMENTATION DANS SAS

2.1. Externaliser le processus d'authentification

Comme indiqué en introduction, le serveur de métadonnées exploite le système d'authentification de la machine qui l'héberge pour valider les utilisateurs.

En fonction de votre environnement, plusieurs approches sont envisageables pour externaliser le processus d'authentification. Par externaliser, on entend réaliser la tâche d'authentification par un annuaire externe (LDAP/AD) au lieu d'être réalisé par le serveur de métadonnées. Dans ce cas, les utilisateurs se connecteront aux différentes applications clientes de l'architecture SAS à l'aide de leur compte LDAP.

Nous verrons dans les chapitres suivants qu'il est possible de gérer plusieurs méthodes d'authentifications, LDAP, active directory, compte système, compte interne SAS, en simultané.

2.1. SAS et LDAP, quelles solutions ?

SAS supporte les méthodes suivantes pour l'intégration avec LDAP :

host use of LDAP

L'hôte du serveur SAS utilise un fournisseur LDAP en tant que fournisseur d'authentification back-end. Du point de vue du serveur SAS, ceci est l'authentification de l'hôte. Ainsi, ce mode d'intégration avec LDAP est transparent et ne demande aucune configuration SAS.

Par exemple, Active Directory est le fournisseur d'authentification back-end standard sur Windows.

Certains hôtes UNIX reconnaissent les comptes LDAP (ou peuvent être configurés pour le faire). Pour plus d'informations sur ce point, consultez la documentation relative à [Pluggable Authentication Modules](#) (en abrégé PAM). Ce mécanisme permet d'intégrer différents schémas d'authentification de bas niveau dans une API de haut niveau.

sasauth use of LDAP (Unix uniquement)

Cette méthode fournit une connexion directe entre sasauth (le module d'authentification de l'hôte UNIX) et une base de données LDAP pour l'authentification. Cette méthode fournit une identité d'hôte UNIX pour chaque utilisateur authentifié.

metadata server use of LDAP

Le serveur de métadonnées valide certains utilisateurs par l'intermédiaire d'un annuaire LDAP tiers. Cette méthode permet au serveur de métadonnées de reconnaître les comptes qui ne sont pas connus par son hôte.

- Dans cet article, nous vous présentons l'implémentation « metadata server use of LDAP ».
- Si vous souhaitez obtenir des informations et détails sur l'implémentation « sasauth use of LDAP », vous pouvez lire l'article [CONFIGURATION DE L'AUTHENTIFICATION PAM POUR UNE UTILISATION AVEC SAS® 9.2 OU 9.3](#)

2.1. Authentification ou Autorisation ?

Avant de poursuivre, il est important de faire la distinction entre l'authentification et l'autorisation pour comprendre le fonctionnement de SAS :

- L'authentification consiste à vérifier les informations d'identification de la tentative de connexion.
- L'autorisation consiste à vérifier que la tentative de connexion est légitime puis à affecter les droits à l'utilisateur. L'autorisation intervient après une authentification réussie.



Déléguer les tâches d'authentification à un annuaire LDAP ou ACTIVE DIRECTORY n'empêche pas de devoir gérer les autorisations dans SAS.

2.2. Comment est déterminée l'identité d'un utilisateur SAS ?

Comme nous venons de le voir, lorsqu'un utilisateur se connecte à un serveur de métadonnées SAS, nous rentrons dans un processus d'authentification. Ce processus est composé de deux phases :

- Vérification
- Identification

La **phase de vérification** veille à ce que l'utilisateur soit bien celui qu'il prétend être. Par exemple, avec une authentification basée sur l'hôte :

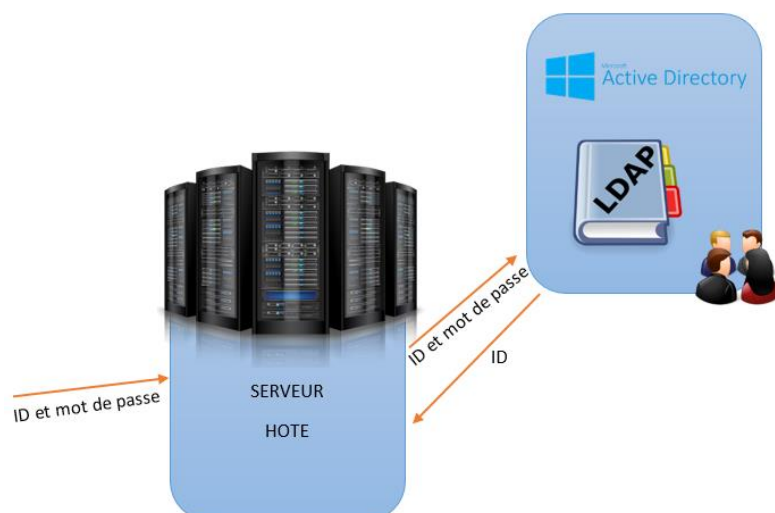
1. Le serveur demande un compte utilisateur et un mot de passe
2. L'utilisateur saisit son compte et son mot de passe. Ces deux informations sont connues par le serveur hôte, hébergeant le serveur de métadonnées SAS.
3. Le serveur de métadonnées SAS soumet ses deux informations au serveur hôte pour authentification. Le serveur de métadonnées SAS ne connaît pas le mot de passe.
4. Si le serveur hôte valide le compte, une confirmation est retournée au serveur de métadonnées SAS.

La seconde **phase d'identification** associe le compte utilisateur authentifié à une identité SAS. Dans cette phase, SAS examine ses utilisateurs et tente de trouver celui qui correspond au compte de l'utilisateur authentifié :

- Si un utilisateur SAS est trouvé, une connexion est établie sous l'identité du propriétaire. Cette identité est un utilisateur ou un groupe SAS associé au compte avec laquelle la connexion a été effectuée.
- Si aucun utilisateur SAS associé au compte utilisé lors de la connexion n'est trouvé, une connexion est faite avec une identité PUBLIC, ne disposant d'aucun droit par défaut.



Comme nous l'avons vu dans le chapitre 2.1, dans le cas du *host use of LDAP*, le serveur hôte peut se connecter à un annuaire LDAP ou Active Directory. Comme indiqué précédemment, dans ce mode de fonctionnement, la connexion à l'annuaire et le processus d'authentification sont transparents pour SAS :



2.3. Connecter SAS à un annuaire LDAP (metadata server use of LDAP)

Pour utiliser l'annuaire LDAP pour l'authentification, vous devez modifier les scripts de démarrage du serveur de métadonnées en ajoutant des variables d'environnement spécifiques pour LDAP.

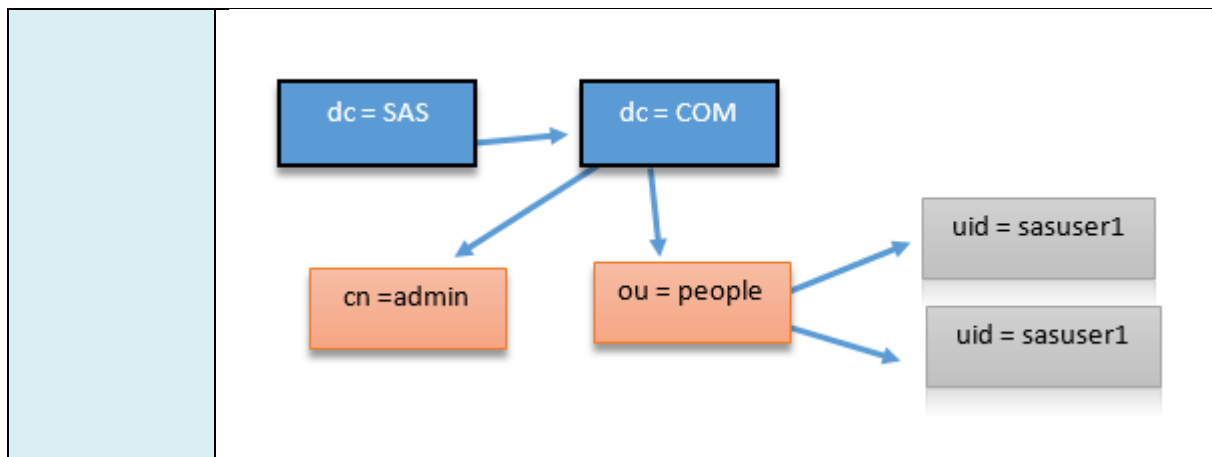
Le fichier à modifier, `sasv9_usermods.cfg`, se trouve dans `<config>/LevX/SASMeta/MetadataServer/`

Ajoutez les variables suivantes :

```
-set LDAP_HOST ldap-france.monserveur.fr
-set LDAP_PORT 389
-set LDAP_BASE "ou=people,dc=sas,dc=com"
```

Voici une description des principales variables nécessaires à une connexion LDAP :

Champ	Description
LDAP_PORT	Numéro de port d'écoute de l'annuaire LDAP (389 par défaut).
LDAP_HOST	Machine connectée au réseau hébergeant l'annuaire LDAP.
LDAP_IDATTR	Attribut LDAP utilisé pour l'authentification qui définit le nom logique de l'utilisateur.
LDAP_BASE	Lien DN pour retrouver les utilisateurs.



Dans notre exemple, nous avons indiqué au serveur de métadonnées comment se connecter à l'annuaire LDAP et le chemin pour trouver les identités dans l'organisation, via LDAP_BASE.

Maintenant, nous devons ajouter de nouvelles variables afin de préciser le domaine d'authentification.

En effet, par défaut, le serveur de métadonnées supporte deux types de compte :

- Les comptes internes, portant le suffixe @saspw
- Les comptes physiques, sans suffixe.

Pour router correctement l'authentification, nous devons donc créer un domaine d'authentification qui indiquera aux métadonnées si l'authentification doit se faire en interne, sur le host ou au niveau LDAP.

Nous allons donc définir la variable AUTHPROVIDERDOMAIN :

```
-AUTHPROVIDERDOMAIN LDAP:DOMAINEFRANCE
```

Grâce à cette variable, nous pouvons spécifier au serveur de métadonnées où diriger l'authentification. Notez que vous pouvez nommer ce domaine comme vous le souhaitez.

Une fois la configuration faite, vous devez simplement redémarrer le serveur de métadonnées pour prendre en compte ces nouveaux paramètres.

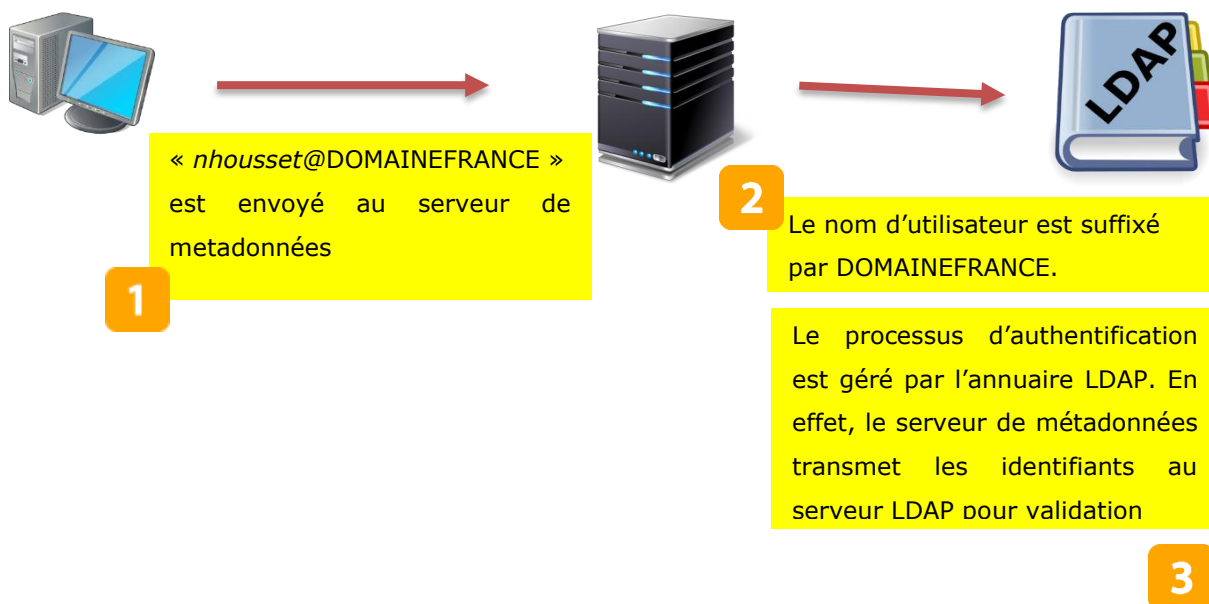
2.4. Comprendre le routage de l'authentification en fonction du domaine d'authentification

Pour comprendre le routage d'un utilisateur, utilisons un exemple. Dans notre cas, l'utilisateur Nicolas dispose d'un compte local « nhouset » et d'un compte sur LDAP. Il peut également se connecter en tant qu'administrateur SAS. C'est grâce à ce domaine d'authentification, précisé à la connexion, que le serveur de métadonnées sera en mesure d'authentifier l'utilisateur :

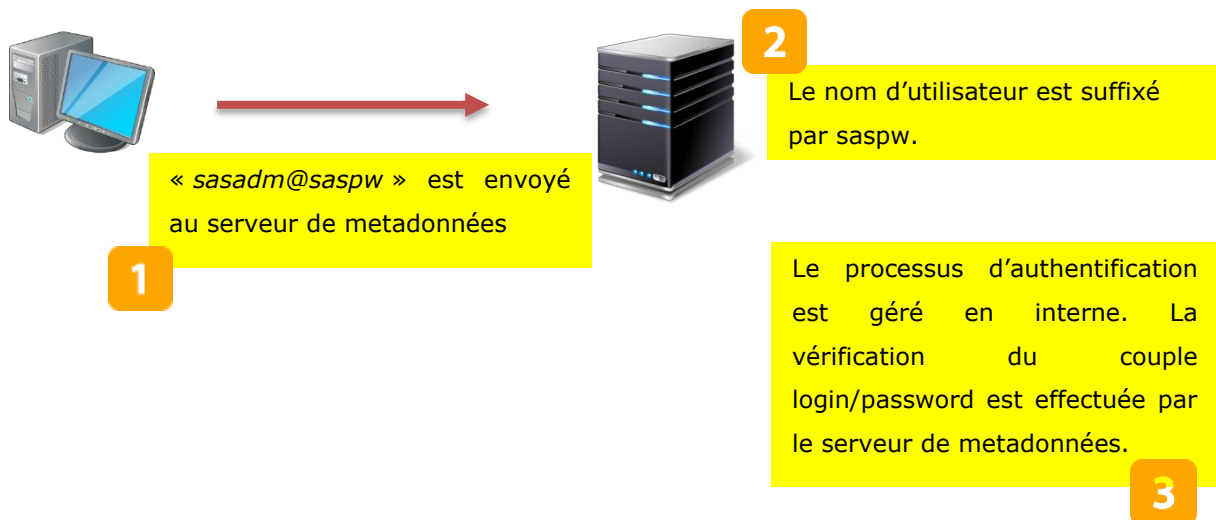
Cas 1 - L'utilisateur utilise le compte « nhouset » pour se connecter aux métadonnées SAS :



Cas 2 - L'utilisateur utilise son compte LDAP pour se connecter aux métadonnées SAS :



Cas 3 - L'utilisateur utilise le compte d'administration pour se connecter aux métadonnées SAS :



2.5. Utiliser LDAP comme authentification par défaut

Comme nous l'avons vu dans le chapitre « Routage de l'authentification en fonction du domaine d'authentification », si un utilisateur souhaite se connecter en utilisant son compte LDAP, il doit ajouter un suffixe (@DOMAINEFRANCE, dans nos exemples) afin d'indiquer au serveur de métadonnées que l'authentification doit être effectuée au niveau de l'annuaire.

Il est possible de configurer son serveur de métadonnées pour rendre l'authentification LDAP transparente pour l'utilisateur, c'est-à-dire qu'aucun suffixe n'est nécessaire pour router l'authentification vers LDAP.

Pour cela, positionner la variable PRIMARYPROVIDERDOMAIN :

```
-set PRIMARYPROVIDERDOMAIN DOMAINEFRANCE
```

La valeur de PRIMARYPROVIDERDOMAIN correspond à la valeur définie dans la variable AUTHPROVIDERDOMAIN :

```
-set AUTHPROVIDERDOMAIN LDAP:DOMAINEFRANCE
```

```
-set PRIMARYPROVIDERDOMAIN DOMAINEFRANCE
```

Ainsi, avec cette configuration, il n'est plus nécessaire de préciser @DOMAINEFRANCE pour que l'authentification soit réalisée par LDAP.

Avant de positionner un domaine d'authentification par défaut, il est important d'avoir une bonne connaissance des utilisateurs devant se connecter à l'environnement SAS. En effet, si dans votre entreprise, les utilisateurs SAS peuvent être identifiés soit via un annuaire, soit via un compte local, positionner le domaine de l'annuaire par défaut entraîne la nécessité d'utiliser un suffixe spécifique (@host) pour orienter l'authentification au niveau local, plutôt qu'au niveau du l'annuaire par défaut. Pour plus de précisions, vous pouvez vous référer au chapitre 3. *Configuration des utilisateurs dans SAS pour un usage dans SAS Enterprise Guide*.

3. CONFIGURATION DES UTILISATEURS DANS SAS POUR UN USAGE DANS SAS® ENTERPRISE GUIDE®

La configuration de vos utilisateurs dans les métadonnées dépend de la façon dont vous souhaitez que vos utilisateurs se connectent à SAS.

Tous les utilisateurs de SAS doivent y être référencés. Un utilisateur peut avoir plusieurs comptes différents. Il peut y avoir une déclaration de compte pour une authentification avec LDAP, et une autre pour une authentification machine.

Reprenons le contexte de l'exemple du chapitre 2.3.2 et examinons en détail la configuration de l'utilisateur « nhousset » dans les métadonnées.

Pour bien comprendre la façon dont vous devez configurer vos métadonnées, nous allons partir de la fenêtre d'authentification de SAS Enterprise Guide et, à partir de là, présenter la configuration dans les métadonnées.

- 1) Dans notre premier cas de test, l'utilisateur souhaite se connecter, par défaut à son compte local, sans passer par l'authentification LDAP :

Modifier le profil

Nom :
localhost - lev 3

Description :

Machine
☒ Distant ☐ Locale Port :
 localhost 8563

Utilisateur : nhousset Mot de passe : <mot de passe>

Domaine d'authentification :

Dans les métadonnées, l'utilisateur doit être configuré de cette manière :

Propriétés de Nouvel utilisateur

Général Groupes et Rôles Comptes Droits

Comptes définis pour Nouvel utilisateur

Domaine d'authentification :	Identifiant	Mot de passe
DefaultAuth	nhousset	

- 2) Deuxième cas, l'utilisateur souhaite se connecter à SAS en utilisant son identité LDAP, la configuration dans SAS Enterprise Guide donnera donc :

Utilisateur : nhousset@DOMAINEFRANCE Mot de passe : <mot de passe>

Domaine d'authentification :

Dans les métadonnées (via la SAS® Management Console), l'utilisateur doit être configuré de cette manière :

Propriétés de Nouvel utilisateur

Général Groupes et Rôles Comptes Droits

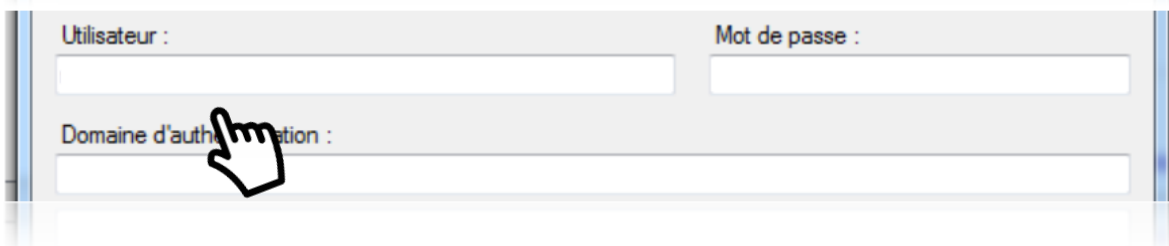
Comptes définis pour Nouvel utilisateur

Domaine d'authentification :	Identifiant	Mot de passe
DefaultAuth	nhousset@DOMAINEFRANCE	

La valeur du suffixe **@DOMAINEFRANCE** est la même que celle définie dans la variable **AUTHPROVIDERDOMAIN** du fichier sasv9.cfg.

Si aucun compte n'est créé avec cette identité **@DOMAINEFRANCE**, et comme nous l'avons vu au chapitre 2.3, l'utilisateur sera associé au profil PUBLIC.

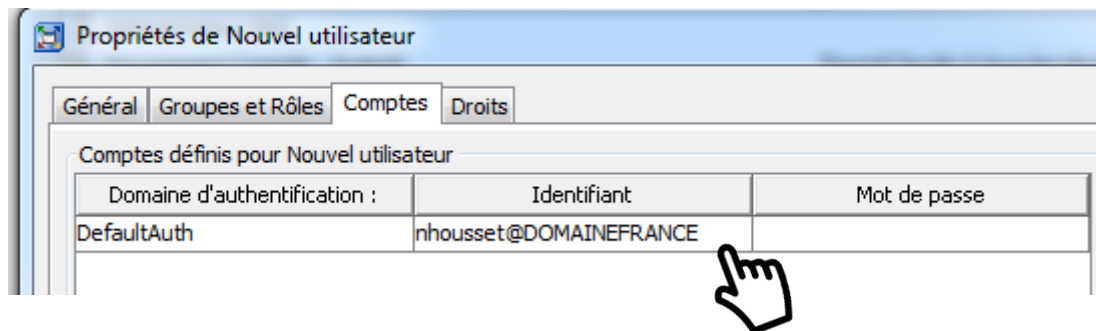
- 3) L'utilisateur souhaite se connecter à SAS via son identité LDAP, mais sans avoir à spécifier le suffixe **@DOMAINEFRANCE** :



Utilisateur : Mot de passe :

Domaine d'authentification :

Dans les métadonnées, l'utilisateur doit être configuré de cette manière :



Domaine d'authentification :	Identifiant	Mot de passe
DefaultAuth	nhousset@DOMAINEFRANCE	

Mais pour que ce routage vers LDAP fonctionne par défaut, il faut avoir spécifié la variable **PRIMARYPROVIDERDOMAIN** (chapitre 2.3.3). Dans notre exemple, la variable est à positionner à **DOMAINEFRANCE**.

- 4) Dernier cas de figure, l'utilisateur souhaite se connecter via son compte local alors que l'authentification LDAP par défaut est activée. Dans ce cas, il faut indiquer au serveur de métadonnées de ne pas router l'authentification vers LDAP, c'est-à-dire contourner l'authentification par défaut. Pour cela, l'utilisateur « nhousset » doit suffixer avec **@HOST** :



Utilisateur : Mot de passe :

Domaine d'authentification :

En ajoutant le suffixe **@HOST**, nous indiquons au serveur de métadonnées de ne pas tenir compte des directives LDAP et d'effectuer l'authentification via l'hôte, et donc d'utiliser un compte local.

Tableau récapitulatif

Login utilisateur	Service d'authentification	Comment le login est stocké dans les métadonnées
utilisateur	LDAP	Utilisateur@domaineldap
utilisateur@domaineldap	LDAP	Utilisateur@domaineldap
utilisateur@mauvaisdomaine	LDAP	Utilisateur@mauvaisdomaine@domaineldap
utilisateur@saspw	Authentification interne SAS	Pas de login pour les SAS internal account
utilisateur@host	Hôte du serveur de metadonnées	utilisateur

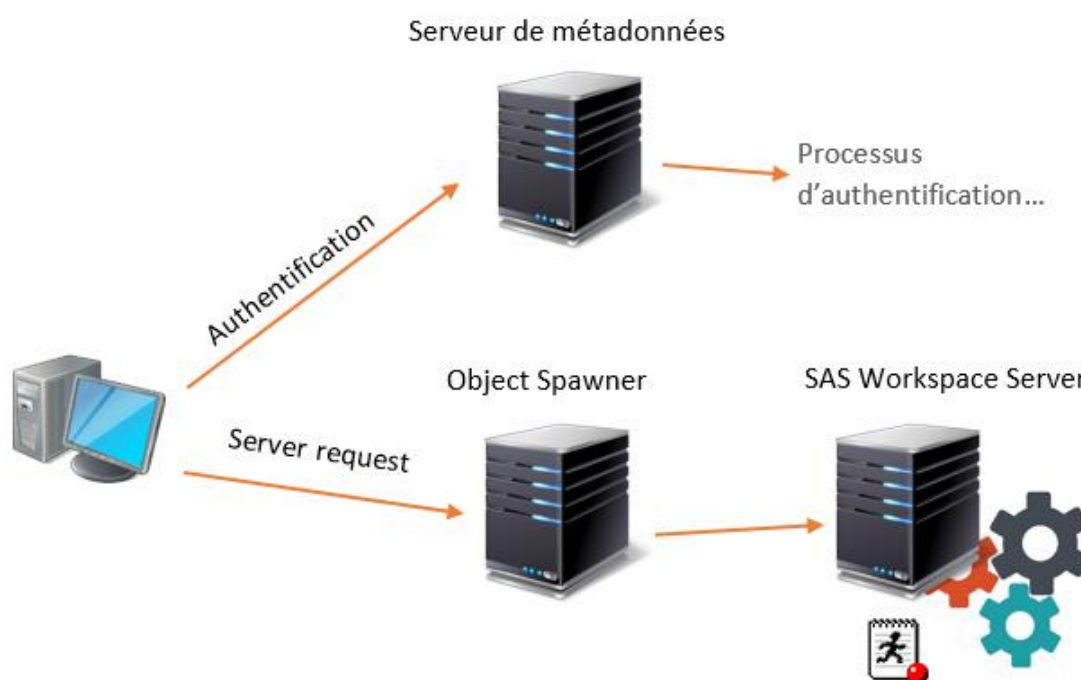
4. LIER UNE IDENTITE EXTERNE A UN COMPTE PHYSIQUE

4.1. Présentation de la problématique.

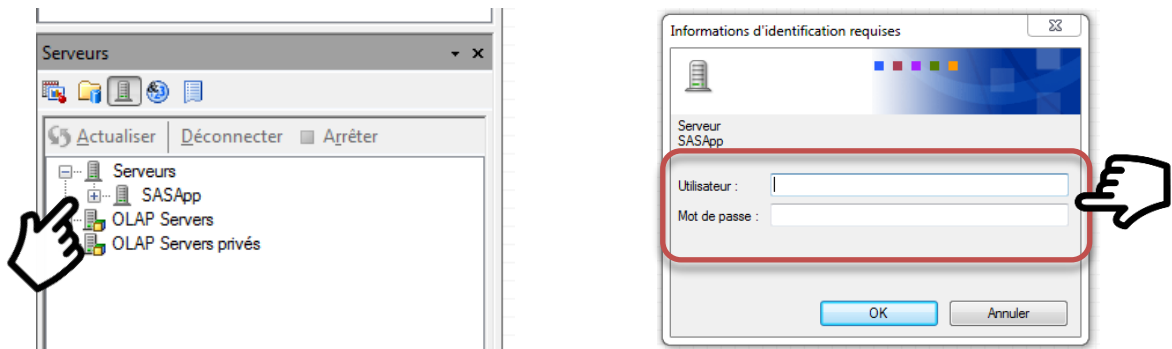
Comme nous l'avons vu au début de cet article, déléguer le mécanisme d'authentification à un service d'annuaire distant présente des avantages. Il n'est plus nécessaire de gérer les utilisateurs au niveau du serveur. Il n'y a donc plus besoin de créer un compte local pour chaque utilisateur.

Mais cela pose des problèmes dans le fonctionnement de SAS. En effet, l'utilisation de SAS Enterprise Guide nécessite l'utilisation d'un compte machine pour pouvoir démarrer et exécuter des sessions SAS. Vous n'êtes pas sans savoir que lorsqu'un utilisateur exécute du code SAS, un processus (Workspace Server) est exécuté.

Ce processus est exécuté par l'utilisateur associé à l'identité dans les métadonnées :



Avec une authentification LDAP, il n'y a pas d'utilisateur local. Il est impossible de lancer le Workspace Server et donc d'exécuter du code SAS. Vous serez confronté au problème suivant : une fois authentifié via LDAP et connecté au serveur de métadonnées, il vous sera impossible d'exécuter du code SAS sur le serveur :



Pour résoudre cette situation, plusieurs solutions sont envisageables, nécessitant des étapes de configurations supplémentaires afin d'associer un compte système aux identités LDAP.

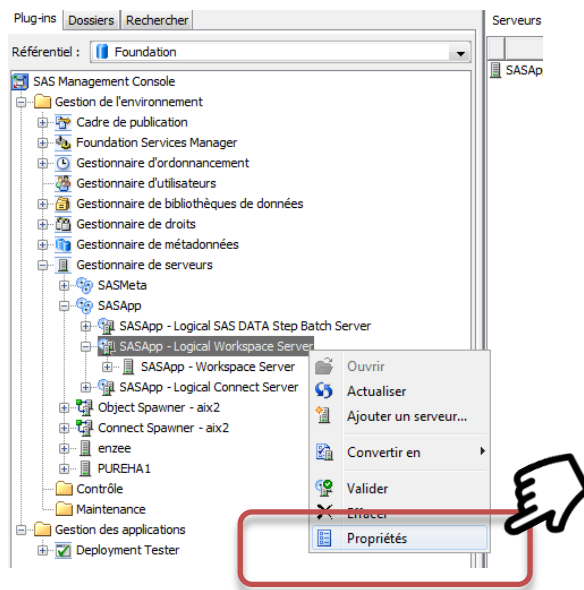
Dans les chapitres suivants nous vous présentons deux méthodes possibles.

4.2. L'authentification de jeton pour le Workspace Server.

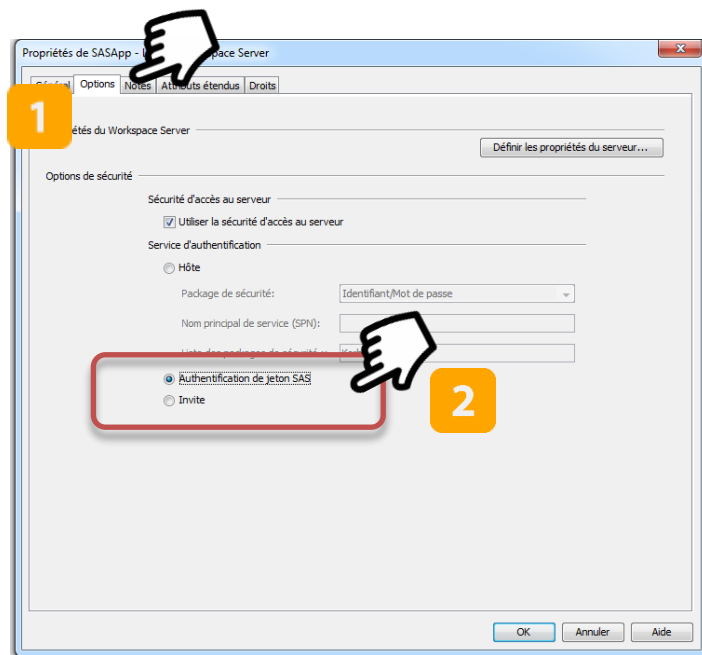
Avec l'authentification de jeton ([SAS Token authentication](#)), le serveur de métadonnées génère et valide un jeton d'identité à usage unique pour chaque événement d'authentification. Ainsi, aucun compte système individuel n'est nécessaire, et aucun mot de passe utilisateur n'est stocké dans les métadonnées. A noter également, qu'avec ce mécanisme, les informations d'identification transmis au serveur ne sont pas réutilisables dans une autre session.

4.2.1. Configuration de l'authentification de jeton

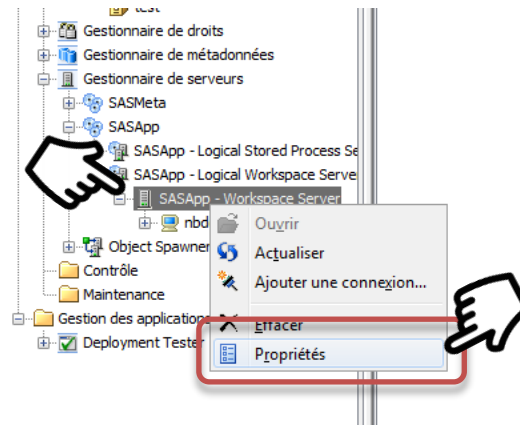
- Ouvrez une session sur SAS® Management Console avec un utilisateur possédant les droits d'administration des utilisateurs.
- Dans l'onglet Plug-ins, développez le **Gestionnaire de serveurs** et le serveur de votre choix (par exemple, **SASApp**). Puis, cliquez sur le serveur logique (par exemple, **SASApp - Logical Workspace Server**) et sélectionnez **Propriétés** :



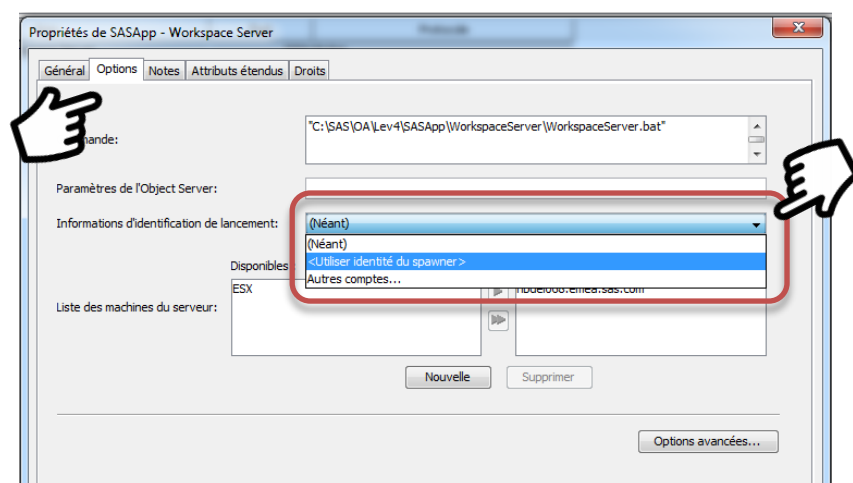
- Dans l'onglet **Options**, sélectionnez **SAS authentification par jeton**. Cliquez sur OK pour enregistrer ce paramètre.



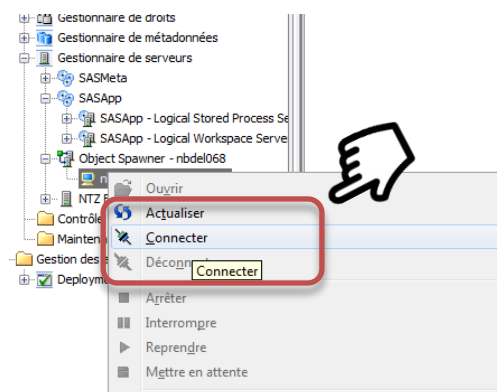
- Une fois validé, retournez dans l'onglet Plug-ins, sélectionnez le **SASAPP – Workspace Server** et cliquez sur **Propriétés** :



- Dans l'onglet Options, dans la liste déroulante **Informations d'identification de lancement**, sélectionnez une connexion, puis validez en cliquant sur OK.



- Pour que les modifications prennent effet, actualisez l'Objet Spawner :



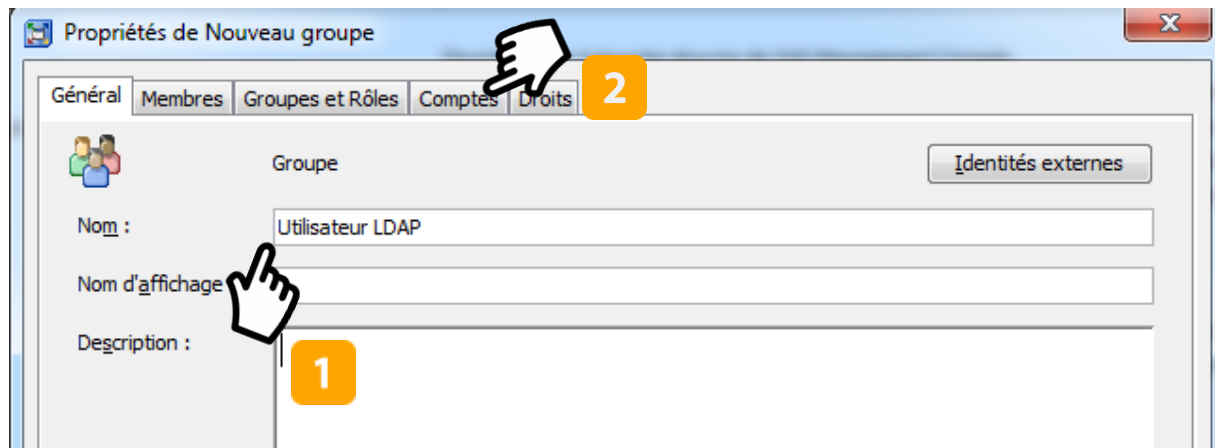
4.3. Création d'un groupe d'utilisateurs

L'implémentation de l'authentification par jeton est une solution pour lier, rapidement et facilement, les comptes utilisateur avec un compte système. Toutefois, cette solution est limitée. En effet, tous les utilisateurs utilisent le même compte, il n'est donc pas possible de définir des droits spécifiques au niveau système pour interdire l'accès à certaines ressources.

Une seconde solution consiste à créer des groupes d'utilisateurs et, pour chaque groupe, associer un compte système qui sera utilisable par les utilisateurs LDAP définis préalablement :

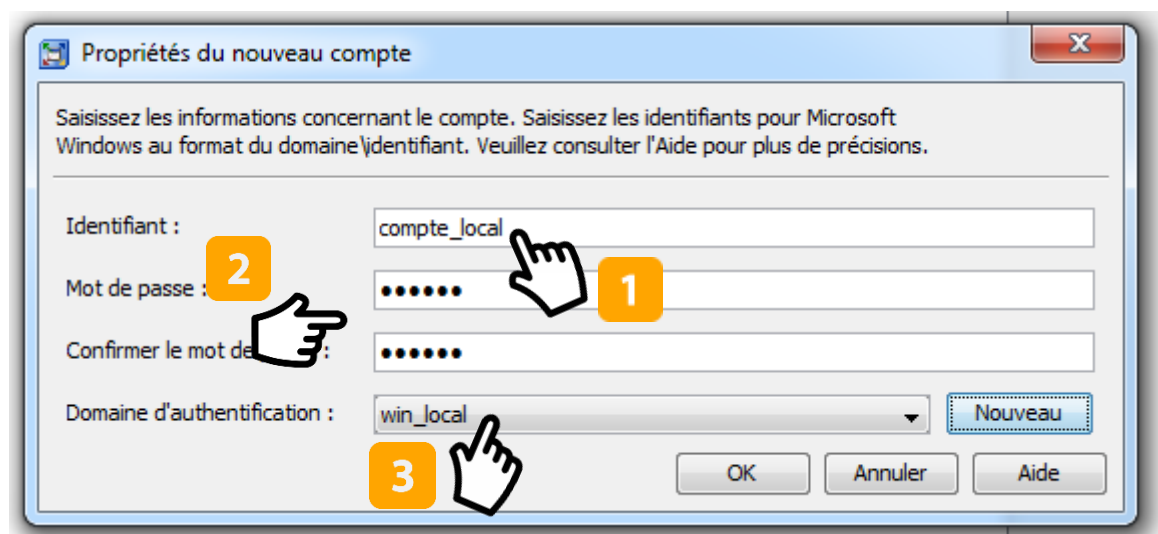
La définition du groupe d'utilisateurs devra contenir les informations suivantes :

- 1 – Spécifiez un nom pour votre groupe. Ici, Utilisateur LDAP
- 2 – Puis cliquez sur l'onglet « Comptes »

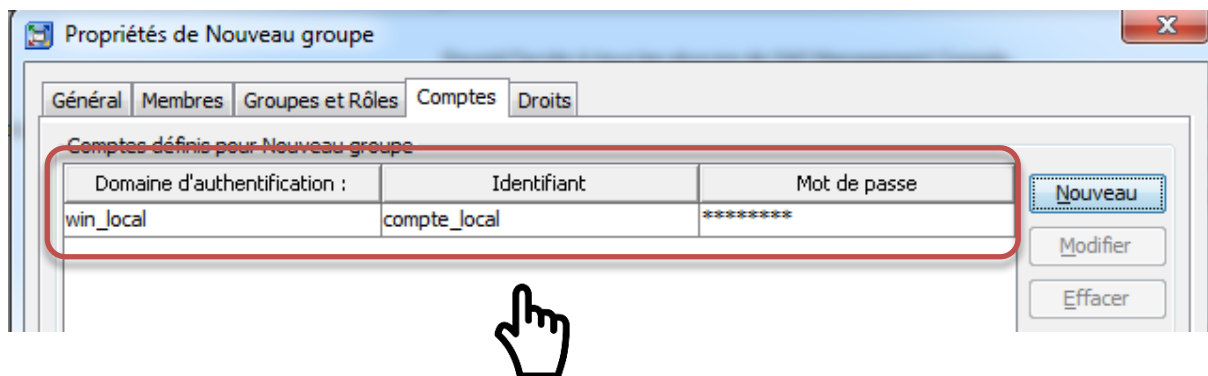


Cliquez ensuite sur le bouton « Nouveau » pour saisir les propriétés du nouveau compte.
Puis :

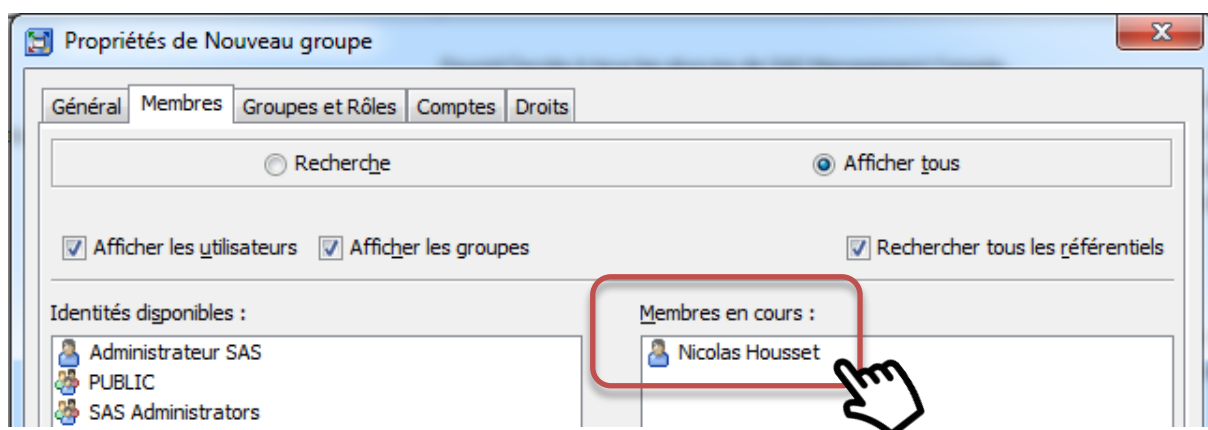
- 1 – Indiquez l'identifiant de connexion d'un compte local au serveur.
- 2 – Indiquez le mot de passe lié à cet utilisateur. Ce mot de passe sera stocké dans les métadonnées
- 3 – Créez un nouveau domaine de connexion appelé, par exemple, « win_local » pour identifier les comptes utilisateurs locaux au serveur hébergeant le serveur SAS.



Suite à cette saisie, vous obtenez le résultat suivant :



Puis, attachez vos utilisateurs LDAP à ce groupe :



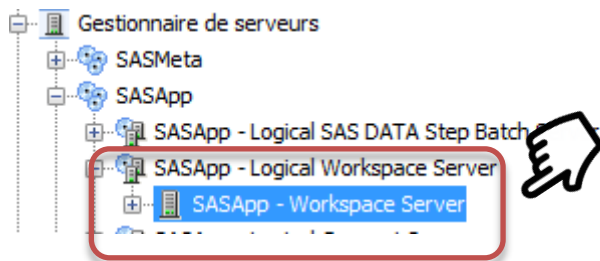
4.4. Modification de la configuration du Workspace Server

Nous avons maintenant deux domaines d'authentification :

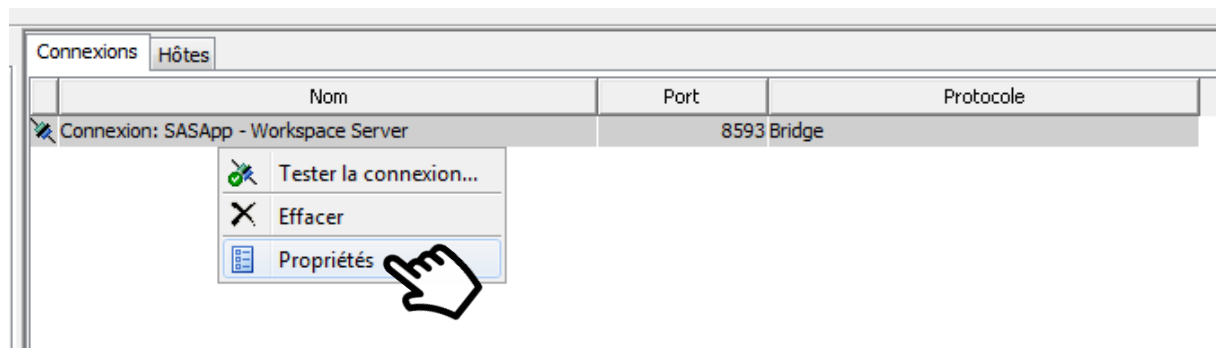
- DefaultAuth
- win_local

Le domaine DefaultAuth contient les identités LDAP et le domaine win_local contient les informations d'authentification d'un compte physique local au serveur SAS.

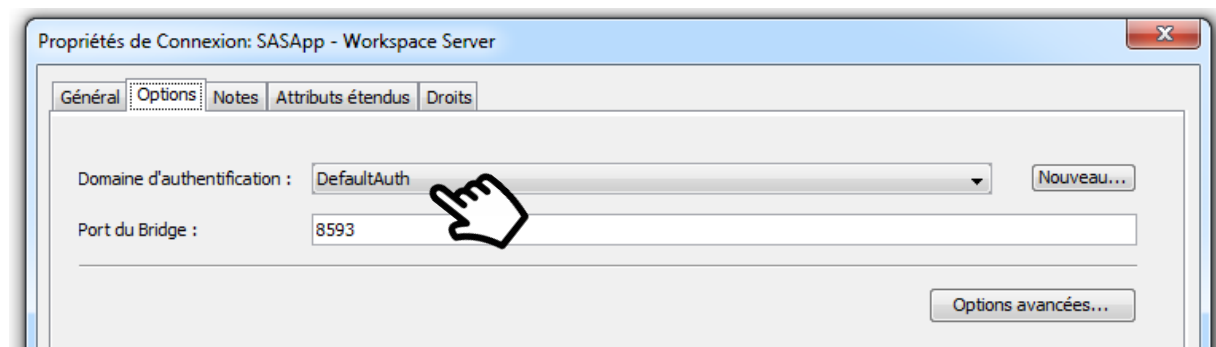
Comme je l'ai déjà indiqué, lorsque le Spawner va initialiser un Workspace Server, il va s'authentifier au serveur en utilisant le compte utilisateur défini dans DefaultAuth puis lancer un processus SAS avec ce compte utilisateur.

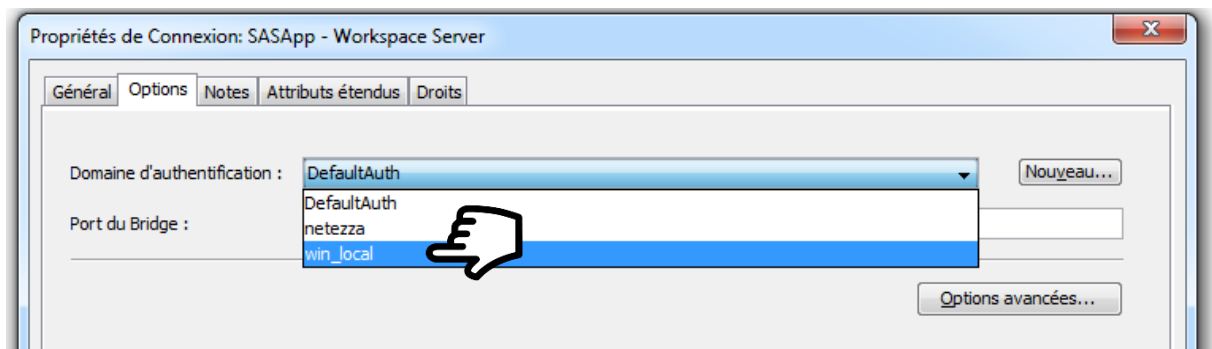


Puis dans la fenêtre de droite, rendez-vous dans les propriétés :



Dans l'onglet « Options » nous allons modifier le « Domaine d'authentification » :





En choisissant « win_local », on indique à l'object Spawner d'utiliser un compte défini sur le domaine d'authentification SAS « win_local » plutôt que sur le domaine « DefaultAuth » pour lancer le Worspace Server.

5. TESTER ET VALIDER SA CONNEXION

La validation de la configuration est une étape importante, si ce n'est primordiale, lors de la mise en place de l'authentification.

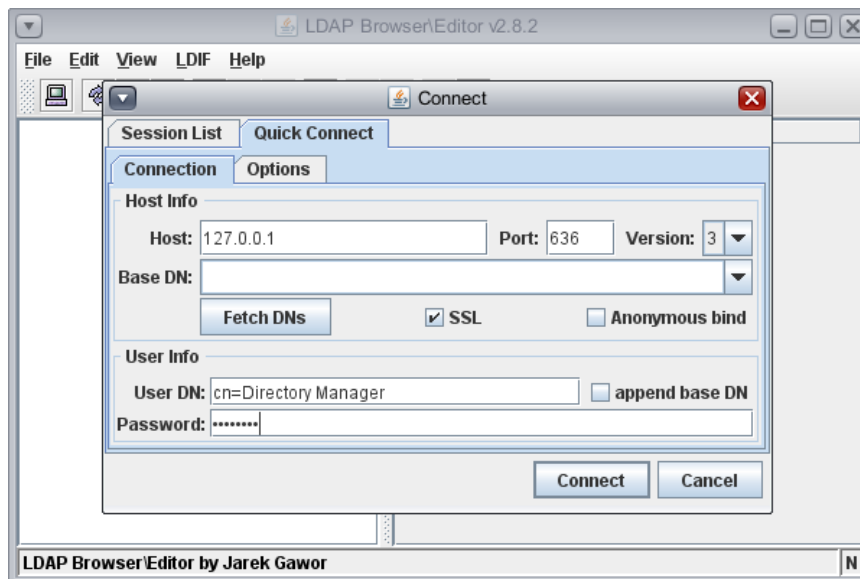
Dans le chapitre suivant nous allons aborder plusieurs méthodes pour valider sa connexion et vérifier le bon fonctionnement de l'authentification. Notez que ces différents protocoles de tests s'appliquent si vous utilisez une authentification via un annuaire ou via un autre mécanisme (hôte ou compte internet SAS). Aussi, nous vous proposons 4 approches différentes pour valider l'authentification :

- Une validation, en dehors de SAS,
- L'utilisation de la PROC METAOPERATE,
- L'utilisation de la PROC PERMTEST,
- L'utilisation de l'outil SASUMGMT.

Enfin, à la fin de ce chapitre, nous expliquons comment activer les traces, étape utile pour une investigation efficace.

5.1. Valider la connexion au serveur LDAP, en dehors de SAS

La première étape consiste à valider la connexion en dehors de SAS, soit en utilisant un outil tiers permettant de vous connecter à un serveur LDAP à distance, soit en soumettant du code SAS pour simuler et valider la connexion au serveur LDAP, sans passer par la couche Métadonnées.



Exemple de test de connexion à LDAP avec l'outil JAVA LDAPBrowser Editor

5.2. Utilisation de la procédure METAOPERATE

En cas de problème de connexion, la première chose à faire est de valider la connexion en dehors de SAS afin de s'assurer que « tout fonctionne correctement ». Puis, nous pouvons tenter une validation « dans » SAS. Pour tester l'authentification simplement, nous allons utiliser la [PROC METAOPERATE](#). Cette procédure permet d'effectuer toute sorte de tâches administratives associées à un serveur de métadonnées SAS (ou un cluster de serveur de métadonnées). Globalement, la syntaxe est la suivante :

```
PROC METAOPERATE ACTION=value;
```

Dans notre cas, nous allons utiliser l'action "STATUS".

La PROC METAOPERATE ACTION=status renvoie des informations sur les propriétés et l'état du serveur de métadonnées.

Pour exécuter cette action, il est nécessaire de se connecter au serveur en positionnant des options de connexion, telles que le login ou le mot de passe. Cette procédure SAS est donc un moyen simple de valider ses identifiants de connexion.

Voici un exemple de syntaxe, à exécuter dans une session SAS :

```
proc metaoperate
```

```
server="localhost"
port =8561
userid="sasadm@saspw"
password="sasadm"
action=status;
run;
```

L'exécution doit retourner, dans le journal SAS, les informations suivantes :

```
NOTE: Server localhost SAS Version is 9.4.
NOTE: Server localhost SAS Long Version is 9.04.01M3P06242015.
NOTE: Server localhost Operating System is X64_7PRO.
NOTE: Server localhost Operating System Family is WIN.
NOTE: Server localhost Operating System Version is Service Pack 1.NOTE:
Server localhost Client is sasadm@saspw.
NOTE: Server localhost Metadata Model is Version 16.01.
NOTE: Server localhost is PAUSED on 17 mars 2016 13 h 56.
```

Il est possible de valider la connexion avec un compte LDAP, par exemple :

```
proc metaoperate
server="localhost"
port =8561
userid="nicolas.housset@domaineLDAP"
password="nicolas"
action=status;
run;
```

Le résultat vous permet de valider ou non les identifiants. Si vous obtenez un message d'erreur, celui-ci vous permettra d'effectuer un premier diagnostic sur l'origine de l'erreur.

Par exemple :

```
ERROR: Invalid credentials
ERROR: Access denied.
ERROR: Error authenticating user nicolas.housset@domaineldap in function
LogonUser. Error 1326
(Échec d'ouverture de session : nom d'utilisateur inconnu ou mot de passe
incorrect.)
```


5.3. Validation de son authentification via la proc permtest

Lorsque vous utilisez SAS dans un environnement de type UNIX, vous pouvez utiliser la [PROC PERMTEST](#). La PROC PERMTEST est un outil que nous pouvons qualifier de « bas niveau » pour tester l'authentification. Vous pouvez l'utiliser pour déterminer l'origine de vos problèmes d'authentification.

```
./sas -path ./utilities/src/auth -nodms
```

```
Proc permtest;  
run;
```

Ce qui donne :

```
Authentication Test  
Enter userid: nhousset  
Enter password:  
Authentication successful.  
  
Permissions Test  
Enter a scratch filename:  
/tmp/testfile  
Test file written successfully.
```

5.4. Utilisation de l'outil SASUMGMT

Utilisez l'utilitaire SASUMGMT pour valider que le nom d'un utilisateur et son mot de passe sont bien valides et peuvent être utilisés pour l'authentification SAS.

L'utilitaire SASUMGMT est stocké dans le répertoire SASROOT d'une installation SAS standard. Voici un exemple d'utilisation :

```
/SASFoundation/9.4/utilities/bin/sasumgmt -u sasdmo -p pass_sas_demo -v
```

Ce qui affiche :

NOTE: [sasumgmt: SASUMGT_STATUS_OK]

Si vous indiquez un mauvais mot de passe, le message suivant s'affiche :

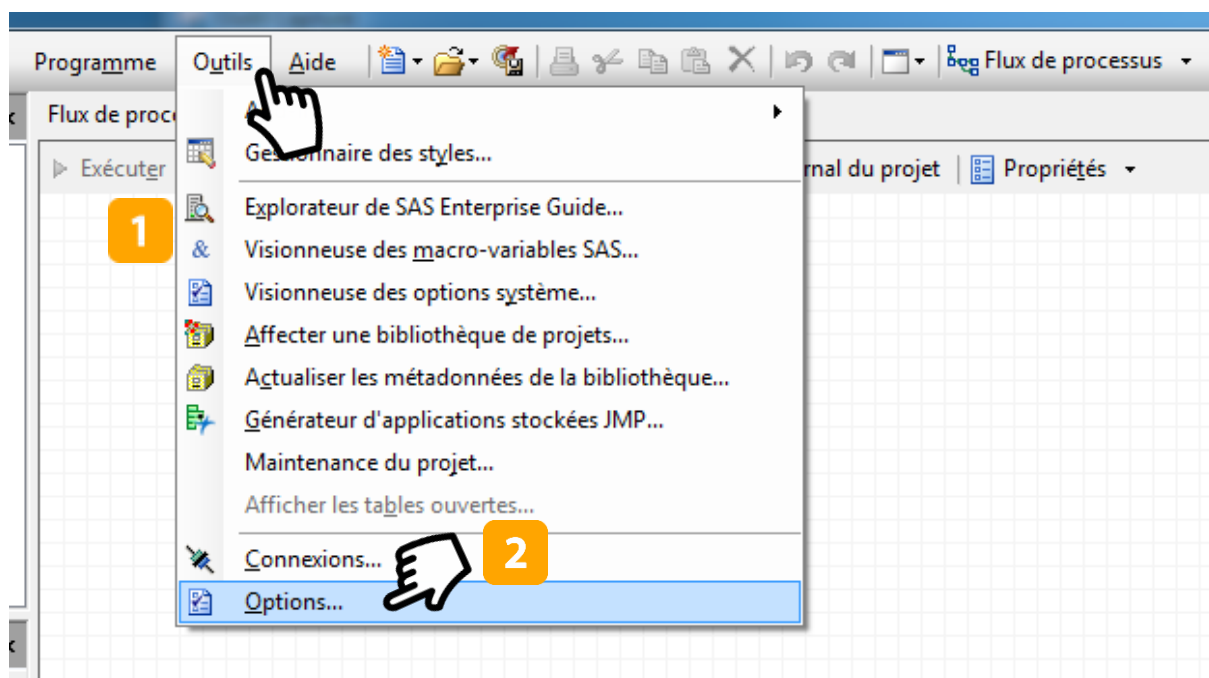
NOTE: [sasumgmt: SASUMGT_STATUS_ACCESS_DENIED]
NOTE: Access denied.

Pour plus d'informations concernant le fonctionnement de cet outil ainsi que la liste de messages d'erreurs, la documentation est disponible sur le site du support SAS ([SASUMGMT Utility](#)).

5.5. Activation des traces SAS Enterprise Guide

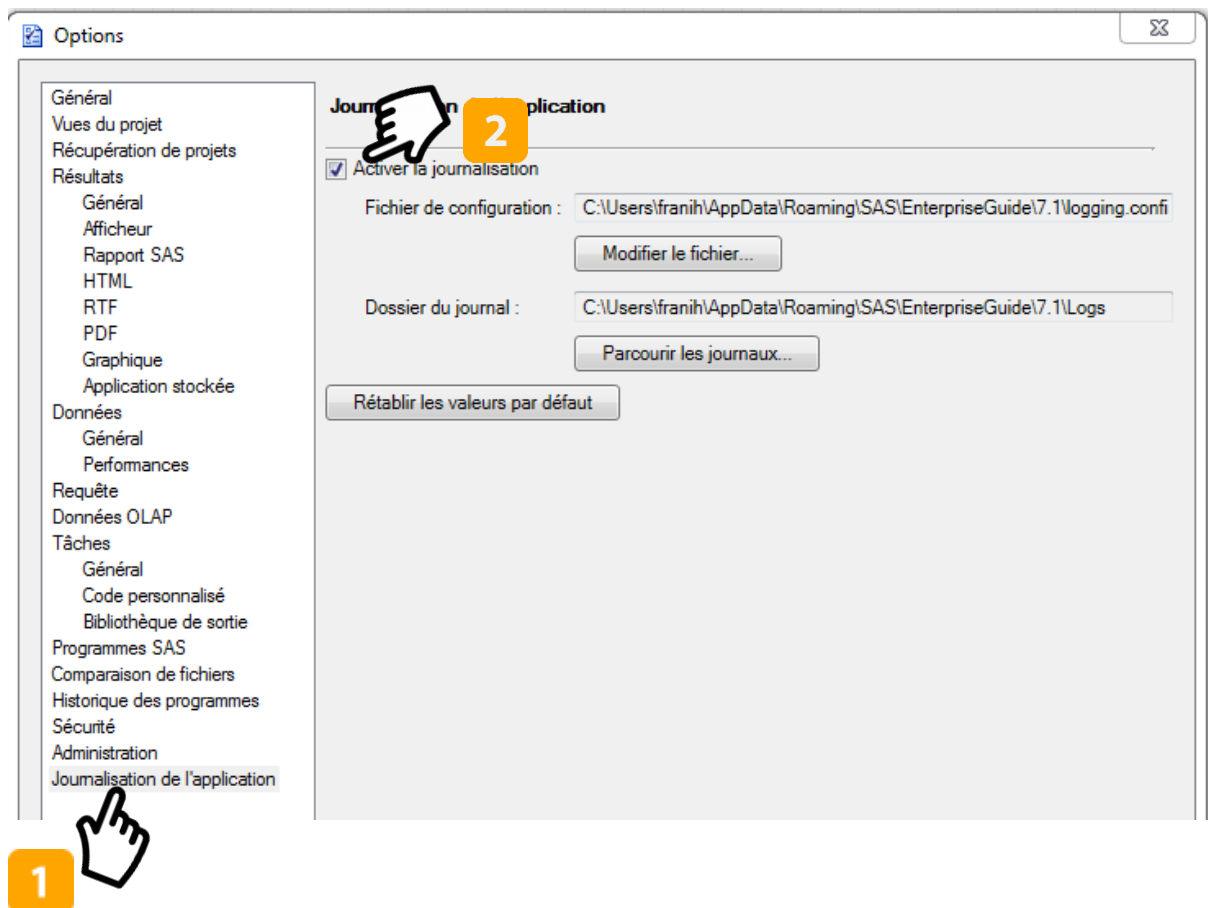
A partir de la version 7.1 de SAS Enterprise Guide, il est possible d'activer les traces via les options de l'application. Voici les étapes à suivre :

- 1 – Cliquez sur « **outils** » dans la barre de menu.
- 2 - Cliquer sur « **Options** »



Dans la fenêtre d'options :

- 1- Cliquez sur « **Journalisation de l'application** »
- 2- Puis cochez « **Activer la journalisation** »



Vous obtenez alors la cause de l'erreur de connexion ainsi que la « stack java » complète :

```
System.Runtime.InteropServices.COMException (0x8007052E): <?xml version="1.0"
?><Exceptions><Exception><SASMessage severity="Error">Access
denied.</SASMessage></Exception><Exception><SASMessage severity="Error">Error
authenticating user sasdemo@DOMAINEFRANCE in function LogonUser. Error 1326 (Échec
d'ouverture de session : nom d'utilisateur inconnu ou mot de passe
incorrect.)</SASMessage></Exception></Exceptions>
```

```
SASObjectManager.ObjectFactoryMulti2Class.CreateObjectByServer(String Name, Boolean
synchronous, IServerDef pIServerDef, String LoginName, String Password)
```

5.6. Activer les traces SAS Metadataserver

Pour [activer les traces côté serveur](#), soumettez le code suivant dans une session SAS (en ayant remplacé les variables *host-name*, *port-number*, *user-ID* et *password*) :

```

proc iomoperate;
    connect host='host-name'
            port=port-number
            user='user-ID'
            pass='password';

    set attribute category="Loggers" name="App" value="Info";
    set attribute category="Loggers" name="App.LDAP" value="Trace";
    set attribute category="Loggers" name="App.OMI.Security"
value="Trace";
    set attribute category="Loggers" name="App.tk.LDAP" value="Trace";
    set attribute category="Loggers" name="App.tk.eam" value="Trace";
    set attribute category="Loggers" name="Audit" value="Info";
    set attribute category="Loggers" name="Audit.Authentication"
value="Trace";
    set attribute category="Loggers" name="Audit.Meta.Security"
value="Trace";
    set attribute category="Loggers" name="IOM" value="Info";

    set attribute category="Properties" name="IOM.JnlStrMax"
value="1000000";
    set attribute category="Properties" name="IOM.JnlLineMax"
value="1000000";

quit;

```

Pour lister les logger activés, vous pouvez soumettre le code ci-dessous :

```

proc iomoperate;
    connect host='host-name'
            port=port-number
            user='user-ID'
            pass='password';

    list stime;
    list information;
    list log configuration;
    list attributes category="Loggers";
    list attributes category="Properties";

quit;

```

Maintenant que vous avez soumis ce code, des traces détaillées sont visibles dans le fichier journal du serveur de métadonnées :

```

InteropServices 2016-06-07T10:06:38,993 TRACE [00000265] :Système@NBDEL068 - Create
Authenticated Token
2016-06-07T10:06:38,993 TRACE [00000265] :Système@NBDEL068 - Client
connection id: 10

```

```

2016-06-07T10:06:38,993 DEBUG [00000265] :Système@NBDEL068 - User/Pass
authentication for user sasdemo@DOMAINEFRANCE
2016-06-07T10:06:38,993 TRACE [00000265] :Système@NBDEL068 - User:
sasdemo, domain: DOMAINEFRANCE
2016-06-07T10:06:38,993 TRACE [00000265] :Système@NBDEL068 - Calling auth
provider...2016-06-07T10:06:38,993 TRACE [00000265] :Système@NBDEL068 - Windows OS
auth provider called
2016-06-07T10:06:38,993 TRACE [00000265] :Système@NBDEL068 - UPN name
sasdemo@DOMAINEFRANCE being authenticated
2016-06-07T10:06:45,795 INFO [00000265] :Système@NBDEL068 - Error authenticating
user sasdemo@DOMAINEFRANCE in function LogonUser. Error 1326 (Échec d'ouverture de
session : nom d'utilisateur inconnu ou mot de passe incorrect.).
2016-06-07T10:06:45,795 DEBUG [00000265] :Système@NBDEL068 - Provider failed:
80bfd100

```

Dans le cadre d'un débogage LDAP, une information est intéressante dans la log ci-dessus. Nous constatons une erreur de connexion. Notre utilisateur devrait s'authentifier via le serveur LDAP, toutefois le journal contient les deux lignes suivantes :

```

2016-06-07T10:06:38,993 TRACE [00000265] :Système@NBDEL068 - Calling auth
provider...
2016-06-07T10:06:38,993 TRACE [00000265] :Système@NBDEL068 - Windows OS
auth provider called

```

Cela nous permet de constater que le routage n'est pas celui attendu. L'authentification utilisée par le serveur de métadonnées est l'authentification au niveau du serveur hôte alors qu'avec l'utilisation du domaine DOMAINEFRANCE, nous aurions souhaité que ce soit le serveur LDAP qui se charge du processus d'authentification.

```

2016-06-07T10:06:38,993 DEBUG [00000265] :Système@NBDEL068 - User/Pass
authentication for user sasdemo@DOMAINEFRANCE
2016-06-07T10:06:38,993 TRACE [00000265] :Système@NBDEL068 - User:
sasdemo, domain: DOMAINEFRANCE

```



En utilisant cette méthode, les SAS loggers activés ne le seront plus au redémarrage du serveur de métadonnées.

5.6.1. Exemple de traces et analyse détaillée

Dans le cas d'une authentification via LDAP, vous devriez avoir les traces ci-dessous.

D'abord, le journal indique les informations d'authentification soumises au serveur de métadonnées :

```
User/Pass authentication for user nicolas.housset@DOMAINEFRANCE
User: nicolas.housset, domain: DOMAINEFRANCE
```

Puis le serveur vérifie que le domaine existe bien, et en fonction de ce domaine, redirige l'authentification vers le service idoine :

```
Domain match found
Calling auth provider...
Entering LDAP provider for user nicolas.housset
```

Le serveur de métadonnée vérifie les variables positionnées côté SAS, s'assure que le service LDAP est bien disponible puis s'y connecte :

```
Found LDAP_HOST: ldap-france.monserveur.fr
Did not find LDAP_PORT
Missing LDAP_PORT, defaulting to 389
...
ldap_open (ldap-france.monserveur.fr, 389)
ldap_create
```

Une fois la connexion au serveur effectuée, le serveur de métadonnée cherche l'utilisateur dans l'annuaire distant :

```
Searching for DN for user nicolas.housset
```

Puis, valide l'authentification et se déconnecte de l'annuaire :

```
request 1 done
res_errno: 0, res_error: <>, res_matched: <>
ldap_free_connection
ldap_send_unbind
```

Enfin, le serveur de métadonnées prend le relais et vérifie que l'utilisateur authentifié via LDAP existe dans les métadonnées (ou si ce n'est pas le cas, lui affecte un profil PUBLIC) :

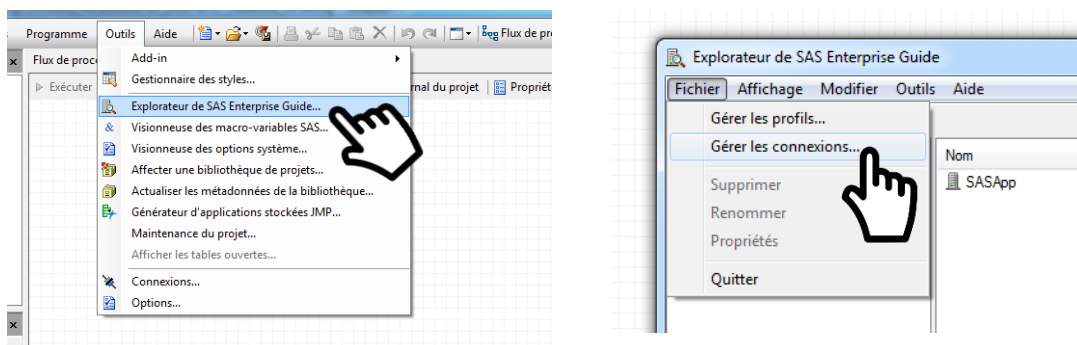
```
New client connection (3) accepted from server port 8563 for user
Nicolas.housset@DOMAINEFRANCE
```

En cas d'erreur, vous pourriez avoir le message suivant dans les traces :

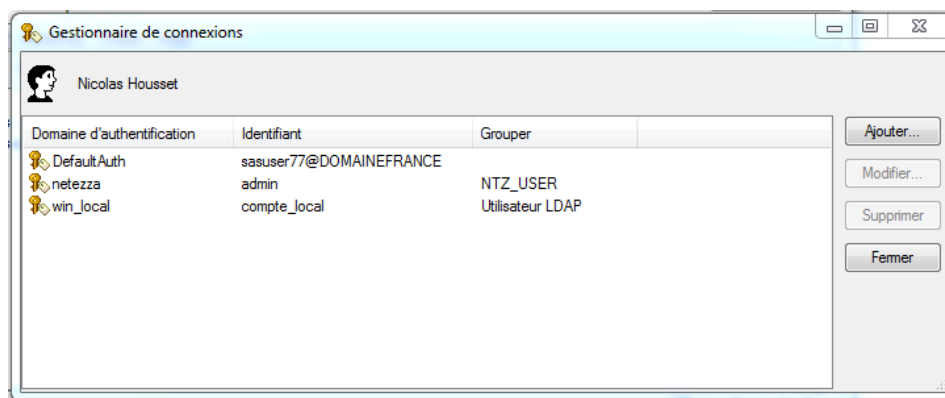
```
Bind to ou=people,dc=sas,dc=com failed getting user DN
Provider failed: 80bfd100
```

5.7. Visualiser les identités associées à votre compte

Dans la phase de résolution de problème, il peut s'avérer nécessaire de visualiser les différentes identités associées à son compte SAS. Une fois connecté au serveur de métadonnées, via SAS Enterprise guide, vous disposez d'une fonctionnalité permettant de lister les identités et profils de connexion :



Vous pouvez alors visualiser les informations du compte connecté au serveur de métadonnées :



6. IMPLEMENTATION AVANCEE

Maintenant que vous êtes à l'aise sur le fonctionnement de SAS avec un service d'authentification distant, nous pouvons vous présenter certaines configurations avancées et vous montrer les possibilités offertes en matière de connexions.

6.1. Les nouveautés SAS 9.4

Comme à chaque nouvelle version, la dernière apporte son lot de nouveautés. A partir de SAS 9.4 M3, il est possible de relier le serveur de métadonnées à plusieurs annuaires LDAP.

Il est également possible de s'authentifier à plusieurs groupes LDAP au sein d'un même serveur LDAP.

Deux nouvelles variables ont été ajoutées, AD_TIMEOUT et LDAP_TIMEOUT, pour définir la durée de la première tentative de connexion avant son expiration.

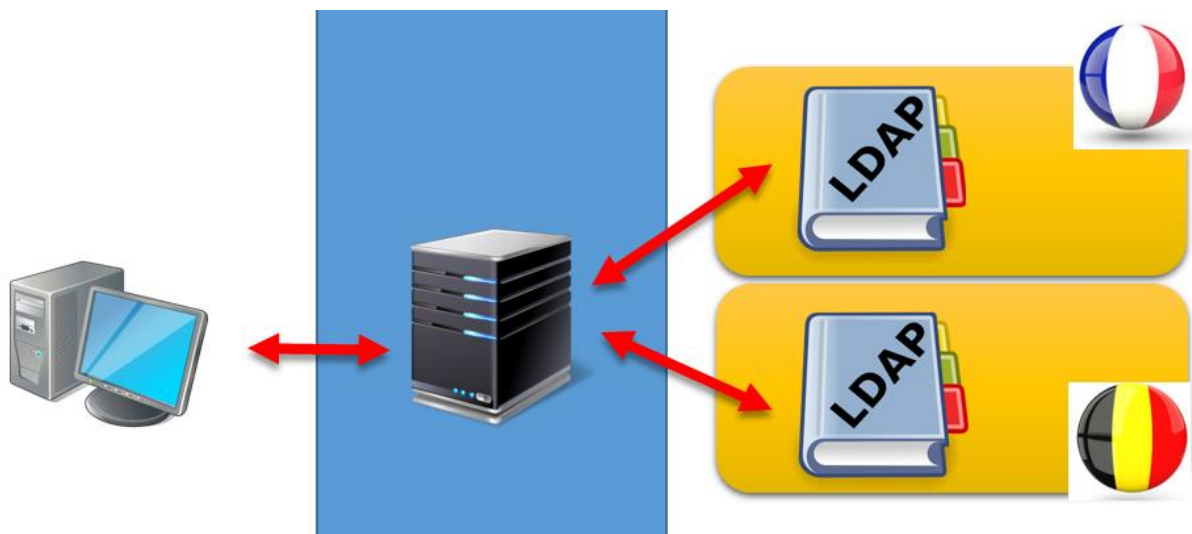
Enfin, vous pouvez utiliser la variable d'environnement AD_STYLE pour limiter l'activité d'authentification à une unique tentative d'ouverture de session.

Pour la mise en œuvre de ces nouveautés, vous pouvez vous référer aux chapitres suivants.

6.2. Relier SAS à plusieurs annuaire LDAP

SAS peut reconnaître plusieurs serveurs LDAP en tant que fournisseurs d'authentification, indépendamment du fait qu'il existe des relations de confiance entre ces serveurs. Dans notre exemple, notre environnement SAS possède des utilisateurs en France et en Belgique.

Nous partons du principe que chaque pays possède son propre annuaire LDAP :



Pour permettre à SAS d'utiliser ces deux annuaires LDAP indépendants, il faut fournir les informations de chaque serveur par le biais de variables d'environnement associées.

Pour indiquer quel serveur LDAP est utilisé par telle variable, ajoutez le nom du serveur au nom de la variable. Par exemple, dans notre cas, nous pouvons définir des variables spécifiques au serveur comme suit:

```
set LDAP_HOST_FR=france.annuaire.masociete.com
set LDAP_HOST_BE=belgique.annuaire.masociete.com
```


Pour activer la possibilité de différencier plusieurs groupes LDAP, vous devez d'abord définir la variable d'environnement LDAP_BASE_SUFFIXES qui enregistre les noms des groupes LDAP.

Dans notre cas :

```
LDAP_BASE_SUFFIXES=FR BE
```

Vous pouvez ensuite définir les variables d'environnement supplémentaires pour établir une base DN et un attribut de recherche d'identité pour chaque groupe.

```
LDAP_BASE_FR=France...
LDAP_IDATTR_FR=CN
LDAP_BASE_BE=OU=Belgique...
LDAP_IDATTR_BE=samaccountname
```

Le suffixe de chaque variable spécifique de groupe correspond à une valeur qui est déjà enregistrée dans la variable d'environnement LDAP_BASE_SUFFIXES.

Comme les valeurs propres au serveur LDAP (Nom, adresse, port), les propriétés spécifiques à un groupe LDAP sont héritées si elles ne sont pas explicitement définies.

Ce type de configuration permet-il la bascule d'un serveur sur l'autre en cas de défaillance d'un des deux annuaires ?

Non. D'un point de vue SAS, s'il y a une perte de connexion avec l'un des serveurs LDAP, aucun mécanisme de bascule sur l'autre n'est possible.

Pour plus d'informations sur les différentes options, vous pouvez consulter la documentation « [How to Configure Direct LDAP Authentication > Advanced Configurations](#) »

6.3. Gérer le délai de connexion

Lorsque vous essayez de vous connecter à un serveur LDAP, un timeout par défaut est positionné à 30 secondes. Concrètement, si le serveur LDAP ne répond pas (routine LDAPS_OPEN_CALL) dans ce laps de 30 secondes, l'authentification sort en erreur.

Il est possible d'étendre la limite de temps au-delà de 30 secondes en réglant la variable d'environnement LDAP_TIMEOUT à une valeur supérieure à 30.

Pour cela, ajoutez la ligne suivante dans le fichier sasv9_usemods.cfg du serveur de métadonnées :

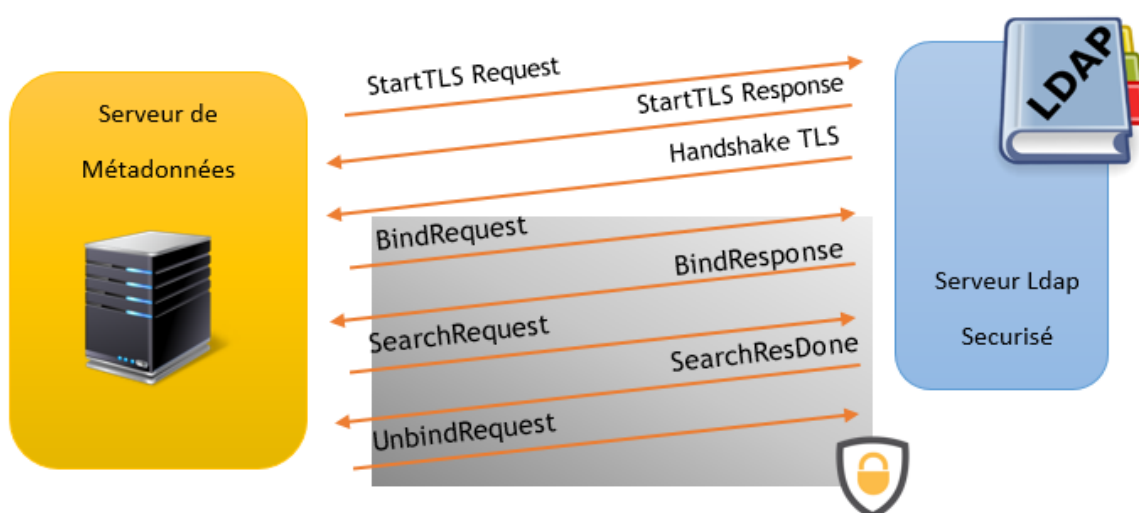
```
-set LDAP_TIMEOUT 120
```



La valeur de LDAP_TIMEOUT doit être un entier supérieur à zéro.

6.4. Se connecter à un serveur LDAP sécurisé via SSL

Nous allons maintenant voir les étapes à suivre pour connecter son serveur de métadonnées à un annuaire LDAP sécurisé. Le protocole Secure Sockets Layer (SSL) utilise une combinaison de cryptage de clé publique et clé symétrique. Point important et souvent source de problème et d'erreur, une session SSL commence toujours par un échange de messages appelé la négociation SSL :



Le protocole de transfert permet au serveur de s'authentifier auprès du client à l'aide de techniques de clé publique, puis autorise le client et le serveur à coopérer pour la création de clés symétriques utilisées pour le cryptage, le décryptage et la détection des fraudes au cours de la session qui suit.

Le tableau ci-dessous explique chaque étape de cette négociation :

Message	Signification
StartTLS Request	Demande de création d'une connexion chiffrée par une couche TLS émanant du client.
StartTLS Response	Réponse de la demande de création d'une connexion par couche TLS
Handshake TLS	L'échange de clés : Le client vérifie la validité du certificat serveur. Si le certificat est valide, il génère une clé maître, la chiffre à l'aide de la clé publique du serveur et la lui envoie. Les données échangées par la suite entre le client et

le serveur sont chiffrées et authentifiées à l'aide de clés dérivées de la clé maître.

bindRequest Demande la connexion à un annuaire

bindResponse Réponse à la demande d'authentification

searchRequest Demande à effectuer une recherche en fonction d'un filtre donné

searchResDone Message indiquant la fin des réponses à une recherche

unbindRequest Demande de déconnexion/fin de session

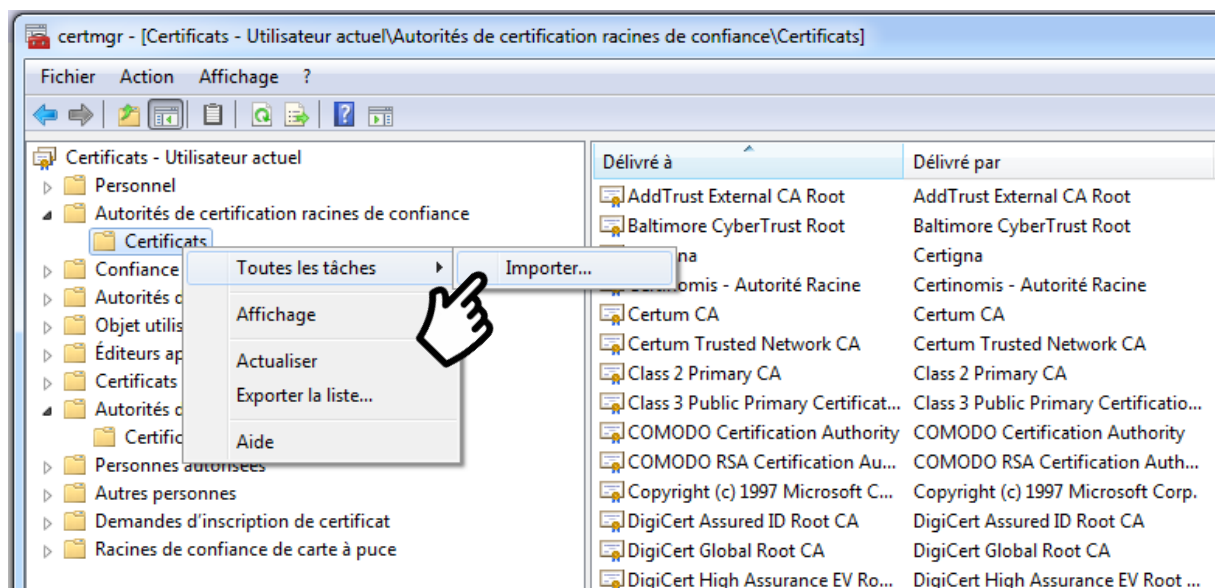
Voyons maintenant comment configurer SAS.

Nous devons d'abord préciser au serveur de métadonnées que la connexion au serveur LDAP sera via TLS :

```
-set LDAP_TLSMODE 1
```

Ensuite, nous devons nous assurer que SAS connaisse le certificat d'autorité ayant signé le serveur LDAP.

- Si votre serveur de métadonnées fonctionne sous environnement Windows, vous devez vous assurer que le certificat de l'autorité est enregistré. Si vous devez ajouter un certificat, ouvrez le gestionnaire de certificat (**certmgr.msc**) puis cliquez sur le dossier dans lequel vous voulez importer le certificat, cliquez sur le menu Action, pointez sur Toutes les tâches puis cliquez sur Importer :



- Sous Unix, il n'y a pas d'outil équivalent au gestionnaire de certificat. Pour que SAS puisse connaître l'autorité, vous devez ajouter la variable SSLCALISTLOC en spécifiant le chemin d'accès au certificat de l'autorité :

```
-SSLCALISTLOC "/etc/ldap/CA.crt"
```

7. EN CAS DE PROBLEME

7.1. Les problèmes les plus fréquents

7.1.1. Messages d'erreurs

Vous trouverez, ci-dessous, les messages d'erreurs les plus fréquents que vous pourriez rencontrer. Pour chaque type d'erreur, nous vous suggérons la cause possible et les pistes à suivre pour la résoudre.

```
ERROR: Unable to contact the LDAP server.
```

```
ERROR: Invalid credentials
ERROR: Access denied.
ERROR: Unable to contact the LDAP server
```

Ces deux messages d'erreur peuvent avoir plusieurs causes.

- Vérifiez les informations de connexion (nom ou adresse IP de votre serveur LDAP, port..)
- Vérifiez que le serveur LDAP ou Active directory est bien opérationnel.
- Vérifiez que le serveur LDAP n'est pas trop surchargé et met du temps à répondre. Dans ce cas, il est possible de modifier le timeout, via l'option LDAP_TIMEOUT (source : <http://support.sas.com/kb/48/238.html>)

```
ERROR: Invalid credentials
ERROR: Access denied.
ERROR: Error authenticating user nicolas.housset@DOMAINEFRANCE in function LogonUser.
Error 1326 (Échec d'ouverture de session : nom d'utilisateur inconnu ou mot de passe incorrect.).
```

Comme pour l'erreur précédente, ce type de d'erreur peut avoir plusieurs causes.

- Vérifiez le mot de passe LDAP.
- Vérifiez le domaine associé à l'utilisateur.

Pour être certain de la cause, vous pouvez activer les traces afin d'obtenir plus de détails sur la source du message.

```
Exception type: SAS.EG.SDS.SDSEException
SAS Message: [Error] Client sas@nbdel068 does not have permission to use server SASApp
- Workspace Server (A5QZJL8B.AY000004).
```

- Ce message survient après le processus d'authentification. En effet, vous pouvez très bien être authentifié via l'annuaire, mais l'utilisateur n'existe pas dans les métadonnées SAS. Il hérite donc d'un profil PUBLIC ne lui permettant pas d'exécuter, par exemple, du code dans SAS Enterprise Guide. Aussi, vérifiez que l'utilisateur LDAP ou AD existe bien dans les métadonnées SAS.

```
ERROR: Invalid credentials
ERROR: Access denied.
ERROR: Unable to contact the LDAP server.
ERROR: Possible cause: Server certificate not found, port not SSL enabled
ERROR: LDAP SSL Message ldapsNegotiate() failed -2143301629.
ERROR: The tcpSockWrite call failed. The system error is 'An invalid pointer parameter was used.'
```

- Vérifiez que le port SSL est actif sur le serveur LDAP ou Active Directory

```
ERROR: Invalid credentials
ERROR: Access denied.
ERROR: Unable to contact the LDAP server.
ERROR: Possible cause: Server certificate not found, port not SSL enabled
ERROR: LDAP SSL Message ldapsNegotiate() failed -2139099128.
ERROR: Windows SSL error -2146893019 (0x80090325) occurred at line 2389, the error message
is "La chaîne de certificats a été fournie par une autorité qui n'est pas approuvée."
```

```
ERROR: Invalid credentials
ERROR: Access denied.
ERROR: Unable to contact the LDAP server.
ERROR: Possible cause: Server certificate not found, port not SSL enabled
ERROR: LDAP SSL Message ldapsNegotiate() failed -2139099128.
ERROR: OpenSSL error 336134278 (0x14090086) occurred in SSL_connect/accept at
line 5377, the error message is "error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed".
```

La connexion au serveur LDAP est opérationnelle (le serveur répond). Toutefois, l'échange des clés, pour sécuriser les échanges, ne fonctionne pas :

- Vérifiez la présence du certificat SSL
- Vérifiez la chaîne de certification.

Ces vérifications peuvent être effectuées avec l'outil tiers Openssl.

7.2. Autres problèmes

Question : L'authentification au serveur de métadonnées est impossible. Comment déterminer l'origine du problème ?

Réponse : Vérifiez si la connexion fonctionne avec un compte n'utilisant pas l'authentification LDAP ou AD. Si la connexion fonctionne avec un compte interne (@saspw) et un compte local (@host), vérifiez si l'ensemble des comptes LDAP ou AD sont impactés ou si seulement quelques comptes sont impactés. Vérifiez ensuite la connexion à l'annuaire, en dehors de SAS.

Question : Je suis bien connecté au serveur de métadonnées mais impossible d'ouvrir SASApp. Pourquoi ?

Vérifiez que le compte connecté et authentifié via l'annuaire distant possède bien une identité dans les métadonnées SAS et que celui-ci n'hérite pas d'un profil PUBLIC.

7.3. Éléments à transmettre au Support Clients

Si vous rencontrez des problèmes lors de l'implantation de votre authentification LDAP et que la solution ne se trouve pas dans cet article, vous pouvez nous écrire à support@sas.com, en attachant à votre message l'erreur reçue et le maximum d'informations concernant le contexte de votre problématique.

8. LIENS UTILES

Quelques liens utiles pour aller plus loin et approfondir les notions abordées dans cet article :

- [Usage Note 39891: Using PROC PERMTEST to diagnose UNIX host authentication issues in SAS® 9.2 and later releases](#)
- [Summary of Methods for LDAP Integration](#)
- [How to Configure Direct LDAP Authentication](#)
- [Authentication Utilities](#)

9. CONCLUSION

Vous l'avez compris, en lisant cet article, les possibilités offertes par l'externalisation de l'authentification sont nombreuses et intéressantes. La mise en œuvre d'un tel projet nécessite une excellente connaissance des besoins, de l'architecture du système d'information dans lequel s'inscrit SAS, mais également une bonne coordination entre les différents intervenants.

Aussi, il est primordial de ne pas négliger une bonne préparation dans la mise en œuvre de cette authentification, afin d'éviter les mauvaises surprises.

Nicolas HOUSSET

Consultant Support Clients SAS France