Version	Auteur : modifications	Date
1.0	Rédaction initiale	04/09/2017
2.0	AA : Modifications mineures	16/05/2019

SOMMAIRE

1 - Introduction _____ 2
2 – Le SSO _____ 2
2.1 - Pré-requis pour KERBEROS / SPNEGO _____ 2
2.1.1 – L'authentification du service Apache Tomcat _____ 2
2.1.2 – La configuration du fichier krb5.conf _____ 2
2.1.2 – La configuration du fichier web.xml _____ 3
2.1.3 – Enregistrement des SPN (Service Principal Names) _____ 4
2.1.4 – Configuration de DamarisRM _____ 4
2.1.5 – Arrêt / relance de Tomcat _____ 4
2.1.6 – Configuration des postes de travail _____ 4
2.1.7 – Configuration des navigateurs _____ 5
3 – La synchronisation AD (Active Directory) _____ 6
3.1 – Le paramétrage de la tâche d'importation _____ 6

1 - Introduction

Ce document décrit les différentes étapes pour la mise en place du mécanisme Single Sign On (SSO) avec le protocole KERBEROS / SPNego.

2 – Le SSO

Le mécanisme SSO consiste à reconnaître automatiquement l'utilisateur dans Damaris RM à partir de son poste de travail sur lequel il s'est connecté et lance le lien URL.

Le lien URL vers Damaris RM est déterminé par le nom du serveur et le nom de l'application.

2.1 - Pré-requis pour Kerberos / SPNEGO

Voici les éléments permettant le paramétrage de ce mécanisme.

Une fois le mécanisme SSO mis en place, il suffit de lancer une URL de type :
http://NomServeur/DamarisRM

Voici les pré-requis techniques nécessaires pour configurer ce protocole :

- La mise en place de la synchronisation de la liste des utilisateurs avec Active Directory (AD). Ce point est déjà acquis
- Eléments de connexion à Active Directory :
  - Nom utilisateur Serveur AD
  - Mot de passe Serveur AD
  - Adresse KDC (Key Distribution Service)
  - Nom de domaine par défaut
  - Fully Qualified Domain Name (FQDN)

2.1.1 – L'authentification du service Apache Tomcat

Nous devons être capables de lancer le service Apache Tomcat sur le serveur Damaris avec le nom d'utilisateur et mot de passe AD. Ainsi, le service Apache Tomcat sera à même d'accéder à la base Active Directory.

Pour cela, sur le serveur Microsoft Windows, allez dans la gestion des services et modifiez la connexion du service Apache Tomcat.

2.1.2 – La configuration du fichier krb5.conf

Mettez à jour le fichier situé dans le répertoire :
tomcat/webapps/DamarisRM/WEB-INF/config/krb5.conf

Voici un contenu d'exemple :

```
[libdefaults]
        default_realm = DAMARIS.SA
```

```
        default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
        default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
        permitted_enctypes   = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc

[realms]
        DAMARIS.SA  = {
                kdc = 10.27.41.160
                default_domain = DAMARIS.SA
}

[domain_realm]
        .damaris.am = DAMARIS.SA
```

Les modifications concernent l'adresse KDC et le nom domaine par défaut.

2.1.2 – La configuration du fichier web.xml

Ce fichier ce trouve dans le répertoire tomcat/webapps/DamarisRM/WEB-INF

Voici les modifications à apporter :

Tout d'abord, enlevez la mise en commentaires de toute la section correspondante à KERBEROS.

```
<!-- ================================== -->
<!-- FILTERS FOR KERBEROS AUTHENTICATION -->
<!-- .................................. -->
<!--          USE ONLY FOR BIELD        -->
<!-- ================================== -->
<filter>
  <filter-name>SpnegoHttpFilter</filter-name>
  <filter-class>net.sourceforge.spnego.SpnegoHttpFilter</filter-class>
  <init-param>
    <param-name>spnego.allow.basic</param-name>
    <param-value>true</param-value>
  </init-param>
  <init-param>
    <param-name>spnego.allow.localhost</param-name>
    <param-value>true</param-value>
  </init-param>
  <init-param>
    <param-name>spnego.allow.unsecure.basic</param-name>
    <param-value>true</param-value>
  </init-param>
  <init-param>
    <param-name>spnego.login.client.module</param-name>
    <param-value>spnego-client</param-value>
  </init-param>
  <init-param>
    <param-name>spnego.krb5.conf</param-name>
    <param-value>webapps/DamarisRM/WEB-INF/config/krb5.conf</param-value>
  </init-param>
  <init-param>
    <param-name>spnego.login.conf</param-name>
    <param-value>webapps/DamarisRM/WEB-INF/config/login.conf</param-value>
  </init-param>
  <init-param>
    <param-name>spnego.preauth.username</param-name>
    <param-value>NomUtilisateurAD</param-value>
  </init-param>
  <init-param>
    <param-name>spnego.preauth.password</param-name>
```

```
    <param-value>MotDePasseAD</param-value>
  </init-param>
  <init-param>
    <param-name>spnego.login.server.module</param-name>
    <param-value>spnego-server</param-value>
  </init-param>
  <init-param>
    <param-name>spnego.prompt.ntlm</param-name>
    <param-value>true</param-value>
  </init-param>
  <init-param>
    <param-name>spnego.logger.level</param-name>
    <param-value>10</param-value>
  </init-param>
</filter>
<filter-mapping>
 <filter-name>SpnegoHttpFilter</filter-name>
 <url-pattern>/*</url-pattern>
</filter-mapping>
```

2.1.3 – Enregistrement des SPN (Service Principal Names)

Pour chaque alias du serveur, lancez l'utilitaire setspn.exe présent dans le répertoire Support Tools (Ou System32) de Windows.

Voici quelques exemples de lancements de cet utilitaire :

setspn.exe -A HTTP/NomServeur NomUtilisateurAD

Où

- NomServeur est le nom du serveur de domaine AD
- NomUtilisateurAD est le nom de l'utilisateur que vous avez défini dans le fichier web.xml

2.1.4 – Configuration de DamarisRM

A ce stade, configurez Damaris RM pour accepter les appels SSO.

Pour cela, modifiez le fichier tomcat/webapps/DamarisRM/WEB-INF/config/dgs3g.properties

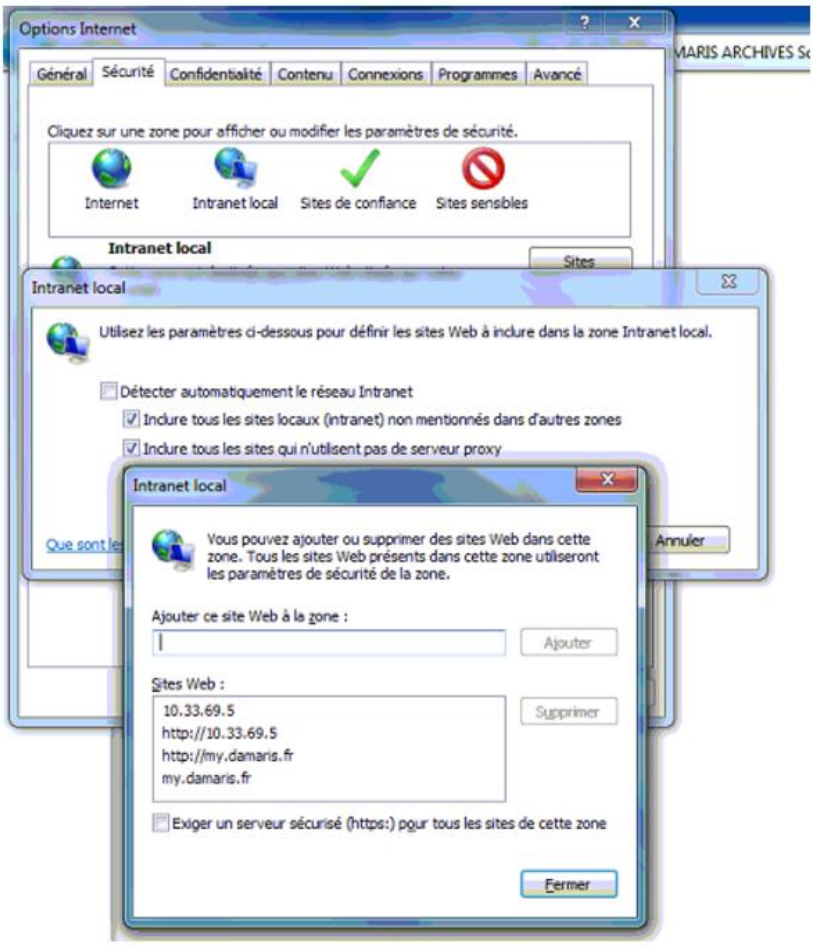
```
isSsoUsed=true
```

2.1.5 – Arrêt / relance de Tomcat

Relancez le service Apache Tomcat pour que les modifications soient prises en compte.

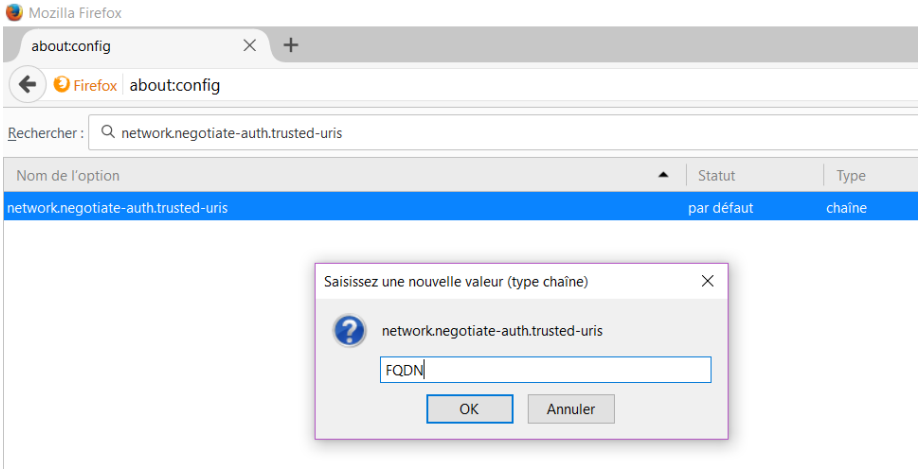
2.1.6 – Configuration des postes de travail

Ajoutez le lien URL vers Damaris RM comme une adresse Intranet :



2.1.7 – Configuration des navigateurs

Configurez les navigateurs pour prendre en compte l'adresse FQDN.
Voici un exemple dans le navigateur FireFox.



3 – La synchronisation AD (Active Directory)

Pour compléter le processus, il convient d'effectuer une synchronisation des comptes utilisateurs de manière périodique.

Cette tâche consiste à exporter la liste des utilisateurs depuis votre base Microsoft Active Directory et de les importer dans Damaris RM.

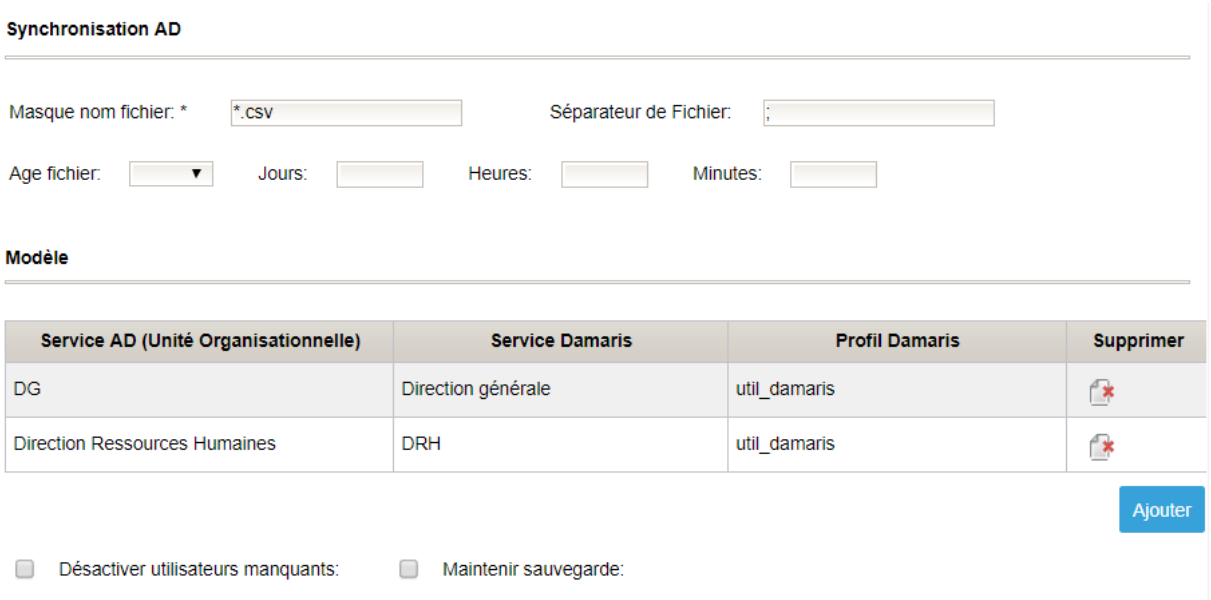
3.1 – Le paramétrage de la tâche d'importation

Un fichier exporté depuis Microsoft Active Directory contient les informations concernant les utilisateurs et leur appartenance à un ou des groupes (Au sens Active Directory).

Pour cela, il convient d'établir un lien entre les groupes AD et les services et profils Damaris RM.

La tâche planifiée Damaris RM comporte un tableau qu'il convient de remplir pour pouvoir créer un lien logique entre les groupes AD et les services / profils Damaris.

Voici une copie d'écran illustrant le paramétrage de cette tâche :



NB : Seuls les utilisateurs habilités pourront se connecter à Damaris RM. Une fois leur identifiant de connexion (Login) reconnu dans Damaris RM, la solution évalue leurs droits d'accès dans le système.

La case à cocher « Désactiver utilisateurs manquants » vous permet de ne plus donner d'accès aux utilisateurs qui auront été supprimé dans Microsoft Active Directory.