9 chemin du Jubin - 69 570 DARDILLY	Projet : Damaris RM	
	Paramétrage du Single Sign On Protocole Kerberos / SPNego	Page 1 sur 6

Version	Auteur : modifications	Date
1.0	Rédaction initiale	04/09/2017

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	2
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

9 chemin du Jubin - 69 570 DARDILLY	Projet : Damaris RM	
	Paramétrage du Single Sign On Protocole Kerberos / SPNego	Page 2 sur 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 : <u>http://NomServeur/DamarisRM</u>

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/DaamrisRM/WEB-INF/config/krb5.conf

Voici un contenu d'exemple :



d d P	default_tkt_enctypes default_tgs_enctypes permitted_enctypes	= aes128-cts = aes128-cts = aes128-cts	rc4-hmac rc4-hmac rc4-hmac	des3-cbc-shal des3-cbc-shal des3-cbc-shal	des-cbc-md5 des-cbc-md5 des-cbc-md5	des-cbc-crc des-cbc-crc des-cbc-crc
[realms]						
D	AMARIS.SA = {					
	kdc = 10.27.4 default_doma	41.160 in = D <mark>AMA</mark> RIS.	SA			
}						
[domain_r	realm]					
•	damaris.am = DAMARI	S.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>spneqo.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>
```

9 chemin du Jubin - 69 570 DARDILLY	Projet : Damaris RM	
	Paramétrage du Single Sign On Protocole Kerberos / SPNego	Page 4 sur 6

<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>
<filter-mapping></filter-mapping>
<filter-name>SpnegoHttpFilter</filter-name>
<url-pattern>/*</url-pattern>

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

2.1.4 – Configuration de DamarisRM

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

Pour cela, modifiez le fichier tomcat/webapps/DaamrisRM/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 :



iénéral Sé	curité Confidentiaité Contenu Connexions Prog	grammes Avancé	MARIS ARCHIV
		Contraction Contraction Contraction	
Cliquez sur	une zone pour afficher ou modifier les paramètres de :	sécurité.	
		\odot	
Inter	et Intranet local Sites de confiance Sites	s sensibles	
	tranet local		
-	the second se	Sites	52
itranet loca		Part and a second	
Ch. U5	sez les paramètres ci-dessous pour définir les sites We	eb à inclure dans la zone Intra	anet local.
-			
123	Détecter automatiquement le réseau Intranet		
	Inclure tous les sites locaux (intranet) non mention	nnés dans d'autres zones	
	Indure tous les sites qui n'utilisent pas de serveur	DEDXX	
	Indure tous les sites qui n'utilisent pas de serveur	proxy	
	Inclure tous les sites qui n'utilisent pas de serveur	proxy	
	Indure tous les sites qui n'utilisent pas de serveur Intranet local	proxy	
	Indure tous les sites qui n'utilsent pas de serveur Intranet local Vous pouvez ajouter ou supprimer des s	proxy	Annier
Que sont le	Indure tous les sites qui n'utilsent pas de serveur Intranet local Vous pouvez ajouter ou supprimer des si zone. Tous les sites Web présents dans	proxy	Annuler
Que sont le	Indure tous les sites qui n'utilsent pas de serveur Intranet local Vous pouvez ajouter ou supprimer des s zone. Tous les sites Web présents dans les paramètres de sécurité de la zone.	proxy X ites Web dans cette cette zone utiliseront	Annuler
Que sont le	Indure tous les sites qui n'utilsent pas de serveur Intranet local Vous pouvez ajouter ou supprimer des s zone. Tous les sites Web présents dans les paramètres de sécurité de la zone.	proxy X ites Web dans cette cette zone utiliseront	Arnuler
Que sont le	Indure tous les sites qui n'utilsent pas de serveur Intranet local Vous pouvez ajouter ou supprimer des si zone. Tous les sites Web présents dans les paramètres de sécurité de la zone. Ajouter ce site Web à la zone :	proxy X ites Web dans cette cette zone utiliseront	Annuler
Que sont le	Indure tous les sites qui n'utilsent pas de serveur. Intranet local Vous pouvez ajouter ou supprimer des si zone. Tous les sites Web présents dans les paramètres de sécurité de la zone. Ajouter ce site Web à la gone :	proxy ites Web dans cette cette zone utiliseront Ajouter	Annuler
Que sont le	Inclure tous les sites qui n'utilsent pas de serveur. Intranet local Vous pouvez ajouter ou supprimer des sizone. Tous les sites Web présents dans les paramètres de sécurité de la zone. Ajouter ce site Web à la gone : I	proxy x ites Web dans cette cette zone utiliseront Ajouter	Annuler
Que sont le	Indure tous les sites qui n'utilsent pas de serveur. Intranet local Vous pouvez ajouter ou supprimer des sizone. Tous les sites Web présents dans les paramètres de sécurité de la zone. Ajouter ce site Web à la gone : I Sites Web :	proxy ites Web dans cette cette zone utiliseront Ajouter	Annuler
Que sont le	Inclure tous les sites qui n'utilsent pas de serveur. Intranet local Vous pouvez ajouter ou supprimer des sizone. Tous les sites Web présents dans les paramètres de sécurité de la zone. Ajouter ce site Web à la zone : I Sites Web : 10.33.69.5	proxy tes Web dans cette cette zone utiliseront Ajouter Supprimer	Annuier
Que sont le	Indure tous les sites qui n'utilsent pas de serveur. Intranet local Vous pouvez ajouter ou supprimer des si zone. Tous les sites Web présents dans les paramètres de sécurité de la zone. Ajouter ce site Web à la zone : I Sites Web : 10.33.69.5 http://10.33.69.5	proxy ites Web dans cette cette zone utiliseront Ajouter Supprimer	Annuier
Que sont le	Indure tous les sites qui n'utilsent pas de serveur Intranet local Yous pouvez ajouter ou supprimer des si zone. Tous les sites Web présents dans les paramètres de sécurité de la zone. Ajouter ce site Web à la zone : I Sites Web : 10.33.69.5 http://10.33.69.5 http://my.damaris.fr	proxy ites Web dans cette cette zone utiliseront Ajouter Supprimer	Annuler
Que sont le	Indure tous les sites qui n'utilsent pas de serveur. Intranet local Vous pouvez ajouter ou supprimer des sizone. Tous les sites Web présents dans les paramètres de sécurité de la zone. Ajouter ce site Web à la gone : I Sites Web : 10.33.69.5 http://10.33.69.5 http://inv.damaris.fr my.damaris.fr	proxy ites Web dans cette cette zone utiliseront Ajouter Supprimer	Annuker
Que sont le	Inclure tous les sites qui n'utilsent pas de serveur. Intranet local Vous pouvez ajouter ou supprimer des sizone. Tous les sites Web présents dans les paramètres de sécurité de la zone. Ajouter ce site Web à la gone : I Sites Web : 10.33.69.5 http://10.33.69.5 http://my.damaris.fr my.damaris.fr	proxy ites Web dans cette cette zone utiliseront Ajouter Supprimer	Annuler
Que sont le	Inclure tous les sites qui n'utilsent pas de serveur. Intranet local Vous pouvez ajouter ou supprimer des sizone. Tous les sites Web présents dans les paramètres de sécurité de la zone. Ajouter ce site Web à la gone : I Sites Web : 10.33.69.5 http://10.33.69.5 http://my.damaris.fr my.damaris.fr Exiger un serveur sécurisé (https:) pgur tous	proxy ites Web dans cette cette zone utiliseront Ajouter Supprimer les sites de cette zone	Annuler
Que sont le	Indure tous les sites qui n'utilsent pas de serveur. Intranet local Vous pouvez ajouter ou supprimer des si zone. Tous les sites Web présents dans les paramètres de sécurité de la zone. Ajouter ce site Web à la zone : I Sites Web : 10.33.69.5 http://10.33.69.5 http://my.damaris.fr my.damaris.fr my.damaris.fr Exiger un serveur sécurisé (https:) pour tous	proxy ites Web dans cette cette zone utiliseront Ajouter Supprimer les sites de cette zone	Annuler
Que sont le	Indure tous les sites qui n'utilsent pas de serveur. Intranet local Vous pouvez ajouter ou supprimer des si zone. Tous les sites Web présents dans les paramètres de sécurité de la zone. Ajouter ce site Web à la gone : I Sites Web : 10.33.69.5 http://10.33.69.5 http://my.damaris.fr my.damaris.fr Exiger un serveur sécurisé (https:) pgur tous	proxy	Annuler

2.1.7 – Configuration des navigateurs

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

about:config X	+		
Firefox about:config			
echercher : Q network.negotiate-auth.t	rusted-uris		
Nom de l'option		▲ Statut	Туре
etwork.negotiate-auth.trusted-uris		par défaut	chaîne
etwork.negotiate-auth.trusted-uris		par défaut	chaîne
etwork.negotiate-auth.trusted-uris	Saisissez une nouvelle valeur (type chaîne)	par défaut	chaîne
etwork.negotiate-auth.trusted-uris	Saisissez une nouvelle valeur (type chaîne)	par défaut	chaîne
etwork.negotiate-auth.trusted-uris	Saisissez une nouvelle valeur (type chaîne) network.negotiate-auth.trusted-uris FQDN	par défaut	chaîne

9 chemin du Jubin - 69 570 DARDILLY	jet : Damaris RM	
	Paramétrage du Single Sign On Protocolo Korboros / SPNogo	Page 6 sur 6

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.

Synchronisation AD Séparateur de Fichier: Masque nom fichier: * *.CSV ; Minutes: Age fichier: . Jours: Heures: Modèle Service AD (Unité Organisationnelle) Profil Damaris Supprimer Service Damaris DG Direction générale util_damaris × Direction Ressources Humaines DRH util_damaris × Ajouter Désactiver utilisateurs manquants: Maintenir sauvegarde:

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

<u>NB</u>: 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.