Authentification unique Eurécia

Date/Version	Contenu	Etat
27/03/2013	Création du document	Diffusable
03/09/2013	Mise à jour du document	Diffusable
17/07/2013	Ajout du chapitre provisionning	Diffusable

But du document : Ce document constitue un guide des étapes à suivre pour mettre en place une fédération d'identité à partir d'un serveur WINDOWS 2008 R2 incluant ADFS 2.0.

Le serveur de fédération publie les informations nécessaires à la connexion par l'utilisateur à l'application Eurécia

Version: 27 mars 2013

www.eurecia.com

Pré-requis matériel :

Configuration minimum	
Version serveur Windows	Windows Server 2008 Enterprise or Windows Server 2008 R2 Enterprise
Mémoire	2 gigabytes (GB) de RAM
Espace disque	10 GB minimum

Lexique

Dénomination	
IDP	Identity Provider donc vous
SP	Service Provider donc Eurécia
AD	Active Directory

Etape 1 : Télécharger, installer et configurer les logiciels nécessaires

Logiciel/Service	Action	Description	Lien de téléchargement
Serveur IIS (Internet Information, Service)	Utiliser le **Gestionnaire de serveur** pour ajouter le web server (IIS) server role	Ce serveur est essentiel pour servir les pages web	N/A
Microsoft .NET Framework 3.5 Service Pack 1 (SP1)	Télécharger et installer	Normalement installé avec Windows server 2008. Si ce n'est pas le cas, attention à l'installer AVANT d'installer ADFS 2.0	http://go.microsoft.com/fwlink/?linkid=118079
AD FS 2.0	**Télécharger uniquement sans installation**	Ce serveur est nécessaire pour créer un serveur de fédération d'identité	http://go.microsoft.com/fwlink/?linkid=151338

Attention : Pour effectuer les actions qui suivent il vous faudra vous identifier en tant qu'Administrateur.

Etape 2 : Installer AD FS 2.0

Important : Le serveur Identity Provider doit être dans le même domaine Active Directory que les utilisateurs

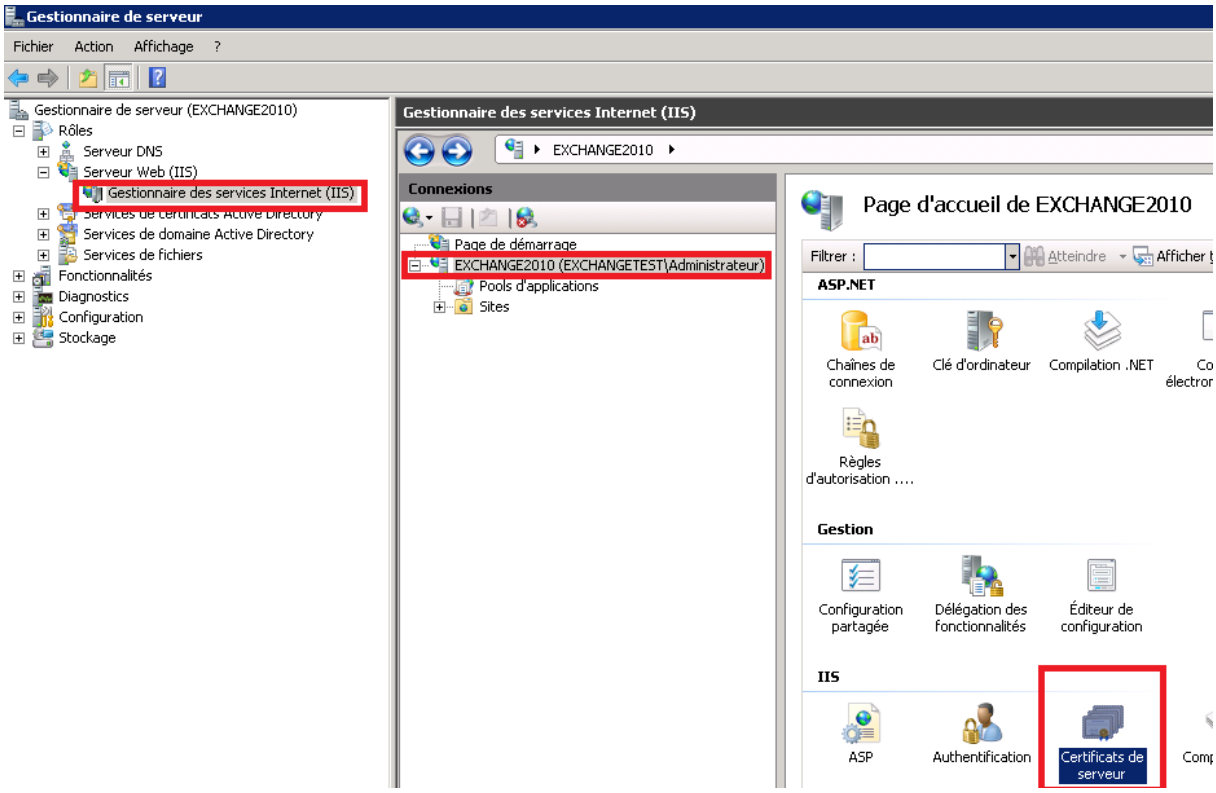
1- Double cliquer sur le fichier exécutable téléchargé précédemment (http://go.microsoft.com/fwlink/?linkid=151338)
2- Cliquer sur le bouton « suivant »
3- Sélectionner la coche d'acceptation puis cliquer sur « suivant »
4- Dans la page suivante sélectionner « Serveur de fédération » puis « suivant »
5- Cliquer sur « Fermer »

Etape 3 : Création d'un certificat auto-signé depuis le serveur IIS

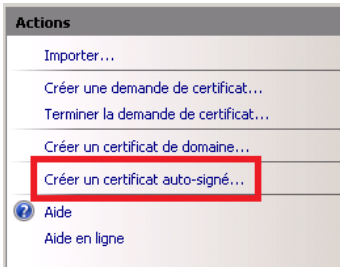
Le but de cette étape est de s'assurer que le SSL est bien activé. Si c'est déjà le cas vous pouvez l'ignorer.

1- Ouvrir depuis le Gestionnaire de service internet IIS depuis la console (Menu démarrer > Gestionnaire des services Internet (IIS))

2- Double clique sur l'icône « Certificats de serveur ». Cf. encadré en rouge de la copie d'écran suivante :

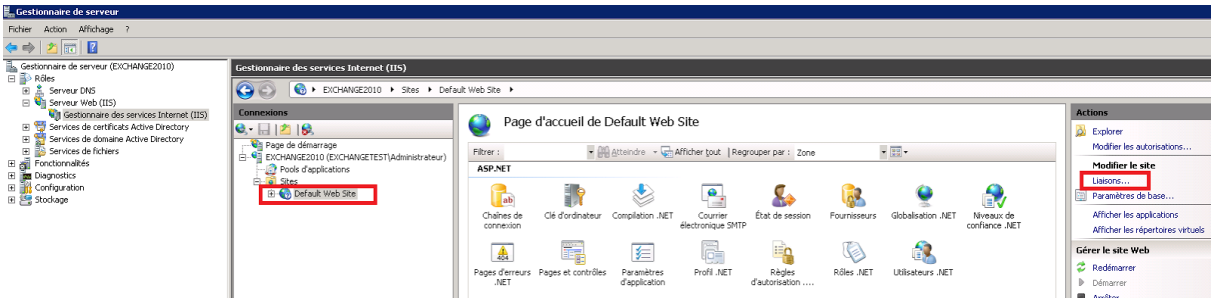


3- Dans la colonne « Actions », cliquer sur le lien « Créer un certificat auto-signé ». Cf. copie d'écran suivant :

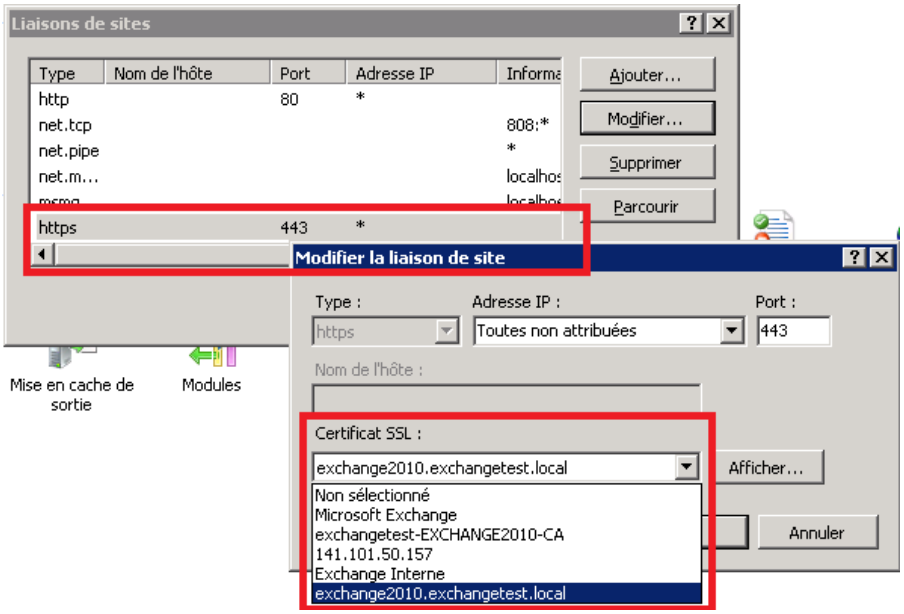


4- Dans le champ « Indiquer un nom convivial pour le serveur », entrer le **FQDN (Full Qualified Domain Name)** de votre serveur

5- Sur la même vue, dans la colonne « Connexion », cliquer sur « default web site » puis cliquer, dans la colonne « Actions » sur le lien « Liaisons »

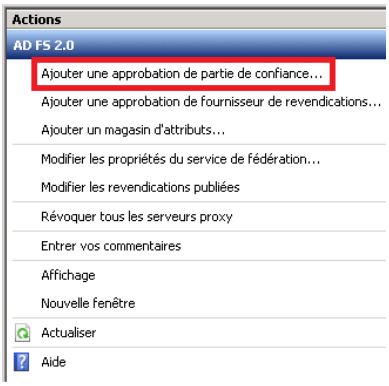


6- Cliquer ensuite sur le bouton « Ajouter » puis dans la liste de valeur « Type » la valeur « https ». Dans la zone « Certificat », sélectionner le nom du certificat crée précédemment. Terminer en cliquant sur « Fermer »



Etape 4 : Configuration du serveur AD FS 2.0

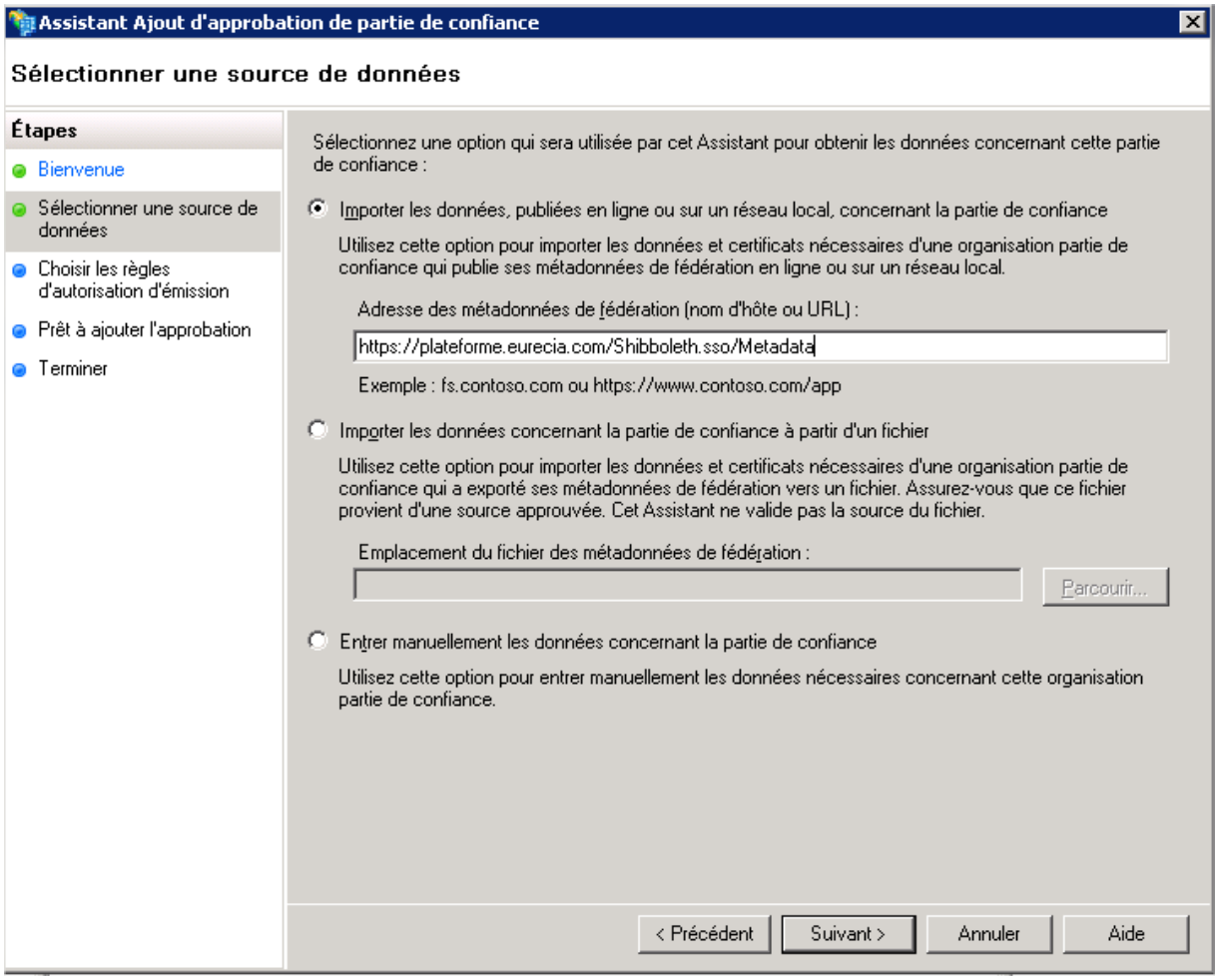
1- Menu « Démarrer », dans la barre de recherche, taper AD puis sélectionner « Gestion AD FS 2.0 »
2- Sur la page d'accueil, dans la partie de droite « Actions », cliquer sur le lien « Ajouter une approbation de partie de confiance »



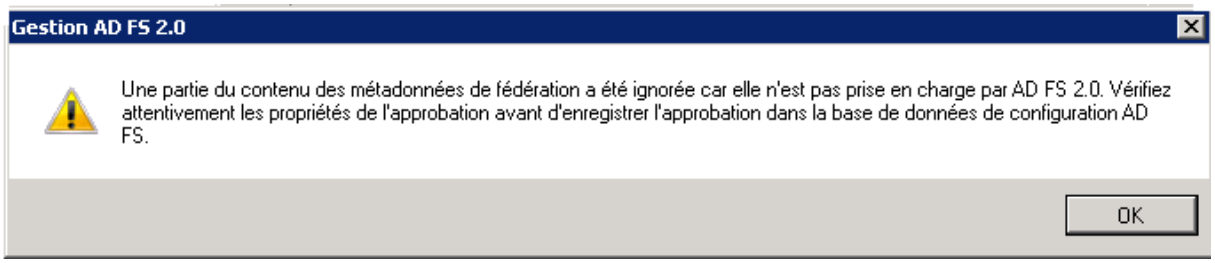
Dans la fenêtre qui s'affiche, cliquer sur le bouton « Démarrer » puis sélectionner « Importer les données, publiées en ligne ou sur un réseau local, concernant la partie de confiance», puis entrez une URL de la forme suivante :
*https://**AdresseDuServeurEurécia**/Shibboleth.sso/Metadata*
La partie ***AdresseDuServeurEurécia*** dépend du serveur Eurécia avec lequel vous souhaitez établir une connexion SSO.

Exemple pour établir une connexion SSO avec la plateforme de production d'Eurécia :
https://plateforme.eurecia.com/Shibboleth.sso/Metadata

Pour la plateforme de démo :
https://demo.eurecia.com/Shibboleth.sso/Metadata

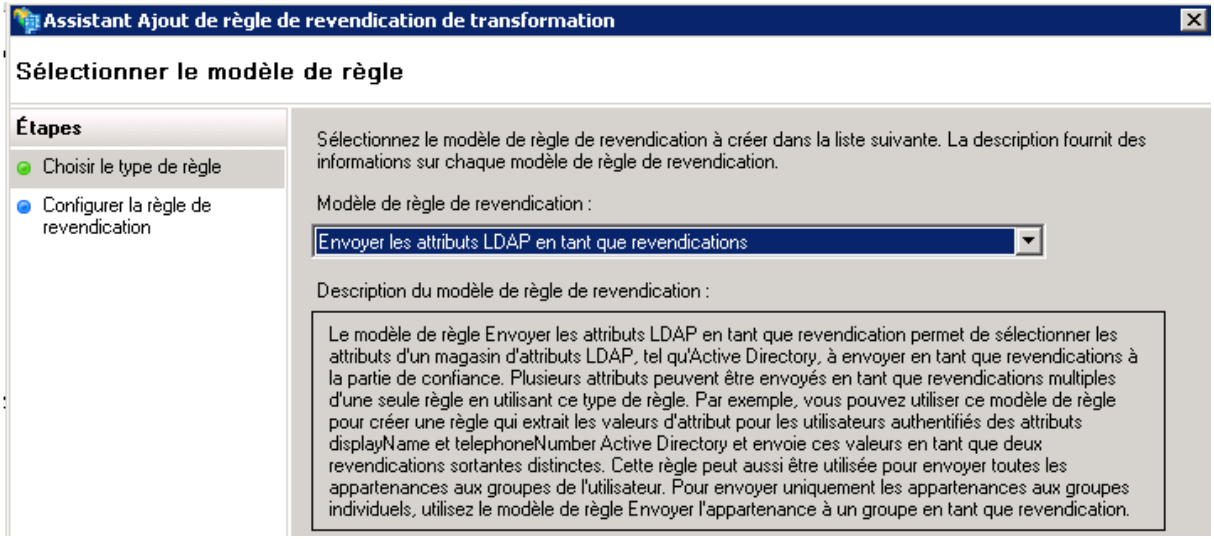


Il se peut que vous ayez le message suivant que vous pouvez ignorer en cliquant sur « OK » :

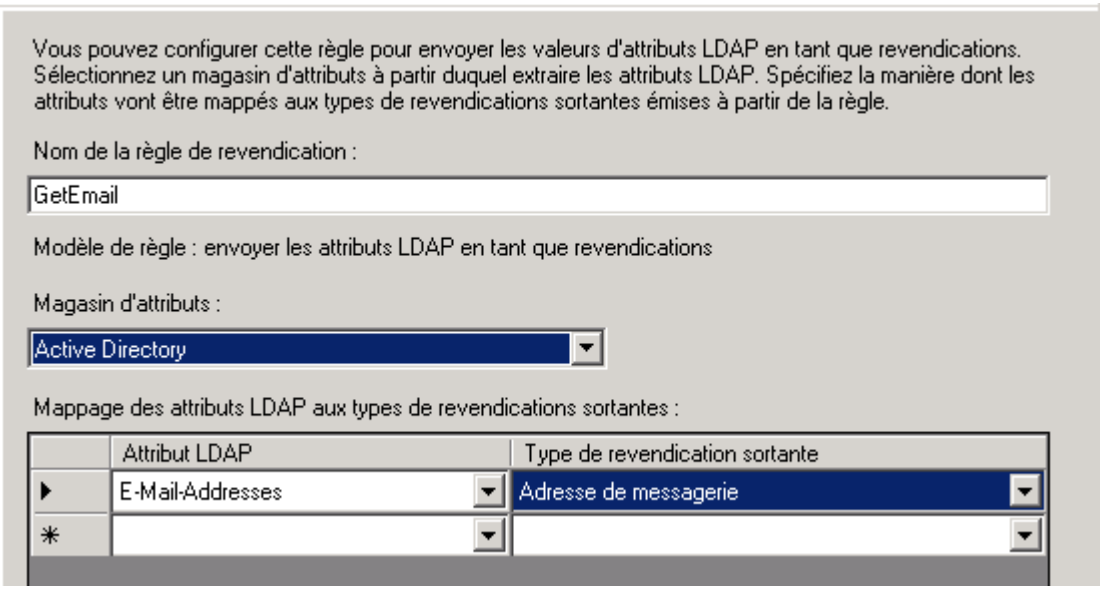


3- Dans la fenêtre suivante, laisser le nom complet pré-rempli qui doit être de la forme **XXX.eurecia.com** puis « Suivant »
4- Sélectionner « Autoriser l'accès de tous les utilisateurs à cette partie de confiance » puis « Suivant ».
5- Une synthèse s'affiche qui fait état des données précédemment entrées. Cliquer sur « Suivant »
6- Laisser cocher la case « Ouvrir la boiter de dialogue Modifier les règles de revendication pour cette approbation de partie de confiance à la fermeture de l'assistant » dans la fenêtre suivante puis « Fermer »
7- Une nouvelle fenêtre s'affiche. Cliquer alors sur le bouton « Ajouter une règle ».

8- Dans la liste de valeur, sélectionner « Envoyer les attributs LDAP en tant que revendications » puis « Suivant » (Cf. Copie d'écran)



9- Entrer **GetEmail** dans le champ « Nom de la règle de revendication ». Dans « Magasin d'attributs », sélectionner « Active Directory ». Dans la section « Mappage des attributs LDAP aux types de revendications sortantes entrer les valeurs définies dans le tableau suivant :



10- Cliquer sur le bouton « Terminer »

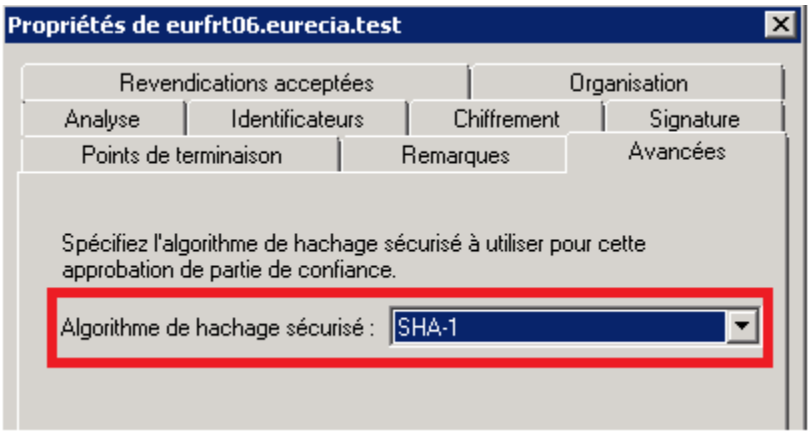
11- Ouvrir un navigateur et entrer l'url suivante (l'URL peut être différente suivant votre version d'ADFS) : **https://localhost/FederationMetadata/2007-06/FederationMetadata.xml**

Attention : localhost peut être remplacé par l'url d'accès à votre ADFS

12- Enregistrer le fichier xml généré sur votre bureau sous le nom IDPFederationMetadata.xml

13- Bouton droit sur « XXX.eurecia.com » puis « Proprietés », onglet « Avancées »

14- Dans la liste de valeur, sélectionner SHA-1 au lieu de SHA-256 en tant qu'algorithme de hachage. Voir copie d'écran



Félicitations, vous venez de mettre en place une fédération d'identité depuis votre Active Directory. Il ne vous reste plus qu'à envoyer le fichier **IdpFederationMetadata.xml** à Eurécia à l'adresse **support@eurecia.com**

Etape 5 : Mise en place des tests pour la recette

- Pré-requis aux tests :
  - ✓ Base salariés installée depuis Eurécia avec des utilisateurs identifiés
  - ✓ Avoir envoyé à Eurécia le fichier metadata (Etape 14 du chapitre "Configuration du serveur AD FS 2.0")
- Création d'un raccourci de test connexion depuis le poste client :

https://**demo.eurecia.com**/Shibboleth.sso/Login?target=https://**demo.eurecia.com**/eurecia/secureshib&entityID=http://**url.access.adfs**/adfs/services/trust

url.access.adfs = Url d'accès à votre ADFS

demo.eurecia.com = Adresse de la plateforme Eurécia avec laquelle la connexion SSO a été mise en place

Note : La méthode utilisant un raccourci pour tester la connexion peut conduire à une erreur de redirection suivant le navigateur utilisé et la configuration de votre ADFS.

En effet, lors du premier accès, il vous sera demandé d'entrer votre nom d'utilisateur et mot de passe Windows. Ce faisant, le navigateur peut "oublier" l'échange qu'il a eu précédemment avec la plateforme Eurécia et donc ne pas transmettre toutes les informations nécessaires à votre ADFS.

Dans ce cas, relancer simplement le raccourci, le nom d'utilisateur et mot de passe ayant déjà été enregistrés, la connexion se fera sans problème.

Etape 6 (optionel) : Mise en place du provisionning de la base salariés Via FTP

L'objet de cette partie est de mettre en place une synchronisation de l'annuaire LDAP avec la base salariés Eurécia. Cette synchronisation se fera à l'aide d'un fichier sous un format particulier défini par Eurécia (script schell ci-dessous). Ce fichier sera déposé sur un dépôt FTP (identifiants du dépôt sont à communiquer à Eurécia pour le paramétrage).

- **Depuis windows**, créer un script schell avec exécution d'une tâche planifiée à fréquence de votre choix. Le fichier de sortie sera à déposer sur un dépôt FTP (annule et remplace)

```
Get-ADUser -Filter { memberOf -RecursiveMatch "CN=EURECIA,CN=Users,DC=XXXX,DC=com" } -Properties emailaddress | Select
@{Name="LASTNAME";Expression={$_.Surname}},@{Name="FIRSTNAME";Expression={$_.GivenName}},@{Name="EMAIL_USER";Expressio
n={$_.emailAddress}}  | Convertto-CSV -Delimiter ";"  -NoTypeInformation > "c:\temp\fichierOut.csv"
```

- **Depuis Eurécia,** il faudra paramétrer le module de transfert de données qui récupèrera, à fréquence régulière, les données (sous format de fichier défini par Eurécia) depuis un dépôt FTP et mettra à jour la base salariés :
  - § En création d'un nouveau salarié
  - § En modification des données d'un salarié
  - § En archivage du salariés dans le cas d'un départ

Problèmes fréquents

- Certaines version de Windows Server peuvent poser des problèmes de redirection lors de la phase d'authentification. Ce problème résulte en un message d'indispobilité de la page web.
  Correctif : Installer le correctif 2896713

Quelques références

http://technet.microsoft.com/fr-fr/library/adfs2-federation-wif-application-step-by-step-guide(v=ws.10).aspx

http://technet.microsoft.com/en-us/library/gg317734(v=ws.10).aspx