

Mettre en place ADFS pour permettre l'identification au sein d'Office 365 et Azure Active Directory via la **fédération des identités**

Introduction
Certificat SSL pour votre ADFS
Installation et configuration du serveurs ADFS
Création de votre serveur ADFS Proxy ou WAP (Web Application Proxy)
Création des entrées DNS (pour l'interne et l'externe)
Configuration de votre serveur AAD Connect
Activer la fédération via votre ADFS
Vérifier et tester la configuration

Introduction

L'objectif de la mise en place d'ADFS étant de permettre à des utilisateurs de s'authentifier « sans avoir à partager le hash des mots de passe avec Microsoft ».

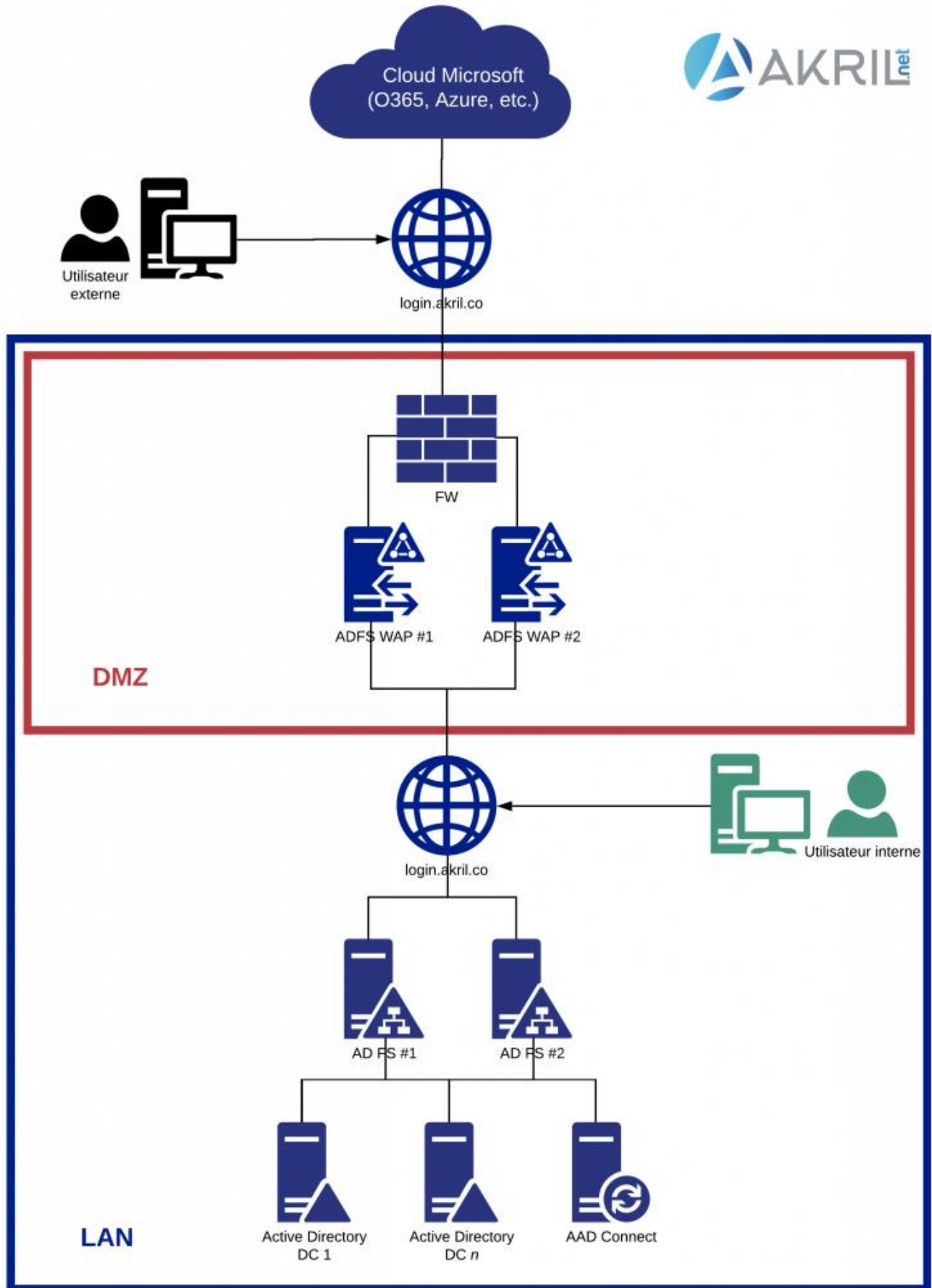
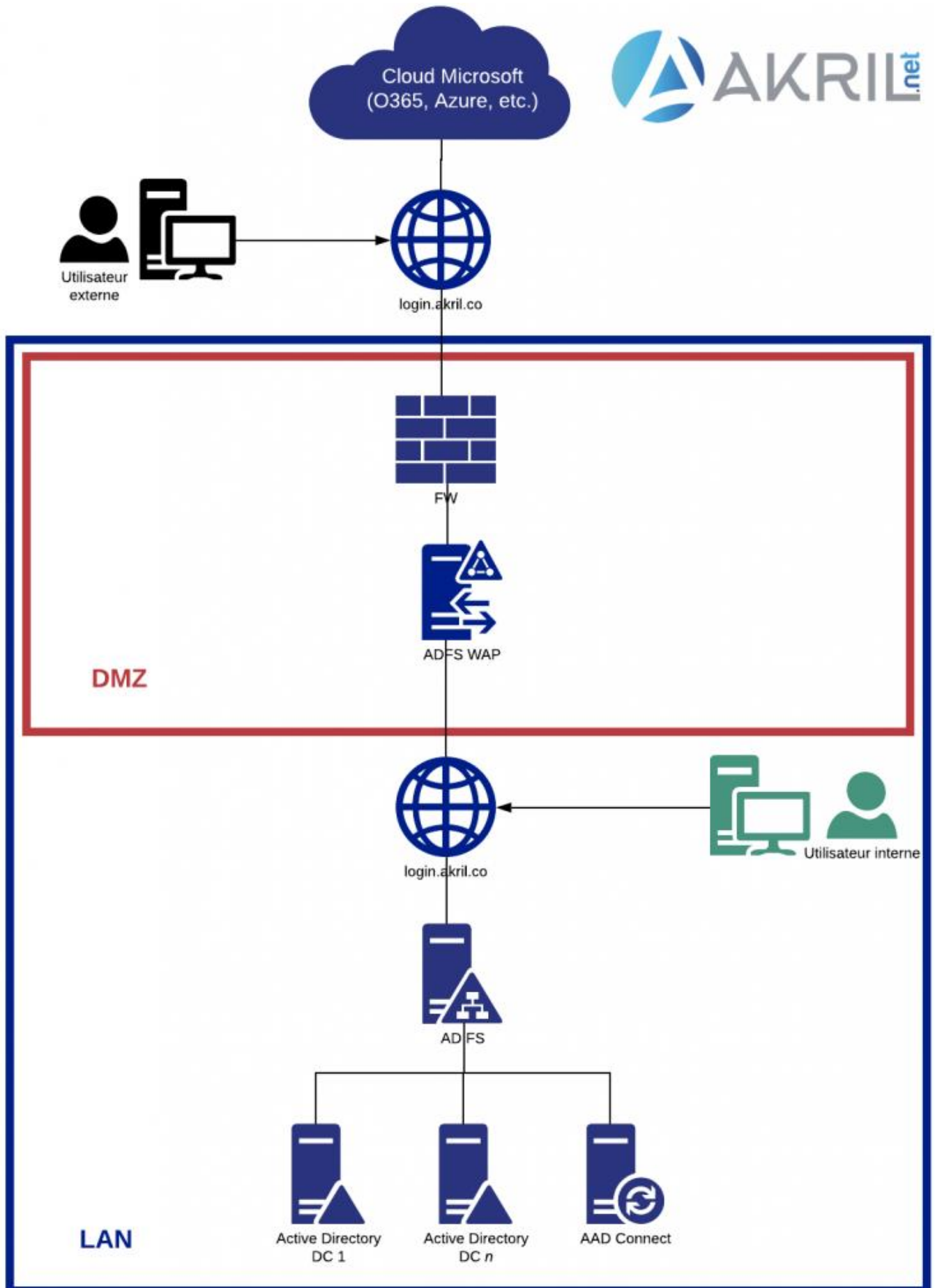


Diagramme pour infrastructure type de Fédération des Identités entre Cloud et On-Prem

Si on détaille un peu ce qu'il se passe :

- Nous aurons besoin de définir une **URL d'accès** qui permettra de s'identifier pour accéder aux services. Dans mon cas j'ai choisi : *login.akril.co*.
- Cette URL doit être résolue depuis l'extérieur de votre réseau. Vous devez donc créer une entrée A auprès de votre *registrar*. L'adresse IP correspond à une IP publique associée à une appliance et/ou Load Balancer qui permettra de rediriger vers nos 2 serveurs ADFS WAP ou **proxy ADFS**. C'est par là que vos utilisateurs "externes" accéderont au service lorsqu'ils ne sont pas dans votre LAN.
- Les **2 serveurs WAP** sont au sein de votre infrastructure mais comme ils sont en DMZ ; ils ne sont pas joint au domaine (WORKGROUP) pour des raisons de sécurité.
- Vous avez besoin de 2 serveurs pour assurer la haute disponibilité. C'est eux qui sont en frontal des 2 serveurs ADFS afin d'éviter de mettre des serveurs membres – qui plus est ADFS – directement en DMZ.
- **Cette URL d'accès doit également être connue au sein de votre LAN.** Dans ce cas, elle pointera également vers un VIP interne qui assurera la haute disponibilité et redirigera vers vos 2 serveurs ADFS.
- Dans le cas d'un accès en interne, vous ne passez donc pas les serveurs WAP mais vous vous identifiez directement auprès des serveurs ADFS.
- L'ADFS vérifiera votre identité avec l'aide de l'Active Directory (DC).
Comme vous pouvez le voir, si vous optez pour ce type d'infrastructure c'est **plus lourd** : 2 serveurs ADFS, 2 serveurs WAP, Load Balancer (*et donc appliance réseau pro*) – en plus des DC et de l'AAD Connect dont vous disposez déjà.
En effet, dans ce scénario l'infrastructure ADFS + WAP devient critique car **si vos 2 serveurs WAP et/ou vos 2 serveurs ADFS sont down – il devient alors impossible d'accéder à vos services Cloud.**
Dans mon scénario, j'effectue ce design en environnement de Lab, j'ai donc réduit à **1 serveur ADFS et 1 serveur WAP**. Dans ce cas, l'infrastructure cible sera donc la

suivante :



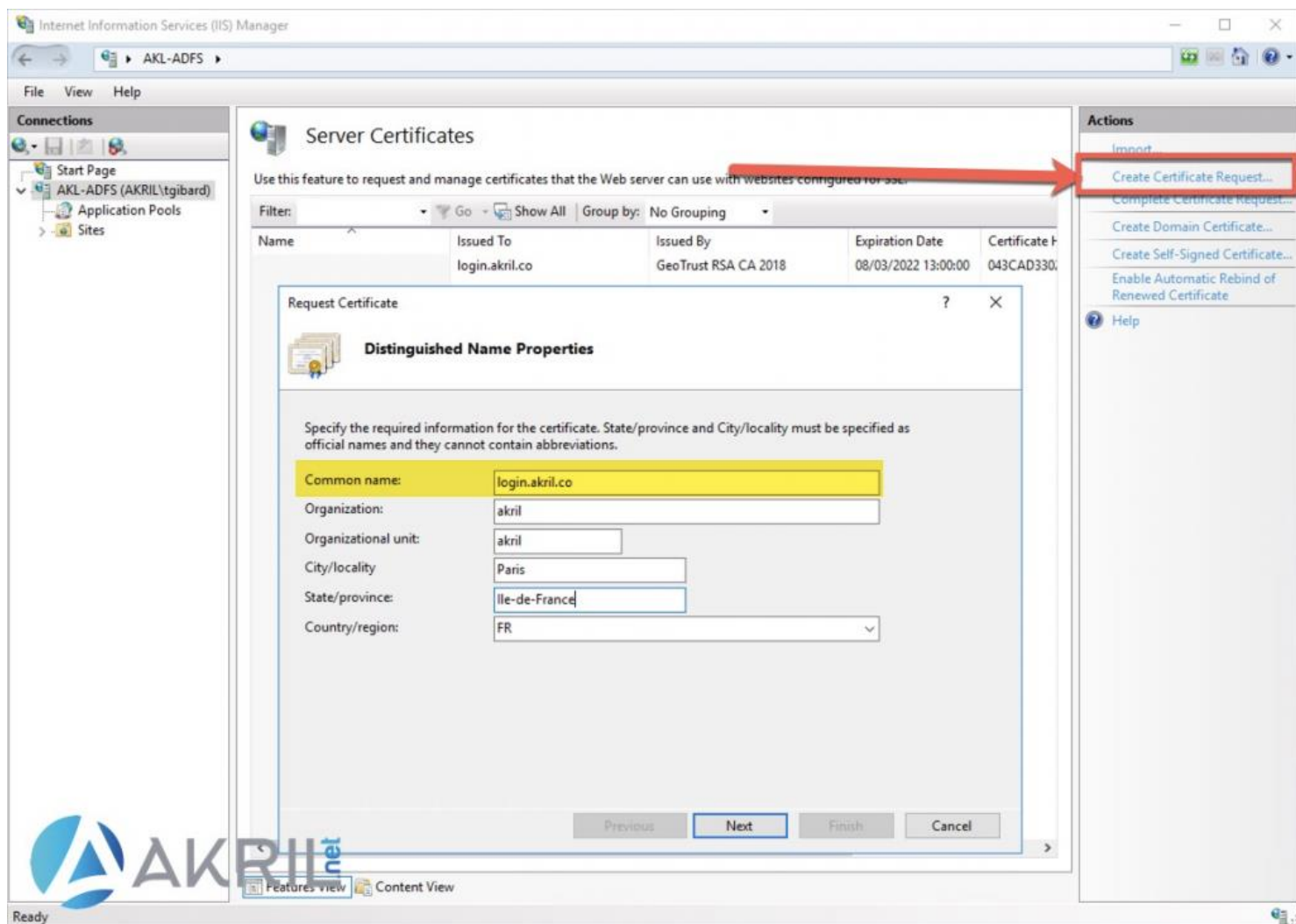
Mon scénario (un peu réduit par souci de capacity planning)

D'où l'intérêt de bien comprendre techniquement comment ça se passe car si vous déployez ce type d'infrastructure au sein de votre Production, il est possible que vous soyez sur une infrastructure multi-sites et ayez même besoin de davantage de serveurs ADFS, Proxy.

Certificat SSL pour votre ADFS

Qui dit authentification dit mot de passe... Et dans ce cas, vous vous doutez que notre URL d'accès sera évidemment sécurisée en https. **Vous devez donc disposer d'un certificat SSL associé à l'URL de connexion** que vous souhaitez créer. Non, **pas de certificat auto-signé** (au cas où vous auriez eu la question).

Commencez par **générer un CSR** depuis votre IIS Manager sur votre serveur ADFS (ou n'importe quel autre serveur).



Internet Information Services (IIS) Manager

AKL-ADFS

Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter: Go Show All Group by: No Grouping

Name	Issued To	Issued By	Expiration Date	Certificate ID
	login.akril.co	GeoTrust RSA CA 2018	08/03/2022 13:00:00	043CAD330...

Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: login.akril.co

Organization: akril

Organizational unit: akril

City/locality: Paris

State/province: Ile-de-France

Country/region: FR

Previous Next Finish Cancel

Actions

- Import
- Create Certificate Request...
- Complete Certificate Request...
- Create Domain Certificate...
- Create Self-Signed Certificate...
- Enable Automatic Rebind of Renewed Certificate
- Help

AKRIL.net

Ready

Génération de votre CSR

Ne vous trompez pas sur le **Common Name** qui doit correspondre exactement à l'URL que vous souhaitez protéger.

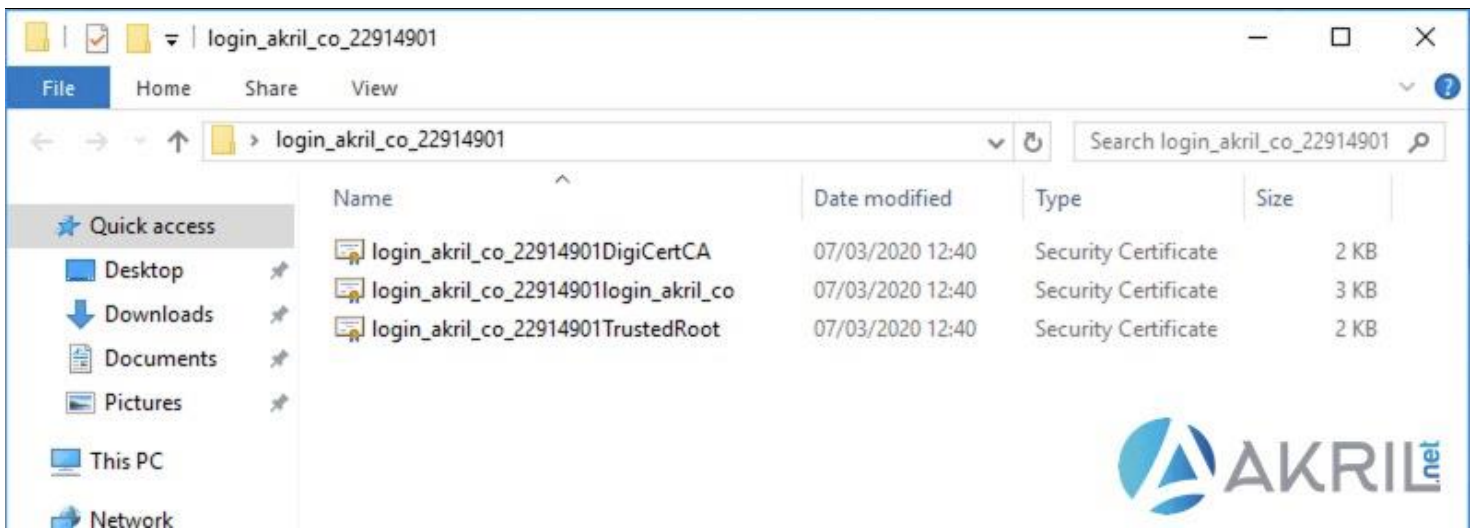


```
csr-login-akril-co - Notepad
File Edit Format View Help
|-----BEGIN NEW CERTIFICATE REQUEST-----
MI...Fu
Y2...wF
YW...EF
AA...fI
EX...94
Yj...ki
z+...di
Kd...sB
1E...EE
AY...wt
QU...YK
Kw...AA
Uw...AA
cg...QE
Aw...qG
SI...F1
Aw...b3
DQ...JF
AA...hI
92...Xd
26...9i
w8...0m
21rak0b1i1nb00z11ogzzwK11b0xL1 y11cp111aQ11T50X1 AA0b01u1F01C1 1Z1 zV10X0uPZ
N4e0fYTStCgj+b06UTGDPMF0wZ1aLQ==
-----END NEW CERTIFICATE REQUEST-----
```

Certificate Request (CSR)

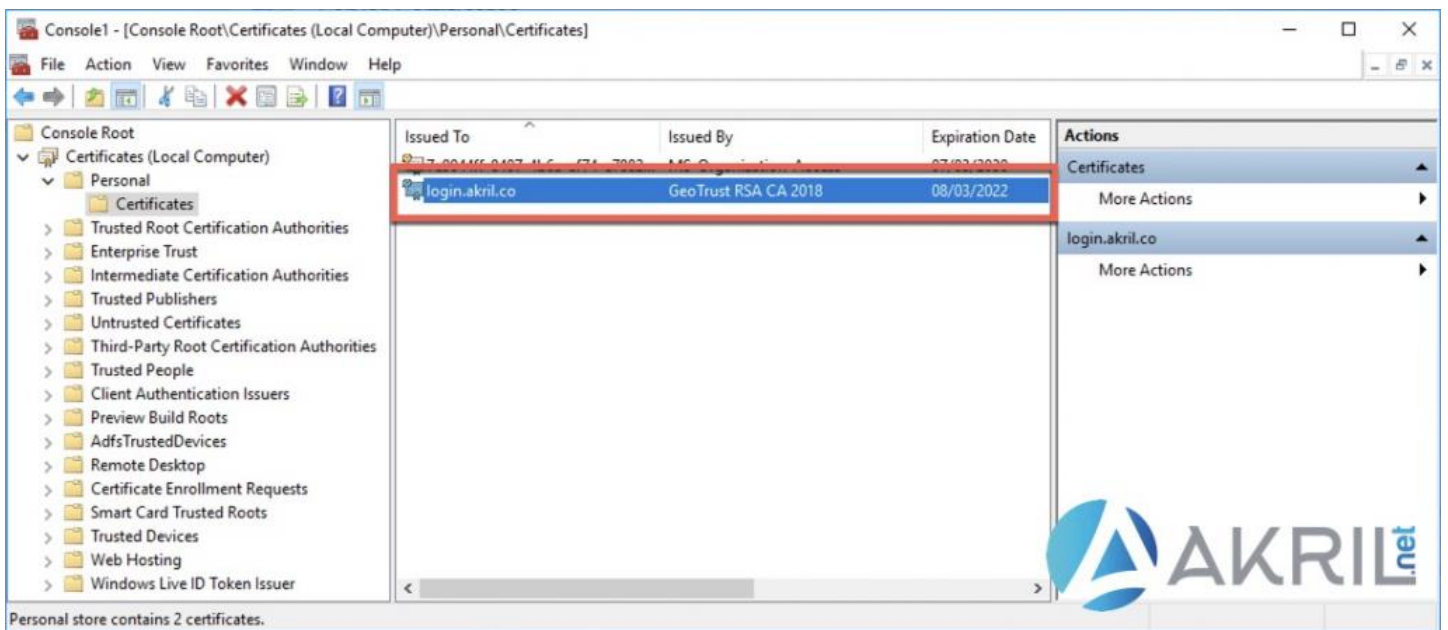
Une fois que vous disposez de votre CSR, vous pouvez demander à votre fournisseur **de créer un certificat SSL**.

Cette partie dépend évidemment de votre fournisseur. Pour ma part, j'utilise **DigitCert**. Une fois que c'est fait, vous devez disposer de un ou plusieurs certificats. Ces derniers doivent être **ajoutés à l'ensemble des magasins sur votre serveur ADFS, WAP et AAD Connect**.



Certificats SSL

Selon votre fournisseur, vous aurez peut-être plusieurs certificats à ajouter au sein de votre magasin.

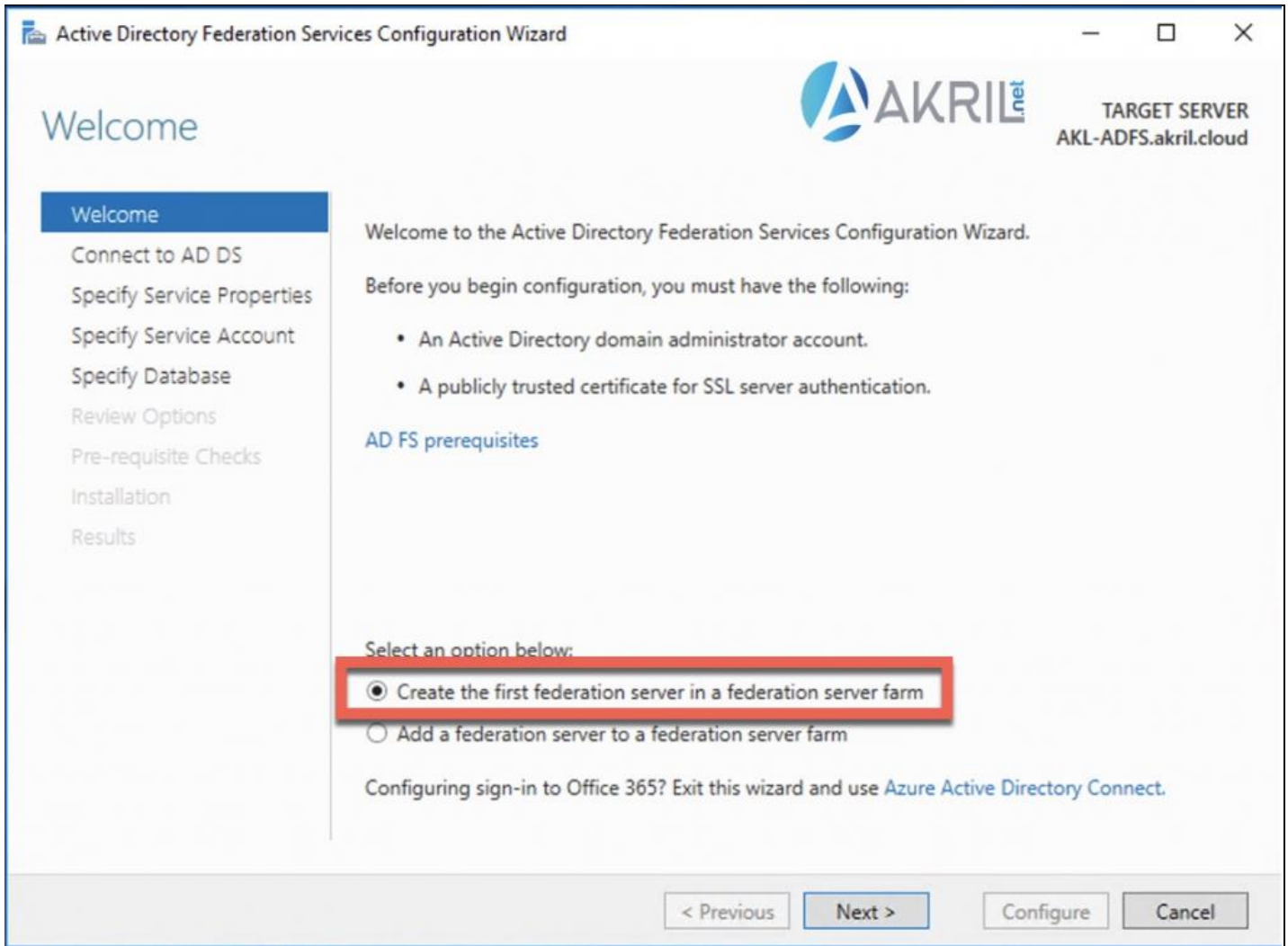


Magasins de certificats

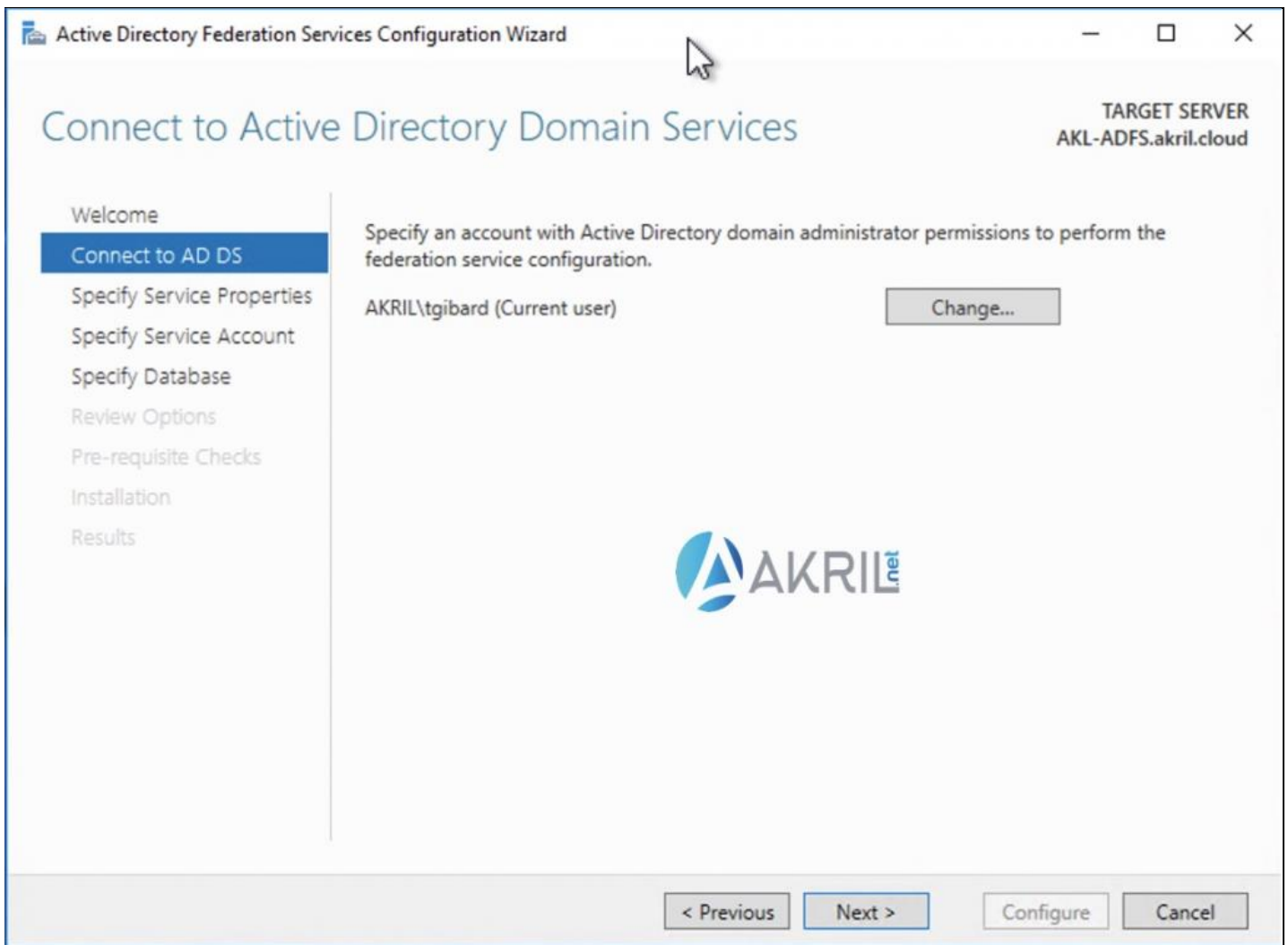
Notre certificat est prêt.

Installation et configuration du serveurs ADFS

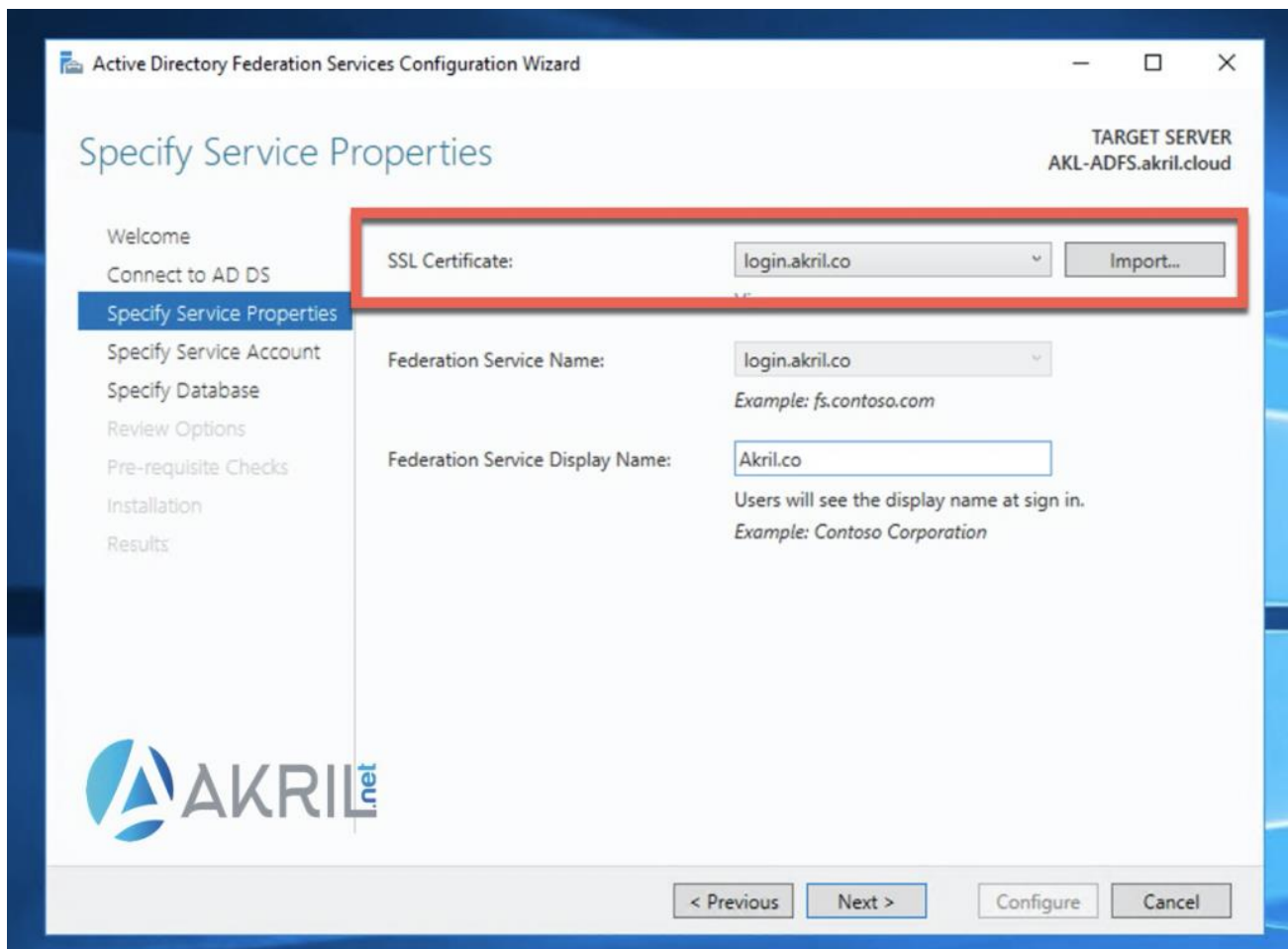
Provisionnez une nouvelle machine virtuelle et intégrez là au sein de votre domaine Active Directory. Depuis le Server Manager, **installez le rôle ADFS** puis démarrez l'assistant de configuration.



Création de votre premier serveur ADFS



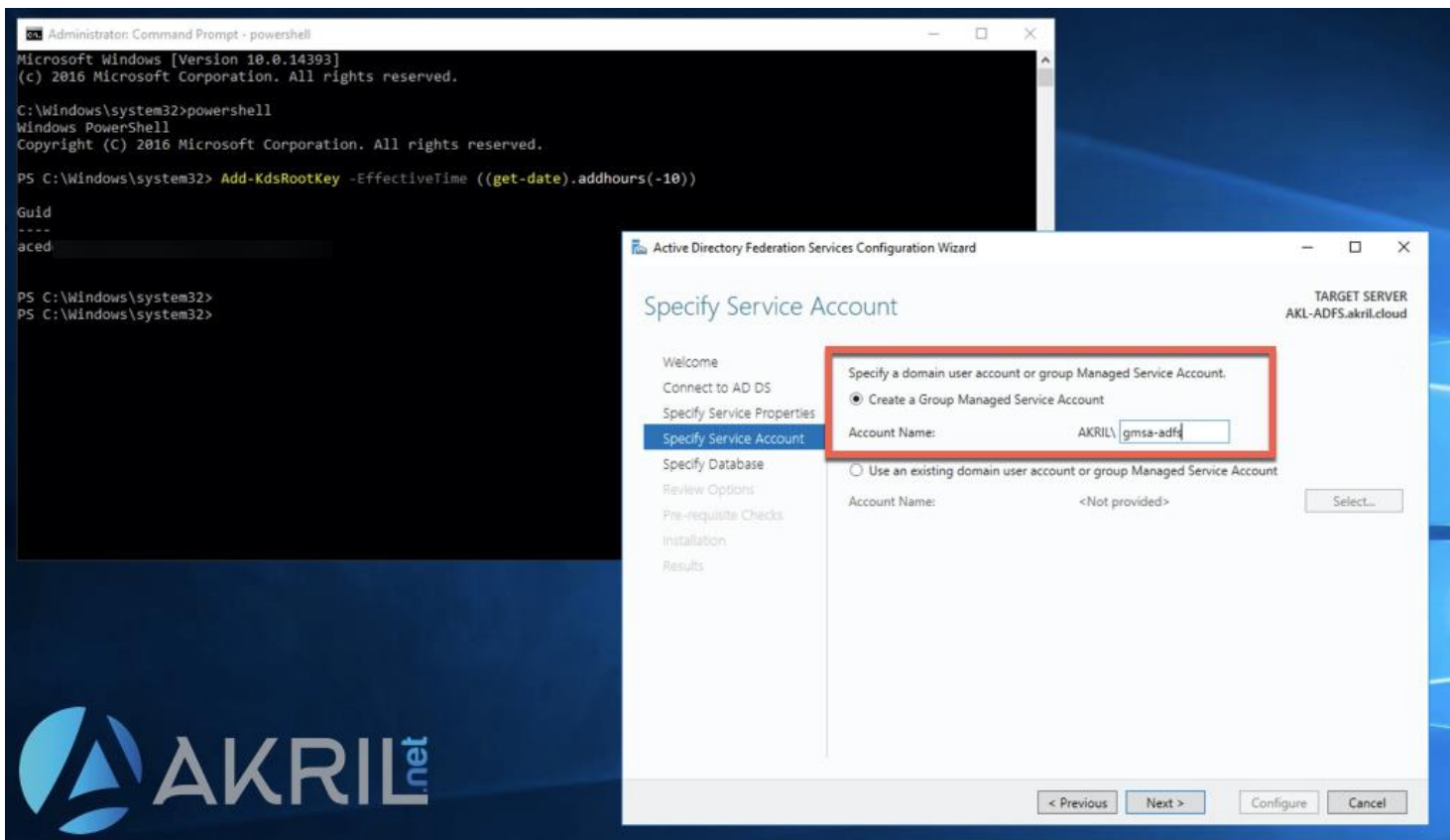
Création de votre premier serveur ADFS



Choix de l'URL et du certificat

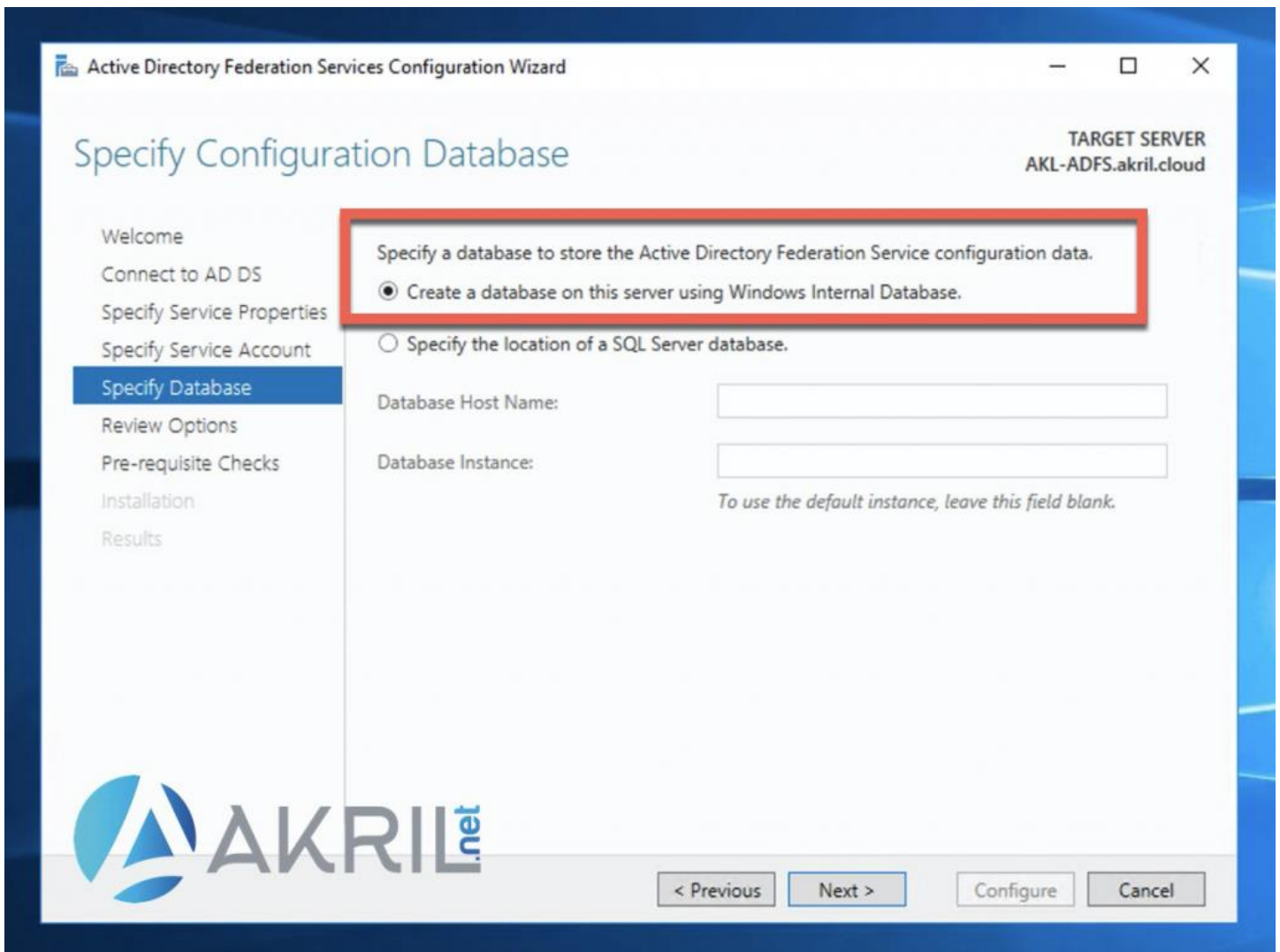
Si vous avez bien importé votre certificat SSL, vous devriez avoir le nom de l'URL que l'on se prépare à configurer directement dans le menu déroulant. Il ne reste plus qu'à la sélectionner.

Vous pouvez également choisir un nom pour la page ADFS de votre organisation (*purement décoratif*).



Compte de service ou gMSA si possible

Vous devez maintenant définir **un compte de service** pour votre serveur ADFS. Si vous en avez la possibilité, je vous encourage à utiliser un compte de type **gMSA** qui est bien meilleur en termes de sécurité. Si ce n'est pas possible dans votre environnement, vous devrez créer un compte de service standard avec login + password (à l'ancienne).

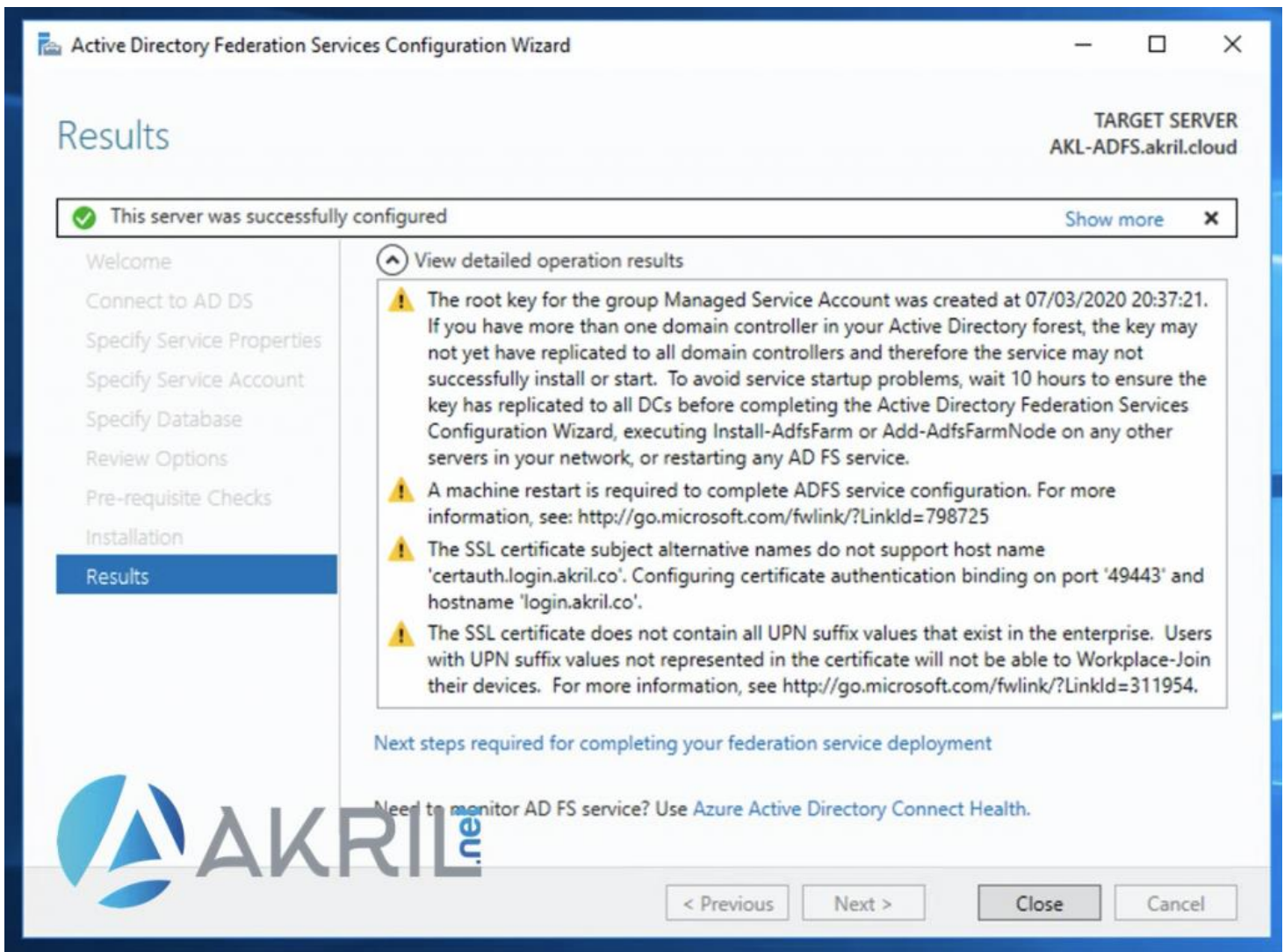


Création de votre base de données

Je vous encourage également à choisir une base de données de type **WID – Windows Internal Database**. Cela convient même pour les environnements de Production. La base de données dédiée SQL Server ne se justifie que pour certains cas rares d'environnements. [Plus d'infos sur le lien suivant](#) (*nombre de serveurs ADFS, nombre d'applications, etc.*).

Récapitulatif de la configuration

Contrôle des pré-requis



Fin de l'installation et de la configuration de votre serveur ADFS

Voilà, globalement c'est terminé pour votre serveur ADFS. Il n'y a rien de particulier à faire en plus sur ce composant. Si vous disposiez d'un 2nd serveur ADFS, vous devrez reprendre l'ensemble de l'assistant et choisir tout au début l'option **Add a federation server to a federation server farm**.

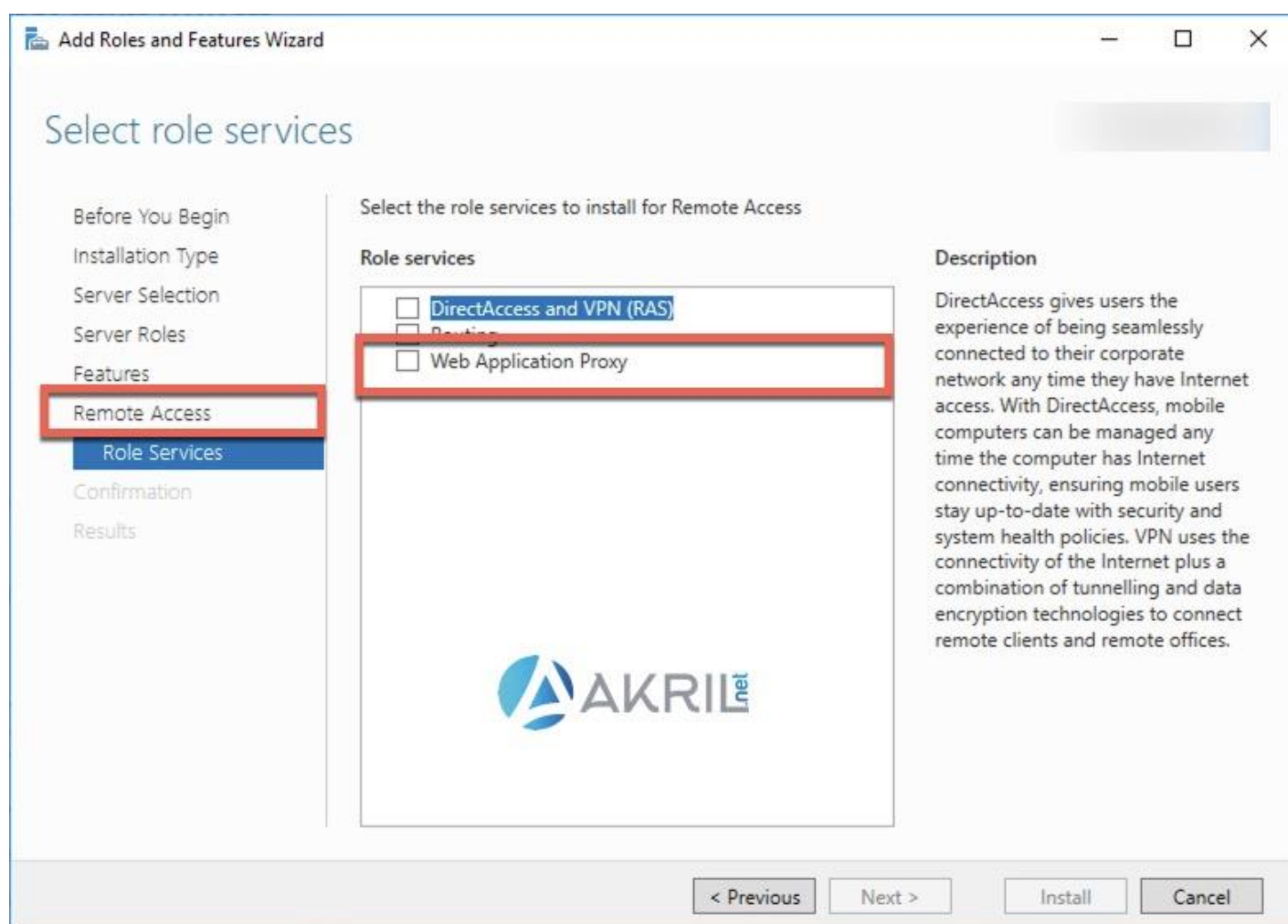
Création de votre serveur ADFS Proxy ou WAP (Web Application Proxy)

Comme expliqué précédemment, c'est ce serveur WAP qui va faire le lien avec "le monde extérieur" et votre serveur ADFS car on ne souhaite pas publier ce dernier sur Internet.

Le serveur WAP est donc configuré en WORKGROUP. Il n'est pas serveur membre de votre domaine Active Directory.

Installez le rôle **Web Application Proxy** depuis le Server Manager. Si vous utilisez Windows Server 2019, le rôle est désormais un peu caché... ☐

Démarrez le Server Manager, installez le Server Role appelé : **Remote Access**. Puis dans les **Role Services**, vous aurez alors accès à **Web Application Proxy**.

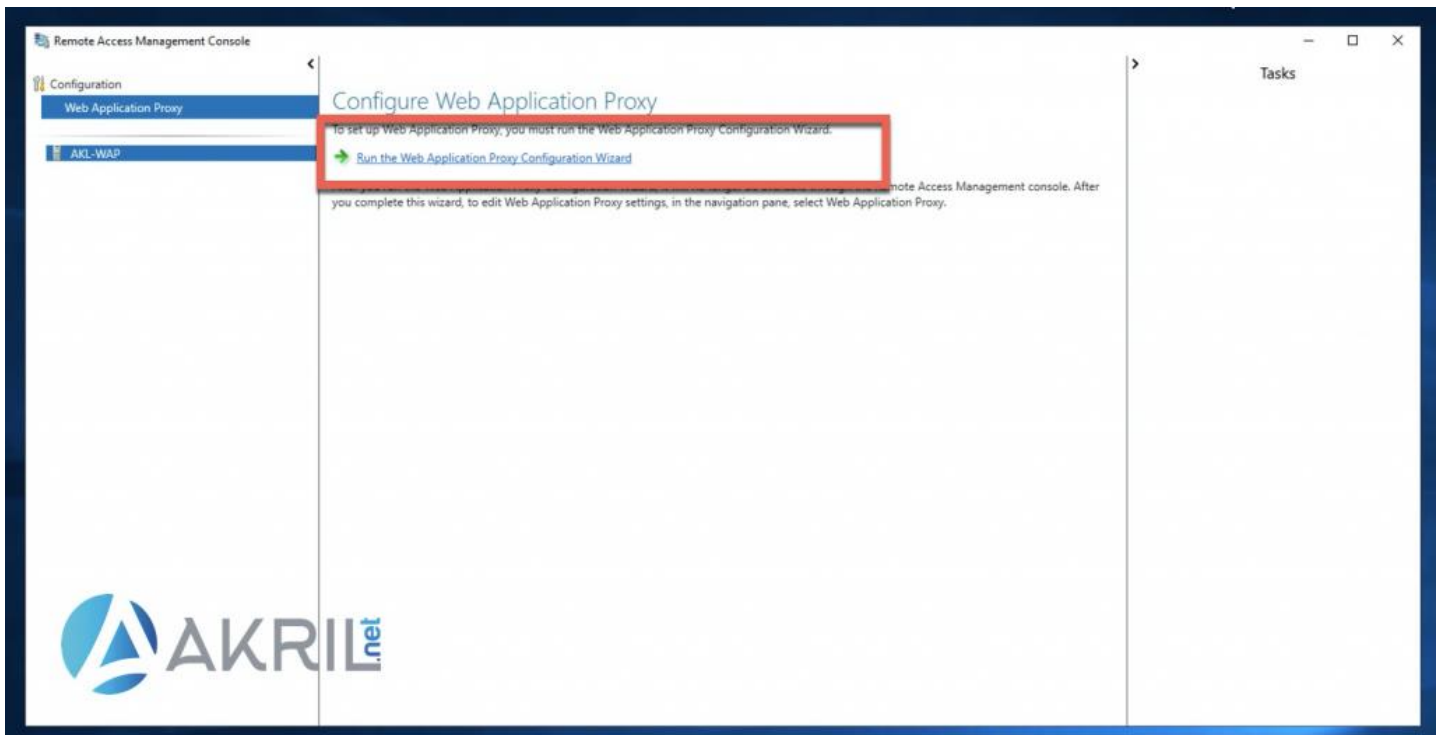


Installation du rôle Web Application Proxy

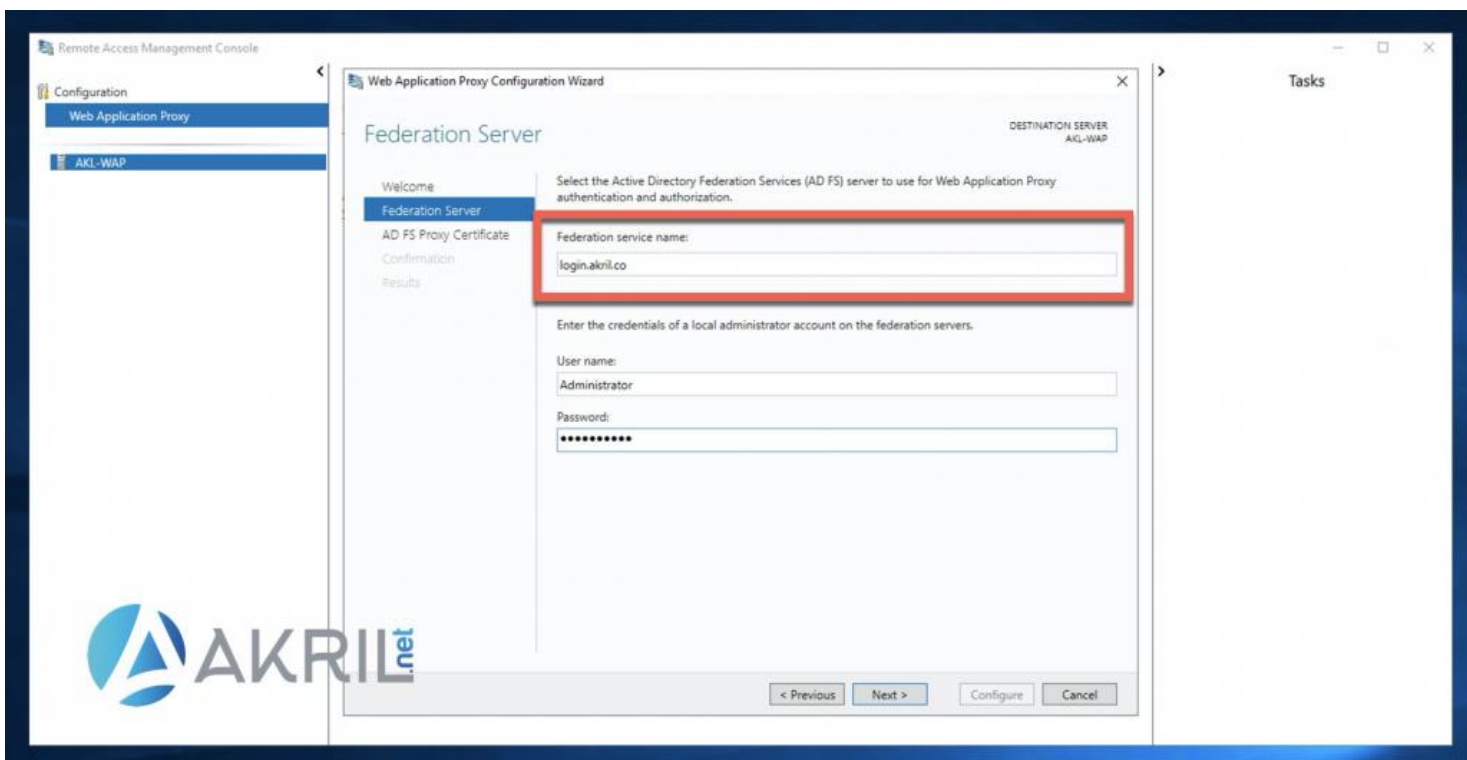
Une fois que l'installation est terminée, nous allons passer à la configuration. Veillez à bien être connecté avec un compte **Local Administrateur**.

Si ce n'est pas déjà fait, n'oubliez pas que vous devez disposer du certificat SSL également sur ce serveur !

Depuis le Menu Démarrer, ouvrez l'outil **Remote Access Management Console** puis lancez l'assistant de configuration.

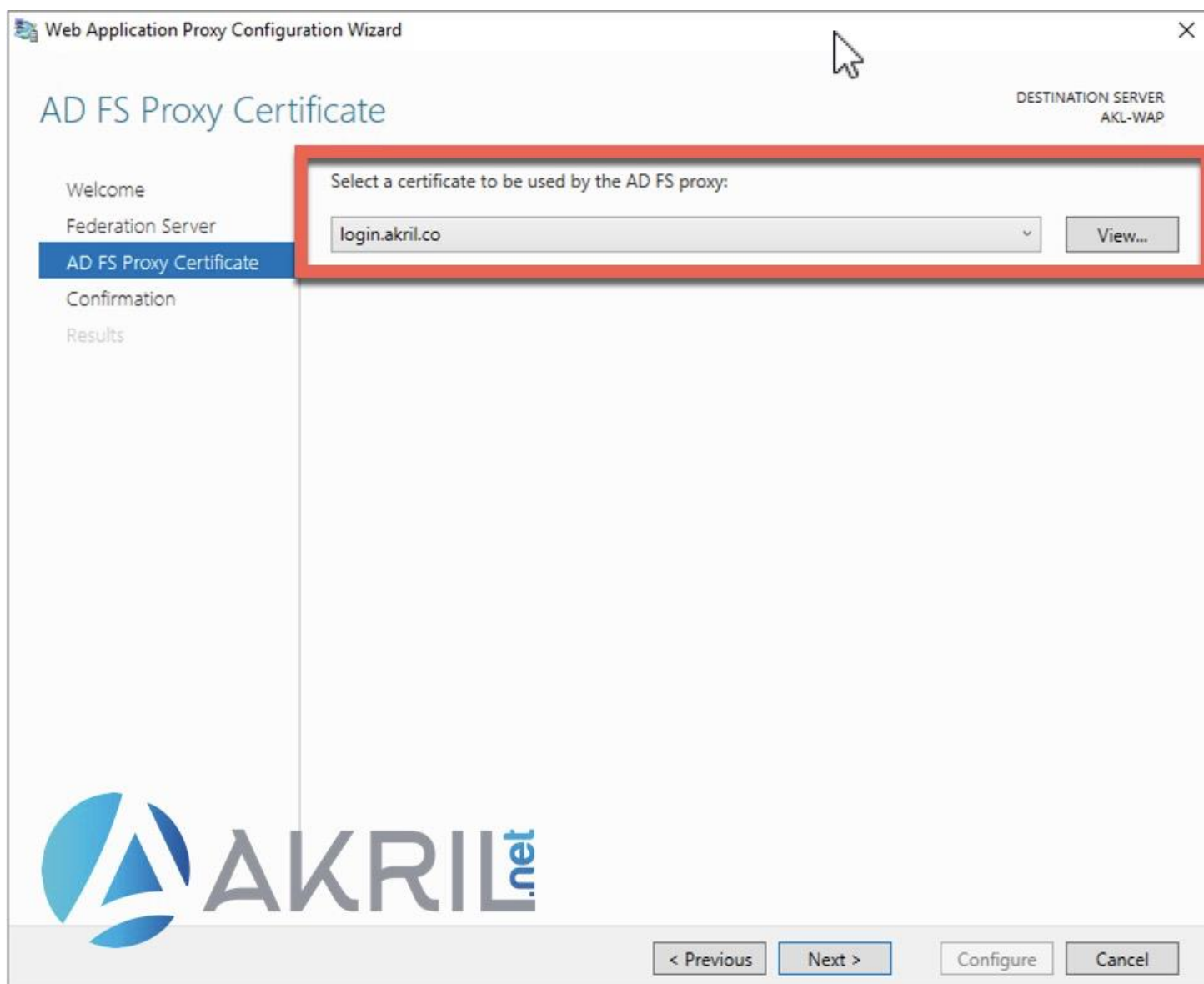


Remote Access Management Console



Remote Access Management Console

Définissez le **nom de votre URL de connexion** ainsi qu'un compte Local Administrator.



Choix de l'URL de connexion

Si votre certificat est correctement installé, vous devriez pouvoir retrouver dans le menu déroulant le nom de votre URL. Il ne reste qu'à cliquer sur Next.

Web Application Proxy Configuration Wizard

Confirmation


DESTINATION SERVER
AKL-WAP

Welcome
Federation Server
AD FS Proxy Certificate
Confirmation
Results

The following PowerShell command will be run when you click Configure. It can also be used to automate additional installations. If you want to use automation, copy the command before you click Configure.

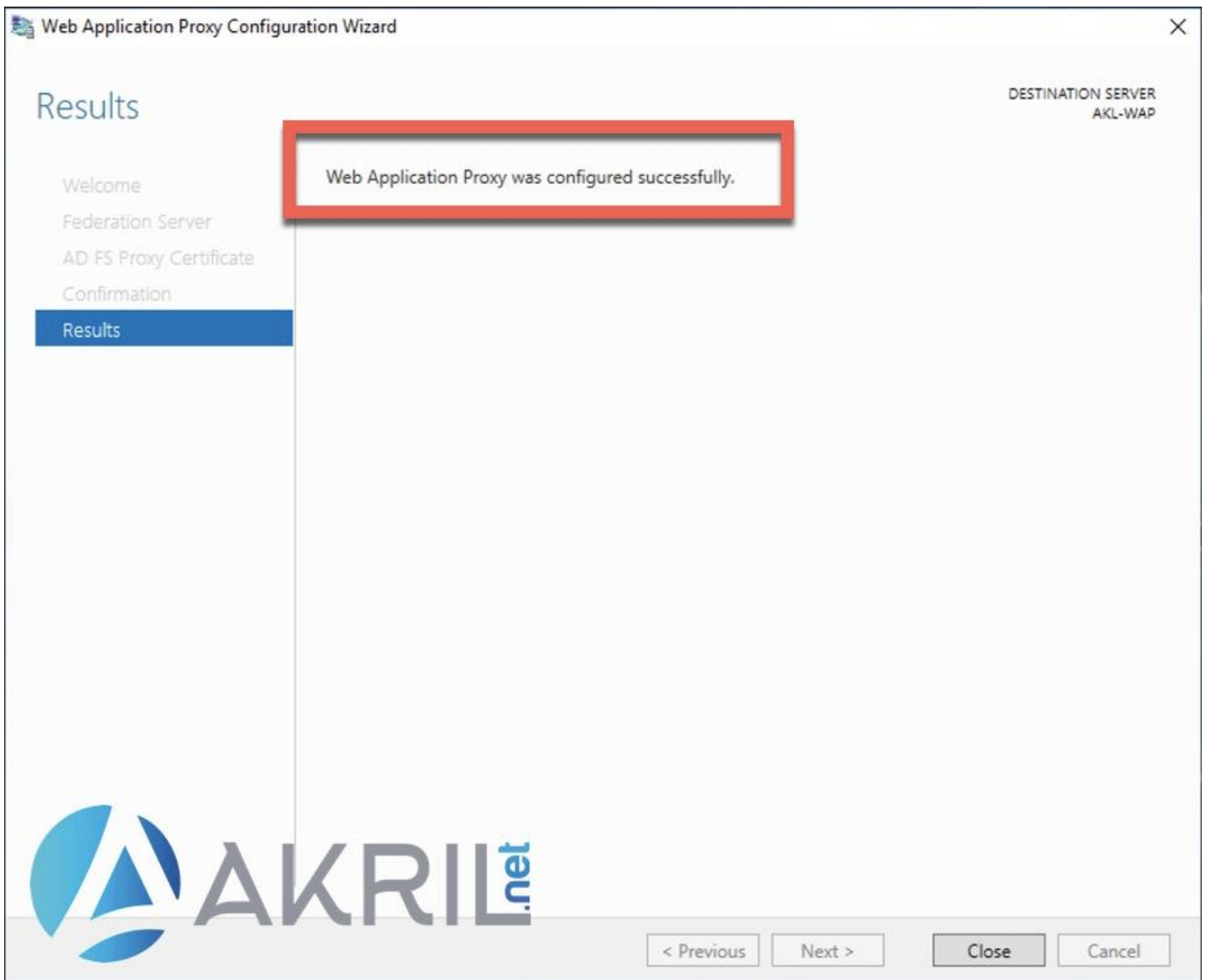
```
Install-WebApplicationProxy  
-FederationServiceTrustCredential System.Management.Automation.PSCredential  
-CertificateThumbprint '043CAD3302928D4E6CCB8792D16361397379324A'  
-FederationServiceName 'login.akril.co'
```

To configure Web Application Proxy, click Configure.



< Previous Next > Configure Cancel

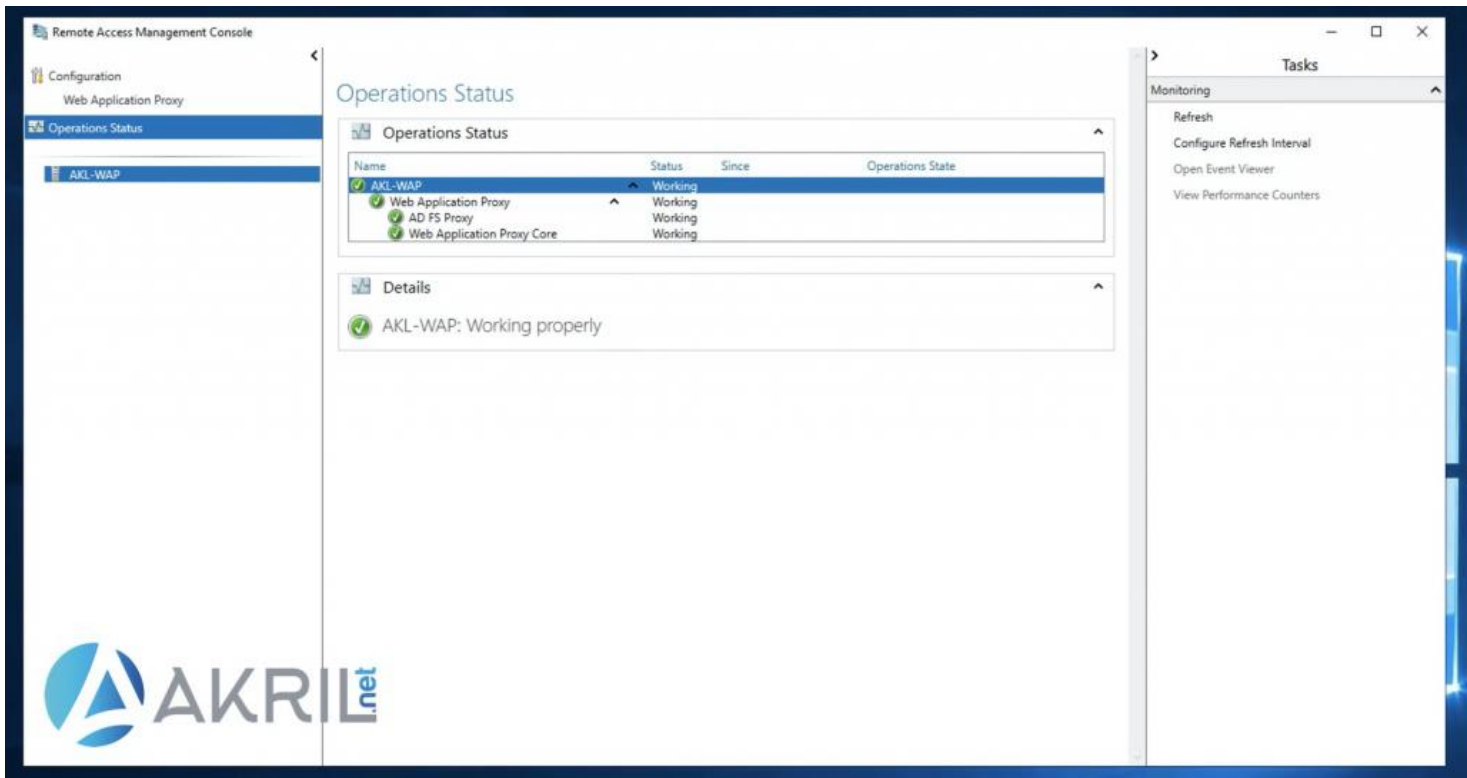
Récapitulatif avant configuration



Fin de la configuration de votre serveur WAP

La configuration est terminée.

Vous pouvez également vérifier que votre serveur WAP et ADFS parviennent bien à communiquer en vérifiant le statut depuis la console **Remote Access Management Console**. Tout devrait être vert.

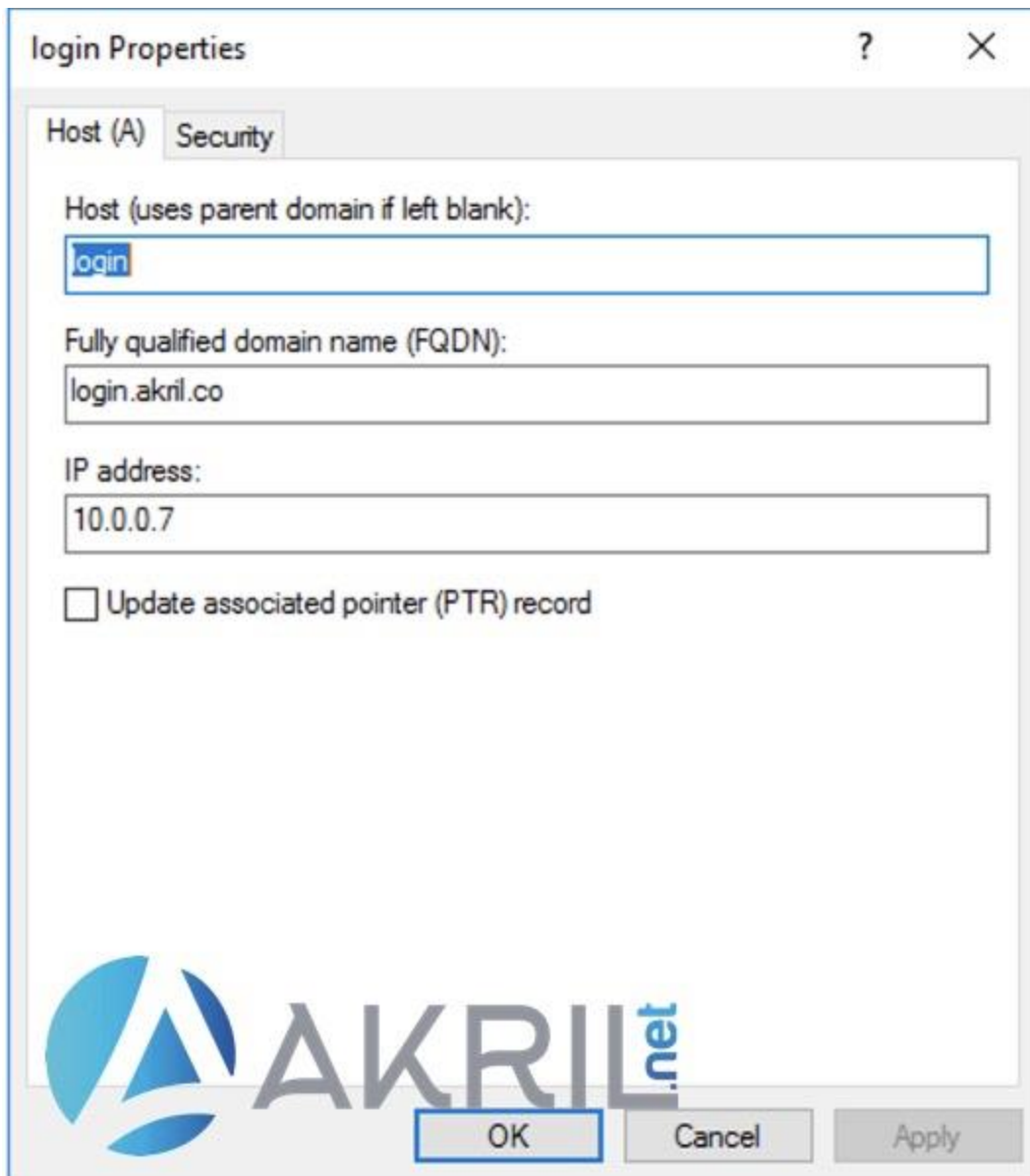


Status de votre serveur WAP

Création des entrées DNS (pour l'interne et l'externe)

Comme je l'ai déjà expliqué précédemment, **notre URL d'accès doit être accessible depuis l'interne et l'externe de votre infrastructure.**

Pour l'interne, il nous suffit de créer une entrée DNS directement depuis le DNS Manager d'un Domain Controller. **Le champs A devra pointer sur votre serveur ADFS (ou bien sur la VIP associée si vous disposez de 2+ serveurs ADFS).**



login Properties

Host (A) Security

Host (uses parent domain if left blank):
login

Fully qualified domain name (FQDN):
login.akril.co

IP address:
10.0.0.7

Update associated pointer (PTR) record

AKRIL.net

OK Cancel Apply

Création d'une entrée DNS interne (sur un DC)

Dans mon cas, je dispose d'un seul serveur ADFS, je fais donc pointer mon login.akril.co vers l'adresse IP interne de mon serveur ADFS.

Pour l'externe, je dois créer une nouvelle entrée de type A dans mes DNS publiques.

Dans mon cas, c'est **Google Domains**. Elle pointera sur l'adresse IP publique associée à mon réseau et je vais ensuite rediriger le flux 443/TCP depuis l'extérieur vers mon serveur WAP (10.0.0.10) en interne. Ce dernier redirigera ensuite le tout vers le serveurs ADFS... ça va vous suivez ?

Création d'une entrée DNS publique auprès de votre registrar

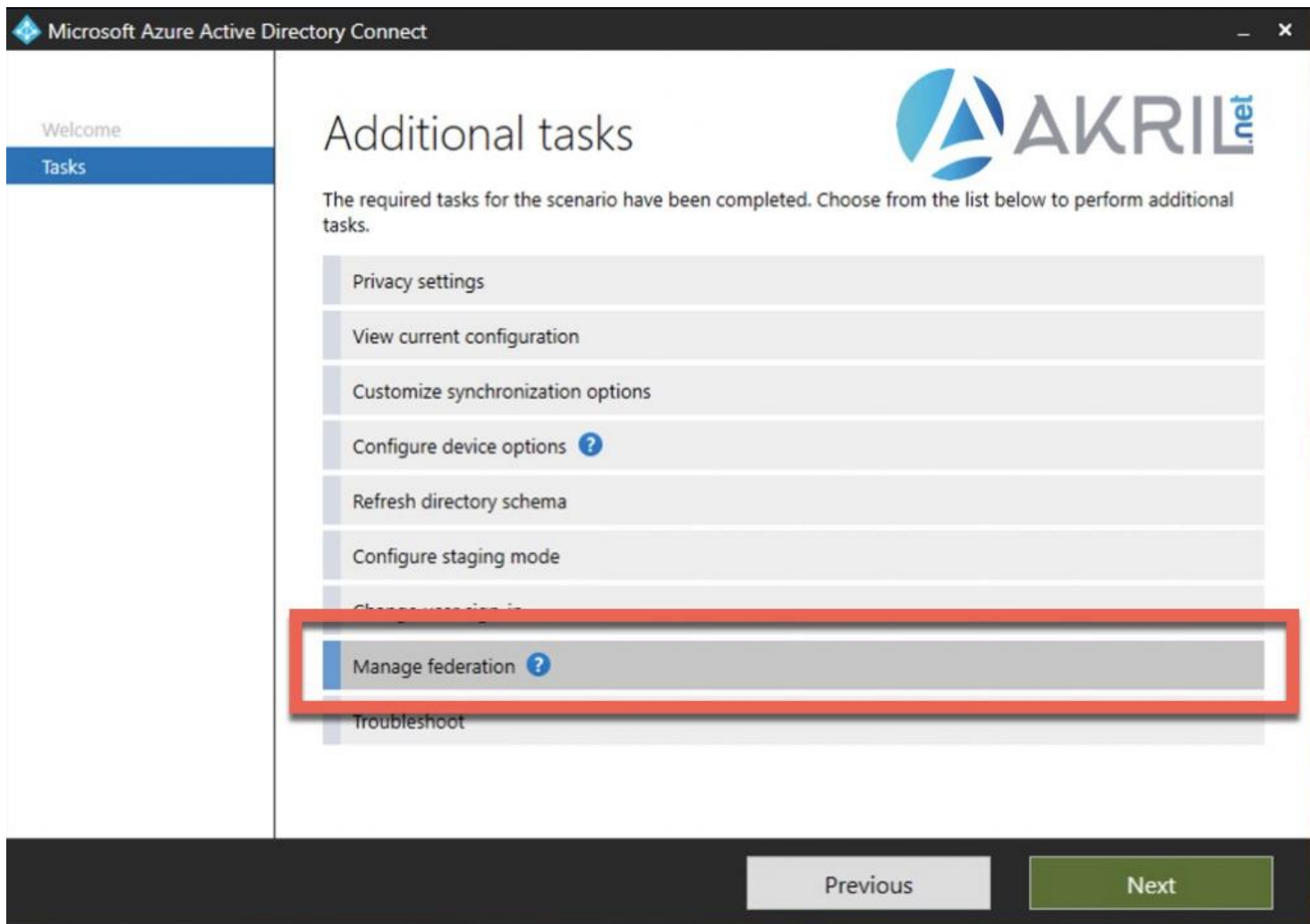
Configuration de votre serveur AAD Connect

Important : les étapes décrites plus haut permettent de **déployer manuellement les composants ADFS et WAP**. Cela étant, dans les versions les plus récentes d'AAD Connect, **l'assistant peut réaliser à distance la configuration des serveurs ADFS et WAP** à condition d'avoir tous les pré-requis. Les étapes que nous allons présenter ci-dessous peuvent donc être redondantes dans certains cas.

Dans mon cas mon serveur AAD Connect était actuellement configuré en mode **Password Hashed Synchronization**.

Nous allons donc maintenant configurer notre AAD Connect afin qu'il ait conscience de notre infrastructure fédérée.

Attendez que votre dernière synchronisation soit terminée puis **démarrez l'assistant AAD Connect**.



Assistant AAD Connect

Choisissez l'option **Manage federation**.

The screenshot shows the Microsoft Azure Active Directory Connect application window. The title bar reads "Microsoft Azure Active Directory Connect". On the left is a navigation pane with the following items: "Welcome", "Tasks", "Manage federation", "Management tasks" (highlighted in blue), "Update SSL", "Connect to AD FS", "Federation servers", "Proxy servers", "SSL Certificate", "Servers", and "Configure". The main content area is titled "Certificate management tasks" and features the AKRIL.net logo. Below the title, it says "Select the task to perform for the AD FS farm." and lists two options: "Update SSL certificate" (selected with a radio button) and "Update token-signing and token-decrypting certificates". At the bottom of the main area, a blue box contains the text: "Your AD FS and Web Application Proxy servers will be updated with a new SSL certificate for the AD FS farm. A PFX file is required for this update." At the very bottom of the window are two buttons: "Previous" (disabled) and "Next" (active).


Assistant AAD Connect

Vous ne devriez avoir que l'option **Update SSL certificate**. Suivez les étapes décrites ci-dessous.


Microsoft Azure Active Directory Connect

Welcome
Tasks
Manage federation
Management tasks
Update SSL
Connect to AD FS
Federation servers
Proxy servers
SSL Certificate
Servers
Configure

Connect to AD FS servers



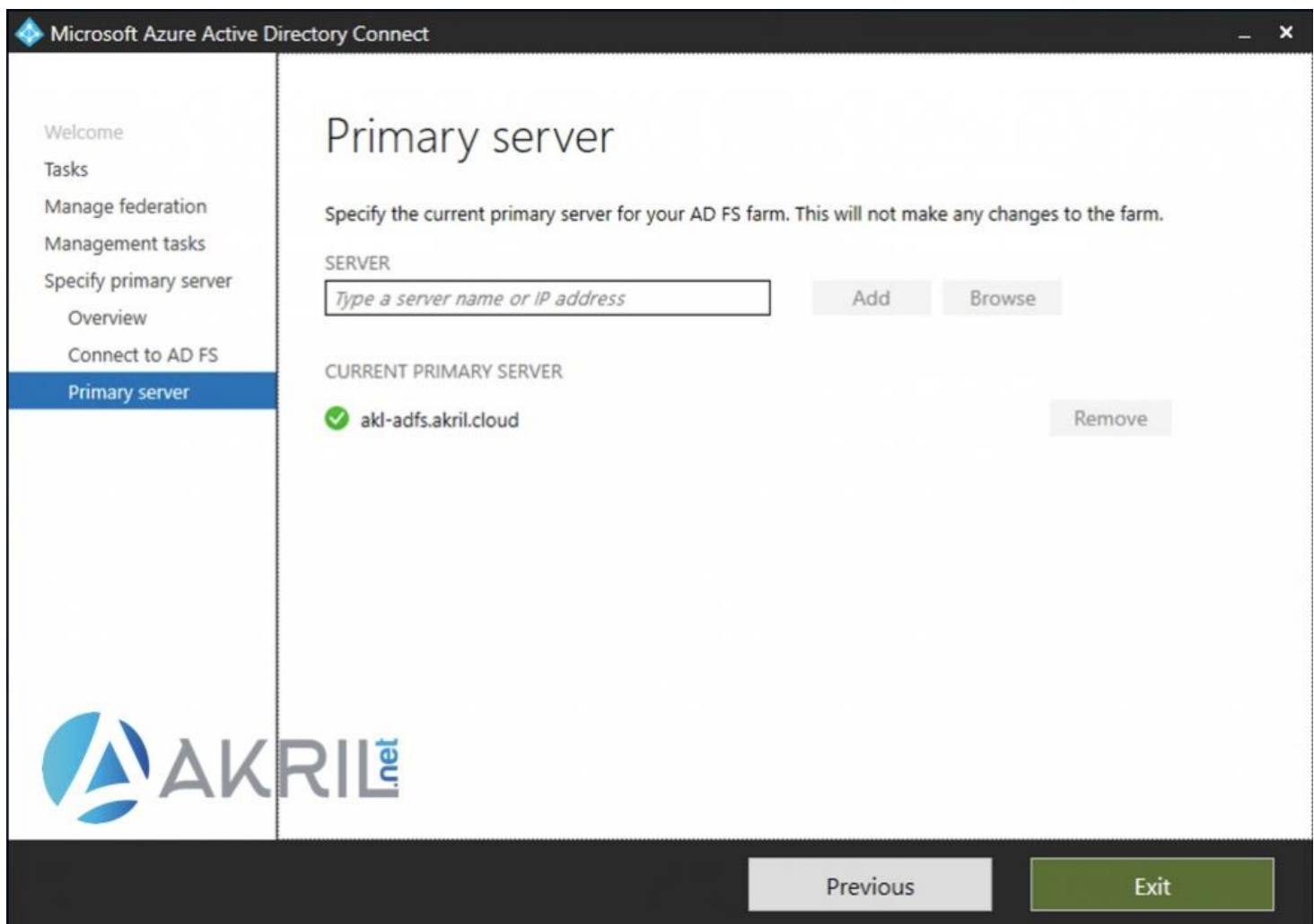
Azure AD Connect requires AD FS administrator credentials with local administrator privileges on the servers to perform the SSL certificate update.

USERNAME 

PASSWORD

Previous Next

Compte Admin pour se connecter à votre ADFS



Ajout du serveur ADFS

Vous pouvez saisir manuellement le nom court ou long de votre serveur ADFS ou bien utiliser le bouton **Browse** pour qu'il soit détecté par votre AAD Connect.

The screenshot shows the 'AD FS servers' configuration page in Microsoft Azure Active Directory Connect. The left sidebar contains a navigation menu with the following items: Welcome, Tasks, Manage federation, Management tasks, Update SSL, Connect to AD FS, Federation servers (highlighted), Proxy servers, SSL Certificate, Servers, and Configure. The main content area is titled 'AD FS servers' and includes the instruction 'Specify the AD FS servers in the farm.' Below this is a 'SERVER' input field with the placeholder text 'Type a server name or IP address', an 'Add' button, and a 'Browse' button. A table below the input field lists the configured servers:

Server	Connectivity	SSL Expiry Date	
akl-ads.akril.cloud	✓	08/03/2022	Remove

At the bottom of the page, there are 'Previous' and 'Next' navigation buttons. The AKRIL.net logo is visible in the bottom left corner.

Ajout du serveur ADFS

Normalement, vous pouvez passer sans rien changer sur l'option **Proxy servers** car le serveur WAP n'est pas géré par le serveur AAD Connect.

The screenshot shows the 'SSL Certificate' configuration window in Microsoft Azure Active Directory Connect. The window title is 'Microsoft Azure Active Directory Connect'. On the left, a navigation pane lists various tasks, with 'SSL Certificate' selected. The main area is titled 'SSL Certificate' and contains the following text: 'Specify the new SSL certificate to update the AD FS and Web Application Proxy servers.' Below this, there is a 'CERTIFICATE FILE' label with a help icon, a text input field containing the path 'C:\Users\tgibard\Desktop\adfsproxy.pfx', and a 'Browse' button. A 'Certificate Details' section lists the following information:

Subject Name:	login.akril.co
Effective Date:	3/7/2020 1:00:00 AM
Cutover Date:	4/2/2022 1:00:00 PM
Expiration Date:	3/8/2022 1:00:00 PM
Thumbprint:	043CAD3302928D4E6CCB8792D16361397379324A
Serial Number:	0D90577FBC11613BBE0D4FF0B77900DF

At the bottom left, there is a watermark logo for 'AKRIL.net'. At the bottom right, there are 'Previous' and 'Next' navigation buttons.

Ajout du certificat

Dans mon cas, je n'ai pas pu utiliser le format de certificat délivré par Digitcert via l'assistant d'AAD Connect. **J'ai donc réalisé un export classique depuis le serveur ADFS.** Le nouveau fichier généré porté l'**extension pfx** et j'ai pu le charger dans l'assistant AAD Connect.


Microsoft Azure Active Directory Connect

Welcome
Tasks
Manage federation
Management tasks
Update SSL
Connect to AD FS
Federation servers
Proxy servers
SSL Certificate
Servers
Configure

Select servers for SSL certificate update

Select the servers on which the SSL certificate will be updated. ?

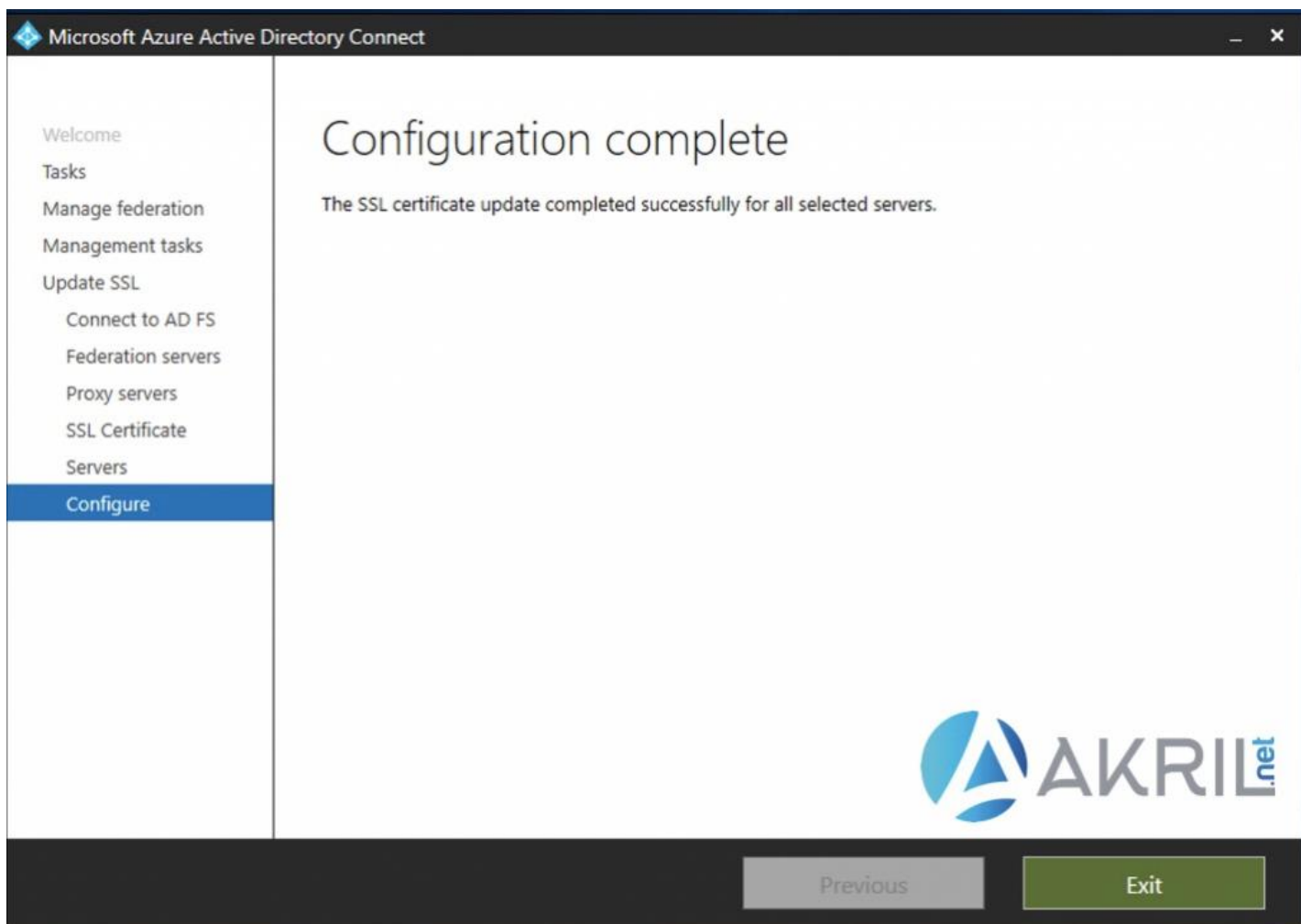
<input checked="" type="checkbox"/>	Server	Role	Connectivity	SSL Expiry Date
<input checked="" type="checkbox"/>	akl-ads.akril.cloud	ADFS [Primary]	✔	08/03/2022



Previous Next

Test de connectivité

Le certificat est confirmé comme étant valide.




Fin de la configuration

La configuration est terminée.

Microsoft Azure Active Directory Connect

Federation configuration



Active Directory Federation Services (AD FS) settings are listed below.

FEDERATION SERVICE NAME	login.akril.co	FEDERATION SERVICE ACCOUNT	AKRIL\gmsa-adfs\$
PRIMARY SERVER	akl-adfs.akril.cloud	FARM BEHAVIOR LEVEL	3

SSL CERTIFICATE

Subject Name:	CN=login.akril.co
Effective Date:	03/07/2020 01:00:00
Expiration Date:	03/08/2022 13:00:00
Thumbprint:	043CAD3302928D4E6CCB8792D16361397379324A

TOKEN SIGNING CERTIFICATE

Subject Name:	CN=ADFS Signing - login.akril.co
Effective Date:	03/07/2020 20:40:02
Expiration Date:	03/07/2021 20:40:02
Thumbprint:	7514462DCCF3DCCE331FFCD0E46C2F250E391E98

This page is updated when you perform a federation management task that connects to AD FS.

Previous Exit

Récapitulatif de la configuration fédérée

Si besoin, vous pouvez relancer l'assistant d'AAD Connect pour voir un résumé de la configuration en mode Fédération (URL, certificat, etc.).

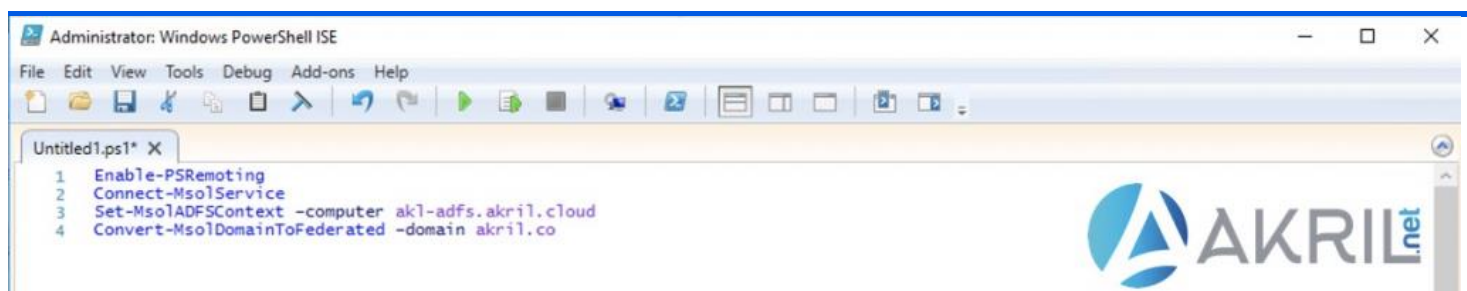
Activer la fédération via votre ADFS

Tous les éléments sont en place pour nous permettre de nous identifier en mode fédérée auprès de O365 et des services Cloud Microsoft.

Il nous reste maintenant à **activer notre domaine en mode fédéré** pour que cela fonctionne.

Depuis le serveur AAD Connect, exécutez maintenant les quelques commandes PowerShell ci-dessous (à adapter à votre cas bien entendu) :

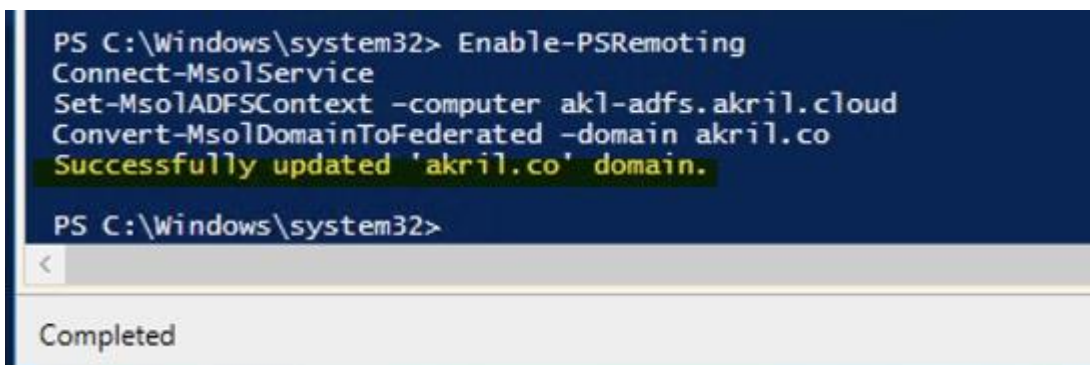
```
Connect-MsolService  
  
Set-MsolADFSContext -Computer akril-adfs.akril.cloud  
  
Convert-MsolDomainFederated -domain akril.co
```



Remplacez les noms en fonction de votre infrastructure

Lorsque vous devrez vous identifier, utilisez un compte "*pure-cloud*" et non pas un compte synchronisé.

Identifiez-vous avec un compte `user@tenant.onmicrosoft.com`



Confirmation PowerShell, c'est terminé !

Vérifier et tester la configuration

Avant de tester, sachez que vous pouvez vérifier que votre domaine est désormais fédéré depuis le portail Azure Active Directory, AAD Connect.

The screenshot shows the Azure Active Directory portal interface. On the left is a navigation pane with a search bar and a list of categories: Overview, Getting started, Diagnose and solve problems, and Manage. Under 'Manage', 'Azure AD Connect' is highlighted with a red box. The main content area is divided into several sections:

- PROVISION FROM ACTIVE DIRECTORY**
 - Azure AD Connect cloud provisioning**: This feature allows you to manage provisioning from the cloud. [Manage provisioning \(Preview\)](#)
 - Azure AD Connect sync**

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled
- USER SIGN-IN** (highlighted with a red box)

Federation	Enabled	1 domain
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Disabled	0 agents
- STAGED ROLLOUT OF CLOUD AUTHENTICATION**

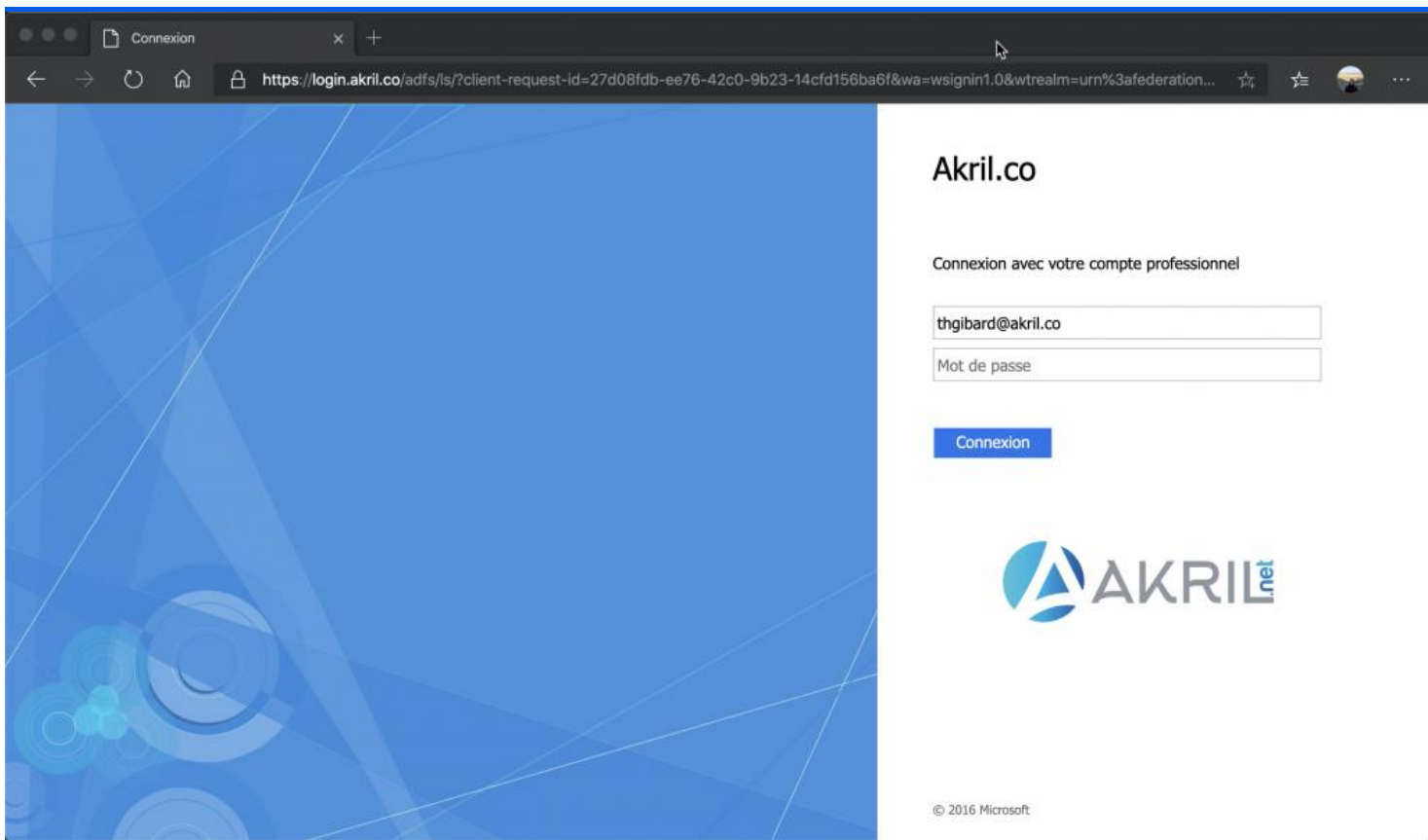
This feature allows you to test cloud authentication and migrate gradually from federated authentication. [Enable staged rollout for managed user sign-in \(Preview\)](#)
- ON-PREMISES APPLICATIONS**

Looking to configure remote access for on-premises applications? [Head to Application Proxy](#)
- HEALTH AND ANALYTICS**

Monitor your on-premises identity infrastructure and synchronization services in the cloud. [Azure AD Connect Health](#)

Statut Fédération depuis portail Azure Active Directory

Si vous aviez bien ouvert les flux (*depuis l'extérieur vers votre serveur WAP, 443/TCP*), alors vous pouvez tenter de vous identifier en accédant à portal.office.com ou au portail Azure. **Une fois votre adresse email saisie, vous devriez être redirigé vers votre page ADFS pour finaliser l'authentification.** Si elle est validée, vous serez ensuite redirigé vers le service désiré.



Test d'authentification en mode fédéré avec ADFS

C'est terminé !

Vous pouvez désormais vous identifier sans partager avec Microsoft la version hashé de vos mots de passe.

Et ajoutons à cela que cette ferme ADFS peut être utilisée pour de nombreux autres besoins.