Guide technique

Fédération canadienne d'accès

Installation d'ADFSToolkit

Version : 1.0.0

Dernière révision : 16 avril 2018

Soutien technique : tickets@canarie.ca

canarie.ca | @canarie_inc

Table des matières

1. Comment utiliser ce guide

1.1 Préambule

ADFSToolkit a été conçu pour assurer une configuration rapide des Active Directory Federation Services (AD-FS v3 ou version plus récente) et vous aider à vous connecter au service de gestion fédérée des identités (GFI) de la Fédération canadienne d'accès de CANARIE. ADFSToolkit accélère l'installation et la configuration des services de la FCA, qui ne nécessitent que quelques minutes, et propose des techniques permettant de gérer la fiabilité de façon évolutive.

1.2 Public visé

Ce guide est destiné à ceux qui planifient, préparent, installent et administrent les services de la FCA à leur institution.

1.3 Compétences et connaissances requises pour l'installation

Bien que les outils et le processus d'installation aient été conçus pour exiger le savoir le plus rudimentaire possible, de manière générale, les compétences et les connaissances que voici auraient leur utilité.

1.3.1 Connaissance du fonctionnement de l'institution

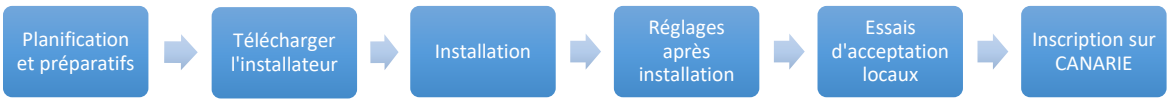
- Technologies d'ouverture de séance à partir d'Internet
- Stratégie de gestion des services et du déploiement
- Administration de l'Active Directory Federation Service
- Capacité à parcourir, configurer et gérer les volets de l'Active Directory Federation Service (services démarrage/arrêt, gestion de la configuration du service AD-FS, examen des registres, etc.)
- Capacité à télécharger, configurer et exécuter les scripts PowerShell
- Configuration et gestion du pare-feu, et capacité d'obtenir les mises à jour

1.3.2 Compétences et technologies dont la connaissance est recommandée

- Stratégies et techniques d'ouverture de séance par Internet
- Méthodes d'essai et de contrôle des modifications

2 Déroulement de l'installation

Pour mener à bien l'installation, la configuration et la vérification des services de la FCA sur une plateforme d'essai ou de production, on suivra les étapes illustrées ci-dessous.



3 Planifier l'installation

3.1 Exigences du système

On installera ADFSToolkit de CANARIE sur Windows Server (votre hôte AD-FS) présentant les caractéristiques que voici :

- Microsoft AD-FS v3 ou version plus récente;
- administrateur local autorisé à ordonnancer les tâches privilégiées;
- autorisations du niveau administrateur AD-FS permettant l'usage des commandes PowerShell;
- acceptation des considérations de sécurité applicables à l'usage de PowerShell obtenues de PowerShellgallery.com de Microsoft.

Bien que l'exigence ne soit pas indispensable, nous vous suggérons vivement d'installer AD-FS sur une plateforme d'essai avant de l'installer sur l'environnement de production. Sachez qu'une fois l'installation terminée, le jeu d'outils servant à l'administration, Microsoft Management Console (MMC) d'AD-FS, affichera quelques milliers de certificats de fiabilité.

3.1.1 Système d'exploitation minimal du serveur

Le serveur devrait utiliser au moins Windows Server 2012 R2 ou une version plus récente comme système d'exploitation. Vous devriez aussi avoir installé les plus récents correctifs de sécurité fournis par Microsoft.

3.1.2 Version minimale de PowerShell

ADFSToolkit utilise PowerShell de Microsoft avec Windows Management Framework (WMF) 5.1. Pour savoir si votre hôte accepte WMF5.1, veuillez consulter le tableau Compatibilité de WMF 5.1 avec les systèmes d'exploitation de Microsoft.

Pour déterminer rapidement la version de PowerShell que vous utilisez, ouvrez une fenêtre PowerShell ou PowerShell ISE et saisissez $PSVersionTable. Si la version affichée n'est pas 5.1, vous devrez d'abord actualiser la plateforme.

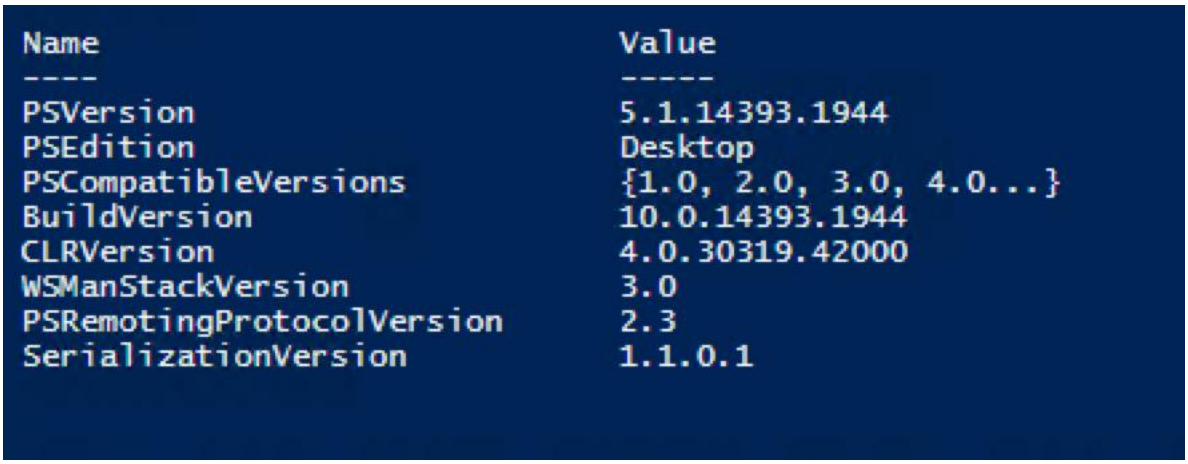


Figure 1 – Version 5.1 de PowerShell, le minimum requis pour l'installation

Pour télécharger WMF 5.1 : https://docs.microsoft.com/fr-fr/PowerShell/wmf/5.1/install-configure

ADFSToolkit ne pourra être installé tant que la plateforme n'a pas été actualisée au moins avec cette version de PowerShell.

3.1.3 Diffusion des attributs

ADFSToolkit est un composant créé par et pour le milieu de la recherche et de l'éducation (R-E). Il intègre les principes de gestion évolutifs de la diffusion des attributs adoptés par les fédérations R-E. Un de ces principes concerne l'usage de catégories d'entités pour diffuser les attributs, c'est-à-dire des balises désignant des entités en langage SAML2, soit des métadonnées indiquant l'appartenance à un groupe de services particulier. La politique de diffusion des attributs du modèle qui utilise les catégories d'entités se fonde sur la catégorie, pas l'entité.

Quand il répartit les entités à charger dans AD-FS et rencontre l'entité « Research & Scholarship » (R&S)[1], ADFSToolkit crée automatiquement de multiples règles de transformation AD-FS qui reflètent le minimum d'attributs à diffuser, ce qui n'est pas sans ressembler aux pages publiques de l'annuaire de l'institution. Pour les entités R&S, ces attributs sont les suivants :

- eduPersonPrincipalName (la partie à gauche du signe @ de l'UPN, combinée au domaine)
- adresse courriel
- displayName (nom affiché)
- givenName (prénom)
- sn (nom de famille)

[1] https://refeds.org/category/research-and-scholarship

- eduPersonScopedAffiliation (selon la terminologie arrêtée pour les groupes dans AD)

ADFSToolkit procède de cette façon par défaut. En utilisant cet outil, vous activez le modèle de diffusion des attributs par défaut. Nous vous incitons à communiquer avec CANARIE pour indiquer que votre organisation accepte la catégorie d'entités « Research & Scholarship » pour profiter de tous ses avantages. Suivez le lien que voici pour en apprendre davantage : https://www.canarie.ca/identity/fim/research-and-scholarship-entity-category/,

4 Installation

Le téléchargement d'ADFSToolkit s'effectue par le service PowerShellGallery.com de Microsoft qui en devient le canal de distribution officiel, ADFSToolkit étant un module PowerShell. De cette façon, on pourra profiter de l'approche retenue par Microsoft pour gérer la diffusion et la mise à jour des modules PowerShell durant le cycle de vie complet d'ADFSToolkit.

Pour installer ADFSToolkit, vous devrez :

- visiter https://PowerShellgallery.com et suivre les instructions pour installer le plus récent module PowerShellGet de PowerShellGallery;
- modifier votre politique d'exécution pour les scripts PowerShell sur le serveur AD-FS.

4.1 Sécurité – Conditions requises

On présume que l'installation sera effectuée en totalité par un utilisateur détenant les privilèges à la fois d'un administrateur local et d'un administrateur AD-FS. CANARIE a amorcé le processus pour obtenir un certificat qui sécurisera la diffusion d'ADFSToolkit par la PowerShellGallery, source reconnue pour sa fiabilité. En attendant que la certification soit chose faite, ADFSToolkit devra pouvoir exécuter les modules AD-FS d'origine incertaine.

Pour que le système accepte les paramètres de la politique d'exécution d'ADFSToolkit, on assouplira cette dernière en exécutant la commande PowerShell que voici.

```
PowerShell

Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
```

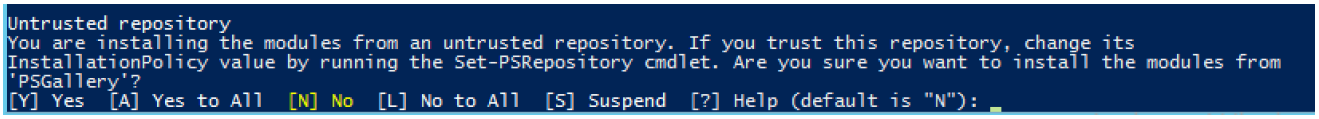
4.2 Installation du module

Pour installer le module, lancer la commande que voici.

```
PowerShell

Install-Module –name ADFSToolkit
```

Si vous n'avez jamais installé d'éléments de la PowerShell Gallery, il se pourrait que l'avertissement suivant s'affiche à l'écran :



Actualisez PowerShell Gallery pour lui accorder le statut de source fiable ou répondez « Y » afin de poursuivre.

Le module s'installera une fois la connexion établie. Le répertoire d'installation par défaut est :

C:\Program Files\WindowsPowerShell\Modules\ADFSToolkit\[version #]

4.3 Configuration d'ADFSToolkit pour la Fédération canadienne d'accès de CANARIE

La Fédération canadienne d'accès (FCA) de CANARIE produit deux agrégats de métadonnées fiables qu'AD-FS doit charger : l'agrégat national, qui regroupe les éléments canadiens, et l'agrégat inter-fédération, qui rassemble les entités de recherche et d'éducation mondiales auxquelles adhère le Canada. Avec ces deux agrégats, plus d'un millier de parties utilisatrices (PU) s'ajouteront à l'infrastructure AD-FS de l'institution.

Par souci de simplicité, ADFSToolkit a été conçu de manière à ne charger qu'un agrégat à la fois. Pour être totalement connecté à la FCA, vous aurez besoin de deux fichiers de configuration, c'est-à-dire un par agrégat. Une commande d'ADFSToolkit crée le fichier de configuration requis et peut s'occuper du chargement (mise à jour automatique des agrégats de métadonnées).

4.4 Initialisation automatique de la fiabilité

La seule vérification qu'AD-FS effectue au niveau des données consiste à déterminer si le point terminal de l'adresse HTTPS est valable. Une validation aussi restreinte est insuffisante pour que l'AD-FS fasse partie du cercle de confiance d'une fédération. ADFSToolkit rehausse la fiabilité d'AD-FS en en faisant un point terminal de confiance au sein de la fédération. Il y parvient de la manière suivante :

- en vérifiant la véracité de la clé servant d'empreinte SHA256 que fournit l'institution;

- à partir de cette clé, vérification que l'agrégat n'a pas changé depuis l'utilisation de la signature cryptographique.

ADFSToolkit s'assure que le contenu est valable et sécuritaire avant le chargement d'AD-FS et que le tout vient d'une autorité fiable, en l'occurrence la FCA de CANARIE.

Cette méthode de validation employée par ADFSToolkit dépend de la transmission par l'utilisateur de l'empreinte du certificat auquel il accorde sa confiance.

L'empreinte SHA256 du certificat de CANARIE est :

36CFD8090A88B8D75264E790FEA1B6F7ECBECF42C881AAF6F459D3AE3B459304

Il est possible de vérifier manuellement cette empreinte comme suit :

- en récupérant la partie publique du certificat que CANARIE utilise pour signer ses agrégats à l'adresse https://caf-shib2ops.ca/CoreServices/caf_metadata_verify.crt;
- en utilisant la commande OpenSSL ci-dessous pour trouver l'empreinte du certificat qui vient d'être téléchargé :

```
canlt084:tmp$ openssl x509 -noout -fingerprint -sha256 -inform pem -in ./caf_metadata_verify.crt
SHA256
Fingerprint=36:CF:D8:09:0A:88:B8:D7:52:64:E7:90:FE:A1:B6:F7:EC:BE:CF:42:C8:81:AA:F6:F4:59:D3:AE:3
B:45:93:04
```

Les informations les plus récentes concernant la configuration sont disponibles dans la section « identité » du site Web de CANARIE, sous la rubrique « Soutien FCA, Outils GFI » : (https://www.canarie.ca/identity/support/fim-tools/)

4.5 Configuration de l'agrégat canadien de la FCA

Pour créer le fichier de configuration de l'agrégat canadien de la FCA, exécuter la commande que voici :

```
PowerShell

New-ADFSTkConfiguration
```

Vous devrez fournir les réponses indiquées dans le tableau ci-dessous, ce qui créera un fichier de configuration sur le disque. Une autre possibilité serait de créer une tâche afin que l'agrégat soit traité à une heure précise. La tâche inscrite au calendrier est désactivée par défaut.

Question	Réponse
Agrégat de métadonnées	https://caf-shib2ops.ca/CoreServices/caf_metadata_signed_sha256.xml
Empreinte du certificat	Empreinte de la Fédération canadienne d'accès : 36CFD8090A88B8D75264E790FEA1B6F7ECBECF42C881AAF6F459D3AE3B459304
Préfixe des métadonnées	• Il s'agit du préfixe ajouté à chaque partie utilisatrice (PU, ou fournisseur de service) dans AD-FS. Le préfixe par défaut est ADFSTk. • Nous préconisons l'usage de préfixes différents pour chaque agrégat, car cela permet d'en distinguer l'origine quand on s'efforce de détecter les différences dans le service AD-FC en effectuant la comparaison avec l'agrégat. • Précisons que le symbole (:) est employé comme séparateur et ne peut faire partie préfixe.
Nom de l'institution	• Sert à peupler l'attribut « o » correspondant au nom de l'organisation. • Le titre officiel de l'organisation est la valeur recommandée.
Nom du pays	• Sert à peupler l'attribut « co » correspondant au nom du pays. • La valeur recommandée est « Canada ».
Code du pays	• Sert à peupler l'attribut « c » correspondant au code du pays. • La valeur recommandée est « CA ».
Domaine de l'institution	• La valeur recommandée est le domaine de l'institution. • Sert à établir la portée de certains attributs pour garantir l'usage d'identifiants uniques dans le monde.
Nom abrégé de l'institution	• La valeur recommandée est l'abréviation couramment employée pour désigner l'institution, par exemple UdM pour Université de Montréal.
DNS externe de votre infrastructure AD-FS	• Nom de domaine complet (FQDN) de l'instance AD-FS de l'organisation

Une fois la configuration terminée, vous trouverez le fichier XML résultant dans le répertoire « /config » de l'arborescence de base de PowerShell Module. C'est ce fichier qui sera traité lors de l'exécution ultérieure de la commande PowerShell qui chargera (ou synchronisera) l'agrégat de métadonnées dans AD-FS.

```
PowerShell Hint: Use this to see ADFSToolkit's Module base directory

Get-Module –Name ADFSToolkit).ModuleBase
```

Un nouveau répertoire sera également créé sur le disque dans C:\ADFSToolkit\. Un sous-répertoire indiquera la version du module utilisée. Ce sous-répertoire contiendra la tâche inscrite au calendrier sync-ADFSTkAggregates.ps1 et les configurations spécifiques aux versions antérieures d'ADFSToolkit. De cette façon, on pourra charger (ou recharger) un ou plusieurs agrégats avec la même commande et les versions précédentes d'ADFSToolkit seront conservées lors des mises à jour. Dans le présent document,

le répertoire de la plus récente version d'ADFSToolkit (C:/ADFSToolkit/#.#.#.#/) correspond au dernier répertoire principal d'ADFSToolkit.

Les exécutions subséquentes de la commande « New-ADFSTkConfiguration » de PowerShell annexeront une commande pour que cet agrégat soit chargé dans le script sync-ADFSTkAggregates.ps1 de PowerShell.

4.6 Chargement de l'agrégat canadien de la FCA

Après configuration de l'agrégat canadien, le plus récent répertoire principal d'ADFSToolkit contiendra le script PowerShell <sync-ADFSTkAggregates.ps1> servant à le charger. Pour ce faire, il suffit de lancer la commande sync-ADFSTkAggregates.ps1 et d'observer le résultat sur l'écran ou avec l'utilitaire Event Viewer, dans le registre des événements d'ADFSToolkit.

Cette commande est conçue pour s'exécuter en boucle et synchroniser l'agrégat afin qu'il reste à jour. À la première exécution, la synchronisation de toutes les entités prendra un peu plus d'une minute, à raison d'environ cent entités par minute. Les exécutions suivantes seront plus rapides, puisque les fichiers auront déjà été créés et ne seront actualisés que quand une modification est détectée.

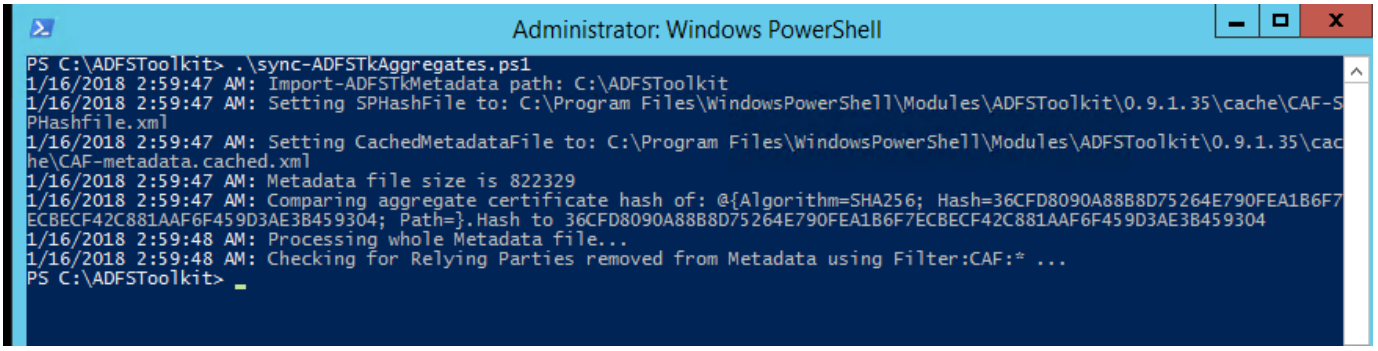


Figure 2 – Illustration du chargement de l'agrégat canadien de la FCA

Si tout semble être dans l'ordre, on ajoutera le deuxième agrégat de la FCA (inter-fédération) en lançant de nouveau la commande New-ADFSTkConfiguration, avec les modifications mineures indiquées à la partie 4.9.

Remarque : Vous noterez quelques erreurs ou avertissements dans la fenêtre de la console PowerShell. La chose est normale. Vous pourrez vérifier les détails avec l'utilitaire Event Viewer et déterminer la gravité des erreurs puis prendre des mesures, si besoin est (lire la partie 4.11 pour en savoir plus).

4.7 Que faire en cas de problème

Si vous voulez annuler ou retrancher les certificats de confiance créés après chargement de l'agrégat pour quelque raison que ce soit, nous avons créé une commande dans ADFSToolkit intitulée unpublish-

ADFSTkAggregates le permettant. Si la commande est lancée sans argument, le système présumera que le préfixe par défaut est « ADFSTk ». Ce préfixe correspond à la valeur établie pour chaque entité à son chargement et se trouve dans le fichier de configuration. Il est inutile d'utiliser le symbole « : » comme séparateur entre les préfixes.

Cette commande sélectionnera toutes les entités comportant le préfixe et les supprimera. Faites très attention en l'utilisant, car la destruction est définitive.

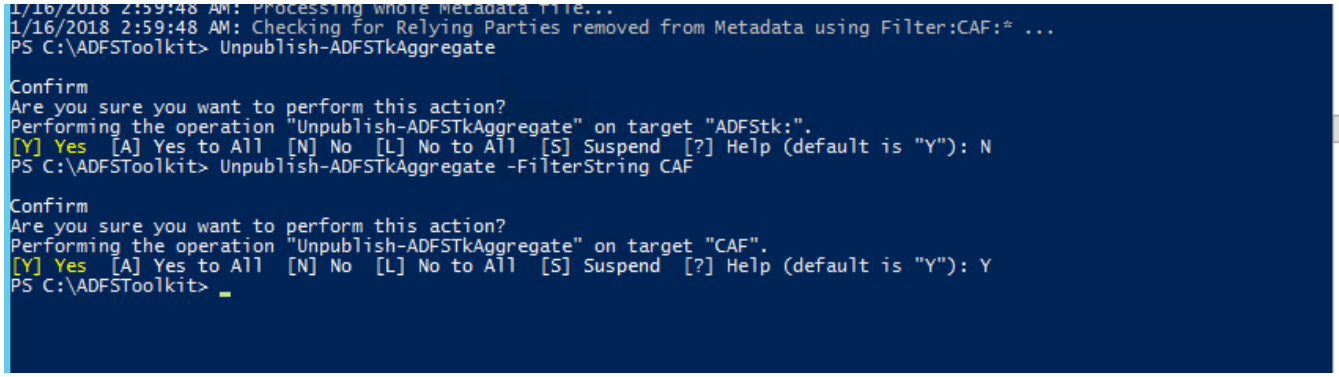


Figure 3 – Illustration de unpublish-ADFSTkAggregates (avec et sans argument FilterString)

4.8 Configuration de l'agrégat inter-fédération de la FCA

Pour créer le fichier servant à configurer l'agrégat inter-fédération de la FCA, relancer la commande New-ADFSTkConfiguration en utilisant les réponses déjà fournies (section 4.5), mais en modifiant l'URL de l'agrégat et le préfixe des métadonnées.

Remarques

- Vous devez changer le préfixe des métadonnées pour qu'il n'y ait pas collision avec d'autres agrégats et les mémoires caches qu'ADFSToolkit utilise en dehors d'AD-FS.
- Cet agrégat utilise la même clé de signature de la FCA, donc l'empreinte reste la même.

URL des métadonnées de l'agrégat inter-fédération de la FCA
https://caf-shib2ops.ca/CoreServices/caf_interfed_signed.xml

Empreinte du certificat
36CFD8090A88B8D75264E790FEA1B6F7ECBECF42C881AAF6F459D3AE3B459304

Nouveau préfixe des métadonnées
CAF-Interfed

Cette configuration annexera la commande sync-ADFSTkAggregates.ps1 au plus récent répertoire principal d'ADFSToolkit, pourvu que laissiez faire le système quand il vous le demandera.

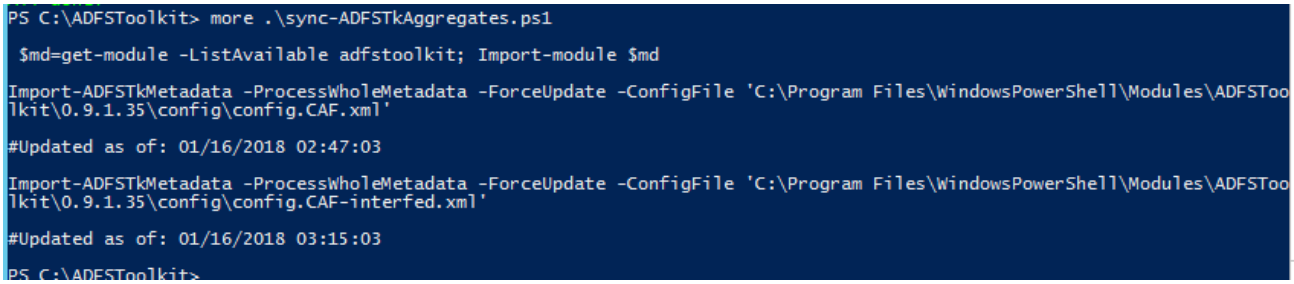


Figure 4 - sync-ADFSTkAggregates.ps1 une fois la deuxième configuration terminée

4.9 Chargement de l'agrégat inter-fédération de la FCA

Pour charger l'agrégat inter-fédération, il suffit d'exécuter de nouveau la commande sync-ADFSTkAggregates.ps1 dans le plus récent répertoire principal d'ADFSToolkit et d'observer ce qui se passe sur l'écran ou dans le registre des événements de l'utilitaire Event Viewer d'ADFSToolkit.

Remarque : *L'agrégat inter-fédération est passablement plus important. Le chargement devrait donc prendre entre 45 et 60 minutes.*

L'agrégat inter-fédération de la FCA comprend plus de 1 100 entités (30 Mo). Pour ne pas congestionner AD-FS ou éviter une trop grande latence, ADFSToolkit importe les entités par lot de 80 (valeur par défaut) lors du processus de création.

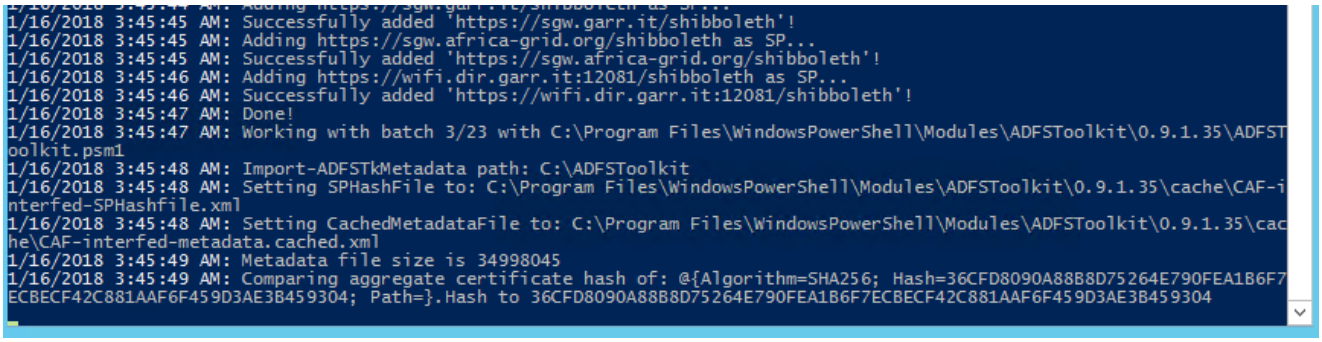
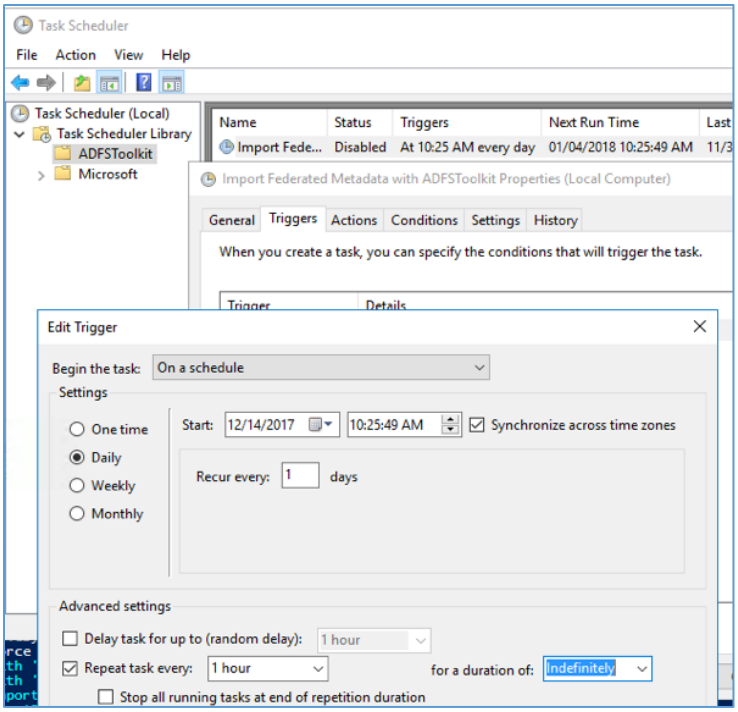


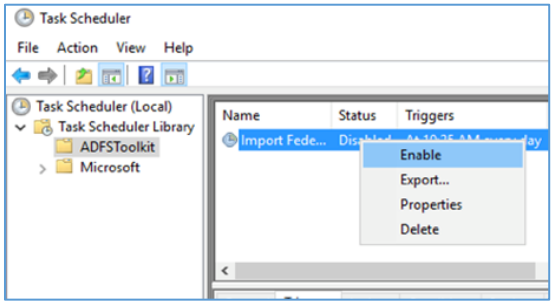
Figure 5 – Illustration du chargement par lot automatique d'ADFSToolkit

4.10 Ordonnancement de l'exécution de sync-ADFSTkAggregates

ADFSToolkit inscrit automatiquement une tâche au calendrier en lui donnant par défaut le statut « désactivé », ce qui vous permet de modifier les paramètres de configuration et de les tester avant que la tâche ne s'exécute automatiquement au moment voulu.

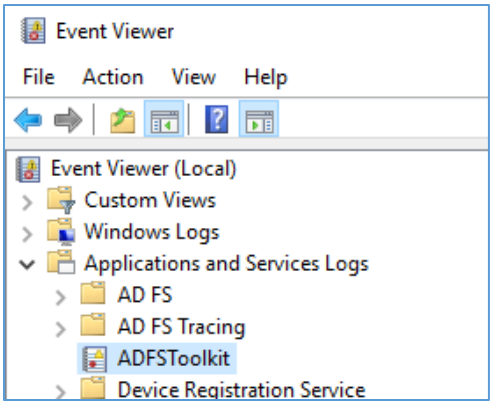
Nous préconisons un cycle horaire afin que le système AD-FS soit toujours synchronisé avec les métadonnées de la FCA. L'activation devrait être confiée à l'administrateur.





4.11 Examen des registres d'exécution

ADFSToolkit se sert de l'architecture du journal des événements de Microsoft Windows pour enregistrer les applications, qu'on peut ensuite consulter avec l'utilitaire Event Viewer. Chaque événement exécuté manuellement qui apparaît sur la ligne de commande s'ajoute au journal, conformément aux recommandations de Microsoft pour la rotation des registres.



5 Configuration de la diffusion des attributs

ADFSToolkit externalise les paramètres de diffusion de chaque partie utilisatrice (PU) en plaçant les politiques de diffusion hors d'AD-FS, dans un script de PowerShell situé dans le sous-répertoire « config » du plus récent répertoire principal d'ADFSToolkit (C:/ADFSToolkit/#.#.#.#/config/get-ADFSTkManualSPSettings.ps1).

De cette manière, l'administrateur peut actualiser la diffusion des attributs d'une PU quelconque chaque fois qu'il y a exécution du script PowerShell. L'administrateur du système AD-FS dispose ainsi d'un moyen commode pour gérer centralement la diffusion des attributs au lieu d'avoir à retrouver un élément dans la console d'administration du système, qui pourrait énumérer des milliers de PU.

Le script comprend plusieurs jeux d'attributs qu'on peut copier puis appliquer après suppression des commentaires qui les accompagnent. Les lignes commençant par le signe dièse « # » signalent un commentaire et le code ou la commande qui suit ne sera donc pas exécuté.

Le script PowerShell à modifier pour diffuser les attributs est le suivant :

```
PowerShell

~<latest_ADFSToolkit_home_dir>/config/get-
ADFSTkLocalManualSPSettings.ps1
```

Il est possible de voir des illustrations de paramètres avec la fonction Get Help de PowerShell de MicroSoft une fois qu'on a établi PowerShell comme source pour accéder à cette commande :

```
PowerShell

. ~<latest_ADFSToolkit_home_dir>/config/get-
ADFSTkLocalManualSPSettings.ps1
Get-help get-ADFSTkLocalManualSPSettings -Detailed
```

```
PS C:\ADFSToolkit\0.9.1.60\config> . .\get-ADFSTkLocalManualSpSettings.ps1

PS C:\ADFSToolkit\0.9.1.60\config> get-help get-ADFSTkLocalManualSPSettings -Detailed

NAME
    get-ADFSTkLocalManualSPSettings

SYNOPSIS
    This is the file that site admins edit to locally control per Relying Party/Service provider attribute release.
    ADFSToolkit attempts to detect the presence of variable ADFSTkSiteSPSettings and then ingest it to control specific rules.
```

6 Comportement opérationnel d'ADFSToolkit

ADFSToolkit (PowerShell Module) est conçu pour être installé une seule fois par appareil. Nous ne recommandons pas d'installer plusieurs instances actives d'ADFSToolkit sur le même hôte et cette solution ne bénéficie d'aucun soutien technique. Plusieurs versions du module existeront pendant sa mise à jour. Après être passé à la version la plus récente, mais avant de relancer le service, nous vous recommandons de placer l'ancien répertoire (version) ailleurs qu'à l'emplacement par défaut que consulte Powershell quand il fonctionne.

À cause de sa conception modulaire, ADFSToolkit favorise la simplification et la réutilisation du code. En d'autres termes, les paramètres et les configurations peuvent être réemployés, peu importe le nombre d'agrégats chargés. Les décisions et les considérations sur le plan opérationnel devraient prendre en compte les règles de l'art que voici.

- Les modifications apportées au script de PowerShell ADFSTkLocalManualSPSettings.ps1 dasn le plus récent répertoire principal d'ADFSToolkit doivent respecter la syntaxe et la fonction de PowerShell.
    - Le script s'applique à l'exécution, pour toutes les tâches et installations prévues au calendrier. Si vous modifiez le script et en enregistrez une version incomplète, la tâche en sera affectée, avec possibilité d'échec ou d'exécution incomplète, deux situations qui pourraient influer sur la stabilité du service de production.
    - Avant d'apporter des changements au script, exécutez toujours une copie de sauvegarde pour pouvoir revenir au dernier « état stable » s'il y a lieu.
    - Nous préconisons vivement d'utiliser une plateforme externe, distincte de l'environnement de production, lors du développement et des essais. Une fois qu'on aura vérifié toutes les modifications, on pourra copier et exécuter le script en toute confiance sur la plateforme de production.
- Le script ADFSTkLocalManualSPSettings.ps1 n'est installé qu'une fois et s'applique quel que soit l'agrégat traité.
    - Par conséquent, la diffusion des attributs est centralisée dans un fichier, PEU IMPORTE le nombre d'agrégats, et il est inutile de copier le script pour effectuer une autre tâche.

- **ATTENTION.** Une fois les modifications à ADFSTkManualSPSettings.ps1 terminées, vous DEVREZ relancer la commande Import-Module d'ADFSToolkit pour saisir les changements. Par la même occasion, vous validerez vos paramètres PowerShell au cas où un problème surviendrait (à savoir, échec du rechargement du module).

6.1 Gestion du cycle de vie d'ADFSToolkit

Le module d'ADFSToolkit utilise la commande Update-Module de PowerShell Gallery pour gérer les mises à jour. Les institutions qui recourent à ADFSToolkit sont vivement encouragées à mettre en place un système d'essai pour vérifier les changements apportés d'une version à l'autre. En l'absence d'un tel système, on préconise de saisir un instantané de l'environnement ou de procéder à une copie de sauvegarde.

Veuillez noter que certaines mises à jour pourraient nécessiter la suppression des fichiers de la mémoire cache, puis devoir être exécutées de nouveau pour que les nouvelles fonctions s'appliquent. Les notes accompagnant la mise à jour indiqueront si c'est le cas. L'exploitant du site établira quand procéder et réservera assez de temps pour que les nouveaux et meilleurs paramètres soient recalculés. ADFSToolkit a été conçu pour être idempotent, ce qui signifie que le jeu d'attributs résultant reste le même, peu importe le nombre de fois où l'outil est utilisé.

La bonne façon de gérer une mise à jour d'ADFSToolkit est décrite ci-dessous.

- Créer une copie de sauvegarde du répertoire C:\ADFSToolkit.
- Saisir un instantané du système ou établir un point de reprise.
- Désactiver ou reporter à plus tard les tâches inscrites au calendrier d'ADFSToolkit.
- Établir « Update-Module ADFSToolkit ».
    - Lors de son exécution, Update-Module vérifiera s'il y a une version plus récente dans PowerShellGallery.com et la téléchargera.
    - Veuillez noter que chaque module est enregistré dans son propre répertoire, qui indiquera la version du script. ADFSToolkit ne fonctionnera pas correctement s'il y a plus d'une version disponible; une fois la nouvelle version installée sur le disque et qu'elle est accessible, nous vous recommandons de placer la version antérieure à un autre endroit afin que PowerShell n'ait accès qu'à la version la plus récente.
- Déplacer le fichier de configuration existant et les fichiers correspondant de la mémoire cache.
    - La chose est possible, mais si vous avez déjà modifié les paramètres manuellement, vous devrez appliquer de nouveau ces corrections au nouveau fichier de configuration. Il y a deux façons de le faire :
        - configurer d'abord, en saisissant les réponses manuellement

          OU

        - tirer parti de la fonction pipeline de New-ADFSTKConfiguration, qui ingèrera la configuration existante et ira chercher la plupart des paramètres existants pour leur donner le bon format.

Quelle que soit la stratégie retenue, vous devrez inspecter le résultat pour vous assurer que les corrections manuelles ont bien été incorporées.

Illustration de l'intégration de l'ancienne configuration à la nouvelle par pipeline

```
PowerShell

"C:\ADFSToolkit\0.9.1.55\config\config.CAF.xml" |New-
ADFSTkConfiguration
```

Après avoir vérifié les paramètres pour voir s'ils ont bien été transférés de l'ancienne configuration à la nouvelle, poursuivre la démarche.

- Identifier les fichiers de la mémoire cache qui doivent être transférés de l'ancienne à la nouvelle configuration.
    - Un sous-répertoire appelé \cache dans le répertoire principal actif d'ADFSToolkit suit les changements apportés aux métadonnées et vous épargne du temps en recalculant les fichiers des entités dans ADFS.
    - Il est possible de copier la mémoire cache de l'ancienne version dans la nouvelle pour préserver le statut de traitement actuel.
    - Si on apporte des changements majeurs à la manière dont ADFSToolkit traite les fichiers, nous vous recommandons de laisser l'outil recréer la mémoire cache. Celle-ci sera réactualisée automatiquement si le répertoire \cache est vide.
- Migrer les annulations spécifiques au site.
    - Le fichier C:\ADFSToolkit\#.#.#.#\get-ADFSToolkitLocalManualSpSettings.ps1 renferme tous les paramètres locaux. Lisez les notes accompagnant la version et s'il n'y a aucune autre instruction, copiez simplement ce fichier dans l'ancienne version pour le coller dans la nouvelle.
        - Si vous ne copiez pas ce fichier dans le nouveau répertoire, créé par la version la plus récente d'ADFSToolkit, tous les paramètres des entités existantes seront supprimés.
- Reprendre la synchronisation des métadonnées.
    - Une fois l'exécution manuelle confirmée, vous devriez valider la tâche d'ADFSToolkit pour que le module :
        - utilise le nouveau fichier sync-ADFSTkAggregates.ps1;
        - utilise le nouveau fichier de configuration.
    - Cela fait, la tâche d'ADFSToolkit peut reprendre dans le Job Scheduler de Microsoft et on peut considérer la migration comme terminée.

6.2 Essai avec la fédération fictive de la FCA

La FCA a créé une fédération fictive que les participants sont encouragés à utiliser. Cette fédération possède son propre service de découverte et son fournisseur de services dont on se servira pour tester l'IdP installé. Pour s'inscrire à la fédération fictive, envoyer une demande en ce sens à tickets@canarie.ca en incluant vos métadonnées (si elles n'ont pas déjà été transmises).

7 Connexion au service de production GFI

Une fois l'installation vérifiée, le contact technique autorisé de l'institution (identifié dans la demande d'adhésion à la FCA) communiquera avec CANARIE à tickets@canarie.ca pour signaler que l'institution est prête à connecter son site au service GFI de la FCA.

Veuillez inclure les renseignements qui suivent dans le courriel envoyé à tickets@canarie.ca.

- L'identifiant de l'entité
    - Habituellement « http://fs.yourschoolname.ca/adfs/services/trust »
- Le nom de l'organisation ou de l'institution
- Le nom affiché par l'organisation
    - C'est celui qui apparaîtra dans les listes de sélection pour l'aiguillage
- Une brève description de l'organisation
- L'URL du logo de l'organisation
    - L'URL devrait être transmis par protocole SSL, habituellement par votre IdP
    - Illustration de 100x100 pixels
- Le domaine sur lequel vous avez autorité
    - Il constituera la portée officielle de l'organisation dans les métadonnées de la FCA
- L'URL des métadonnées de l'entité servant à récupérer les métadonnées
    - https://fs.nomdelinstitution.ca/FederationMetadata/2007-06/FederationMetadata.xml sauf indication contraire
- Les coordonnées du contact approprié
    - un compte de soutien technique basé sur les rôles avec :
        - un numéro de téléphone et une adresse courriel
    - un ou plusieurs contacts techniques avec
        - un numéro de téléphone et une adresse courriel