Guide technique

Fédération canadienne d'accès Installateur de fournisseur d'identités (IdP)

Version : 3.0.1

Révisé le : 22 juin 2017

Soutien technique : tickets@canarie.ca

canarie.ca | @canarie_inc

Table des matières

1. Mode d'emploi

1.1. Avant-propos

L'Installateur de fournisseur d'identités (IdP) est un outil permettant de déployer rapidement les services dispensés par la Fédération canadienne d'accès (FCA), en l'occurrence les services eduroam (RADIUS fédéré) et de gestion fédérée des identités ou GFI (SAML2). Ces deux services se greffent à votre application actuelle d'authentification et de gestion des accès, si bien que l'utilisateur peut se connecter en toute sécurité grâce aux justificatifs d'identité existants.

Grâce à l'Installateur IdP, l'installation et la configuration des services de la FCA ne prend que quelques minutes.

eduroam et la GFI peuvent être installés séparément ou simultanément, au gré du participant. Nous vous recommandons de créer une instance pour tester le ou les services de la FCA avec l'Installateur IdP, avant de les installer à demeure sur la plateforme d'exploitation.

1.2. À qui s'adresse ce guide?

Ce guide est destiné à la ou aux personnes chargées de planifier, préparer, installer et administrer les services de la FCA dans leur institution.

1.3. Compétences requises

Bien que les outils et la méthode d'installation aient été conçus pour exiger aussi peu de connaissances que possible sur les différents éléments, les aptitudes énumérées ci-dessous pourraient avoir leur utilité pour le planificateur ou l'installateur.

1.3.1. Connaissances requises sur le fonctionnement de l'institution

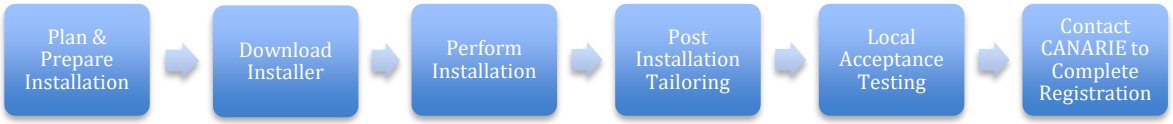
- Systèmes de connexion sans fil (pour installer eduroam)
- Systèmes de connexion par Internet (pour installer la GFI)
- Méthodes d'essai ou de vérification des modifications
- Stratégie de gestion en matière de déploiement et de services
- Répertoire actif ou infrastructure LDAP
- Configuration, gestion ou capacité du pare-feu à solliciter les mises à jour

1.3.2. Aptitudes et connaissances techniques recommandées

- Stratégies et techniques de connexion par Internet
- Navigation, configuration et administration sur une plateforme d'exploitation Linux (services arythmiques, réinitialisation, journaux, fichiers des modifications, etc.)
- Structure et conception des applications Web (HTML et applications créant du HTML dynamique)

2. Aperçu de l'installation

On suivra les étapes décrites à la figure 1 pour installer, configurer et tester les services de la FCA dans un environnement d'essai ou d'exploitation.



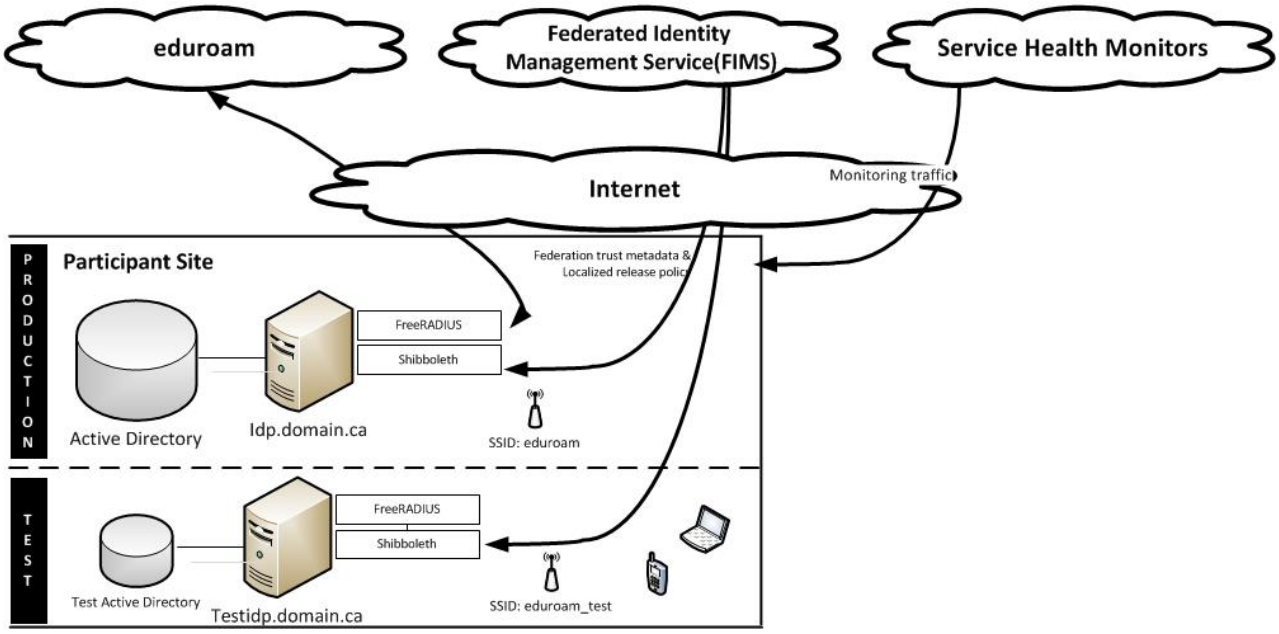


Figure 1. Déploiement typique avec serveurs d'essai et d'exploitation

3. Planifier l'installation

3.1. Exigences

L'Installateur IdP permet l'installation des services eduroam et GFI sur le même serveur ou sur des serveurs distincts (recommandé). Pour plus de simplicité, les exigences physiques des deux serveurs sont les mêmes.

3.1.1. Système d'exploitation

Le serveur IdP pourra avoir comme système d'exploitation :

- CentOS 6.5 ou une version plus récente
- CentOS 7.2 ou une version plus récente
- Ubuntu 14.04 LTS
- RedHat 7.2
- Debian 8.3

3.1.2. Serveur physique ou virtuel

Nous recommandons vivement d'héberger les services de la FCA sur un serveur virtuel. La virtualisation présente de nombreux avantages, notamment la prise d'instantanés du système, le clonage des instances et une sauvegarde complète de la machine virtuelle sans interruption du fonctionnement de l'instance.

3.1.3. IPv4 et IPv6

Les services de la FCA sont entièrement fonctionnels sur IPv4.

Certaines parties de l'infrastructure de la FCA fonctionnent sur IPv6, mais pas toutes. Il ne s'agit donc pas d'une exigence pour l'instant.

3.1.4. Ressources

Qu'on procède à l'installation dans un environnement d'essai ou d'exploitation, les recommandations suivantes s'appliquent au serveur ou à la machine virtuelle.

Ressource	Quantité
Mémoire	Au moins 6 Go de mémoire vive (RAM)
Permutations (/tmp)	12 Go
Disque avec 1 partition (/)	20 Go

3.2. Préparer le réseau

Le tableau ci-dessous indique les adresses IP et les ports associés aux services eduroam et GFI de la FCA auxquels sera connecté votre serveur IdP. CANARIE propose des outils de surveillance et d'exploitation supplémentaires pour les services de la FCA que les participants sont encouragés à utiliser. Ils autorisent l'accès à CANARIE au moyen des ports énumérés ci-dessous. La liste des adresses IP, des protocoles et des ports devrait être accessible après diffusion des règles applicables au pare-feu du site.

Emplacement	DNS CNAME	Adresse IPv4	Adresse IPv6	Ports requis du participant de la FCA	Ports acceptés par l'hôte
Kelowna, BC	prod1-west.eduroam.ca	128.189.5.5		icmp ping, UDP & TCP 1812, 1813, 2083, 3799	UDP: 1812, 1813
Vancouver, BC	Prod2-west.eduroam.ca	142.231.112.1		icmp ping, UDP & TCP 1812, 1813, 2083, 3799	UDP: 1812, 1813
Ottawa, ON	prod1-east.eduroam.ca	205.189.33.100	2001:410:102:1::100	icmp ping, UDP & TCP 1812, 1813, 2083, 3799	UDP: 1812, 1813
Ottawa, ON	prod2-east.eduroam.ca	205.189.33.101	2001:410:102:1::101	icmp ping, UDP & TCP 1812, 1813, 2083, 3799	UDP: 1812, 1813
Ottawa, ON	monitor.canarie.ca	205.189.33.55	2001:410:102:1::55	icmp, ping, UDP & TCP: 1812, 1813, 2083, 3799, TCP: 443	UDP: 1812, 1813
Ottawa, ON	amidala.canarie.ca	205.189.33.75	2001:410:102:1::75	icmp, ping, UDP & TCP: 1812, 1813, 2083, 3799, TCP: 443	UDP: 1812, 1813
Ottawa, ON	tools.canarie.ca	205.189.33.111	2001:410:102:1::111	icmp, ping, UDP & TCP: 1812, 1813, 2083, 3799, TCP: 443	TCP: 443, 80
Ottawa, ON	logger.canarie.ca	205.189.33.23	2001:410:102:1::23	icmp, ping, UDP & TCP: 1812, 1813, 2083, 3799, TCP: 443	UDP: 514, TCP: 514
Toronto, ON	caf-shib2ops.ca	128.100.132.106			UDP:ping TCP: 443, 80

Tableau 1 : Adresses IP et ports du serveur d'exploitation de la FCA

Service	Transport/Port	Visibilité
eduroam	UDP/1812,1813	Votre réseau, serveur de la Fédération à CANARIE
FIM	TCP/443	Votre réseau, Internet
SSH	TCP/22	Administrateur, sur votre réseau uniquement
Mysql	TCP/3306	Hôte local et hôte de rechange, avec la version évoluée

Tableau 2 : Principaux ports de votre serveur IdP

3.3. Préparer l'environnement

3.3.1. Connexion au service d'annuaire

L'Installateur IdP doit avoir accès au service d'annuaire pour effectuer ce qui suit :

- valider les noms d'utilisateur et les mots de passe;
- récupérer et produire les attributs, s'il y a lieu.

L'Installateur IdP peut se connecter à l'annuaire de Microsoft (Microsoft Active Directory) ou à n'importe quel annuaire dont l'interface se conforme à la version 3 de LDAP. Il effectuera les corrections voulues aux champs qui servent à rechercher et à authentifier les utilisateurs dans l'annuaire.

3.3.2. Restrictions du service s'appliquant à l'annuaire

3.3.2.1. eduroam

On recommande vivement que le site accepte le protocole MS-CHAPv2 pour RADIUS d'eduroam. Pour que MS-CHAPv2 fonctionne, l'hôte IdP DOIT utiliser une instance d'Active Directory comme serveur LDAP et être jumelé au domaine AD par la ligne de commande. De cette façon, MS-CHAPv2 pourra valider le mot de passe.

D'autres solutions existent, avec d'autres annuaires LDAP, mais elles nécessiteront une configuration plus poussée avec des ajustements manuels, après que l'Installateur IdP aura terminé sa tâche.

3.3.2.2. GFI

La GFI n'introduit aucune restriction pour ce qui est de la connexion à un annuaire, mais pour établir un canal de communication sécurisé, le service doit disposer d'une connexion TLS sur le port 636.

Si votre annuaire ne peut établir de connexion TLS sur ce port, vous pourriez installer stunnel[1] et créer une connexion sécurisée pour l'Installateur IdP.

3.3.2.3. Annuaires d'essai

Nous vous recommandons vivement d'installer et de configurer les services de la FCA sur une plateforme d'essai. Pareil environnement devrait être totalement séparé du système d'exploitation.

3.3.3. Certificats TLS (*Transport Layer Security*)

Ces certificats jouent un grand rôle en protégeant l'information qui transite par les services eduroam et GFI.

[1] https://www.stunnel.org

Par défaut, l'Installateur utilise les certificats auto signés. Dans le cas d'eduroam, il créera automatiquement une autorité de certification (AC) selon l'information recueillie.

3.3.3.1. Certificats vus par l'utilisateur

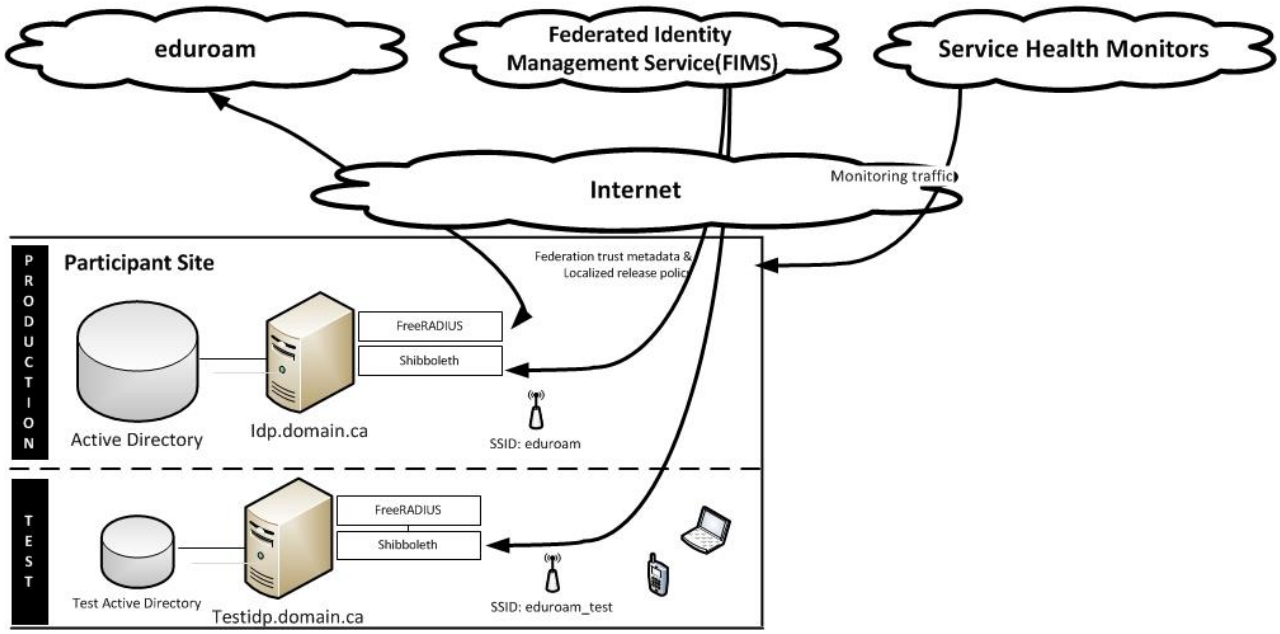
Avec eduroam, l'utilisateur doit accepter le certificat employé par FreeRADIUS comme preuve que le serveur d'authentification RADIUS est bien ce qu'il est. Ce certificat n'est présenté qu'une fois, au moment où la connexion sans fil est configurée sur l'appareil mobile utilisant le SSID d'eduroam.

3.3.3.2. Autres certificats

Le service GFI utilise le logiciel Shibboleth qui crée le certificat de longue durée (10 ans) auto signé, employé avec les métadonnées SAML2. Ce certificat ne devrait être ni remplacé ni modifié.

3.4. Déploiement

3.4.1. Approche recommandée



L'approche recommandée pour le déploiement convient aux organisations comptant un nombre moyen d'utilisateurs (de 10 000 à 20 000 ETP) et de services. On peut aisément y recourir pour configurer deux serveurs d'exploitation (un actif et l'autre en attente), en plus du serveur d'essai qui simulera l'environnement d'exploitation

On installera d'abord le serveur d'essai pour s'exercer, avant de procéder à l'installation sur la plateforme d'exploitation. Déployer les services sur le serveur d'essai fera ressortir les étapes supplémentaires éventuelles et les modifications particulières à apporter au serveur d'exploitation lors de l'installation.

3.4.2. Déploiement avancé

Habituellement, les raisons que voici justifient un déploiement avancé :

- continuité des activités (résilience et reprise);
- disponibilité élevée (HA);
- fonctionnalités spéciales.

Avant de procéder, il importe d'examiner les besoins relatifs à la continuité des activités et les ajustements qu'exigera un déploiement plus poussé que celui recommandé.

On préconise de suivre autant que possible l'approche recommandée pour le déploiement de l'Installateur IdP, puis d'effectuer les configurations supplémentaires pour parvenir au résultat souhaité.

De cette façon, on réduira les manipulations au minimum et l'installation de l'IdP s'effectuera automatiquement dans une certaine mesure.

3.4.2.1. Configuration de la GFI en vue d'une disponibilité élevée

Il n'est pas rare que les systèmes d'exploitation possède deux instances IdP, la première active et la seconde en attente, toutes deux configurées de la même façon, sans pour autant être groupées. Le regroupement[2] des IdP est inutile si une deuxième IdP prend le service en charge pendant qu'on s'occupe de la première. Toutefois, le regroupement rehausse le taux de disponibilité.

Si on regroupe les IdP, nous recommandons de les configurer après installation avec l'Installateur IdP.

3.4.2.2. Configuration de la GFI en raison de fonctions spéciales

Le serveur GFI (Shibboleth) est déployé pour que les identificateurs persistants des services soient conservés dans la mémoire cache. Si l'usage d'un service exige la transmission d'un identificateur particulier (par ex., Uniqueld d'Office365 ou un NameID persistant spécial pour SAML2), vous devrez établir comment cette valeur sera créée et gérée. La base de données de l'IdP peut stocker les attributs de ce genre pour en faciliter la récupération localement. Il faudra en tenir compte dans la configuration pour parvenir à une disponibilité élevée, car les données relatives à l'attribut devront se retrouver dans toutes les instances de la base de données. Pour en savoir plus à ce sujet, on consultera la documentation à l'adresse :

https://collaboration.canarie.ca/elgg/file/view/3164/idp-task-cheat-sheet

3.5. Considérations relatives à la disponibilité et à la fiabilité

Plusieurs facteurs devront être envisagés au moment du déploiement. Habituellement, l'Installateur IdP effectuera une installation de base sur un serveur d'essai. Pour passer de l'installation de base à celle d'exploitation, vous devrez prendre en compte de certaines choses lors du déploiement.

[2] https://wiki.shibboleth.net/confluence/display/IDP30/Clustering

3.5.1. Fiabilité des services

Diverses stratégies permettent d'accroître la fiabilité d'un service, mais elles nécessitent habituellement l'équilibrage de la charge entre plusieurs serveurs.

Une autre solution consiste à établir une adresse IP qui passera d'un serveur à l'autre et à mettre en place un processus rythmique afin de suivre l'état des serveurs. Si le service fonctionne, mais qu'on détecte subitement une interruption (grâce au processus rythmique), le serveur de secours prendra la relève. On peut recourir à cette méthode avec les services qu'installe l'Installateur IdP, mais il revient au technicien de configurer ceux-ci pour en garantir la fiabilité.

L'usage de plusieurs entrées DNS et des techniques de circuit cyclique n'est pas recommandé, car on n'a pu démontrer que ces méthodes augmentent la fiabilité.

3.5.1.1. Fiabilité d'eduroam

eduroam utilise le protocole RADIUS, qui ne conserve pas les informations sur la séance. Ce protocole utilise UDP sur les ports 1812 et 1813 pour assurer le transport de l'information sur le réseau et a été conçu pour fonctionner avec les serveurs de reprise. L'Installateur IdP n'installe qu'une instance de FreeRADIUS, que prennent en charge les serveurs Federation Lever RADIUS (FLR) en amont, au Canada.

Les clients (téléphones intelligents, ordinateurs portables, points d'accès, autres serveurs RADIUS) qui communiquent avec le serveur FreeRADIUS local le font en consultant le DNS.

3.5.1.2. Fiabilité de la GFI

La GFI utilise le logiciel Shibboleth pour appliquer le protocole SAML sur un canal sécurisé (port 443 de HTTPS). L'authentification de Shibboleth et la genèse des attributs dans la réponse d'assertion n'ont pas besoin d'être dynamiques. Le navigateur de l'utilisateur transmet l'assertion d'authentification au fournisseur de service dans une seule demande, avec l'assertion SAML2 sur HTTPS. Les visites subséquentes à un IdP de GFI établiront un lien avec les données de la séance gardées en mémoire. L'utilisateur ne sera obligé de reconfirmer son identité que s'il met fin à la séance. La gestion de la séance sur plusieurs serveurs est une option avancée de Shibboleth que ne supporte pas l'Installateur IdP pour l'instant.

Le redémarrage du serveur Shibboleth efface les séances de l'utilisateur. Le service n'est pas interrompu, mais l'utilisateur devra s'authentifier à nouveau pour reprendre la séance.

3.5.1.3. La GFI et eduPersonTargetedID/persistentID

Le serveur Shibboleth utilise une base de données MySQL comme mémoire cache locale et y stocke les valeurs eduPersonTargetedID[3] et persistentID employées par l'identificateur NameID de SAML2.

[3] http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html#eduPersonTargetedID

Si on répartit la charge entre deux serveurs d'exploitation dans le cadre d'une stratégie serveur actif/serveur en attente, il suffira de reproduire la base de données MySQL sur le serveur de secours.

4. Installation

4.1. Fonctionnement de l'installateur

L'Installateur IdP comporte trois éléments :

- un configurateur qui s'exécute sur l'appareil de l'utilisateur (script HTML produisant le fichier de configuration);
- un installateur qui s'exécute sur le serveur IdP, lit le fichier de configuration et effectue les mises à jour en procédant aux modifications requises par la configuration;
- des interventions après installation pour une configuration avancée ou spéciale.

Ces éléments sont regroupés dans un fichier comprimé (ZIP) qui devrait être copié sur l'ordinateur de l'utilisateur et les serveurs IdP concernés. Le fichier ZIP est disponible à l'adresse :

http://bit.ly/idpinstaller300zip

4.2. Hypothèses associées à l'installation

- L'utilisateur qui effectue l'installation ouvre le configurateur (URL) localement, sur son appareil, avec Firefox, Google Chrome ou Safari.
- Le ou les serveurs disposent des ressources nécessaires (voir 3.1.4).
- Le réseau a été configuré de la façon requise (voir 3.2).
- On a retenu une approche pour le déploiement et configuré la cible en conséquence (voir **Error! Reference source not found.**).

4.3. Établir la configuration

Ouvrez le configurateur dans le navigateur en accédant à l'URL :

file:///<location_of_unzipped_installer>/idp-installer-CAF/www/appconfig/CAF/index.html

Après avoir répondu aux questions, cliquez « Generate Configuration File ».

Le configurateur intègre d'autres informations sur les principaux aspects de la configuration. Peut-être aurez-vous besoin de l'assistance de la personne responsable de l'annuaire dynamique ou du pare-feu pour répondre à certaines questions.

4.3.1. Chargement d'une configuration existante

Pour rebâtir ou reproduire rapidement une des instances du serveur IdP, il est possible d'importer une configuration sauvegardée antérieurement. Ceci vous épargnera le temps qu'il faudrait pour remplir manuellement les champs du formulaire. Pour cela, cliquer « Import an Existing Configuration » dans le coin supérieur droit du configurateur, puis couper et coller les éléments du fichier de configuration existant dans la zone texte sur la page, et cliquer « Import My Existing Config From Below ».

4.4. Déploiement sur le serveur IdP

Sur le serveur IdP visé, ouvrir la séance comme un segment racine, puis suivre les étapes que voici :

1) assurez-vous que l'hôte est bien configuré pour le DNS et le réseau dans /etc/resolv.conf et /etc/hosts
2) copiez idp-installer-<version>.zip dans un répertoire temporaire (par ex., /tmp) sur le serveur IdP server
3) au besoin, installer l'utilitaire unzip avec « yum -y install unzip » ou « apt-get –y install unzip », selon le système d'exploitation
4) cd /tmp
5) ouvrez idp-installer-<version>.zip
6) cd dans le sous-répertoire idp-installer-<version>
7) copiez ou coupez et collez la configuration (créée à la partie 4.3) en modifiant le fichier « config » puis sauvegardez-le
8) exécutez le script ./deploy_idp.sh au niveau racine
9) effectuez les modifications nécessaires après l'installation

5. Mesures suivant l'installation

5.1. Mesures spécifiques à eduroam

5.1.1. Tester l'installation eduroam par défaut (site local)

En connectant l'instance RADIUS à votre point d'accès ou contrôleur, vous pourrez vérifier l'installation par défaut avec un client (téléphone intelligent ou ordinateur portable) afin d'authentifier le SSID qui vient d'être configuré.

La configuration du point d'accès sans fil peut être très laborieuse, mais au strict minimum, l'authentification WPA2, 802.1x devrait pointer vers l'instance RADIUS.

Le client choisi pour l'essai devra soumettre un userid du genre « untel_id@mondomaine.ca » avec le mot de passe approprié.

Les clients Windows pourraient avoir besoin d'une configuration supplémentaire pour attester le certificat (auto signé) et l'autorité qui l'émet.

Vous ne pourrez pas valider ni tester eduroam d'une extrémité à l'autre tant que le serveur d'exploitation ne sera pas connecté aux serveurs RADIUS du plus haut niveau de la Fédération.

5.1.2. Utilisation asynchrone du service eduroam

Le service freeRADIUS utilise la méthode asynchrone habituelle de Linux et devrait être configuré pour démarrer automatiquement à la réinitialisation du serveur.

Pour lancer manuellement le service : *service radiusd start.*

Pour arrêter manuellement le service : *service radiusd stop.*

Remarque : pour utiliser le service de cette façon, vous devrez vous connecter au serveur au niveau racine.

5.1.3. Remplacer le certificat auto signé automatique (facultatif)

L'Installateur IdP produit automatiquement des certificats TLS avec le processus cert bootstrap de freeRADIUS. Voici comment procéder si vous voulez actualiser ce certificat ou le remplacer par un certificat commercial.

- Ouvrir une séance au niveau racine
- cd /etc/radddb/certs
- Produire une nouvelle Certificate Signing Request (CSR) ou utiliser la demande existante
    - Assurez-vous que les valeurs élargies de la clé du certificat TLS peuvent être utilisées par le serveur RADIUS
- Remplacer server.crt par le certificat approprié
- Relancer le service freeRADIUS en saisissant « service radius restart »

5.2. Mesures spécifiques à la GFI

5.2.1. Tester l'installation GFI par défaut

Un test très simple consiste à invoquer l'URL

https://<yourserverFQDN>/idp/status

qui devrait indiquer l'état du serveur, si tout est en ordre.

Ce test valide ce qui suit :

- que le serveur Web et le certificat sont opérationnels et ont été bien configurés;
- qu'IPTables fait bien ce qu'il est censé faire;
- que la configuration ne présente aucune erreur de syntaxe;
- que la connexion avec l'annuaire fonctionne pour le résolveur d'attributs;
- que la connexion avec l'annuaire fonctionne pour l'authentification (mêmes justificatifs, mais emplacements différents pour la configuration).

5.2.2. Tests supplémentaire facultatifs

5.2.2.1. Test avec testshib.org

Le service de test public testshib.org utilise un simple service open IdP et protocole SP pour procéder à une vérification complète. Pour effectuer le test, supprimez les balises commentaires dans la section correspondante de metadata-providers.xml, relancez le service IdP et suivez les instructions sur le site testshib.org.

5.2.2.2. Test avec Test Federation de la FCA

La FCA propose un service de test fédéré à ses adhérents. Ce service combine un service de découverte et un fournisseur de service d'essai que l'on peut utiliser pour vérifier l'installation du service IdP. Pour y recourir, envoyer une demande à tickets@canarie.ca en incluant vos métadonnées, si elles n'ont pas encore été transmises.

5.2.3. Lancer et arrêter le service GFI

Le service GFI fonctionne avec Tomcat comme contenant. Il repose sur la méthode arythmique usuelle et devrait démarrer automatiquement à la réinitialisation du serveur.

Pour lancer manuellement le service : */etc/init.d/jetty start*

Pour arrêter manuellement le service : */etc/init.d/jetty stop*

Remarque : pour procéder de la sorte, vous devez ouvrir une séance sur le serveur au niveau de la racine.

5.2.4. Remplacer le certificat Webserver par un certificat commercial (facultatif)

L'Installateur IdP produit automatiquement des certificats TLS pour le logiciel Shibboleth avec openSSL. Ces certificats sont destinés :

- au Java Key Store (JKS) du serveur Web Tomcat;
- au JKS du logiciel Shibboleth.

Le certificat CSR du serveur Tomcat est le seul à remplacer si on veut utiliser un certificat commercial au lieu du certificat auto signé.

On pourra alors produire un CSR ordinaire. Si on recourt à eduroam et à la GFI, utiliser le MÊME CSR, car l'hôte portera le même nom.

Pour en savoir plus, lisez notre FAQ à :

https://tts.canarie.ca/otrs/public.pl?Action=PublicFAQZoom;ItemID=83

5.2.5. Individualiser la page d'ouverture de séance de la GFI / de Shibboleth

L'Installateur IdP utilise le service GFI qui vient avec Shibboleth et ne modifie pas la page d'accueil pour qu'elle s'harmonise avec le site de l'organisation. Pour savoir comment individualiser cette page, veuillez consulter les documents de référence que voici :

- FCA :

    - https://tts.canarie.ca/otrs/public.pl?Action=PublicFAQZoom;ItemID=79
- consortium Shibboleth :
    - https://wiki.shibboleth.net/confluence/display/SHIB2/IdPAuthUserPassLoginPage

5.3. Sauvegarde et gestion du changement

L'Installateur IDP est conçu pour réutiliser les fichiers de configuration qu'il produit, ce qui permet de reconstituer rapidement la plateforme. Cependant, il n'est pas conçu pour remplacer les sauvegardes, ni conserver les données des journaux ou de débogage que pourrait engendrer l'usage des différents services. La reconstitution du service effacera les données historiques et les paramètres d'individualisation. C'est pourquoi on recommande d'effectuer une sauvegarde et de prendre des instantanés régulièrement.

Nous préconisons vivement d'appliquer des pratiques quelconques de gestion du changement conformes aux politiques du département TI de l'organisation à ces services. Il est également recommandé de documenter les modifications effectuées pour individualiser le service lors de l'installation.

5.4. Connexion du serveur GFI ou eduroam au serveur d'exploitation de la FCA

Une fois que vous aurez vérifié l'installation, veuillez communiquer avec CANARIE à tickets@canarie.ca pour signaler que vous être prêt à connecter votre site au service GFI de la FCA. Cette tâche devrait être confiée au technicien responsable, identifié sur la demande d'adhésion à la FCA.

Pour eduroam, vous devrez fournir l'adresse IP de vos serveurs. En retour, CANARIE vous transmettra une clé secrète conjointe pour sécuriser les échanges entre sites.

Pour connecter le service IdP de Shibboleth au service GFI de la FCA, vous devrez fournir les informations qui suivent (annexez-les au courriel envoyé à tickets@canarie.ca) :

- votre entityid :
    - habituellement « https://idp.yourschoolname.ca/idp »
- le nom de l'organisation ou de l'institution
- le nom public de l'organisation :
    - c'est ce nom qui apparaîtra dans les listes, lors des recherches
- une brève description de l'organisation
- l'URL du logo de l'organisation :
    - l'URL devrait être accessible par SSL, habituellement à partir du service IdP
    - l'illustration devrait mesurer 100x100 pixels
- le domaine dans lequel vous avez autorité :
    - ce sera le domaine officiel qui apparaîtra dans les métadonnées de la FCA
- l'url des métadonnées de l'entité où seront récupérées les métadonnées :
    - https://your_server.ca/idp/shibboleth est l'url par défaut
        - cet URL permet de récupérer le fichier /opt/shibboleth/idp/metadata/idp-metadata.xml
- les coordonnées des personnes-ressources concernées :
    - compte d'un service de dépannage basé sur les rôles avec :
        - numéro de téléphone

        - adresse courriel
    - nom du ou des techniciens responsables avec :
        - numéro de téléphone
        - adresse courriel

6. Annexe

6.1. Logiciels installés et répertoires

L'Installateur IdP installe les logiciels mentionnés ci-dessous. Cette liste n'indique pas tous les progiciels Linux installés, car beaucoup de progiciels créent des liens automatiquement. Si vous utilisez RPM (ou un utilitaire similaire) avant l'installation, vous pourrez répertorier les progiciels, puis comparer leur liste une fois l'installation terminée.

- Progiciels relatifs à la GFI :
    - jetty
        - **Installé par :** téléchargement du progiciel
        - **Répertoire d'installation :** /opt/jetty
        - **Répertoire du journal :** /opt/jetty/jetty-base/
    - shibboleth-identityprovider-3.2.1
        - **Installé par :** extracteur tar du progiciel
        - **Répertoire d'installation :** /opt/shibboleth/idp
        - **Répertoire du journal :** /opt/shibboleth-idp/logs
    - cas-client-3.3.3-release
        - **Installé par :** extracteur tar du progiciel d'extension de Tomcat
        - **Répertoire d'installation :** /opt/cas-client-3.3.3
        - **Répertoire du journal :**
    - mysql-connector-java-5.1.35 (pour EPTID et persistentID)
        - **Installé par :** Installateur IdP à l'extraction du fichier zip
        - **Répertoire d'installation :** /opt/shibboleth-idp/edit-webapp/WEB-INF/lib/
        - **Répertoire du journal :** s/o
    - MySQL Community Service 5.6 (pour EPTID et persistentID)
        - **Installé par :** extracteur tar du progiciel
        - **Répertoire d'installation :** /usr/sbin
        - **Répertoire du journal :** /var/log/mysql/
- Progiciels associés à eduroam :
    - freeRADIUS-2.1.12
        - **Installé par :** installateur rpm du progiciel
        - **Répertoire d'installation :** /usr/sbin, /etc/raddb
        - **Répertoire du journal :** /var/log/radiusd
    - samba-3.6.9 (connexion à AD pour MS-CHAPv2)
        - **Installé par :** installateur rpm du progiciel
        - **Répertoire d'installation :** /usr/bin, /etc/samba/
        - **Répertoire du journal :** /var/log/syslog