L’hébergement d’IdP par RENATER

Anass Chabli
RENATER
c/o CRI Campus de Beaulieu, Bat 12 D
263, Avenue du Gal Leclerc CS 74205
35042 RENNES Cedex
France

Résumé

Actuellement, pour utiliser les ressources accessibles via la fédération Éducation-Recherche et notamment les services proposés par RENATER, (RENdez-vous, FileSender, RENAvisio, Universalistes, etc.), les sites doivent être raccordés à la fédération Éducation-Recherche et doivent déployer et configurer dans leurs établissements un fournisseur d’identités. Les petites structures sont découragées par ce déploiement pour des raisons budgétaires, techniques ou organisationnelles et sont ainsi dans l’incapacité d’utiliser les services de la fédération Éducation-Recherche.

Avec l’offre d’hébergement d’IdP les fournisseurs d’identités sont déployés, configurés et hébergés par RENATER. Tous les aspects technologiques (monitoring et mises à jour) sont inclus dans l’offre. Le service permet non seulement d’héberger des fournisseurs d’identités, mais aussi éventuellement un annuaire LDAP comme référentiel utilisateurs de l’établissement. Les établissements disposent d’un accès Web à cet annuaire permettant d’ajouter, de supprimer et de définir des utilisateurs et leurs droits.

Mots-clefs

IdP, hébergement, fournisseur d’identités, fédération, shibboleth, OpenLdap, RENATER, LDAP

1 Introduction

Le service d’hébergement d’IdP de RENATER permet aux organismes membres de la fédération Éducation-Recherche d’externaliser le déploiement et la configuration d’un fournisseur d’identités, *Identity Provider* en anglais, dénommé IdP dans la suite de l’article.

Ce service est principalement à destination des structures qui ne peuvent pas opérer un fournisseur d’identités en interne, pour des raisons budgétaires, techniques ou organisationnelles.

L’exposé présentera l’architecture mise en œuvre pour déployer le service d’hébergement d’IdP, les différentes méthodes et outils mis en place pour garantir la disponibilité quasi permanente du service, ainsi que les modalités d’accès au service.

En fin de document seront décrites les éventuelles évolutions de l’offre d’hébergement d’IdP.

2 La Fédération Éducation-Recherche

2.1 Acteurs et organisation

La fédération Éducation-Recherche est un cadre organisationnel et technique qui permet de valoriser ou d'élargir le cercle d'utilisateurs en donnant accès aux ressources des établissements de façon sécurisée.

L'utilisateur final peut accéder à des services (outils collaboratifs, documentations électroniques, applications métier, accès Wi-Fi) opérés en dehors de son établissement mais en utilisant le mode d'authentification de son établissement.

Actuellement, la communauté Éducation-Recherche contient 248 fournisseurs d'identités et 657 ressources.

Les différents types d'acteurs :

1. les **utilisateurs finaux** sont les personnes qui vont effectivement se connecter à des sites web via une fédération d'identités. En général elles ne savent pas et ne voient pas que leur connexion a lieu vers une fédération d'identités, c'est transparent pour elles.
2. les **ressources** sont les sites web auxquels peuvent accéder les utilisateurs finaux via une fédération d'identités. Il peut s'agir par exemple de sites d'enseignement à distance, d'outils collaboratifs en ligne, de portails de documentations numérisées…
3. les **fournisseurs d'identités** sont les organismes auxquels sont rattachés les utilisateurs finaux. Par exemple dans la fédération Éducation-Recherche, il s'agit d'organismes de recherche ou d'établissements d'enseignement. Un fournisseur d'identités a pour rôle d'authentifier ses utilisateurs désirant accéder à une ressource via la fédération d'identités.
4. l'**opérateur de la fédération** est l'entité qui gère la fédération, il définit ses règles de fonctionnement et prend en charge l'inscription des fournisseurs d'identités et des ressources dans la fédération.

Interactions basiques pour accéder à un service dans la fédération :

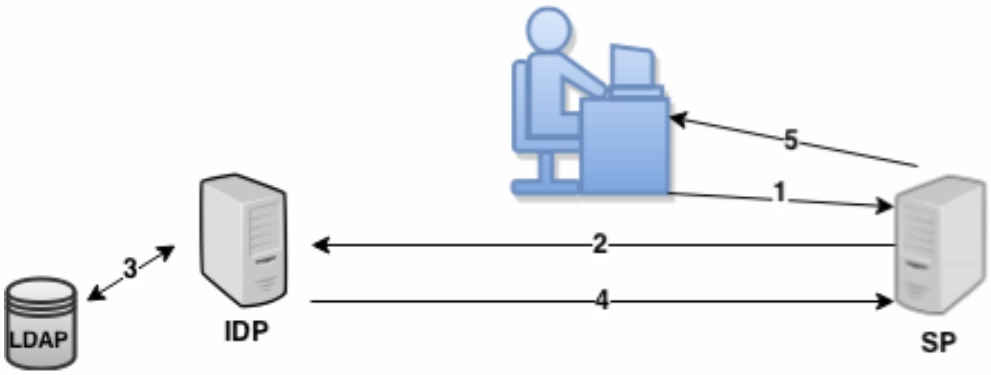

Figure 1 - Intéractions dans la fédération

Le fournisseur de services (SP - *Service Provider*) détecte qu'un utilisateur désire accéder à un service sécurisé (1), il génère et transmet une requête au fournisseur d'identités (IdP) auquel l'utilisateur est rattaché (2), ce dernier authentifie l'utilisateur en se basant sur un annuaire d'établissement (LDAP, AD…) (3) et répond une requête contenant les attributs de l'utilisateur (4), le fournisseur de services vérifie les informations fournies par le fournisseur d'identités, puis donne accès à l'utilisateur aux ressources demandées (5).

2.2 Services accessibles via la fédération

Différents services sont accessibles à la communauté Éducation-Recherche, à titre d'exemples:

- RENAvisio : plate-forme de réservation de pont de visioconférence.
- TCS : service de délivrance de certificats de serveurs/personnes TCS.
- FileSender : service de transfert de fichiers.
- RENdez-vous : visioconférence de poste à poste.
- Point d'accès wifi Eduspot.

Pour plus d'informations concernant les services référez-vous au lien suivant :
https://www.renater.fr/spip.php?page=categorie&id_rubrique=425

3 Pourquoi un service d'hébergement d'IdP ?

L'inscription au service de fédération d'identité Éducation Recherche est gratuite mais les établissements doivent cependant déployer et configurer une brique de fournisseur d'identités *Shibboleth*. Bien que généralement et suivant les compétences techniques disponibles, ce déploiement est de l'ordre de quelques jours, les petites structures sont découragées par ce déploiement pour des raisons budgétaires, techniques ou organisationnelles, elles sont donc dans l'incapacité de profiter des services de la communauté Éducation-Recherche.

3.1 Description général du service

Le service d'hébergement d'IdP de RENATER s'appuie sur une offre logicielle en tant que service (SaaS) et sur une méthodologie de développement (DevOps) permettant d'automatiser et de simplifier la création et la maintenance des fournisseurs d'identités.

Il facilite le déploiement et le management des fournisseurs d'identités en minimisant les complexités technologiques pour les organismes demandeurs. En effet, la mise à disposition et le déploiement des briques nécessaires sont simplifiés, elles deviennent rapides à mettre en place grâce à l'automatisation des tâches d'installations et de configurations.

Dans le cas où l'établissement ne détient pas de référentiel utilisateur, RENATER peut prendre en charge son hébergement. Cependant, l'approvisionnement de ce référentiel reste à la charge de l'établissement, il peut se faire via une plate-forme web mise à disposition pour permettre l'administration d'un LDAP (ajout d'utilisateurs, des droits, des attributs etc.).

3.2 Qui peut en bénéficier ?

Le service est proposé à l'ensemble des établissements titulaires d'un agrément RENATER.

Les établissements qui n'opèrent pas de fournisseur d'identités peuvent faire une demande d'hébergement d'IdP en envoyant simplement les documents nécessaires pour activer le service (charte, formulaire contenant les données de configuration des fournisseurs d'identités, etc.). Une fois la demande validée par RENATER, le processus de déploiement du fournisseur d'identités est initié en prenant compte les configurations nécessaires aux spécificités de l'établissement demandeur.

4 Offres proposées par RENATER

RENATER propose deux offres de service d'hébergement d'IdP qui répondent à des besoins différents.

La première offre est mutualisée, elle consiste à fournir un IdP commun à plusieurs structures. La deuxième repose sur un IdP dédié, comme l'illustre la figure suivante :

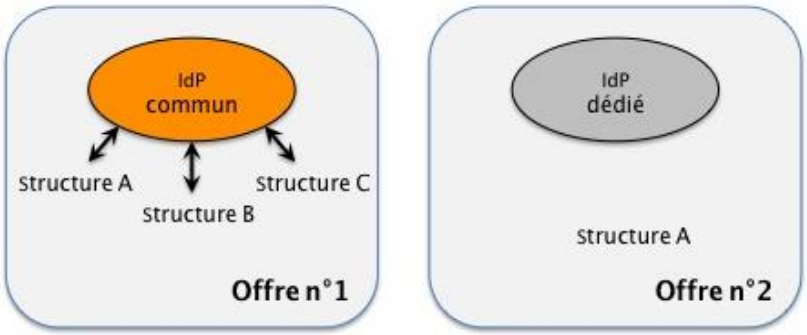

Figure 2 - Offres d'hébergement d'IdP

4.1 Offre d'IdP mutualisé

L'offre d'hébergement d'IdP mutualisé est une solution légère pour les petites structures, qui désirent bénéficier de quelques services de la fédération d'identités sans pour autant gérer un fournisseur d'identités.

4.1.1 Description de l'architecture du service

L'établissement est responsable de l'approvisionnement et des déclarations d'attributs conformes au cadre technique de la fédération d'identités.

Voici les briques qui sont configurées avec L'IdP :

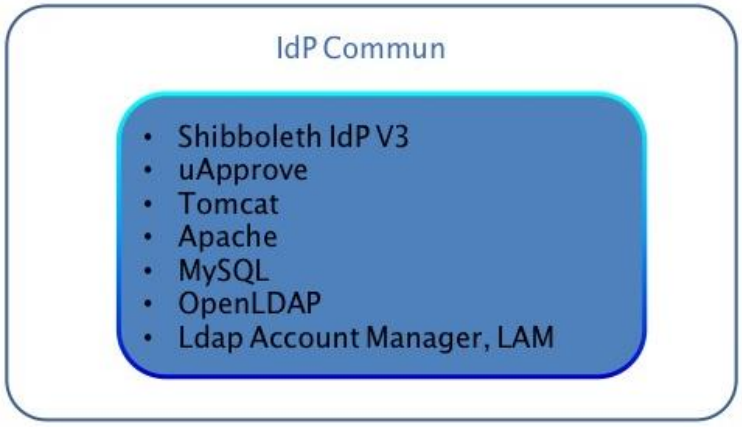

Figure 3 - Configuration de la VM pour l'IdP Commun

4.1.2 Avantages

- Faible coût pour les établissements ;

- l'établissement doit juste approvisionner un annuaire LDAP via une interface web ;

- haute disponibilité du service ;

- mise à jour de l'Idp automatisée.

4.1.3 Limites

- Utilisation de l'annuaire LDAP fourni par RENATER pour approvisionner les utilisateurs, les attributs ;
- pas de raccordement à un annuaire déjà existant ;
- accès à quelques services en ligne de la fédération Éducation-Recherche ;
- page de login non personnalisée pour les établissements ;
- IdP non configurable selon le besoin de chaque établissement.

4.2 Offre d'IdP dédié

L'offre d'hébergement d'IdP dédié est une solution pour les structures qui désirent plus de souplesse et une configuration personnalisée de leurs IdP.

Le fournisseur d'identités est déployé, hébergé, et configuré par RENATER selon le besoin de l'établissement faisant la demande.

4.2.1 Description de l'architecture du service

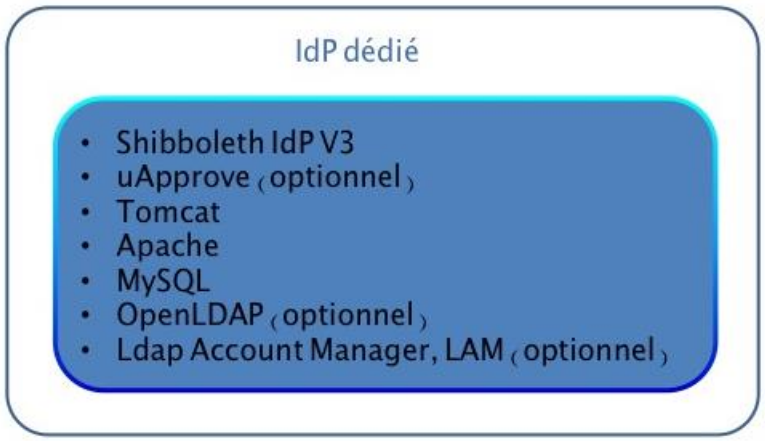

Figure 4 - Configuration de la VM pour l'IdP dédié

4.2.2 Avantages

- Possibilité de raccorder l'IdP à plusieurs sources de données (LDAP, AD...) ;
- configuration personnalisée de la page d'authentification de l'IdP ;
- accès à plus de services (ex : Antispam, fédération hébergée) ;
- IdP avec nom de domaine de l'établissement ;
- possibilité d'utiliser un serveur CAS ;
- haute disponibilité du service ;
- mise à jour de l'IdP automatisée.

4.2.3 Limites

Le coût financier de déploiement plus important, il est dépendant du besoin de chaque établissement.

5 Evolution possible du service:

RENATER envisage de compléter l'offre en y ajoutant deux services importants, Eduroam (service d'accès à Internet sans fil sécurisé pour les personnels et éventuellement les étudiants des établissements d'enseignement supérieur et de recherche) et des statistiques de supervision (nombre de connexions aux IdP, les services auxquels les utilisateurs accèdent le plus…).