Adapter un service pour la fédération d'identités

Olivier Salaün, RENATER
ANF Mathrice 2014

Supports de formation

https://services.renater.fr/federation/docs/installation

- supports des formations RENATER
  - disponibles en ligne
  - mis à jour régulièrement
  - utilisables en auto-formation
    - 1j IdP puis 1j SP
- autres ressources disponibles
  - présentations utilisées lors des formations
  - des videos

Le menu

1. Adapter un service
2. Etapes de mise en oeuvre
3. La population cible
4. Identifier les utilisateurs
5. Le service de découverte

Adapter un service
Différents cas de figure

- Application nativement compatible avec SAML2
  - Utilisant le SP Shibboleth ou pas
- Application implémentant des modes d'authentification externes
  - Possibilité d'utiliser REMOTE_USER ?
- Application devant être adaptées
  - Cas logiciel open source
    - Contacter les développeurs
    - Prévoir un développement (plugin)
  - Cas logiciel propriétaire
    - Demander un développement

Quelques applications déjà compatibles

https://federation.renater.fr/technique/applications/index

Les applications

Les applications listées ci-dessous sont celles qui ont été mises en oeuvre par des établissements d'en
supérieur français.

- DokuWiki (wiki)
- Drupal (CMS)
- EZProxy (reverse-proxy)
- Foodle (sondage)
- FusionForge (forge développement)
- LimeSurvey (sondage)
- Mediawiki (wiki)
- Moodle (LMS)
- NoCatAuth (portail captif Wi-Fi)
- Nuxeo
- PepperSpot (portail captif Wi-Fi)
- Request Tracker
- SAP (progiciel de gestion)
- SharePoint 2007 (CMS, GED)
- SharePoint 2010 (CMS, GED)
- SPIP (CMS)
- Squirrelmail (webmail)
- Sympa (listes de diffusion)
- Typo3 (CMS)

Modèle de fiche : modele

Adapter un service

- Remplacer l'authentification
  - désactiver l'authentification native
  - ou la faire cohabiter avec la fédération
- Désactiver la gestion des mots de passe
  - rappel, réinitialisation
- Exploiter les attributs utilisateur
  - pour association à un profil applicatif
  - pour déduire dynamiquement des droits
    - exemple : eduPersonAffiliation=researcher
- Gérer le logout

Adapter un service

https://services.renater.fr/federation/docs/installation/sp

- support de formation de RENATER
- un exemple fictif complet d'application adaptée
  - exemple en Perl
  - exemple en Php
- étapes
  1. intégration minimale
  2. le logout
  3. les lazy sessions
  4. le embedded WAYF
  5. limiter la liste des IdPs

Choix de l'implémentation
les critères

- architecture
  - Shibboleth nécessite un serveur Apache
    - pas de module Shibboleth pour nginx
- mode d'intégration
  - Shibboleth : un module d'authentification en frontal
  - simpleSAMLPhp : chargement d'une librairie
- langage de programmation de l'application
  - Shibboleth : neutre car pas d'inclusion de code
  - simplSAMLPhp : PHP
  - OIOSAML : Java

Mise en oeuvre
installer le SP Shibboleth

1. Installation des pré-requis
2. Installation du SP Shibboleth
3. Configuration Apache + SP
4. Test du SP
5. inscription dans la fédération de production

Mise en oeuvre
1/ les pré-requis

- certificats serveur
  - service TCS de RENATER
  - attention : Shibboleth utilise d'autres certificats pour les échanges SAML
- Apache
- configuration NTP
  - important car les assertions SAML ont une durée de validité courte

Mise en oeuvre
2/ installation du SP Shibboleth

- les développeurs fournissent
  - les sources
  - des RPMs pour Linux RedHat

- **# yum install shibboleth**

Mise en oeuvre
3/ configuration Apache

```
ScriptAlias /secure /etc/shibboleth/shibenv.php
<Location /secure>
    AuthType shibboleth
    ShibRequestSetting requireSession 1
    ShibRequestSetting applicationId default
    require shib-session
</Location>

## Activation globale de l'authentification
Shibboleth
## C'est nécessaire pour activer les handlers
<Location />
     AuthType shibboleth
     Require shibboleth
</Location>
```

Mise en oeuvre
3/ configuration Shibboleth

- les fichiers de configuration
  - shibboleth2.xml
    - fichier de configuration principal
  - attribute-map.xml
    - association attributs SAML / variables d'environnement
  - attribute-policy.xml
    - politique d'acceptation des attributs reçus
  - shibd.logger
    - conf des logs

Mise en oeuvre
3/ configuration Shibboleth

```
<ApplicationDefaults entityID="https://monserveur.fr"
REMOTE_USER="mail eppn persistent-id targeted-id">
   <Sessions lifetime="28800" timeout="3600"
checkAddress="false" relayState="ss:mem"
handlerSSL="false">
    <SSO discoveryProtocol="SAMLDS"
         discoveryURL="https://discovery.renater.fr/
test"> SAML2 SAML1
    </SSO>

<MetadataProvider type="XML"
  uri="https://federation.renater.fr/test/renater-test-
metadata.xml" backingFilePath="renater-test-
metadata.xml" reloadInterval="7200"> <MetadataFilter
type="Signature" certificate="metadata-federation-
renater.crt"/>
</MetadataProvider>
```

Mise en oeuvre
3/ configuration Shibboleth

```
# service httpd restart

# service shibd start
```

Mise en oeuvre
3/ test du fonctionnement

- enregistrement dans la fédération de test
  - auprès du guichet RENATER
  - https://federation.renater.fr/registry
- test d'authentification
  - `https://monserveur.fr/secure`
  - utiliser le compte de test
    - Fédération Education-Recherche – IdP de Test
    - etudiant1/etudiant1

Mise en oeuvre
4/ test du fonctionnement

(REMOTE_USER)	jean.dupont@univ-test.fr
(HTTP_REMOTE_USER)	
SCRIPT_URL	/test/ressource
SCRIPT_URI	https://test.federation.renater.fr/test/ressource
Shib-Application-ID	default
Shib-Session-ID	_caaf1f00f92e6813748d77b2c4dd15c8
Shib-Identity-Provider	https://test.federation.renater.fr/idp/shibboleth
Shib-Authentication-Instant	2014-09-24T20:39:23.946Z
Shib-Authentication-Method	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Shib-AuthnContext-Class	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Shib-Session-Index	_843df0bab884d49ce6fddf58595ab1a3
ScriptAffiliation	CustomValue
affiliation	student@univ-test.fr;member@univ-test.fr
cn	Dupont Jean
displayName	Jean Dupont
eppn	etudiant1@univ-test.fr
facsimileTelephoneNumber	0102030405
freeBusyUrl	http://calendar.univ-x.fr/jean.dupont@univ-test.fr?fmt=freebusy
givenName	Jean
l	Paris
mail	jean.dupont@univ-test.fr

Mise en oeuvre
5/ passage en production

- inscription dans la fédération Education-Recherche
  - via le guichet RENATER

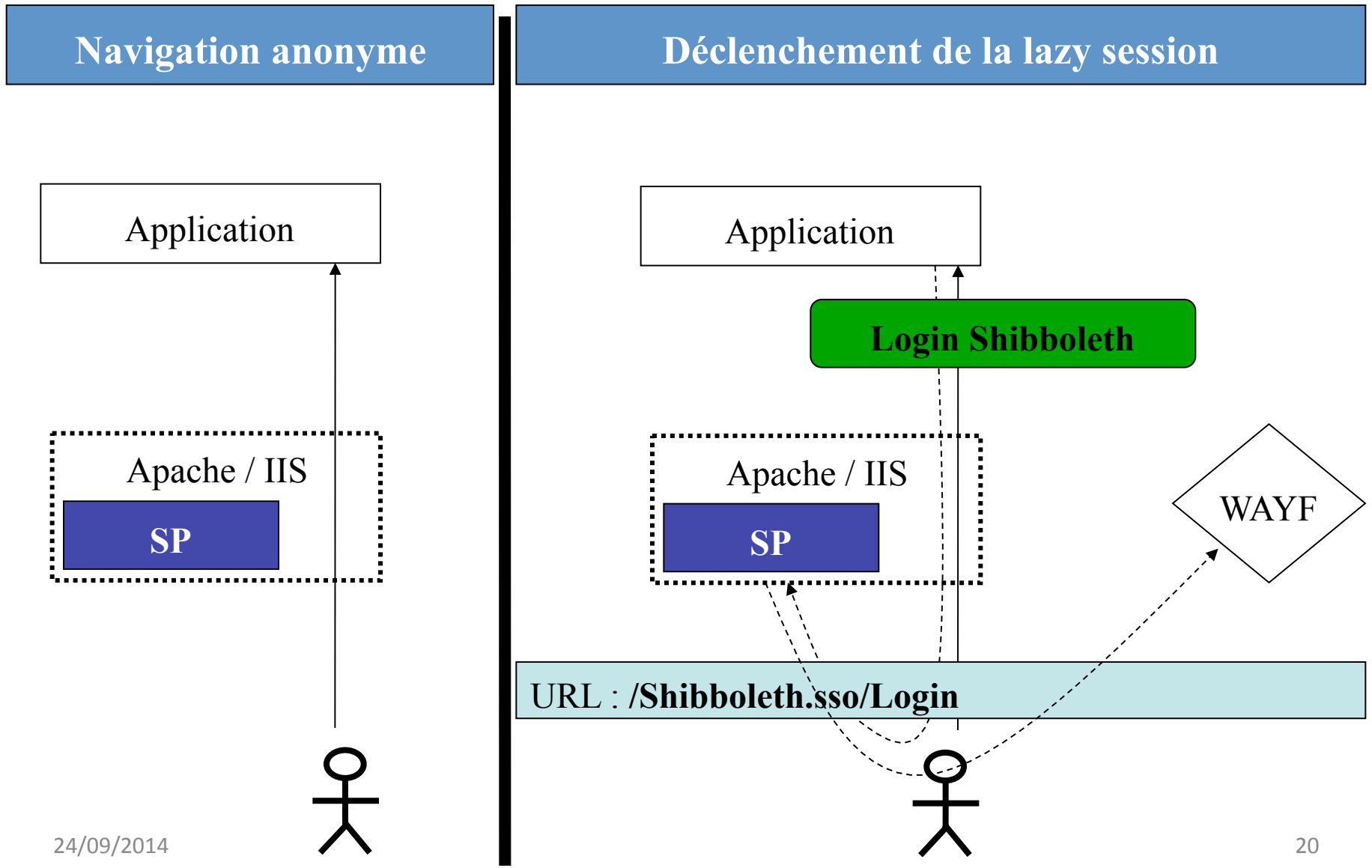
1 7

Description de l'entité SAML			Fédérations disponibles		
Type	Intitulé et identifiant	Organisme de rattachement	Fédération de Test	Fédération Education-Recherche	Interfédération eduGAIN
idp	Mathrice - Test LF https://cas.mathrice.org/idp/shibboleth	Université Bordeaux 1	●	●	●
sp	(en cours de creation - ne pas activer tout de suite) CNRS - Service d'Authentification pour les Mathématiques https://sam.math.cnrs.fr/sp	CNRS	●	⛔	⛔
sp	CNRS - Forge Mathrice https://forge.math.cnrs.fr/sp	CNRS	●	●	●
sp	CNRS - Portail de services Mathrice https://plm.math.cnrs.fr/sp	CNRS	●	●	●
sp	Listes2 Mathrices https://listes2.math.cnrs.fr	aucun	●	⛔	⛔
sp	Mathrice - Test LF https://cas.mathrice.org	Université Bordeaux 1	●	●	●
sp	Mathrice - Test LF Doc https://webmail.math.cnrs.fr	Université Bordeaux 1	●	●	●
sp	Portail Mathrice - Test LF https://plm.math.cnrs.fr	Université Bordeaux 1	●	●	●

Fonctionnement du SP Shibboleth

- un module d'authentification pour Apache
  - activé sur des URLs
  - attributs SAML transmis sous forme de
    - variables d'environnement
    - champs d'entête HTTP
- fonctionnement classique
  - authentification en rupture de flux
- mais ça ne suffit pas pour :
  - la navigation anonyme
  - le support de plusieurs modes d'authentification

Le mécanisme des lazy sessions



La population cible

- Une question importante
  - la population cible du service est-elle couverte ?
- élargir la population
  - maintenir plusieurs modes d'authentification
  - les comptes CRU
  - eduGAIN
- rétrécir la population
  - relations bilatérales
  - fédération hébergée par RENATER

Les comptes CRU

- IdP ouvert à tous
  - Pas limité à la communauté ESR
  - Validation de l'adresse email
- Les attributs utilisateurs
  - Email + nom + prénom + eppn + eptid
  - Pas de notion de privilèges
- **Ne fait pas partie de la fédération**
- Pour qu'un SP utilise les comptes CRU
  - Ajouter confiance dans sac-metadata.xml
  - Inscription du SP dans la Fédération Education-Recherche

Compte CRU
Passerelles sociales

- IdP comptes CRU devient (en plus) client des IdP sociaux
  - Facebook
  - Twitter
  - Yahoo
  - Google
  - Microsoft
- Passerelle monde social vers SAML
- Evite création d'un compte supplémentaire
- Évite l'installation de connecteurs au niveau d'une application « fédérée »
- ISO fonctionnelle avec Comptes CRU
  - Preuve d'authentification
  - Adresse email + identifiant pérenne (d'IdP Social)
- Mise en production
  - fin 2014

Identifier les utilisateurs
Objectif

- Utilisation des attributs utilisateur
  - gérer des contrôles d'accès
  - personnaliser les contenus
- Gestion des attributs pas l'application
  - associer le compte fédéré à un compte utilisateur
  - attribuer dynamiquement des droits
    - population non connue a priori
- Quel attribut SAML utiliser comme identifiant ?

Identifier les utilisateurs
Quel identifiant utiliser ?

attribut	exemples	Persistant?	Opaque ?	Facilement Manipulable ?
nameID	_e2310ee043088cfda1941eacbb50a6fb"	NON	OUI	NON
eduPersonTargetedID	https://services-federation.renater.fr/test/idp!https://services-federation.renater.fr/test/ressource!JO/UJs5h2MoXPRzgoLLl2xywf4o=	OUI	OUI	NON
uid	Jdupont120 267883736335	OUI	NON	VARIABLE
eduPersonPrincipalName	jdupont120@univ-x.fr 26788376335@univ-x.fr	OUI	NON	VARIABLE
mail	Jean.dupont@univ-x.fr	OUI, mais	NON	OUI

Identifier les utilisateurs
Où est le référentiel utilisateurs ?

- côté IdP
  - l'IdP fournit tous les attributs nécessaires
    - cas standard
- côté application
  - l'application interroge son propre référentiel
    - LDAP, SQL, Web Service
- ailleurs
  - plusieurs applications partagent un référentiel utilisateur
    - exemple : Mathrice
  - possibilité d'utiliser un Attribute Provider SAML
    - cf le service d'autorisation de RENATER

Le Discovery Service (ex-WAYF)

- Possibilité d'utiliser un DS par établissement ou National
  - Il faut redonder cette brique logicielle
  - Car, si en panne, il bloque l'accès à toutes les applications qui se basent sur lui
- Plusieurs implémentations existent :
  - SWITCH WAYF
  - Shibboleth DS
  - Disco juice

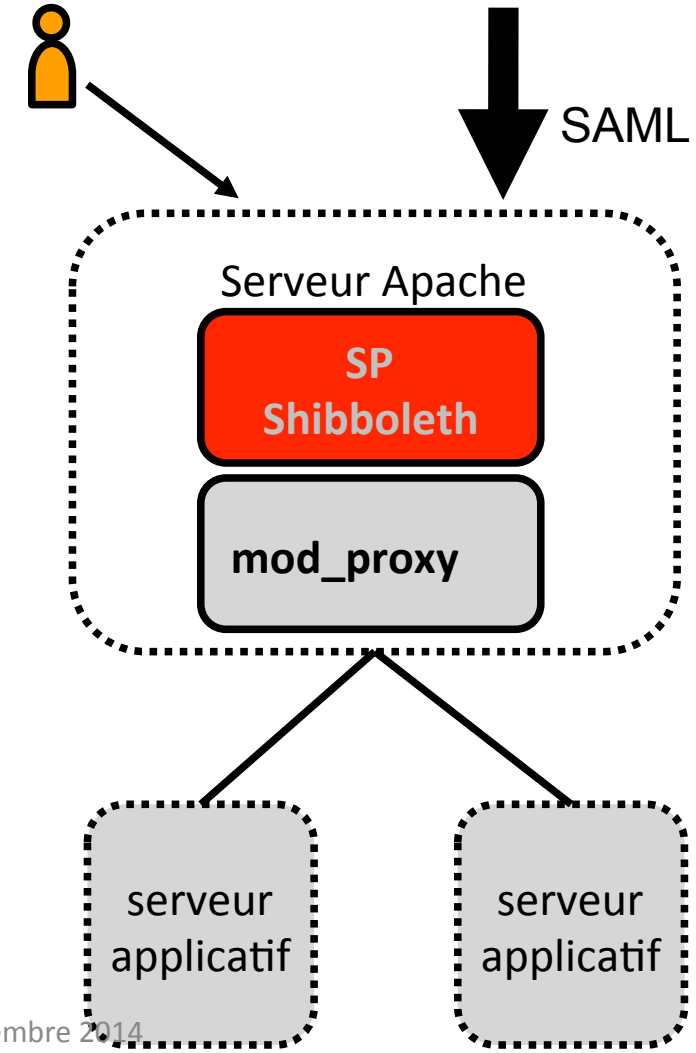
Un WAYF mieux intégré

- Objectif
  - intégrer le menu déroulant dans l'application
  - avec une liste d'IdP contextuelle
  - fonction « search as you type »
- Fonction Embedded WAYF
  - native dans le SWITCH WAYF
- Principe de fonctionnement
  - application inclut du code Javascript
  - paramétrage possible
- Documentation
  - https://services.renater.fr/federation/docs/fiches/filtreridp

Un WAYF mieux intégré

Un SP sur un reverse proxy

- Permet de mutualiser la fonction SP
  - Un seul serveur serveur à administrer
- Attributs utilisateurs transmis sous forme d'entêtes HTTP
  - ShibUseHeaders On
  - Il faut sécuriser...
- Haute disponibilité



Pour finir

- Le service, la documentation
  - https://services.renater.fr/federation
- Support collaboratif - Forum
  - Federation-utilisateurs@listes.renater.fr
- Support RENATER
  - support@renater.fr