EoleSSO

EOLE 2.7

création : Juin 2018 Version : révision : Juin 2019 Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

EOLE 2.7

Version : révision : Juin 2019

Date : création : Juin 2018

Editeur : Pôle national de compétences Logiciels Libres

Auteur(s) : Équipe EOLE

Copyright : Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Licence : Cette documentation, rédigée par le Pôle national de compétences Logiciels Libres, est mise à disposition selon les termes de la licence :

Creative Commons Attribution - Partage dans les Mêmes Conditions 3.0 France (CC BY-SA 3.0 FR) : http://creativecommons.org/licenses/by-sa/3.0/fr/.

Vous êtes libres :

- de **reproduire, distribuer et communiquer** cette création au public ;
- de **modifier** cette création.

Selon les conditions suivantes :

- **Attribution** : vous devez citer le nom de l'auteur original de la manière indiquée par l'auteur de l'œuvre ou le titulaire des droits qui vous confère cette autorisation (mais pas d'une manière qui suggèrerait qu'ils vous soutiennent ou approuvent votre utilisation de l'œuvre) ;
- **Partage des Conditions Initiales à l'Identique** : si vous modifiez, transformez ou adaptez cette création, vous n'avez le droit de distribuer la création qui en résulte que sous un contrat identique à celui-ci.

À chaque réutilisation ou distribution de cette création, vous devez faire apparaître clairement au public les conditions contractuelles de sa mise à disposition. La meilleure manière de les indiquer est un lien vers cette page web.

Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits sur cette œuvre.

Rien dans ce contrat ne diminue ou ne restreint le droit moral de l'auteur ou des auteurs.

Cette documentation est basée sur une réalisation du Pôle national de compétences Logiciels Libres. Les documents d'origines sont disponibles sur le site.

EOLE est un projet libre (Licence GPL).

Il est développé par le Pôle national de compétences Logiciels Libres du ministère de l'Éducation nationale, rattaché à la Direction des Systèmes d'Information de l'académie de Dijon (DSI).

Pour toute information concernant ce projet vous pouvez nous joindre :

- Par courrier électronique : eole@ac-dijon.fr
- Par FAX : 03-80-44-88-10
- Par courrier : EOLE-DSI - 2G, rue du Général Delaborde - 21000 DIJON
- Le site du Pôle national de compétences Logiciels Libres : http://eole.orion.education.fr

Table des matières

Chapitre 1 - Présentation du produit EoleSSO 4
Chapitre 2 - Onglet Eole sso : Configuration du service SSO pour l'authentification unique 6
Chapitre 3 - Protocoles supportés 15
1. Compatibilité CAS 15
2. Compatibilité SAML2 15
3. Compatibilité RSA Securid 16
4. Compatibilité OpenID Connnect 17
4.1. Configuration du fournisseur d'identité France Connect 21
4.2. Configuration du fournisseur d'identité Google (Google APIs). 23
Chapitre 4 - Gestion des attributs des utilisateurs 25
1. Ajout d'attributs calculés 25
2. Filtrage des données par application 28
3. Définition de filtres d'attributs 29
Chapitre 5 - Fédération avec une entité partenaire 32
1. Déclaration d'un serveur parent 32
2. Fédération SAML : Gestion des Associations 33
3. Fédération SAML : Gestion des méta-données 38
4. Fédération SAML : Accès aux ressources 38
5. Gestion des sources d'authentification multiples 41
Chapitre 6 - Personnalisation de la mire SSO 45
Chapitre 7 - Configuration d'EoleSSO en mode cluster 48
Chapitre 8 - Répartition de charge EoleSSO en mode cluster 52
Chapitre 9 - Compléments de configuration EoleSSO 66
1. Résumé des fichiers et liens 66
2. Astuces d'exploitation 68
3. Exemple de Fédération avec RSA/FIM 68
4. Fédération entre 2 serveurs EoleSSO 70
5. Mise en place de l'authentification OTP 71
6. Application de redirection : Eole-dispatcher 72
7. Configuration du fournisseur d'identité France Connect 78
8. Configuration du fournisseur d'identité Google (Google APIs). 80
Chapitre 10 - Questions fréquentes 82
1. Questions fréquentes propres à EoleSSO 82
Glossaire 83

Chapitre 1

Présentation du produit EoleSSO

Description du produit

EoleSSO est un serveur d'authentification développé pour répondre à la problématique du SSO[p.86] (authentification unique) dans différentes briques de l'architecture EOLE. Il est développé en langage Python à l'aide du framework Twisted[p.86].

Ce produit implémente en premier lieu un serveur d'authentification compatible avec le protocole CAS[p.83].

Une partie du protocole SAML[p.85] a été implémentée par la suite pour permettre de répondre à des problématiques de fédération avec d'autres produits (ou entre 2 serveurs EoleSSO).

Ce document décrit la configuration, l'administration et l'utilisation du serveur EoleSSO.

Principe de fonctionnement général

La gestion du Single Sign On[p.86] (SSO) dans EoleSSO est basée sur le protocole CAS[p.83].

Le principe est que l'utilisateur fournit ses identifiants sur la page d'authentification du service EoleSSO. Une fois les identifiants validés, le service pose un cookie de session SSO dans le navigateur. Ce dernier n'est valide que sur une durée définie.

Tant que le cookie est valide, le service reconnaît automatiquement l'utilisateur à chaque fois qu'une application demandera de vérifier son authentification. Ce système présente plusieurs intérêts : l'utilisateur ne saisit qu'une fois ses identifiants pour se connecter à un ensemble d'applications et celles-ci n'ont jamais accès à ses identifiants réels (La liste des informations envoyées aux applications par le service SSO est configurable par application grâce à un système de filtres).

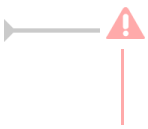
Le serveur d'authentification possède plusieurs caches de sessions :

- tickets utilisateurs (session SSO) : longue durée, réutilisable. Ces tickets sont la preuve d'authentification de l'utilisateur et sont stockés dans un cookie sécurisé dans le navigateur de l'utilisateur ;
- tickets d'application : courte durée (5 minutes par défaut), utilisable une seule fois et pour une seule application.

  Ces tickets sont également utilisés pour mémoriser une session de fédération avec un autre système (se reporter aux chapitres traitant de la fédération d'identité).

Les applications clientes n'ont pas accès à l'identifiant de la session utilisateur, il est échangé uniquement entre le serveur d'authentification et le navigateur.

Une fois qu'une application a obtenu un ticket, elle peut utiliser de façon classique une session interne pour ne pas surcharger le serveur par des appels trop nombreux.

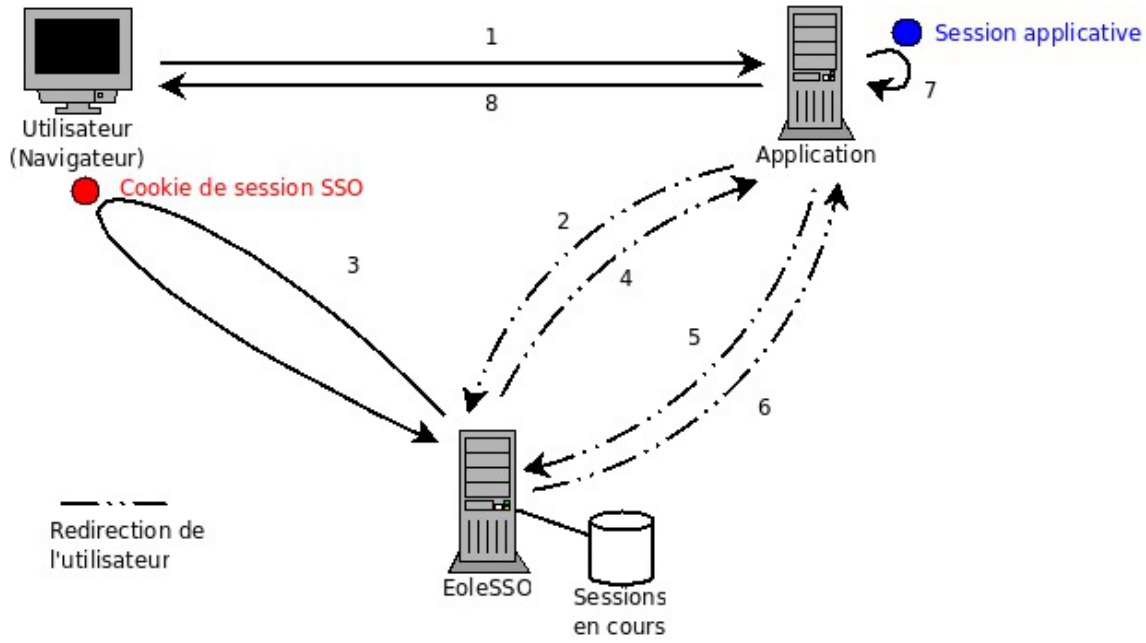


La session SSO étant gérée par un cookie placé dans le navigateur du client, celui-ci doit être

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

configuré pour accepter les cookies.

Déroulement de l'accès à une application via EoleSSO



1. L'utilisateur accède à une page d'une application (service) configurée pour utiliser le système SSO (application utilisant un client CAS).
2. L'application redirige l'utilisateur sur le serveur SSO en passant une URL de retour (paramètre `service`). Le serveur SSO vérifie qu'un cookie de session est présent et qu'il correspond à une session valide.
3. Si ce n'est pas le cas, il demande à l'utilisateur de saisir ses identifiant et mot de passe pour établir une nouvelle session SSO.
4. Une fois la session validée, le serveur SSO génère un ticket d'application valable pour une courte durée et réservé à l'URL du service. Il redirige alors l'utilisateur sur cette URL en passant le ticket en paramètre.
5. L'application récupère le ticket. Elle redirige l'utilisateur sur l'URL de validation du serveur SSO en passant en paramètre le ticket reçu et son URL de service.
6. Le service SSO vérifie que le ticket est encore valide et correspond à l'URL de service. puis redirige sur l'URL de service en incluant une réponse. Si cette réponse est positive (le ticket est valide), elle contient également des informations sur l'utilisateur (les informations renvoyées dépendent de l'application, se reporter au chapitre traitant des filtres).
7. L'application reçoit la réponse et crée éventuellement une session interne pour l'utilisateur.
8. La page de l'application est renvoyée à l'utilisateur

Le fonctionnement peut être plus complexe dans le cas de l'utilisation du mode proxy pour accéder à des services non web (par exemple, pour accéder à un service IMAP ou FTP).

Se reporter à la description du site officiel du protocole CAS pour plus de détail :

http://www.apereo.org/cas

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 2

Onglet Eole sso : Configuration du service SSO pour l'authentification unique

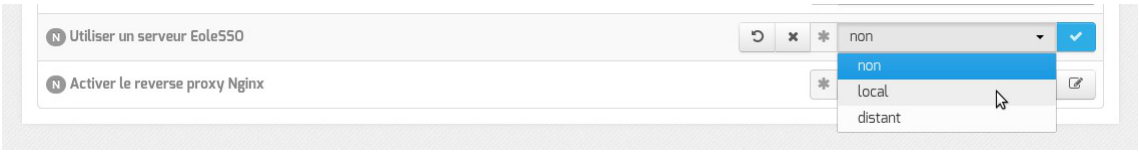
Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

Il est cependant possible de l'utiliser dans un autre environnement en modifiant manuellement le fichier de configuration `/usr/share/sso/config.py`.

Cette section décrit la configuration du serveur depuis l'interface de configuration du module disponible sur tous les modules EOLE. Les valeurs définies par défaut simplifient la configuration dans le cadre d'une utilisation prévue sur les modules EOLE.

Serveur local ou distant

L'activation du serveur EoleSSO s'effectue dans l'onglet `Services`.



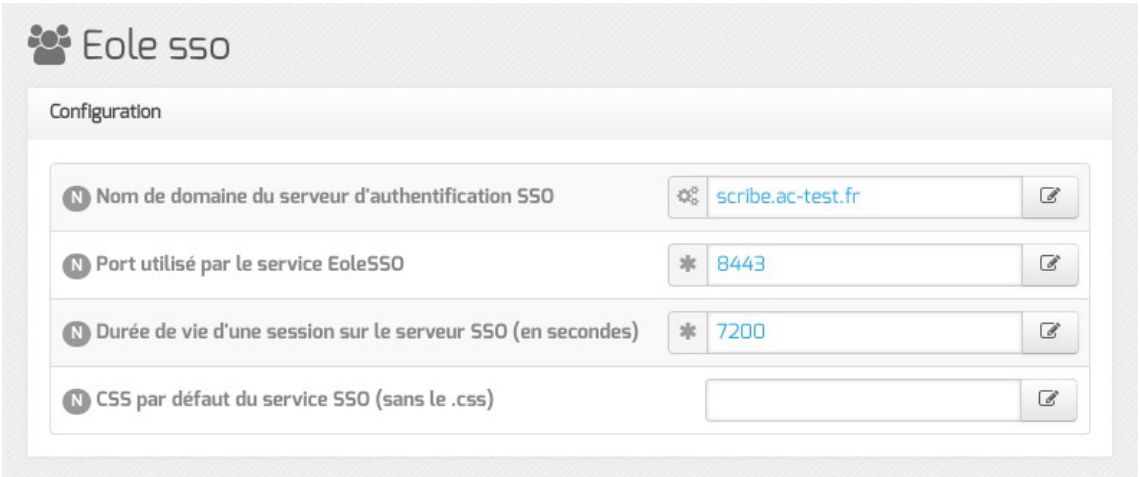
La variable `Utiliser un serveur EoleSSO` permet :

- `non` : de ne pas utiliser de SSO sur le serveur ;
- `local` : d'utiliser et de configurer le serveur EoleSSO local ;
- `distant` : d'utiliser un serveur EoleSSO distant (configuration cliente).

Adresse et port d'écoute

L'onglet supplémentaire `Eole-sso` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.

Dans le cas de l'utilisation du serveur EoleSSO local, `Nom de domaine du serveur d'authentification SSO` doit être renseigné avec le nom DNS du serveur.

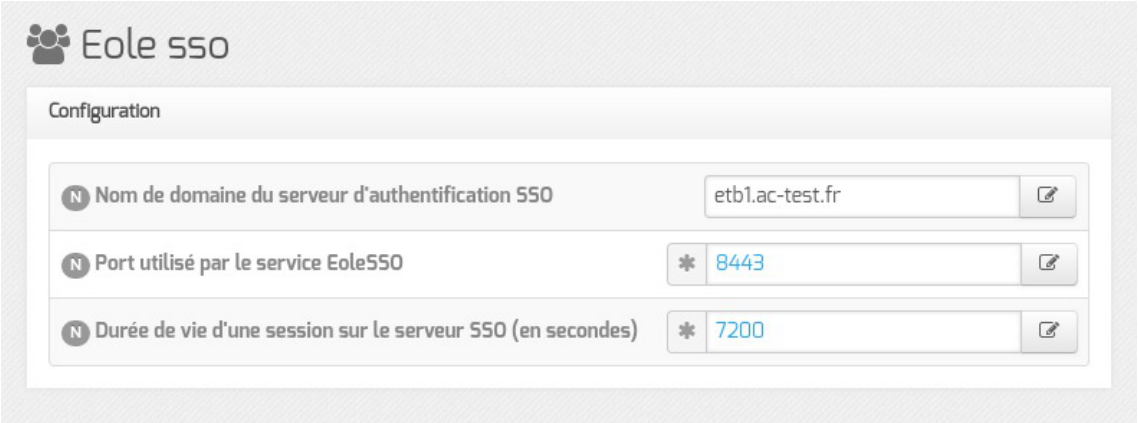


création : Juin 2018 Version : révision : Juin 2019
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Configuration d'un serveur EoleSSO local

- `Durée de vie d'une session (en secondes)` : indique la durée de validité d'une session SSO sur le serveur. Cela n'influence pas la durée de la session sur les applications authentifiées, seulement la durée de la validité du cookie utilisé par le serveur SSO. Au delà de cette durée, l'utilisateur devra obligatoirement se ré-authentifier pour être reconnu par le serveur SSO. Par défaut, la durée de la session est de 3 heures (7200 secondes).
- `CSS par défaut du service SSO (sans le .css)` : permet de spécifier une CSS différente pour le formulaire d'authentification affiché par le serveur EoleSSO. Le fichier CSS doit se trouver dans le répertoire `/usr/share/sso/interface/theme/style/<nom_fichier>.css`. *Se reporter au chapitre personnalisation pour plus de possibilités à ce sujet.*

Dans le cas de l'utilisation d'un serveur EoleSSO distant, seuls les paramètres `Nom de domaine du serveur d'authentification SSO` et `Port utilisé par le service EoleSSO` sont requis et les autres options ne sont pas disponibles car elles concernent le paramétrage du serveur local.



Configuration d'un serveur EoleSSO distant

Par défaut le serveur communique sur le port `8443`. Il est conseillé de laisser cette valeur par défaut en cas d'utilisation avec d'autres modules EOLE.

Si vous décidez de changer ce port, pensez à le modifier également dans la configuration des autres machines l'utilisant.

À partir d'EOLE 2.7.2, le serveur SSO local est est également accessible sur le port HTTPS avec l'URL : `https://<nom du serveur>/sso`.

Si le port HTTPS (`443`) est déclaré pour ce service, alors celui-ci n'est accessible que via l'URL `https://<nom du serveur>/sso`.

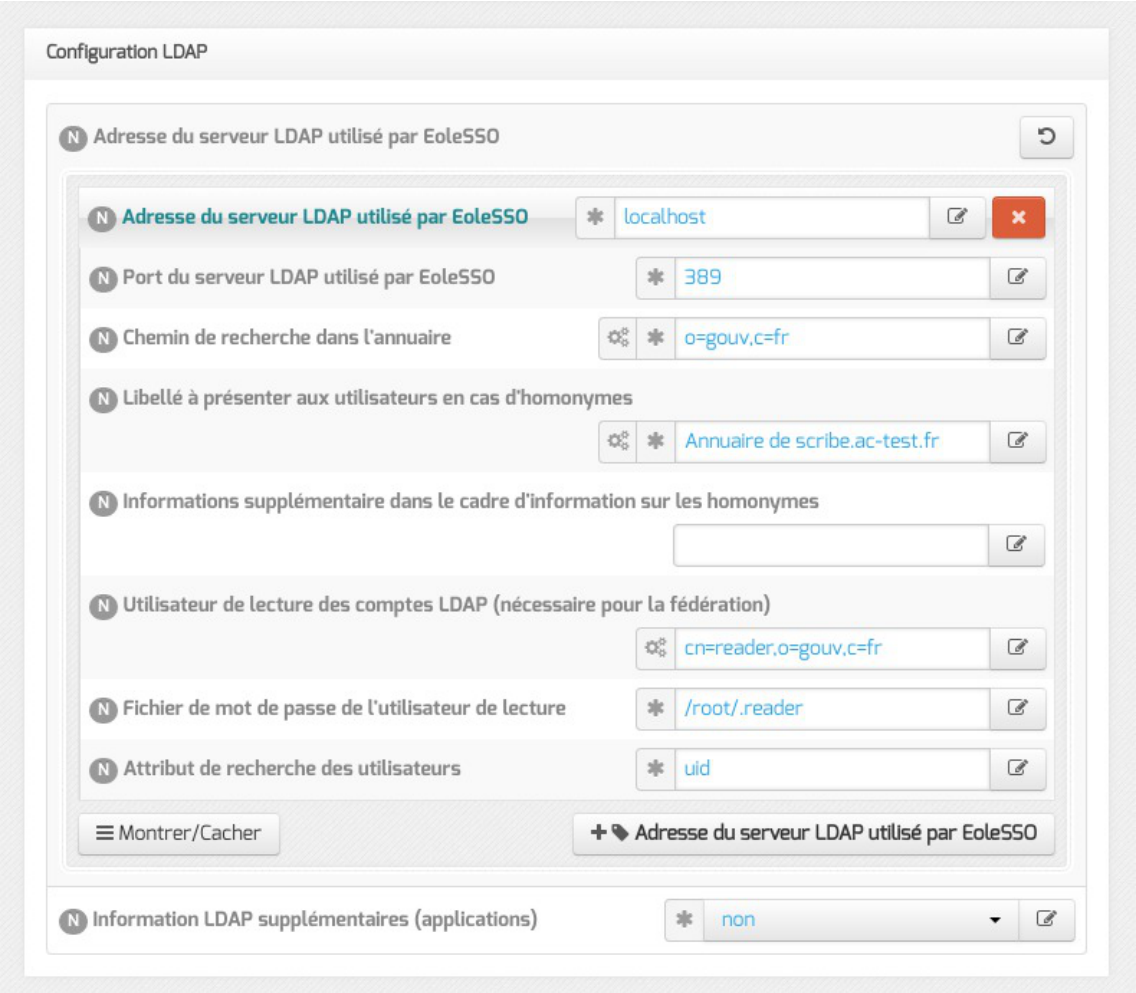
L'URL de la forme `https://<nom du serveur>:<port>/` reste valable pour les autres valeurs de port que 443.

Configuration LDAP

Le serveur EoleSSO se base sur des serveurs LDAP[p.84] pour authentifier les utilisateurs et récupérer

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

leurs attributs.



Il est possible ici de modifier les paramètres d'accès à ceux-ci :

- l'adresse et le port d'écoute du serveur LDAP ;
- le chemin de recherche correspond à l'arborescence de base dans laquelle rechercher les utilisateurs (basedn) ;
- un libellé à afficher dans le cas où un utilisateur aurait à choisir entre plusieurs annuaires/établissements pour s'authentifier (voir le chapitre `Gestion des sources d'authentifications multiples`) ;
- un fichier d'informations à afficher dans le cadre qui est présenté en cas d'homonymes. Ces informations apparaîtront si l'utilisateur existe dans l'annuaire correspondant. Les fichiers doivent être placés dans le répertoire `/usr/share/sso/interface/info_homonymes` ;
- DN[p.83] et mot de passe d'un utilisateur en lecture pour cet annuaire ;
- attribut de recherche des utilisateurs : indique l'attribut à utiliser pour rechercher l'entrée de l'utilisateur dans l'annuaire (par défaut, uid)
- choix de la disponibilité ou non de l'authentification par clé OTP[p.84] si disponible *(voir plus loin)*.

Dans le cas où vous désirez fédérer EoleSSO avec d'autres fournisseurs de service ou d'identité (ou 2 serveurs EoleSSO entre eux), il est nécessaire de configurer un utilisateur ayant accès en lecture au serveur LDAP configuré.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Il sera utilisé pour récupérer les attributs des utilisateurs suite à réception d'une assertion d'un fournisseur d'identité (ou dans le cas d'une authentification par OTP).

Cet utilisateur est pré-configuré pour permettre un accès à l'annuaire local sur les serveurs EOLE.

Sur les modules EOLE, la configuration recommandée est la suivante :

- utilisateur : `cn=reader,o=gouv,c=fr`
- fichier de mot de passe : /root/.reader

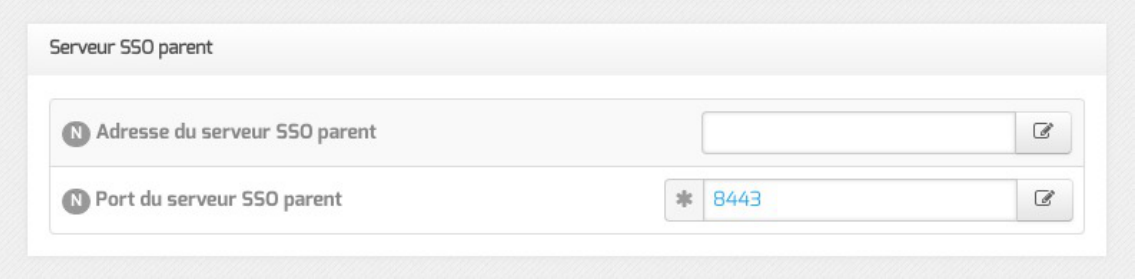
Si vous connectez EoleSSO à un annuaire externe, vous devez définir vous même cet utilisateur :

- `Utilisateur de lecture des comptes ldap` : renseignez son *dn* complet dans l'annuaire
- `fichier de mot de passe de l'utilisateur de lecture` : entrez le chemin d'un fichier ou vous stockerez son mot de passe (modifiez les droits de ce fichier pour qu'il soit seulement accessible par l'utilisateur `root`)

Passer la variable `Information LDAP supplémentaires (applications)` à `oui` permet de configurer pour chaque annuaire LDAP déclaré des attributs supplémentaires qui seront utilisés par les applications web (DN racine de l'arbre utilisateurs, DN racine de l'arbre groupes, Champ 'nom d'affichage' de l'utilisateur, Champ 'mail' de l'utilisateur, Champ 'fonction' de l'utilisateur, Champ 'categorie' de l'utilisateur, Champ 'rne' de l'utilisateur, Champ 'fredurne' de l'utilisateur...).

Serveur SSO parent

Un autre serveur EoleSSO peut être déclaré en tant que serveur parent dans la configuration (adresse et port). Se reporter au chapitre traitant de la fédération pour plus de détails sur cette notion.



Si un utilisateur n'est pas connu dans le référentiel du serveur EoleSSO, le serveur essayera de l'authentifier auprès de son serveur parent (dans ce cas, la liaison entre les 2 serveurs s'effectue par l'intermédiaire d'appels XML-RPC[p.86] en HTTPS, sur le port défini pour le serveur EoleSSO).

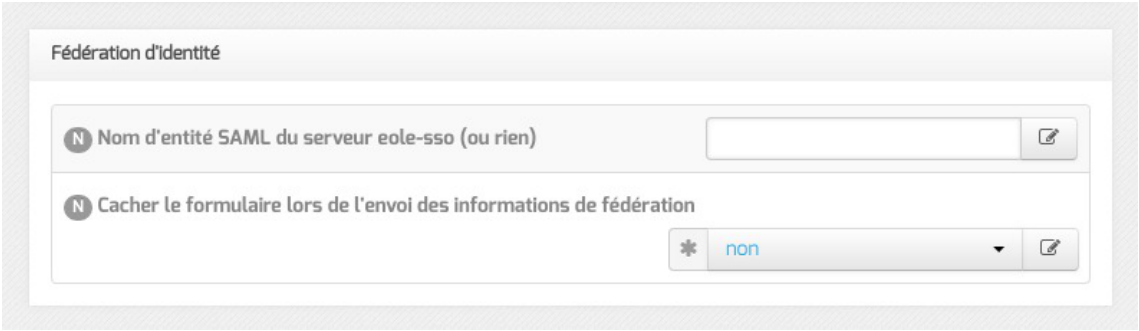
Si le serveur parent authentifie l'utilisateur, il va créer un cookie de session local et rediriger le navigateur client sur le serveur parent pour qu'une session y soit également créée (le cookie de session est accessible seulement par le serveur l'ayant créé).

Ce mode de fonctionnement n'est plus recommandé aujourd'hui. Il faut préférer à cette solution la mise en place d'une fédération par le protocole SAML.

Fédération d'identité

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le serveur EoleSSO permet de réaliser une fédération vers un autre serveur EoleSSO ou vers d'autre types de serveurs compatibles avec le protocole SAML[p.85] (version 2).

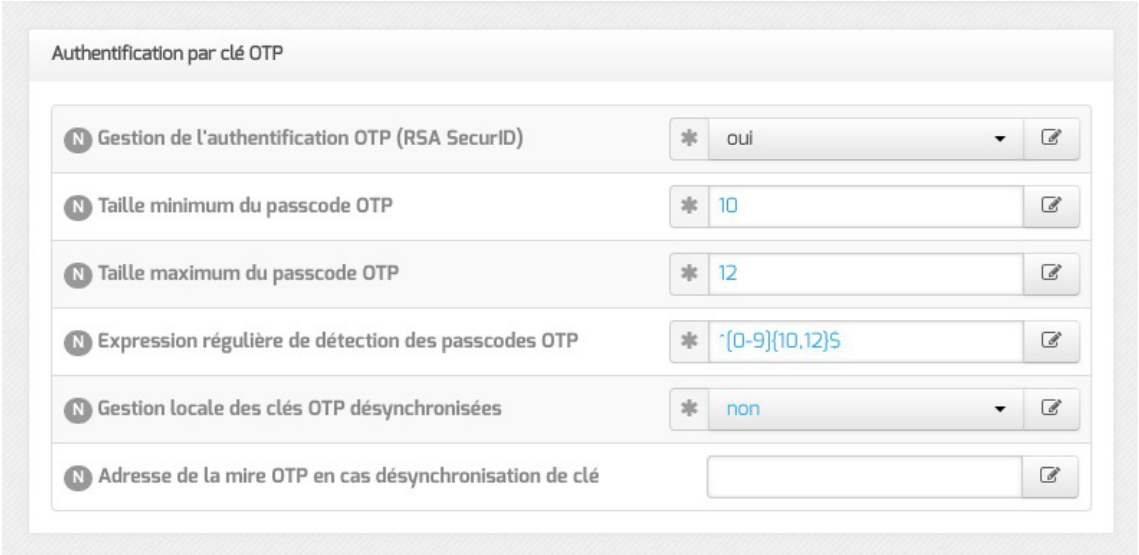


`Nom d'entité SAML du serveur eole-sso (ou rien)` : nom d'entité du serveur EoleSSO local à indiquer dans les messages SAML. Si le champ est laissé à vide, une valeur est calculée à partir du nom de l'académie et du nom de la machine.

`Cacher le formulaire lors de l'envoi des informations de fédération` : permet de ne pas afficher le formulaire de validation lors de l'envoi des informations de fédération à un autre système. Ce formulaire est affiché par défaut et indique la liste des attributs envoyés dans l'assertion SAML permettant la fédération.

Authentification OTP

Il est possible de configurer EoleSSO pour gérer l'authentification par clé OTP à travers le protocole securID[p.85] de la société EMC (précédemment RSA).



Pour cela il faut :

- installer et configurer le client PAM/Linux proposé par EMC (voir annexes)
- Répondre `oui` à la question `Gestion de l'authentification OTP (RSA SecurID)`

Des champs supplémentaires apparaissent :

- Pour chaque annuaire configuré, un champ permet de choisir la manière dont les identifiants à destination du serveur OTP sont gérés. '`inactifs`' (par défaut) indique que l'authentification OTP n'est pas proposée à l'utilisateur. Avec `'identiques'`, le login local (LDAP) de l'utilisateur sera également utilisé comme login OTP. La dernière option est '`configurables`', et indique que les

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

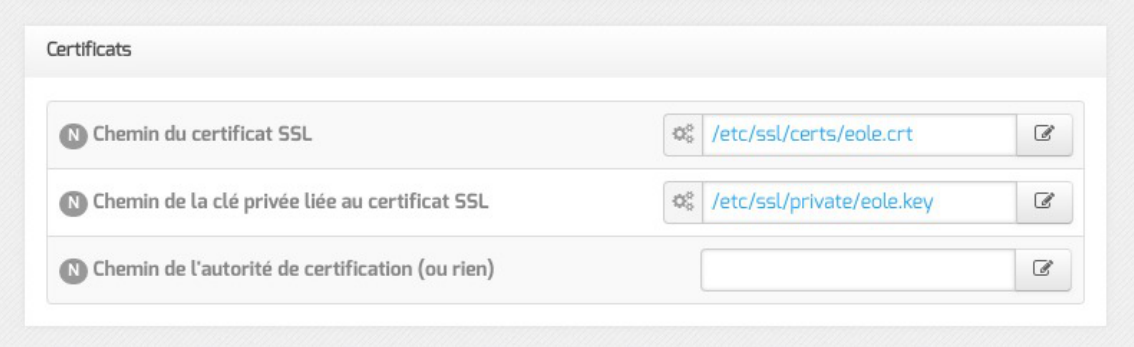
utilisateurs doivent renseigner eux même leur login OTP. Dans ce dernier cas, l'identifiant est conservé sur le serveur EoleSSO pour que l'utilisateur n'ait pas à le renseigner à chaque fois (fichier `/usr/share/sso/securid_users/securid_users.ini`).

- Le formulaire d'authentification détecte automatiquement si le mot de passe entré est un mot de passe OTP. Il est possible de modifier la reconnaissance si elle ne convient pas en réglant les tailles minimum et maximum du mot de passe et en donnant une expression régulière qui sera vérifiée si la taille correspond. Les options par défaut correspondent à un mot de passe de 10 à 12 caractères uniquement numériques.

Certificats

Les communications de et vers le serveur EoleSSO sont chiffrées.

Sur les modules EOLE, des certificats auto-signés sont générés à l'instanciation[p.83] du serveur et sont utilisés par défaut.



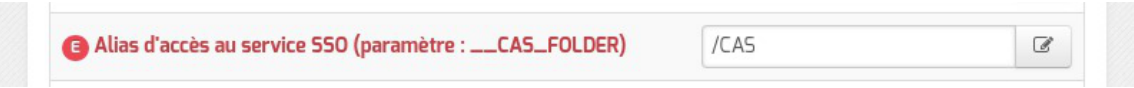
Il est possible de renseigner un chemin vers une autorité de certification et un certificat serveur dans le cas de l'utilisation d'autres certificats (par exemple, des certificat signés par une entité reconnue).

Les certificats doivent être au format PEM.

Configuration en mode expert

Autres options

En mode expert plusieurs nouvelles variables sont disponibles :

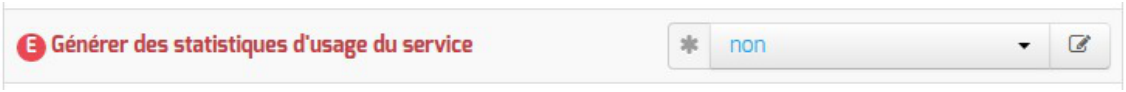


- `Alias d'accès au service SSO (paramètre : __CAS_FOLDER)` permet de créer un alias spécifique en plus du domaine et du port pour certains serveurs SSO tels que lemonLDAP[p.84] ou keycloak[p.84].

  Cette variable est disponible uniquement à partir de la version 2.6.2 d'EOLE.

- `Nom du cookie EoleSSO` et `Domaine du cookie EoleSSO` permettent la gestion d'un cluster EoleSSO.

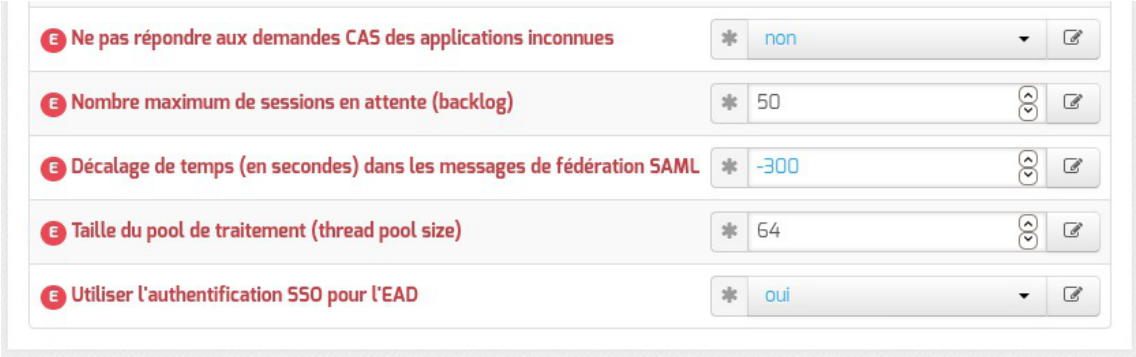
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- `Générer des statistiques d'usage du service` est à `non` par défaut.

  Si ce paramètre est à `oui`, EoleSSO va générer des statistiques sur l'usage du service (consommation mémoire, nombre de session...). Ces statistiques sont générées par la librairie python prometheus-client. Elles peuvent être intégrées à un outil tel que Grafana, et sont disponibles sur l'URL suivante : https://<adresse_serveur>:8443/metric [https://<adresse_serveur>:8443/metrics] .

- `Activer la balise meta viewport (CSS responsive)` permet d'inclure la balise HTML meta `viewport` dans les pages de l'application (avec content="width=device-width, initial-scale=1"). Elle est à activer en cas d'utilisation d'une feuille de style CSS responsive.



- `Ne pas répondre aux demandes CAS des applications inconnues` est à `non` par défaut

  Si ce paramètre est à `oui`, seules les applications renseignées dans les fichiers d'applications (`/usr/share/sso/app_filters/*_apps.ini`) sont autorisées à recevoir des réponses du serveur en mode CAS. Si il est à non, le filtre par défaut leur sera appliqué ;

- `Nombre maximum de sessions en attente (backlog)` permet de définir la taille de la file d'attente des sessions.

  Augmenter cette valeur est susceptible de résoudre des problèmes de lenteur voir de rejet des demandes d'authentification ;

- `Décalage de temps (en secondes) dans les messages de fédération SAML` est à `-300` secondes par défaut

  Ce décalage est appliqué aux dates dans les messages de fédération SAML. Cela permet d'éviter le rejet des messages lorsque le serveur partenaire n'est pas tout à fait synchrone (par défaut, on décale de 5 minutes dans le passé). Ce délai est aussi pris en compte pour la validation des messages reçus ;

- `Taille du pool de traitement (thread pool size)` permet de configurer la valeur du paramètre THREAD_POOL_SIZE.

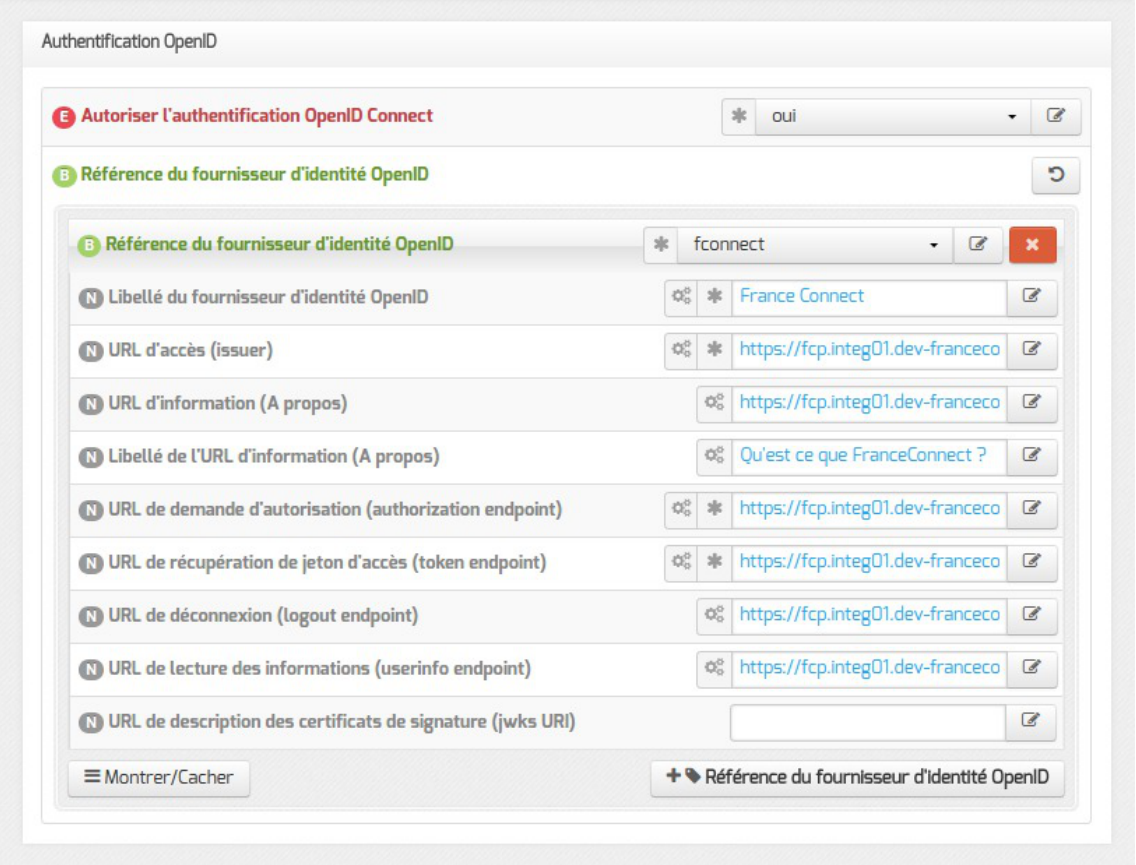
  Augmenter cette valeur est susceptible de résoudre les problèmes de charge rencontrés sur certaines infrastructures ;

- `Utiliser l'authentification SSO pour l'EAD` est à `oui` par défaut.

  Le passer à `non` permet de ne plus utiliser le serveur SSO pour l'authentification de l'EAD.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Authentification OpenID Connect



- `Autoriser l'authentification OpenID Connect` est à `non` par défaut

  Si ce paramètre est à `oui`, il devient possible de configurer un ou plusieurs fournisseurs d'identité OpenID Connect ;
- `Référence du fournisseur d'identité OpenID` : renseigner un libellé pour identifier le fournisseur. Ce libellé est interne à l'application EoleSSO. Il est utilisé pour définir le nom des fichiers contenant les logos/boutons du fournisseur :
  - `/usr/share/sso/interface/images/<libelle>.png` : bouton de connexion présenté sur la page de login (par exemple : "se connecter avec France Connect") ;
  - `/usr/share/sso/interface/images/logo-<libelle>.png` : logo du fournisseur qui sera affiché sur la page d'association de comptes.
- `Libellé du fournisseur d'identité OpenID` : libellé à destination des utilisateurs pour décrire le fournisseur ("France Connect", "Google", ...) ;
- `URL d'accès (issuer)` : URL décrivant le fournisseur d'identité (la plupart du temps, l'URL de base de son service d'authentification) ;
- `URL de demande d'autorisation (authorization endpoint)` : URL permettant au client d'initier le processus d'authentification ;
- `URL de récupération de jeton d'accès (token endpoint)` : URL permettant de récupérer un jeton (éventuellement l'identifiant de l'utilisateur) après authentification ;
- `URL de déconnexion (logout endpoint)` : URL permettant de demander une déconnexion. Ce paramètre est ignoré pour les fournisseurs utilisant une cinématique de déconnexion spécifique

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

comme Google, Facebook et Microsoft ;

- `URL de lecture des informations (userinfo endpoint)` : URL permettant de récupérer les informations de l'utilisateur à l'aide du jeton fourni ;
- `URL de description des certificats de signature (jwks URI)` : URL décrivant les certificats utilisés par le fournisseur (si disponible) ;

Définition de l'identifiant client (Client ID) et clé secrète (Client secret)

L'identifiant client (Client ID) et la clé privée secrète (Client secret) renvoyés par le fournisseur d'identité utilisés pour valider les échanges doivent être, pour des raisons de sécurité, stockés dans un fichier à part avec des droits restreints.

Pour chaque fournisseur d'identité, ajouter une ligne dans le fichier `/etc/eole/eolesso_openid.conf` :

```
<nom_fournisseur> = "<client id> :<client secret>"
```

Le `nom fournisseur` doit correspondre au paramètre `Référence du fournisseur d'identité OpenID` renseigné dans l'interface de configuration du module.

Si ces informations ne sont pas renseignées pour l'un des fournisseurs déclarés, un message l'indiquera au lancement de la commande `diagnose`.

Voir aussi...

Gestion des sources d'authentification multiples [p.41]

Compatibilité OpenID Connnect [p.17]

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 3

Protocoles supportés

1. Compatibilité CAS

Fonctions implémentées au niveau serveur

Le serveur EoleSSO implémente le protocole CAS[p.83].

Vous pouvez retrouver la description de ce protocole sur le site officiel du protocole :

http://www.apereo.org/cas/protocol

Les version 1 et 2 du protocole sont gérées.

En plus des fonctionnalités de base décrites dans le protocole, les fonctions suivantes ont été ajoutées pour permettre une meilleure compatibilité avec des versions plus récentes (CAS 3) :

- échange de messages au format SAML 1.1 dans une enveloppe SOAP ;
- implémentation d'une déconnexion centralisée pour les sessions établies via le protocole CAS. Cette fonctionnalité peut être activée ou désactivée au niveau du serveur (active par défaut) ;
- envoi d'attributs utilisateur supplémentaires dans la réponse du serveur, avec un système de filtres suivant l'URL de destination.

Les protocoles 1 et 2 de CAS utilisent un format de messages différent. Le serveur peut être configuré pour répondre à l'un ou l'autre des formats, mais ne peut pas gérer les 2 en même temps. La version 1 du protocole est disponible pour permettre au serveur de répondre à des clients plus anciens, mais dans ce cas les fonctionnalités du serveur seront très limitées (en particulier, le mode proxy et l'envoi d'attributs ne sont pas gérés).

Compatibilité du client

Suivant le client utilisé, certaines fonctionnalités peuvent ne pas être disponibles.

- La prise en compte des requêtes de déconnexion envoyées par le serveurs nécessitent l'utilisation d'un client récent (phpCAS version 1.1.0 ou supérieur).

Une version modifiée du client phpCAS est disponible dans les dépôts de la distribution EOLE.

2. Compatibilité SAML2

Pour permettre de répondre à des problématiques de fédération de l'identité des utilisateurs dans des

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

référentiels différents, le serveur EoleSSO est désormais capable d'échanger des messages au format SAML 2[p.85] . Cela permet, par exemple, que des utilisateurs authentifiés au niveau d'un établissement scolaire puissent accéder à des ressources gérées en académie sans s'authentifier à nouveau.

Les fonctionnalités implémentées correspondent à un certain nombre de scénarios envisagés. Les profils et bindings définis par le standard ne sont pas tous implémentés. En particulier, les binding `HTTP Artifact` et `SOAP` ne sont pas gérés, le serveur EoleSSO ne peut donc pas actuellement être considéré comme pleinement conforme au standard SAML 2.

Pour plus de détail, se reporter au document [http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf] publié sur le site d'OASIS.

Les fonctionnalités absentes seront éventuellement implémentées dans des versions ultérieures selon les besoins.

Les mécanismes suivants sont implémentés :

- WebSSO : AuthnRequest (POST/Redirect) / IDP Response (POST) ;
- Single Logout : LogoutRequest (POST/Redirect) / LogoutResponse (POST/Redirect).

Le serveur EoleSSO met à disposition un fichier de méta-données pour faciliter la mise en relation avec une entité partenaire.

Il gère également un répertoire de fichiers de méta-données pour récupérer les informations sur ces entités. Se reporter au chapitre `gestion des méta-données` pour plus de détails.

Les requêtes et assertions échangées doivent être signées. La clé de signature de l'entité partenaire doit être inclue dans le fichier de méta-données.

Scenarii gérés :

1. En tant que fournisseur d'identité :
   - émission d'une assertion d'authentification à destination d'un fournisseur de service (initié par le fournisseur d'identité ou suite à réception d'une requête authentification émise par un fournisseur de service valide) ;
   - déclenchement du processus de déconnexion globale à l'initiative du fournisseur ou suite à la réception d'une requête de déconnexion valide.
2. En tant que fournisseur de service :
   - création d'une session locale suite à la réception d'une assertion d'authentification d'un fournisseur d'identité (et redirection vers l'adresse spécifiée par le paramètre *relayState* si il est présent) ;
   - émission d'une requête de déconnexion en direction du fournisseur d'identité en cas de demande de déconnexion depuis une application cliente.

3. Compatibilité RSA Securid

Principe de fonctionnement

Le service EoleSSO est capable de vérifier l'authentification d'un utilisateur auprès d'un serveur RSA

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

utilisant le protocole SecurID[p.85] (authentification de type One Type Password).

L'authentification est effectuée par l'intermédiaire du module PAM[p.85] SecurID fourni par la société RSA.

Le principe est de vérifier l'authentification de l'utilisateur auprès du serveur RSA, et de conserver cette information dans la session SSO de l'utilisateur.

Lorsque l'utilisateur essaie ensuite de se connecter à un fournisseur de service, les messages SAML envoyés pour établir la fédération seront adaptés pour refléter le niveau d'authentification de l'utilisateur (mot de passe à utilisation unique).

Actuellement, cette fonctionnalité n'est disponible que sur un serveur EoleSSO configuré pour gérer l'authentification OTP[p.84].

Il est prévu par la suite de pouvoir déléguer cette validation à un autre serveur EoleSSO (moyennant l'établissement d'un lien de fédération entre les deux serveurs).

Utilisation

Lors de la première utilisation, l'utilisateur se connecte au serveur EoleSSO avec ses identifiants habituels (authentification LDAP). Avant de valider le formulaire d'authentification, il peut cocher la case `Enregistrer mon identifiant OTP`. Il peut alors renseigner l'utilisateur associé à sa clé OTP sur le serveur RSA, ainsi que son code PIN et le mot de passe actuel.

Le serveur SSO ne gère pas la saisie initiale du code PIN d'un utilisateur. Dans le cas d'un nouvel utilisateur, il faudra au préalable que celui-ci se connecte sur la mire RSA pour créer son code PIN.

Le serveur EoleSSO va vérifier l'authentification LDAP, puis va valider l'authentification auprès du serveur RSA. Si les deux authentifications réussissent, il va enregistrer l'identifiant de l'utilisateur sur le serveur RSA et va l'associer à l'utilisateur LDAP.

Par la suite, lorsque l'utilisateur revient sur la page d'authentification, le système détecte qu'il s'est déjà enregistré (après saisie de son identifiant habituel). L'utilisateur a alors la possibilité de cocher la case '`Connexion par clé OTP`'. Dans ce cas, il lui suffit de saisir son code PIN et mot de passe OTP pour s'authentifier.

4. Compatibilité OpenID Connnect

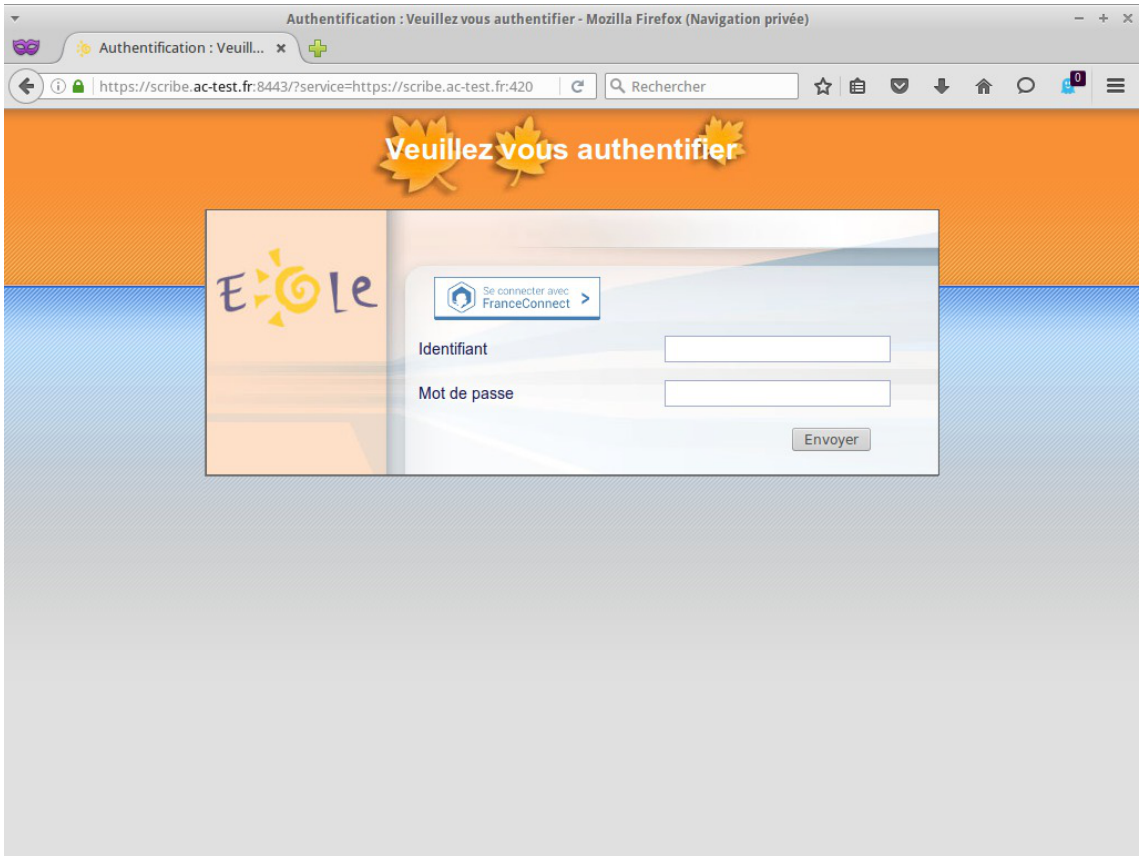
Des modifications ont été apportées à EoleSSO pour permettre d'authentifier les utilisateurs auprès du fournisseur d'identité France Connect[p.83].

Il est également possible de configurer d'autres fournisseurs d'identité OpenID Connect[p.84] dans les limites des fonctionnalités implémentées. Seul France Connect et l'authentification OAuth[p.84] 2.0 de Google ont été testés à ce jour.

Le principe de fonctionnement est le suivant :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- l'utilisateur se connecte à une application protégée par EoleSSO et est redirigé sur la mire d'authentification ;
- la mire d'authentification EoleSSO présente un bouton pour chaque fournisseur d'identité OpenID configuré ;

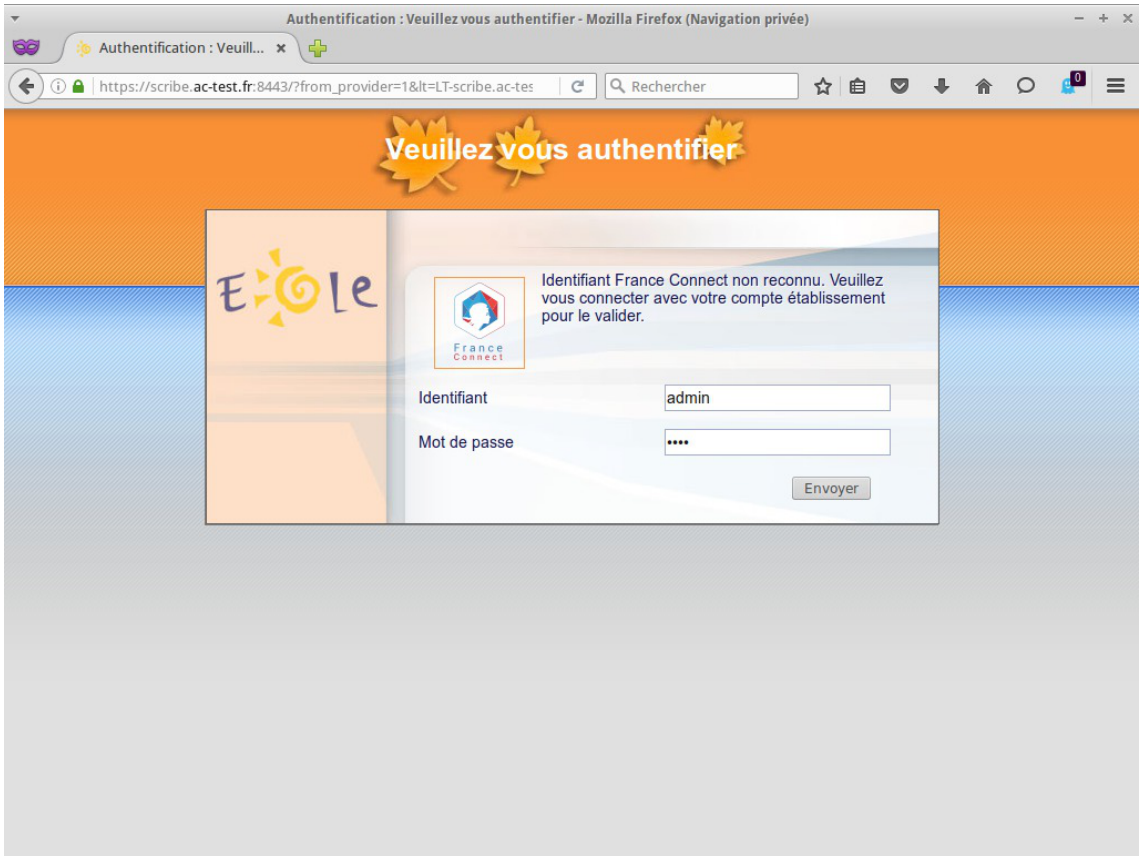


- lorsqu'un utilisateur clique sur un de ces boutons, il est redirigé vers le portail de connexion du fournisseur correspondant ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- après authentification, il est renvoyé sur le portail EoleSSO ;
- lors de la première connexion de l'utilisateur avec ce fournisseur, EoleSSO demande de renseigner le couple identifiant/mot de passe habituel, et l'associe à l'identifiant retourné par le fournisseur ;
- si l'association a déjà été réalisée, EoleSSO retrouve le compte associé, et créer directement la session de nécessaire à l'utilisateur ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- l'utilisateur est redirigé vers l'application à laquelle il souhaite accéder.

Données échangées

Le protocole OpenID Connect prévoit que le fournisseur de service précise un ensemble de données auxquelles il veut accéder (scope dans le vocabulaire OpenID).

Cela peut permettre de récupérer diverses informations (sous réserve du consentement de l'utilisateur) , comme l'adresse de messagerie, le numéro de téléphone…

Pour l'implémentation de OpenID réalisé dans EoleSSO, le but est de récupérer un identifiant pérenne et que l'utilisateur l'associe à son compte local. Le scope minimal nommé `openid` est utilisé et seul l'attribut `sub` est récupéré par EoleSSO (identifiant nom nominatif de l'utilisateur et sans informations personnelles).

La correspondance entre l'identifiant local et l'identifiant OpenID est stockée dans un fichier `/usr/share/sso/openid_users/<référence_fournisseur>_users.ini`

Pré-requis à la mise en œuvre

OpenID Connect repose sur un principe de confiance entre un fournisseur de service (Relying Party, par exemple EoleSSO), et un fournisseur d'identité (OpenID Provider, par exemple France Connect).

Pour mettre en place cette relation de confiance, le fournisseur de service va effectuer une demande d'enregistrement auprès du fournisseur d'identité. Celui-ci lui renverra un identifiant et une clé secrète.

Le fournisseur d'identité met à disposition un certain nombre d'URLs nécessaires à la configuration du client.

Un principe de configuration automatique est prévu par le protocole, mais il est rarement

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> utilisé dans la pratique et n'a pas été implémenté dans EoleSSO.

Les modalités de cet échange d'informations sont spécifiques à chaque fournisseur.

Dans la plupart des cas, il sera demandé :

- une adresse dite de callback : c'est l'adresse sur laquelle est renvoyé l'utilisateur après authentification.

  Dans le cas d'EoleSSO cette adresse est :

  `https://<adresse_serveur_eolesso>:8443/oidcallback`
- une adresse électronique de contact ;
- un logo représentant le fournisseur de service (logo EOLE, logo de l'académie…) qui apparaîtra sur la page d'authentification du fournisseur d'identité.

Gestion de la déconnexion

La cinématique de déconnexion (single logout) n'est pas implémentée par tous les fournisseurs.

Par ailleurs, certains acteurs utilisent une cinématique de déconnexion spécifique. Des adaptations ont ainsi été réalisées pour la déconnexion de Google (testée) ainsi que pour celles de Facebook et Microsoft (non testées).

4.1. Configuration du fournisseur d'identité France Connect

Pour mettre en place la relation de confiance entre EoleSSO et France Connect, il faut effectuer une demande d'enregistrement auprès de France Connect : https://franceconnect.gouv.fr/inscription

Le fournisseur d'identité France Connect renvoi un identifiant client (Client ID) et une clé privée secrète (Client secret) utilisé pour valider les échanges. Il met à disposition un certain nombre d'URLs nécessaires à la configuration du client.

Pour l'inscription il est demandé les informations suivantes:

- le nom du service ;
- une adresse électronique de contact ;
- un logo représentant le fournisseur de service (logo EOLE, logo de l'académie...) qui apparaîtra sur la page d'authentification de France Connect ;
- une adresse dite de callback : adresse sur laquelle est renvoyé l'utilisateur après authentification.

  Dans le cas d'EoleSSO cette adresse est :

  `https://<adresse_serveur_eolesso>:8443/oidcallback`

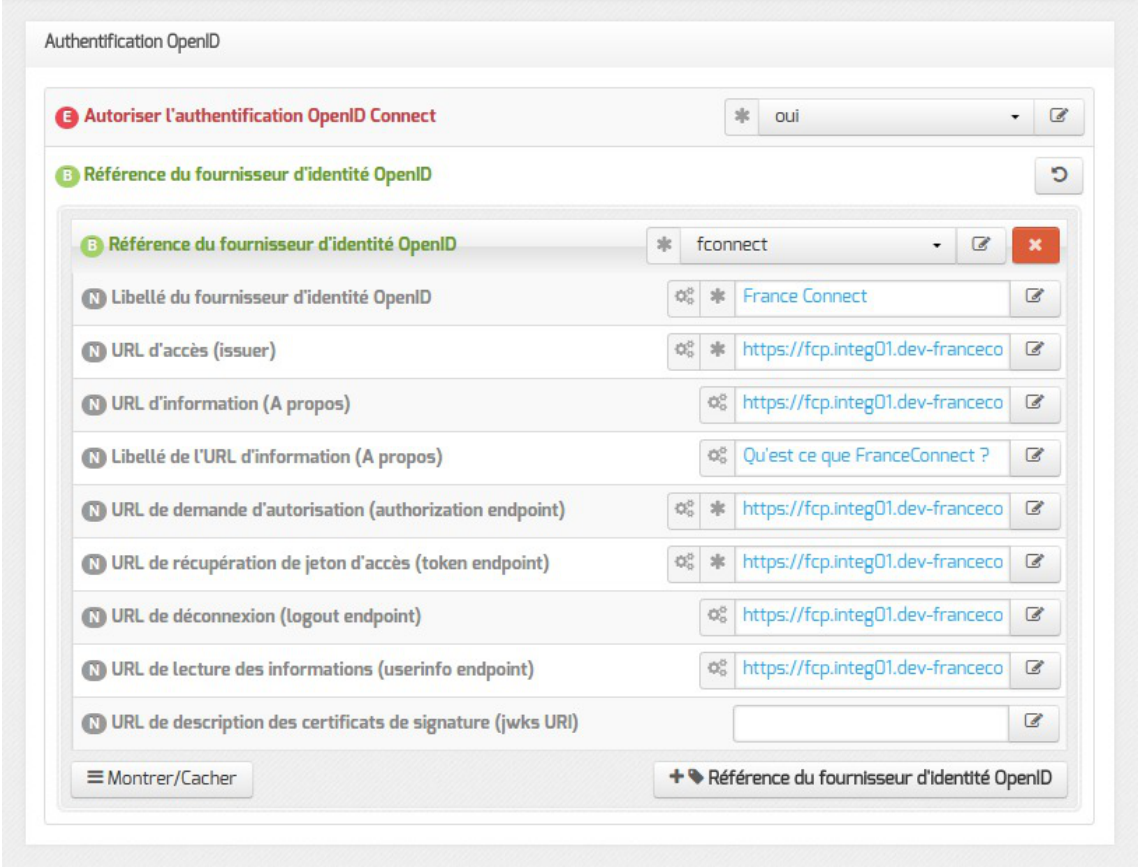
Les logos et bouton de connexion France Connect sont déjà fournis avec EoleSSO.

> Pour plus d'informations sur le fonctionnement et la configuration, se reporter à : https://franceconnect.gouv.fr/fournisseur-service
>
> Les conditions d'utilisation de France Connect et le processus de raccordement sont décrites

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> dans le document PDF suivant :
>
> https://franceconnect.gouv.fr/files/CGU FS - Annexe Processus d'implementation de FC par FS V2.1.pdf [https://franceconnect.gouv.fr/files/CGU%20FS%20-%20Annexe%20Processus%20d'implementation%20de%20FC%20par%20FS%20V2.1.pdf]
>
> À noter que parmi les conditions, une **déclaration CNIL** simplifiée est disponible et une **recette de la solution technique** mise en œuvre doit être effectuée par le SGMAP[p.86].

Une configuration prédéfinie est fournie pour France Connect.



Pour l'activer, choisissez `fconnect` dans la liste déroulante de la variable `Référence du fournisseur d'identité OpenID`, ne pas oublier de valider le choix pour faire apparaître les différentes variables.

> L'identifiant client (Client ID) et la clé privée secrète (Client secret) renvoyés par le fournisseur d'identité utilisés pour valider les échanges doivent être, pour des raisons de sécurité, stockés dans un fichier à part avec des droits restreints.
>
> Pour chaque fournisseur d'identité, ajouter une ligne dans le fichier `/etc/eole/eolesso_openid.conf` :
>
> ```
> <nom_fournisseur> = "<client id> :<client secret>"
> ```
>
> Le `nom fournisseur` doit correspondre au paramètre `Référence du fournisseur d'identité OpenID` renseigné dans l'interface de configuration du module.
>
> Si ces informations ne sont pas renseignées pour l'un des fournisseurs déclarés, un message l'indiquera au lancement de la commande `diagnose`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Voir aussi...

> Onglet Eole sso : Configuration du service SSO pour l'authentification unique

4.2. Configuration du fournisseur d'identité Google (Google APIs).

Déclaration d'EoleSSO comme fournisseur de service

Pour récupérer votre Client ID / Client Secret, vous devez créer un compte développeur depuis cette adresse : https://developers.google.com/

Rendez-vous dans la console développeur de Google afin de déclarer votre service EoleSSO comme application : https://console.developers.google.com

- Créez un nouveau projet (barre supérieure de la console -> `select a project` -> `create a project`) ;
- Une fois le projet créé, cliquez sur la barre de menu gauche (3 barres horizontales), puis sur `API Manager`. Cliquez ensuite sur `Credentials` (à gauche) ;
- Cliquer sur `Oauth Consent Screen` et renseigner au minimum le champ `Product name shown to users` (par exemple 'établissement xxx') ;
- Sauvegarder et dans Credentias, cliquer sur `Create credentials`, *Oauth Client ID" ;
- Choisir `Web application` et renseigner les champs suivants :
  - Name : au choix
  - Authorized JavaScript origins : https://[adresse_serveur_sso]:8443
  - Authorized redirect URIs : https://[adresse_serveur_sso]:8443/oidcallback
- Cliquer sur Create et recopier l'identifiant et la clé secrète fournis ;

Configuration du fournisseur d'identité (Google) dans l'interface de configuration du module

Une fois les identifiants récupérés, vous pouvez configurer les paramètres d'EoleSSO (gen_config, onglet Eole SSO en mode expert)

- Passer à `oui` la variable `Autoriser l'authentification OpenID Connect` ;
- ajouter un forunisseur en cliquant sur `+Référence du fournisseur d'identité OpenID` ;
- `Référence du fournisseur d'identité OpenID` : google (des logos sont présents et utilisés automatiquement en choisissant ce libellé) ;
- `Libellé du fournisseur d'identité OpenID` : Google (ou autre description de votre choix) ;
- `issuer` : https://accounts.google.com ;
- `authorization endpoint` : https://accounts.google.com/o/oauth2/v2/auth ;
- `token endpoint` : https://www.googleapis.com/oauth2/v4/token ;
- `userinfo endpoint` : https://www.googleapis.com/oauth2/v3/userinfo ;
- `jwks uri` : https://www.googleapis.com/oauth2/v3/certs .

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

En cas de problème, les paramètres en cours de validité sont décrits ici : https://accounts.google.com/.well-known/openid-configuration

Pour plus d'informations sur le support d'OpenID de Google : https://developers.google.com/identity/protocols/OpenIDConnect

L'identifiant client (Client ID) et la clé privée secrète (Client secret) renvoyés par le fournisseur d'identité utilisés pour valider les échanges doivent être, pour des raisons de sécurité, stockés dans un fichier à part avec des droits restreints.

Pour chaque fournisseur d'identité, ajouter une ligne dans le fichier `/etc/eole/eolesso_openid.conf` :

```
<nom_fournisseur> = "<client id> :<client secret>"
```

Le `nom fournisseur` doit correspondre au paramètre `Référence du fournisseur d'identité OpenID` renseigné dans l'interface de configuration du module.

Si ces informations ne sont pas renseignées pour l'un des fournisseurs déclarés, un message l'indiquera au lancement de la commande `diagnose`.

Voir aussi...

Onglet Eole sso : Configuration du service SSO pour l'authentification unique [p.6]

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 4

Gestion des attributs des utilisateurs

Le gestionnaire de sessions permet de récupérer des informations de l'utilisateur connecté, par exemple :

- les données LDAP de l'utilisateur (récupérées lors de la phase d'authentification) ;
- le numéro et le libellé de l'établissement hébergeant le serveur d'authentification.

Le serveur EoleSSO permet également :

- d'étendre les données disponibles en définissant des attributs calculés ;
- de créer des filtres définissant quels attributs seront disponibles ;
- de décrire des URL afin de différencier les applications et leur appliquer un filtre.

En cas d'ajout de filtres, de définitions d'applications ou d'attributs calculés, il est possible de demander au serveur de les prendre en compte sans le redémarrer. Pour cela, il faut utiliser l'option `reload` du script de démarrage du service :

```
# CreoleService eole-sso reload
```

1. Ajout d'attributs calculés

EoleSSO permet de définir des attributs calculés en plus des données récupérées dans l'annuaire à la connexion de l'utilisateur. Ces attributs sont calculés par des fonctions écrites en langage Python et ayant accès aux attributs connus de l'utilisateur.

Pour ajouter un attribut calculé, créer un fichier <nom_attribut>.py dans le répertoire /usr/share/sso/user_infos/ :

```
# -*- coding: utf-8 -*-

use_cache = True

... imports et fonctions utilitaires pour le calcul ...

def calc_info(user_info):
    .....
    return valeur_attributs
```

- `use_cache` est une directive spécifiant si l'attribut doit être mis en cache (voir Optimisation des attributs calculés) ;
- `user_info` est le dictionnaire des données existantes, il est passé automatiquement à la fonction par le serveur SSO ;
- `valeur_attributs` peut être
  - une liste Python contenant les valeurs à associer à l'attribut <nom_attribut> :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`return [val1, val2, ...]`

- un dictionnaire Python dont les clés sont le nom de champ et les valeurs la liste de valeurs associées (calcul d'attributs multiples) :

  `return {'attribut1' : [val1, val2, ...], 'attribut2' : [val1, val2, ...], ...}`

Pour que ces données soient envoyées aux applications clientes du service EoleSSO, il faut les assigner dans un filtre de données (cf. paragraphes suivants)

Nom de l'attribut retourné

Dans le cas ou une simple liste de valeur est retournée, c'est le nom du fichier qui détermine le nom d'attribut auquel seront assignées les valeurs (nom du fichier sans l'extension `.py`).

Dans le cas du calcul d'attributs multiples, le nom de fichier n'est pas pris en compte , le nom de l'attribut est indiqué directement dans la structure retournée.

Données à disposition des fonctions de calcul

L'objet `user_infos` est un dictionnaire Python contenant les informations connues sur l'utilisateur (récupérées au moment de sa connexion). Il contient les informations suivantes :

- tous les champs de l'utilisateur dans l'annuaire LDAP qui sont accessibles par lui en lecture, à l'exception des mots de passe. Comme c'est le cas dans l'annuaire, les valeurs des attributs sont multivaluées. Par exemple, pour récupérer la première valeur du champ mail, utiliser `user_infos['mail'][0]` ;
- une entrée `user_groups` qui contient la liste des groupes Samba auxquels l'utilisateur est inscrit (récupérée également dans l'annuaire) ;
- une entrée `info_groups` contenant un dictionnaire dont les clés sont l'attribut `cn` des groupes présents dans `user_groups` et les valeurs sont les attributs du groupe correspondant dans l'annuaire LDAP. Seuls les attributs suivants sont conservés : `sambaGroupType`, `displayName`, `cn`, `objectClass`, `gidNumber`, `mail`, `description` et `niveau` ;
- une entrée `dn` contenant le DN complet de l'utilisateur (utilisé pour récupérer le RNE d'origine d'un utilisateur dans le cas d'un annuaire multi-établissements) ;
- les entrées `rne` et `nom_etab` qui correspondent aux informations présentes dans la configuration Creole du serveur (ou dans le fichier de configuration du serveur EoleSSO le cas échéant) ;
- au fur et à mesure du calcul des attributs, ceux déjà traités sont rendus disponibles dans `user_infos`.

Ordre de traitement et mise à disposition des attributs

2 règles s'appliquent pour déterminer dans quel ordre les attributs calculés sont évalués :

- Les fichiers sont traités par **ordre de tri alphanumérique** sur le noms des fichiers. Si un attribut dépend d'un autre, il est recommandé de préfixer le nom de fichier par un numéro (par exemple `00_attribut1.py`, `01_attribut2.py` si attribut2 doit récupérer la valeur d'attribut1) ;
- Les fichiers renvoyant les valeurs d'**un seul attribut** (renvoi de liste) sont **prioritaires sur celles renvoyant des attributs multiples** (renvoi de dictionnaire, même si celui-ci contient un seul attribut).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Cela permet par exemple de disposer d'un ensemble d'attributs renvoyés par une seule fonction, puis d'écraser au cas par cas certains attributs si des adaptations sont nécessaires d'un serveur à l'autre (ou de redéfinir un des attributs comme non mis en cache).

Optimisation des attributs calculés

Toutes les fonctions présentes sont calculées lors de la création de la session d'un utilisateur et lorsqu'une application accède aux informations de l'utilisateur.

Pour éviter de surcharger le serveur EoleSSO lors de requêtes multiples, les attributs peuvent être mis en cache pour la durée de la session SSO de l'utilisateur. Pour qu'un attribut utilise ce cache, il faut ajouter la ligne suivante dans le fichier de calcul :

```
use_cache = True
```

Il est conseillé d'utiliser cette directive sur tous les attributs, sauf ceux dont la valeur doit être ré-évaluée durant la session de l'utilisateur.

Dans le cas d'une utilisation du produit EoleSSO hors du cadre de la distribution EOLE, certains attributs peuvent ne pas être disponibles (en fonction de l'organisation des données dans l'annuaire). Certaines informations comme le libellé de l'établissement ou son code RNE peuvent être renseignées dans le fichier de configuration principal du serveur : `/usr/share/sso/config.py`.

En plus des données ci-dessus, un certain nombre d'attributs calculés sont livrés par défaut par le serveur :

- `classes` : la classe d'un élève ou les classes d'un professeur (livré par `groupes.py`) ;
- `disciplines` : les matières enseignées pour un professeur (livré par `groupes.py`) ;
- `niveaux` : le niveau (attribut `Mefclf`) d'un élève ou les niveaux dans lesquels un professeur enseigne (livré par `groupes.py`) ;
- `secureid` : identifiant opaque calculé avec un MD5[p.84] de l'UID et du RNE de l'utilisateur ;
- `ENTPersonProfils` : renvoie le profil de l'utilisateur tel que défini dans le SDET (par ex. National_1 pour un élève) ;
- `ENTPersonStructRattachRNE` : le numéro d'établissement d'origine de l'utilisateur, calculé à partir de son DN dans l'annuaire (utile dans le cas d'un annuaire centralisé regroupant plusieurs établissements) ;
- `ecs_profil` et `ecs_rne` : version spécifique des 2 attributs précédents (applications xDesktop et eConnect, voir le site http://envole.ac-dijon.fr) ;
- `entlogin` : renvoie l'attribut `ENTPersonProfil` de l'utilisateur. Si ce champ n'est pas renseigné, l'équivalent de `secureid` est renvoyé.

Attribut calculé secureid (identifiant unique et opaque à destination de services externes)

Contenu du fichier `/usr/share/sso/user_infos/secureid.py` :

```
1 # -*- coding: utf-8 -*-
2
3 def calc_info(user_infos):
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
    """calcule secureid : identifiant crypté unique pour chaque utilisateur"""
    from md5 import md5

    # calcul d'un identifiant crypté unique
    user_hash = md5("%s@%s" % (user_infos['uid'][0], user_infos['rne'][0]))

    return [user_hash.hexdigest()]
```

2. Filtrage des données par application

EoleSSO implémente un mécanisme permettant de renvoyer des informations différentes concernant l'utilisateur en fonction de l'application qui émet la requête.

Ce mécanisme nécessite la mise en place de deux fichiers de configuration :

- un fichier de description de l'application. Ces fichiers doivent être placés dans le répertoire /usr/share/sso/app_filters et leur nom doit se terminer par `_apps.ini`.
- un fichier de filtre (dans le même répertoire), devant se nommer `<nom du filtre>.ini`.

La description d'une application se fait selon le modèle suivant (exemple avec une application fictive) :

`[editeurs]` # nom de l'application (indicatif)

`port=80` # port de l'application (facultatif)

`baseurl=/providers` # url de l'application

`scheme=both` # type de protocole : http/https/both

`addr=^appserv..*.fr$` # adresse des serveurs autorisés

`typeaddr=regexp` # type d'adresse

`filter=mon filtre` # nom du filtre à appliquer

`proxy=default` # proxy http nécessaire pour accéder à l'application

Si `port` est spécifié, il devra apparaître dans l'URL du service désirant s'authentifier. Pour que la définition fonctionne quel que soit le port (ou si le port n'est pas dans l'URL), enlevez la ligne concernant le port, ou mettez `port=` sans valeur

Il y a 2 types de vérification de l'adresse (`typeaddr`) :

1. type **ip** : l'adresse donnée peut être une adresse IP ou un couple adresse/netmask.

   Les formats d'écriture suivants sont possibles :

   - 192.168.230.1
   - 192.168.230.0/255.255.255.0
   - 192.168.230.0/24
2. type **regexp** : l'adresse est donnée comme une expression régulière à comparer à l'adresse DNS du client.

   Dans l'exemple : ^appserv..*.fr$ -> correspond à toutes les adresse du type par appserv.<qqe_chose>.fr

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Ces données seront comparée avec l'URL associée à la session dans le serveur SSO (dans le cadre du protocole CAS, cette URL correspond au champ service donné lors de l'obtention d'un ticket d'application).

Pour vérifier le fonctionnement d'une regexp, lancer un shell python:

```
>>> import re
>>> regexp = '<votre regexp>'
>>> url = '<une url à comparer avec la regexp>
>>> print re.match(regexp, url) is not None
```

`baseurl` correspond au chemin de l'application.

Dans l'exemple ci dessus, une URL du type `http://appserv test.fr:80/providers` sera reconnue (A noter que `http://appserv test.fr:80/providers/toto` est aussi considéré comme valide).

La partie requête de l'URL n'est pas prise en compte (dans cet exemple, `http://appserv test.fr:80/providers?variable=1&variable2=test` sera considérée valide).

Pour vérifier quelle URL est reçue, vous pouvez regarder dans `/var/log/rsyslog/local/eolesso/eolesso.info.log`. L'URL est affichée dans les lignes commençant par : `adding session for service : ....`

`filter` indique le nom du fichier de filtre à utiliser (sans l'extension.ini) pour les applications correspondant à cette description. Voir la section suivante pour plus de détail.

`proxy` indique que l'utilisation d'un proxy est nécessaire pour accéder à l'application depuis la machine hébergeant le serveur EoleSSO.

si la valeur est '`default`', le proxy déclaré dans la configuration (dans l'onglet general de gen_config) est utilisé. Il est aussi possible de spécifier un proxy particulier avec une valeur du type '`nom hote:port`'. Le proxy déclaré sera utilisé dans les procédures suivantes :

- envoi d'une requête de déconnexion CAS à une application
- envoi d'un ticket PGT à un client CAS en mode proxy

3. Définition de filtres d'attributs

Toutes les données connues de l'utilisateur peuvent être propagées vers les applications lorsque celles-ci valident l'authentification de l'utilisateur auprès du serveur EoleSSO.

Pour décider quelles informations seront renvoyées aux différentes applications, un système d'application de filtres a été mis en place. Le principe est de définir dans un fichier un ensemble d'attributs à renvoyer à une(des) application(s), ainsi que le nom à leur donner dans le cadre de ce filtre.

Ces fichiers sont à placer dans le répertoire `/usr/share/sso/app_filters` et doivent avoir le format suivant :

```
[section1]
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

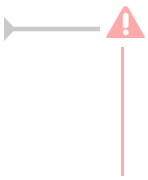
```
libelle=variable
libelle2=variable2
....
[section2]
....
```

- **section** sert à la mise en forme de la réponse (pour CAS, un nœud dans le XML retourné lors de la validation du ticket)
- **variable** correspond à l'identifiant LDAP de la donnée utilisateur à récupérer
- **libelle** est le nom qui sera utilisé pour présenter cette donnée dans la réponse du serveur

Le choix d'un filtre d'attribut est conditionné par l'adresse du service à atteindre (voir chapitre précédent). Il est également possible de créer dans le répertoire `app_filters` des **fichiers de filtres globaux** dont les attributs seront ajoutés à tous les filtres.

Le format est le même, mais ces fichiers doivent avoir l'extension `.global`.

Dans le cas ou un attribut défini dans un filtre global existe également dans le filtre d'une application, c'est la définition spécifique à l'application qui sera prise en compte lors de l'envoi des attributs à celle-ci.



Si vous souhaitez appeler la méthode statique `getUser(…)` dans votre application il est impératif d'utiliser au minimum la correspondance `user=uid` dans votre filtre. Sinon l'authentification ne peut pas aboutir : `CAS Authentification failed !`

Exemple de fichier de profil stocké dans `/usr/share/sso/app_filters/mon_filtre.ini` (correspond à l'exemple du paragraphe précédent).

```
[utilisateur]
user=uid
codeUtil=uidNumber
nom=sn
prenom=givenName
niveau=niveau
mail=mail
[etablissement]
codeRNE=rne
nomEtab=nom_etab
```

Si vous utilisez EoleSSO dans le cadre d'une distribution EOLE, un certain nombre de filtres et de définitions d'applications sont disponibles.

Il faut installer le paquet `envole-conf-sso` avec la commande `apt-get install envole-conf-sso` pour les récupérer.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> Les filtres sont installés dans `/usr/share/sso/filters_available` et `/usr/share/sso/applications/available`.
>
> Pour les utiliser, recopiez les fichiers voulus dans `/usr/share/sso/app_filters` et rechargez la configuration du service avec la commande `service eole-sso reload`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 5
Fédération avec une entité partenaire

Le serveur EoleSSO permet de réaliser une fédération vers un autre serveur EoleSSO, ou vers d'autre types de serveurs compatibles avec le protocole SAML (version 2). Les sections suivantes détaillent la mise en œuvre d'une telle solution suivant 2 méthodes différentes.

- Une première méthode de fédération simplifiée est gérée via la notion de serveur parent. Elle est utilisable uniquement entre deux serveurs EoleSSO et présente un certain nombre de limitations.
- La deuxième méthode, plus complète mais également plus complexe à mettre en œuvre, est gérée par l'implémentation d'un certain nombre d'éléments du protocole SAML[p.85] dans sa version 2. Ce type de fédération est compatible avec d'autres produit, et a principalement été testé pour une fédération avec la plateforme RSA/FIM. Des tests sont également en cours pour une fédération vers des ENT comme k-d'école de la société Kosmos.

1. Déclaration d'un serveur parent

Le fait de renseigner un serveur parent (serveur B) dans la configuration du serveur EoleSSO (serveur A) permet de fédérer ces deux serveurs. Cette solution correspond plus à une agrégation des référentiels des deux serveurs plutôt qu'à une fédération.

On considère par exemple que le serveur A est installé dans un établissement scolaire (annuaire local), et le serveur B est situé dans un rectorat (branché sur un annuaire académique).

Une fois l'adresse du serveur parent renseignée, le comportement sera le suivant :

Lorsqu'un utilisateur se connecte sur le serveur A, le serveur va d'abord vérifier le couple login/mot-de-passe auprès du serveur B (par un échange XMLRPC encapsulé dans le protocole HTTPS).

1. Si le serveur B indique une erreur d'authentification, l'authentification va alors être vérifiée localement (sur l'annuaire du serveur A).

   En cas de réussite, une session SSO est établie pour le serveur A, et l'utilisateur sera authentifié auprès des services configurés pour utiliser A. Dans le cas contraire, on considère que l'authentification a échoué.

   On retrouve donc ici le même schéma de fonctionnement que si le serveur A n'avait pas de serveur parent.
2. Si le couple login/mot-de-passe est accepté par le serveur B, une session locale 'déportée' est créée sur le serveur A. L'utilisateur est considéré comme authentifié, mais lors des échanges avec les applications, les validations seront faites auprès du serveur B.

   Le serveur A va également rediriger le navigateur de l'utilisateur vers le serveur B afin qu'un cookie de session soit créé pour celui-ci (il redirige sur le serveur A une fois le cookie créé). A la fin de cette procédure, l'utilisateur est donc identifié en même temps sur les serveurs A et B. La durée de validité de la session est gérée par le serveur B qui refusera toute validation au serveur A une fois sa session expirée.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Limitations de ce système :

- Cette solution n'est pas à proprement parler un système de fédération des 2 serveurs. Il est recommandé de l'utiliser seulement dans des cas assez simples d'utilisation, par exemple pour permettre aux personnel des équipes académiques de se connecter avec leur identifiants dans un établissement (il faut ensuite prévoir de leur attribuer des droits dans les applications, ou un profil d'administrateur sur l'EAD, ...)
- Le système de serveur parent se base sur l'adresse IP du serveur parent. Pour des raisons de sécurité (attaques de types man in the middle[p.84]), il est conseillé d'utiliser cette solution dans le cadre d'un réseau sécurisé (par exemple, à travers un RVP). Le cas échéant, on préférera la solution proposée dans le paragraphe suivant.

2. Fédération SAML : Gestion des Associations

La solution retenue pour effectuer une fédération entre deux systèmes est l'utilisation de messages SAML[p.85] pour transmettre les informations d'authentification.

La mise en place de cette fédération s'effectue en deux étapes :

- définition des attributs permettant de retrouver les utilisateurs dans les référentiels des deux systèmes (clé de fédération) ;
- échange de fichiers de méta-données (métadata[p.83]) et de certificats entre les deux entités pour établir un lien de confiance.

Pour que la fédération soit possible, il faut pouvoir établir une correspondance entre les utilisateurs des deux entités partenaires.

Pour cela, il est nécessaire de définir les attributs qui seront utilisés de chaque côté pour faire la jointure entre les deux référentiels.

configuration en tant que fournisseur de service

Jeux d'attributs

Le fichier de méta-données du serveur EoleSSO indique quels attributs sont requis pour identifier les utilisateurs dans son référentiel (l'annuaire LDAP).

Cette partie des méta-données est calculée depuis les fichiers de jeux d'attributs présents dans le répertoire `/usr/share/sso/attribute_sets` (voir plus loin). Après création ou modification de ces fichier, le serveur doit être relancé (reload est suffisant) pour que les méta-données soient mises à jour.

Le fichier `attributes.ini` présent sur les anciennes versions n'est plus utilisé. Des jeux d'attributs différents pouvant être assignés à chaque fournisseur d'identité, il peut être gênant de forcer les attributs requis en mode fournisseur de service. (voir paragraphe suivant).

Un numéro d'index est attribué automatiquement à chaque jeu d'attribut au démarrage du serveur (ne le renseignez pas vous même). Dans le cas ou les fichiers de jeux d'attributs seraient perdus, il faudra envoyer à nouveau le fichier metadata du serveur aux entités

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> partenaires afin que la nouvelle numérotation soit prise en compte.

Pour retrouver les utilisateurs après réception d'une assertion en provenance d'un fournisseur de service, le serveur EoleSSO va utiliser un jeu d'attributs. Ceux-ci sont renseignés dans des fichiers au format `.ini` situés dans `/usr/share/sso/attribute_sets/`.

Le format des fichiers est :

```
[user_attrs]
attribut_1=attribut_a
attribut_2=attribut_b
....
[optional]
attribut_3=attribut_c
....
[branch_attrs]
attribut_x=element_dn_y
....
```

Les attributs de gauche correspondent aux attributs reçus dans l'assertion du fournisseur d'identité, ceux de droite correspondent aux attributs auxquels il doivent correspondre localement.

La section `branch_attrs` permet d'utiliser certains attributs pour déterminer une branche de l'annuaire dans laquelle rechercher l'utilisateur.

Cela permet de limiter les problèmes dans le cas où des utilisateurs peuvent avoir le même identifiant dans l'annuaire (par exemple, dans le cas d'une fédération basée sur l'uid de l'utilisateur à destination d'un serveur Seshat répliquant l'annuaire de plusieurs Scribe).

Pour ces attributs, le fonctionnement est le suivant :

- lors de la recherche de l'utilisateur, le serveur va rechercher une correspondance sur 'element_dn_y=valeur_attribut_x' dans la liste des annuaires qui sont répliqués par le serveur LDAP local ;
- si plusieurs attributs de ce type sont renseignés, la branche de recherche devra correspondre à tout ces attributs.

Par exemple, si on renseigne `rne=ou` et que les attributs de l'utilisateur recherché contiennent `rne=0000000A`, le serveur EoleSSO va utiliser une branche d'annuaire dont la base de recherche contient ou=0000000A.

Les attributs de la section `user_attrs` (ou toute autre section différente de `branch_attrs` ou `optional`) seront utilisés pour retrouver l'utilisateur correpondant à la réponse du fournisseur d'identité dans le(s) serveur(s) LDAP utilisé(s) par EoleSSO.

Tous les attributs de droite doivent exister côté fournisseur de service.

Les attributs de la section `optional` seront envoyés ou non à l'initiative du fournisseur d'identité.

Si ils sont envoyés dans la réponse, ils seront intégrés aux attributs stockés dans la session SSO de l'utilisateur. Si un attribut local avec le même nom qu'un attribut optionnel existe, c'est l'attribut local qui sera conservé. Cela permet de rajouter des attributs provenant du fournisseur d'identité aux attributs connus dans le référentiel du fournisseur de service.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Par exemple, avec le fichier ci-dessus, le fournisseur de service peut récupérer l'attribut `attribut_c` dans la réponse du fournisseur d'identité et le stocker en tant qu'`attribut_3` dans la session locale.

Cadre d'utilisation

L'utilisation des attributs de type `branch_attrs` est pour l'instant limitée au cas suivant :

- l'annuaire est sur le serveur hébergeant le service EoleSSO ;
- l'annuaire est configuré pour répliquer l'annuaire d'autres serveurs (les branches de recherche correspondant aux différents serveurs répliqués sont récupérées dans /etc/ldap/replication.conf).

Dans l'état actuel, cela correspond typiquement à un service EoleSSO présent sur un serveur Seshat en académie (avec réplication de plusieurs serveurs Scribe).

Dans le cadre de l'utilisation de serveurs Scribe et Seshat, il est plutôt recommandé d'utiliser la configuration par défaut (fédération sur l'attribut FederationKey récupéré depuis l'annuaire fédérateur AAF).

Configuration de l'association avec un fournisseur d'identité

Le fichier /usr/share/sso/attribute_sets/associations.ini permet de définir les options de fédération pour chaque fournisseur de service partenaire. Sa syntaxe est la suivante

```
[nom entité1]
option=valeur
[nom entité2]
option=...
```

Le nom de l'entité doit être le nom de l'entité SAML apparaissant dans le fichier métadata du partenaire concerné (`entityID`).

Tout fichier de type .ini commençant par '`associations`' pourra également être utilisé. Cela peut permettre, par exemple, de distribuer une association correspondant à un serveur Seshat fournisseur de services en académie sur l'ensemble des serveurs Scribe d'une académie. (en passant par une variante dans Zéphir).

Il est possible de spécifier les paramètres supplémentaires suivants pour chaque association avec un fournisseur d'identité (tous facultatifs) :

- `attribute_set` : nom du jeu d'attributs à utiliser (correspond au nom du fichier de ce jeu, sans l'extension .ini)
- `allow_idp` ('true' par défaut) : si spécifié à 'false', aucune assertion provenant du fournisseur d'identité ne seront prises en compte.
- `allow_idp_initiated` ('true' par défaut) : si spécifié à 'false', les assertions envoyées par le fournisseur d'identité sans requête préalable ne seront pas traitées.
- `force_auth` ('false' par défaut) : si spécifié à 'true', le fournisseur d'identité demandera ses identifiants à l'utilisateur, même si celui ci était déjà connecté.
- `passive` ('false' par défaut) : si spécifié à 'true', le fournisseur d'identité ne demandera pas ses identifiants à l'utilisateur, même si il n'est pas reconnu. Dans ce cas, une réponse négative sera renvoyée par le fournisseur d'identité.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `default_service` (aucun par défaut): si une url est renseignée ici, elle sera utilisée comme service de destination par défaut si aucun service n'est indiqué pendant le processus de fédération.
- `default_logout_url` : Adresse sur laquelle lorsqu'une déconnexion a été initiée par le fournisseur de service (utilisée seulement si la session a été établie depuis ce fournisseur d'identité). Cela permet par exemple de rediriger sur la mire du fournisseur d'identité.
- `force_logout_url` ('false' par défaut) : Force la redirection sur l'url décrite ci dessus, même si une autre url à été spécifiée dans la demande de déconnexion (par défaut, c'est donc l'url passée en paramètre est prioritaire).
- `req_context` : niveau d'authentification requis pour accepter une assertion. Les valeurs reconnues par EoleSSO sont 'urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport' (par défaut, mot de passe saisi depuis une page sécurisée) et 'urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken' (connexion par clé OTP)
- `comparison` : opérateur de comparaison du niveau d'authentification indiqué par le fournisseur d'identité avec le niveau défini dans req_context. Par défaut cet opérateur est `exact` (valeur identique). Il est possible d'utiliser `minimum` (équivalent ou supérieur à), `maximum` (inférieur à) et `better` (strictement supérieur à).

Dans le cas d'une fédération entre des serveurs scribes et un serveur seshat avec réplication des annuaires scribe en central, il peut être utile de définir sur Seshat le paramètre default_logout_url pour chaque établissement fédéré.

Cela permet de revenir automatiquement sur le portail de l'établissement après une déconnexion depuis le portail ou un service de Seshat (l'utilisateur s'étant connecté à l'origine en établissement). Un script est fourni (`/usr/share/sso/get_domains.py`) pour essayer de déterminer automatiquement l'adresse du portail de chaque établissement en s'appuyant sur le serveur Zéphir.

Si le nom d'entité est `default`, les options définies seront utilisées par tous les fournisseurs d'identité n'ayant pas de valeur spécifique définie dans leur section. Dans le cas où aucune association avec `default` n'est présente, le fichier `default.ini` fourni avec le serveur sera utilisé comme association par défaut (et les options par défaut sont celles décrites ci-dessus).

Par défaut, aucun fichier d'association n'est fourni. Il faut ajouter manuellement la section correspondant à un fournisseur d'identité pour modifier les paramètres d'association avec les entités définies dans les métadonnées.

L'option `allow_idp` étant à 'true' par défaut, cela veut dire que tout fournisseur d'identité décrit dans les fichiers de métadonnées sera considéré comme valide (les assertions venant de lui seront traitées).

Pour avoir plus de contrôle sur les fournisseurs d'identité valides, Il est possible par exemple de redéfinir cette valeur à '`false`' pour l'entité `default`, puis de la définir à '`true`' au cas par cas pour chaque fournisseur d'identité que l'on veut autoriser.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Pour vérifier que les jeux d'attributs sont bien pris en compte :

- relancer le serveur ou recharger la configuration avec la commande `CreoleService eole-sso restart (ou reload)`
- consulter les logs du serveur (`/var/log/rsyslog/local/eolesso/eolesso.info.log`). Si un jeu d'attribut est disponible pour une entité, une mention apparaîtra à côté de son nom. Par exemple :

```
2010/06/03 15:22 +0200 [-] - Fournisseur de services configuré : urn:fs:ac-dijon:etablissements:1.0
2010/06/03 15:22 +0200 [-] - Fournisseur de services configuré : urn:fi:ac-dijon:et-Collège du parc:1.0 (jeu d'attributs : parc)
```

Ici, le premier fournisseur utilisera le jeu d'attributs par défaut, alors que le deuxième utilisera un jeu spécifique.

Configuration en tant que fournisseur d'identité

Dans ce mode de fonctionnement, le serveur EoleSSO va envoyer des messages SAML à un partenaire fournisseur de service pour lui permettre de valider l'identité de l'utilisateur connecté. Les attributs envoyés dans ce message dépendent du filtre qui est appliqué lors de l'envoi du message (voir les paragraphes précédents sur la gestion des attributs).

Par défaut, le serveur EoleSSO va utiliser les attributs définis dans le filtre SAML (`/usr/share/sso/app_filters/saml.ini`). Il est également possible de spécifier un filtre d'attributs différent en fonction du fournisseur de service auquel la réponse est envoyée. Pour cela, il faut créer une description d'application correspondant à l'URL de réception des messages du fournisseur de services, et lui associer un filtre renvoyant les attributs voulus.

Dans le cas d'une fédération SAML, il est possible de renseigner directement le nom de l'entité partenaire au lieu de décrire l'URL de réception des messages. Par exemple, la section suivante est suffisante pour déclarer un filtre :

`[mon partenaire saml]` (indicatif, affiché dans les logs au démarrage du serveur) `sp_ident=id_entité_fournisseur_service` (entityID dans le fichier metadata) `filter=nom_filtre` (nom du fichier de filtre sans l'extension `.ini`)

Dans le cas où le filtre appliqué ne permettrait pas d'envoyer au fournisseur de service tous les attributs qu'il a indiqué comme requis (dans son fichier de méta-données), un message d'erreur apparaît à l'envoi des informations d'authentification.

Dans le cadre d'une fédération d'un serveur Scribe en établissement avec un serveur EOLE (par exemple un module Seshat) situé dans les services académiques, nous utilisons l'adresse mail académique comme attribut de fédération (celle-ci est stockée sur Scribe dans l'attribut FederationKey lors de l'import de fichiers extraits de l'annuaire fédérateur).

Par défaut, le serveur est configuré pour utiliser cet attribut comme clé de jointure.

Le filtre utilisé par défaut lors de l'envoi d'assertion d'authentification (

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> `/usr/share/sso/app_filters/saml.ini`) envoie l'attribut FederationKey dans le message envoyé au fournisseur de service.

3. Fédération SAML : Gestion des méta-données

Pour permettre d'établir un lien de confiance avec une entité partenaire, le serveur EoleSSO utilise des fichiers métadata[p.83] comme défini dans les standards SAML.

1. Envoi des informations du service EoleSSO à un partenaire :
   - Le fichier métadata du service EoleSSO doit être mis en place sur le serveur partenaire. La procédure varie suivant le logiciel utilisé. Ce fichier est disponible sur le serveur à l'adresse `https://<adresse_serveur_eolesso>:8443/saml/metadata`
   - Dans le cas où ils ne sont pas pris en compte depuis le fichier de métadata, les certificats du serveur doivent être envoyés séparément, et parfois convertis vers un autre format. Le certificat utilisé par défaut dans le cadre d'un serveur EOLE est /etc/ssl/certs/eole.crt, sauf si l'utilisation d'un autre fichier a été configurée (voir l'exemple de fédération avec un serveur RSA/FIM dans les annexes pour un exemple de conversion du certificat)
2. Mise en place des information du partenaire sur le serveur EoleSSO :
   - Le fichier métadata de l'entité partenaire doit être mis en place sur : `/usr/share/sso/metadata/<nom_fichier>.xml`. Si possible utilisez un nom court, car le nom du fichier (sans le .xml) peut être utilisé dans des URLs pour faire référence à l'entité au lieu d'utiliser son identifiant SAML.
   - Une fois le fichier en place, il faut redémarrer le service EoleSSO pour qu'il soit pris en compte : `CreoleService eole-sso restart` (reload est suffisant dans ce cas)

> Si l'entité partenaire n'est pas un serveur EoleSSO, il faut vérifier que les informations suivantes sont disponibles dans le fichier métadata fourni :
>
> - Certificat de signature des messages
> - L'entité doit être capable de recevoir et envoyer des messages en utilisant les bindings `HTTP-Redirect` ou HTTP-POST. Actuellement, le serveur EoleSSO ne gère pas les bindings `HTTP-Artifact` et `SOAP/PAOS`.
> - En mode fournisseur de service, le serveur EoleSSO ne gère pas le service `Idp Discovery` (détection automatique du fournisseur d'identité à l'aide d'un cookie sur un domaine commun). Il est possible cependant d'initier le processus d'authentification en tant que fournisseur de service en spécifiant le fournisseur d'identité à interroger.

4. Fédération SAML : Accès aux ressources

Activation des différents rôles dans un accord de fédération

Pour résumer, une fois les fichiers de métadata échangés entre EoleSSO et une entité partenaire

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

(protocole SAML), les différents rôles disponibles sont conditionnés comme suit :

- Si un fichier de description de l'entité partenaire (soit par l'URL de réception des assertions, soit par son nom d'entité) est présent dans `/usr/share/sso/app_filters`, EoleSSO pourra envoyer des assertions à ce partenaire en tant que fournisseur d'identité.
- Si le nom d'entité du partenaire est présent dans un fichier d'association dans le répertoire `/usr/share/sso/attribute_sets`, ce partenaire pourra jouer le rôle de fournisseur d'identité auprès d'EoleSSO. Si l'option `allow idp initiated` est à `false` pour ce partenaire, ses assertions ne seront prises en compte que si elles font suite à une requête d'authentification émise au préalable (via l'URL `discovery` décrite ci-dessus).

Accéder à une ressource d'un fournisseur de service

Une fois la fédération mise en place entre EoleSSO et un fournisseur de service (FS), il est possible d'accéder aux services du FS à l'aide d'une URL au format suivant :

https://adresse_serveur_sso:8443/saml?sp_ident=id_fs&RelayState=service [https://adresse_serveur_sso:8443/saml?sp_ident=id_fs&RelayState=adresse_service]

`id fs` est soit l'identifiant du fournisseur de service (entityID tel que défini dans son fichier de méta données), soit le nom de son fichier de méta données placé dans `/usr/share/sso/metadata` (sans l'extension .xml).

`RelayState` est une information indiquant au fournisseur de service ou rediriger l'utilisateur une fois son identité confirmée. Les données à envoyées peuvent être l'URL d'une application protégée par le fournisseur de service, l'identifiant de l'établissement depuis lequel l'utilisateur se connecte, ... (variable suivant le fournisseur de service).

L'accès à cette URL va déclencher la cinématique suivante :

- vérification par le serveur EoleSSO de la session SSO de l'utilisateur (si il n'est pas connecté, une nouvelle session est établie après saisie des identifiants) ;
- génération et envoi d'une réponse SAML au FS pour lui indiquer l'identité de l'utilisateur ;
- Traitement de la réponse reçue par le fournisseur de service et recherche des informations sur l'utilisateur dans le référentiel du FS (profil associé, permissions, ...) ;
- Redirection de l'utilisateur sur la ressource définie par RelayState (ou sur une ressource définie par défaut le cas échéant).

Accéder à une ressource en tant que fournisseur de service

Dans le cas où le serveur EoleSSO est utilisé comme fournisseur de service, l'accès à une ressource peut se faire de 2 façons :

1. en envoyant directement une réponse SAML d'authentification sur l'URL de traitement des assertions d'EoleSSO (FS) depuis le fournisseur d'identité (processus dit 'IDP initiated'). Une URL de service à atteindre peut être fournie par le paramètre RelayState.
2. en envoyant une requête SAML d'authentification depuis EoleSSO (FS) en spécifiant le fournisseur d'identité à interroger et le service à atteindre après authentification (méthode préférable).

Dans les 2 cas, une fois l'assertion reçue validée, une session est établie sur le serveur EoleSSO.

L'utilisateur est ensuite redirigé sur l'URL du service à atteindre (il est possible de définir un service par

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

défaut pour chaque fournisseur d'identité, voir le chapitre précédent concernant la configuration des associations).

Dans le cas d'un serveur Scribe servant de fournisseur de service, il est possible par exemple de spécifier dans RelayState l'accès à l'application Pydio (accès au FTP de Scribe). Si le fournisseur d'identité est également un serveur EoleSSO (adresse_FI), l'accès se fera à travers l'adresse suivante (cas 1) :

```
https://adresse_FI:8443/saml?sp_ident=id_scribe&RelayState=https://
```

L'adresse à utiliser dans le cas 2 serait la suivante :

```
https://adresse_scibe:8443/discovery?idp_ident=id_fournisseur_ident
```

Gestion de la Déconnexion

Le serveur EoleSSO intègre la notion de déconnexion unique (single logout) dans le cadre de l'établissement d'un lien de fédération.

La procédure de déconnexion peut être initiée de deux façons.

1. Directement depuis le service EoleSSO, en accédant à l'URL : https://adresse_serveur_sso:8443/logout;
2. En utilisant le système de déconnexion de l'entité partenaire si celle-ci gère également la déconnexion unique.

Dans le deuxième cas, une demande de déconnexion au format SAML est envoyée au service EoleSSO, qui va enclencher la déconnexion et envoyer une confirmation une fois la procédure terminée (une adresse de redirection peut également être fournie avec la demande de déconnexion).

Une fois la procédure de déconnexion enclenchée, EoleSSO va envoyer une demande de déconnexion SAML à chaque entité partenaire sur laquelle l'utilisateur a établi une session par fédération.

Dans le cas où EoleSSO est également utilisé pour accéder à des applications locales, par exemple, pour le portail Envole du serveur Scribe, Il va également envoyer des requêtes de déconnexion aux applications ayant demandé un ticket au serveur SSO (ce comportement peut être désactivé dans la configuration du serveur).

Le mode de fonctionnement de la déconnexion unique est basé sur une suite d'aller-retours (par redirection) vers les différentes entités.

Dans le cas où une erreur se produit lors de la procédure de connexion sur une entité partenaire, il se peut que la procédure s'arrête dans un état de déconnexion partielle (la déconnexion n'est pas propagée à toutes les entités).

Dans ce cas, plusieurs solutions sont prévues pour limiter le problème :

- si l'URL de déconnexion du serveur EoleSSO est à nouveau sollicitée, le serveur va considérer que la dernière requête de déconnexion envoyée a échoué et va reprendre la procédure en passant au partenaire suivant.

- si une autre URL du serveur est sollicitée (création d'une nouvelle session, demande d'authentification par une application, ...), la session SSO précédente est dans tous les cas invalidée par le serveur (il devra donc se ré-authentifier).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> Dans le dernier cas, il se peut que l'utilisateur possède toujours une session sur une entité partenaire.
>
> La seule façon de résoudre le problème est de **fermer le navigateur**.

5. Gestion des sources d'authentification multiples

Il est possible de se retrouver confronté à des problèmes d'utilisateurs homonymes dans le cas où plusieurs annuaires sont utilisés comme source d'authentification ou dans le cadre d'un réplica d'annuaire distant comme c'est le cas avec le module Seshat.

EoleSSO a été amélioré pour prendre en compte ce problème.

Principe de fonctionnement

Si plusieurs annuaires sont configurés, EoleSSO va gérer une branche de recherche par annuaire. Lorsqu'un utilisateur va saisir son identifiant, une recherche va être effectuée dans chaque annuaire afin de vérifier si celui-ci est présent plusieurs fois. Si c'est le cas, une liste va être affichée pour permettre à l'utilisateur de choisir sa provenance.

La liste affichée est basée sur le libellé renseigné pour chaque annuaire dans l'interface de configuration du module. Il convient donc de bien renseigner ces informations pour que l'utilisateur soit capable de choisir.

Cas particulier : la réplication d'annuaire (Scribe/Seshat)

Gestion de la liste de choix de la source d'authentification

Dans le cadre de la réplication, l'unique annuaire à utiliser est celui du serveur hébergeant EoleSSO.

Des procédures ont été mises en place pour gérer automatiquement des branches de recherche sur chaque annuaire répliqué.

La procédure `active replication` nécessite que les 2 serveurs (serveur répliqué/serveur de réplication) soient enregistrés sur le serveur Zéphir.

Lorsque le serveur Zéphir va envoyer au serveur répliquant les éléments nécessaires à la mise œuvre de la réplication, il va également lui envoyer un fichier décrivant l'établissement dans lequel la machine répliquée est installée (le libellé doit donc être renseigné correctement dans l'application Zéphir).

Sur le module Seshat, il est possible de demander manuellement une récupération de ce fichier auprès du serveur Zéphir en lançant le script :

`/usr/share/sso/update_etabs.py`

Les informations sont stockées dans le fichier `/etc/ldap/replication/zephir/etabs.ini` dont le format est le suivant :

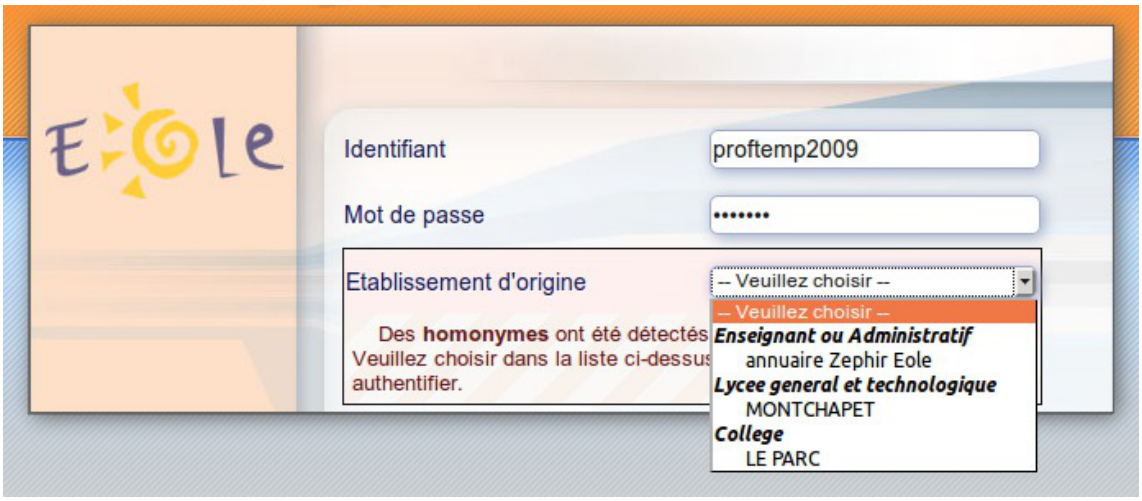
```
[rne]
libelle_etab=....
type_etab=....
portail_etab=...
```

Ces informations sont détectées automatiquement par le serveur Zéphir lorsque c'est possible.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le numéro RNE sert à faire la liaison avec les branches de recherche disponibles dans EoleSSO (en se basant sur le DN qui est du type `ou=<rne>,ou=ac-<academie>,ou=education,o=gouv,c=fr`).

Le type d'établissement permet de créer des sections dans la liste présentée à l'utilisateur afin d'en faciliter la lecture.



Dans le cas où toutes les informations ne sont pas détectées ou en cas de données mal renseignées dans l'application Zéphir, il est possible de modifier ou d'ajouter des informations en créant un(des) fichier(s) au même format.

Ils sont à placer dans le répertoire `/etc/ldap/replication` et doivent se nommer `etabs_xxx.ini` (la partie xxx n'est pas déterminante). Les données présentes dans ces fichiers seront prioritaires sur celles remontées par le serveur Zéphir.

Par exemple, le fichier suivant permet de corriger l'adresse du portail ENT de l'établissement 000000A1 (si celle-ci n'est pas correcte ou absente). Les autres informations remontées par le serveur Zéphir seront conservées (libellé et type d'établissement)

`/etc/ldap/replication/etabs_perso.ini`

```
[000000A1]
portail_etab=ent.mon_etab.ac-acd.fr
```

Dans l'affichage final (voir capture d'écran ci dessus), le libellé de l'établissement sera affiché en majuscules.

Si une description commence par le type d'établissement (ex : COLLEGE VICTOR HUGO), celui-ci sera supprimé pour simplifier l'affichage.

Au démarrage du service `eole-sso`, ces informations sont lues et rassemblées dans le fichier `/usr/share/sso/interface/scripts/etabs.js` qui est utilisé pour générer la liste des établissements dans lesquels un identifiant donné est présent.

Si l'application `eole-dispatcher` est installée sur la machine, un fichier d'informations est également généré pour celle-ci dans `/var/www/html/dispatcher/utils/etabs.ini`. Cette application permet de rediriger automatiquement les utilisateurs vers les portails ENT auxquels ils ont accès (pour plus d'informations, se reporter aux annexes).

Aide au choix de la source d'authentification

Lorsque des homonymes sont détectés, la mire d'authentification va générer la liste des choix

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

disponibles.

Pour aider l'utilisateur dans sa décision, différentes informations sont affichées.

Si un fichier `/usr/share/sso/interface/login_help.tmpl` est présent, un lien apparaîtra sur la mire d'authentification (`Quel est mon identifiant?`). Un survol de ce lien avec la souris fait apparaître le contenu du fichier sous forme d'un cadre en surimpression (classes liées à `a.aide` dans la feuille de style).

Un exemple est fourni dans le fichier `/usr/share/sso/interface/login_help_example.tmpl`.

Le but de ce cadre est d'indiquer à l'utilisateur l'identifiant qu'il doit utiliser.

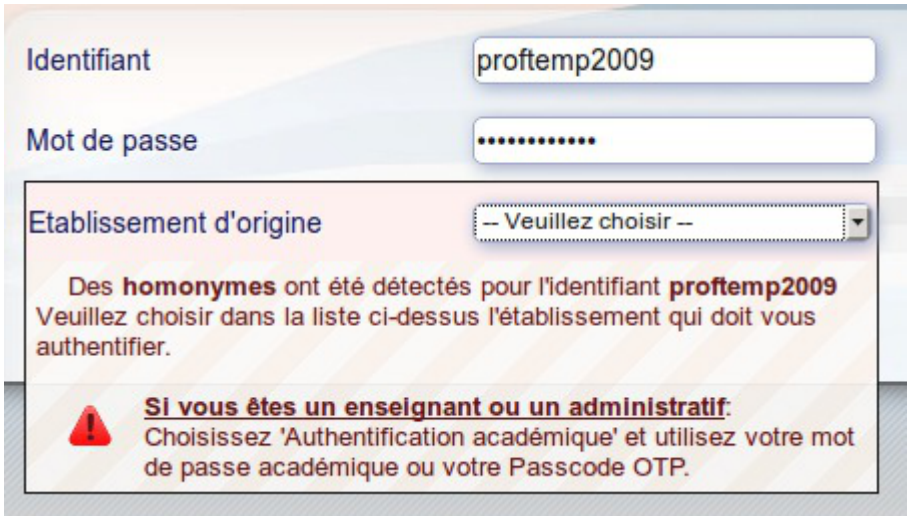
Un deuxième cadre d'information est affiché lorsque des homonymes ont été trouvés pour l'identifiant saisi par l'utilisateur (`#homonyme` et `#homonymetext` dans la feuille de style).

Le contenu de celui-ci est conditionné par les choix disponibles. Le but est d'aider à choisir parmi les sources proposées.

Le début du texte est générique et indique à l'utilisateur que plusieurs entrées sont disponibles pour l'identifiant renseigné.

Il est ensuite possible de spécifier un fichier d'information pour chaque annuaire LDAP, dont le contenu sera ajouté au cadre si l'identifiant entré y est présent (l'information doit donc être au format HTML).

Un exemple est fourni dans `/usr/share/sso/interface/personnel_acad.html`, et donne le résultat suivant :



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Voir aussi...

Onglet Eole sso : Configuration du service SSO pour l'authentification unique [p.6]

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 6

Personnalisation de la mire SSO

Ce chapitre répertorie les différentes possibilités offertes pour personnaliser l'apparence de la page d'authentification du serveur EoleSSO (pour une meilleure intégration dans l'environnement existant, et en particulier dans le cadre d'un portail d'accès aux ressources d'un établissement).

Message d'avertissement (CNIL)

Il est prévu de pouvoir afficher un message relatif à la déclaration CNIL du site.

- mettre le texte du message d'avertissement (formaté en HTML) dans un fichier `avertissement.txt` qui est à placer dans le répertoire `/usr/share/sso/interface/theme` ;
- relancer le service : `CreoleService eole-sso restart`

Exemple de déclaration

Conformément à la loi, nous vous informons que ce site a fait l'objet d'une déclaration de traitement automatisé d'informations nominatives auprès de la CNIL Loi du 6 janvier 1978 relative à l' « Informatique et aux Libertés » :

Conformément à la loi n° 78-17 du 6 janvier 1978, vous pouvez à tout moment accéder aux informations personnelles vous concernant et détenues par l'établissement, demander leur modification ou leur suppression. Ainsi, vous pouvez, à titre irrévocable, demander que soient rectifiées, complétées, clarifiées, mises à jour ou effacées les informations vous concernant qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte ou l'utilisation, la communication ou la conservation est interdite.

Pour toutes demandes, veuillez contacter l'administrateur à l'adresse : administrateur@etablissement.fr

CSS : Méthode 1

La feuille de style par défaut `/usr/share/sso/interface/main.css` importe les feuilles de style `./theme/style/theme.css` et `./leaves.css` :

```
[ …]
@import url(./leaves.css);
@import url(./theme/style/theme.css);
[…]
```

Comme le fichier `./theme/style/theme.css` est appelé en deuxième dans la feuille il va permettre une surcharge de la première feuille de style `./leaves.css`.

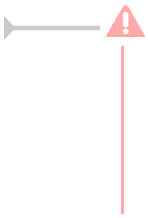
Éditer le fichier vide `./theme/style/theme.css` appelé dont le chemin absolu est `/usr/share/sso/interface/theme/style/theme.css`.

S'inspirer des balises de style utilisées dans le fichier `/usr/share/sso/interface/leaves.css` pour les surcharger.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Utiliser le répertoire `/usr/share/sso/interface/theme/images` pour ajouter vos images.

Recharger votre page d'authentification sans même redémarrer le service `eole-sso`, la feuille de style est importée avec les modifications.



Cette méthode n'est pas compatible avec la personnalisation Envole Thèmes. Celui-ci écrase le contenu du fichier `/usr/share/sso/interface/theme/style/theme.css` à chaque reconfigure. Il est possible d'enlever Envole Thèmes avec la commande suivante : `# apt-get remove eole-envole-themes`

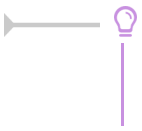
CSS : Méthode 2

Un certain nombre de thèmes sont fournis dans le répertoire `/usr/share/sso/interface/themes/`.

Il suffit de copier le thème voulu pour le rendre actif :

`# /bin/cp -R /usr/share/sso/interface/themes/<nomDuTheme>/* /usr/share/sso/interface/theme`

Recharger votre page d'authentification sans même redémarrer le service `eole-sso`, la feuille de style est importée avec les modifications.



N'hésitez pas à proposer votre thème, il sera ajouté au paquetage et reversé à la communauté d'utilisateurs.

CSS : Méthode 3

La feuille de style CSS par défaut utilisée lors de l'affichage de la page d'authentification au portail est :

`/usr/share/sso/interface/leaves.css`

Il est possible d'utiliser une feuille de style CSS personnalisée pour la mire SSO.

Les fichiers CSS à utiliser sont à placer dans :

`/usr/share/sso/interface/`

Dupliquer la feuille de style originale sous un autre nom.

Modifier à volonté `votre_nouvelle_feuille.css`

Renseigner le nom de votre feuille sans l'extension (`.css`) dans l'onglet `Eole sso` depuis l'interface de configuration du module.

Réaliser autant de feuilles de style que souhaités.

- Si vous faites appel à des images, placez-les dans : `/usr/share/sso/interface/images/`
- Il est possible de passer le nom de la CSS en paramètre dans URL : `http://<adresse serveur>/css=<nom de la feuille CSS>`
- Si vous utilisez un client phpCAS, il faudra modifier le client pour utiliser cette méthode (les URLs sont calculées par le client).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Choix de la CSS par le filtre SSO

Si un fichier CSS porte le même nom qu'un filtre d'application (par exemple, `ead2.css`), cette feuille de style CSS sera automatiquement utilisée lors des demandes à cette application (dans le cadre d'un portail web par exemple).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 7
Configuration d'EoleSSO en mode cluster

Fonctionnement en mode cluster

EoleSSO peut être paramétré pour stocker les sessions SSO dans une base de données Redis[p.85] (locale ou distante).

En branchant plusieurs services EoleSSO sur la même base, il est possible de mettre en place une configuration de type cluster en répartition de charge ou en basculement.

> Cette documentation couvre seulement la configuration d'un (ou plusieurs) services EoleSSO et d'un service Redis pour permettre le stockage des sessions SSO dans une base de données partagée. La configuration de la répartition de charge ou du basculement (à travers ha-proxy ou autre système) n'est pas abordée ici.

La configuration peut se faire :

- en mode serveur (partage d'une base Redis) ;
- en mode client (accès à la base Redis par EoleSSO).

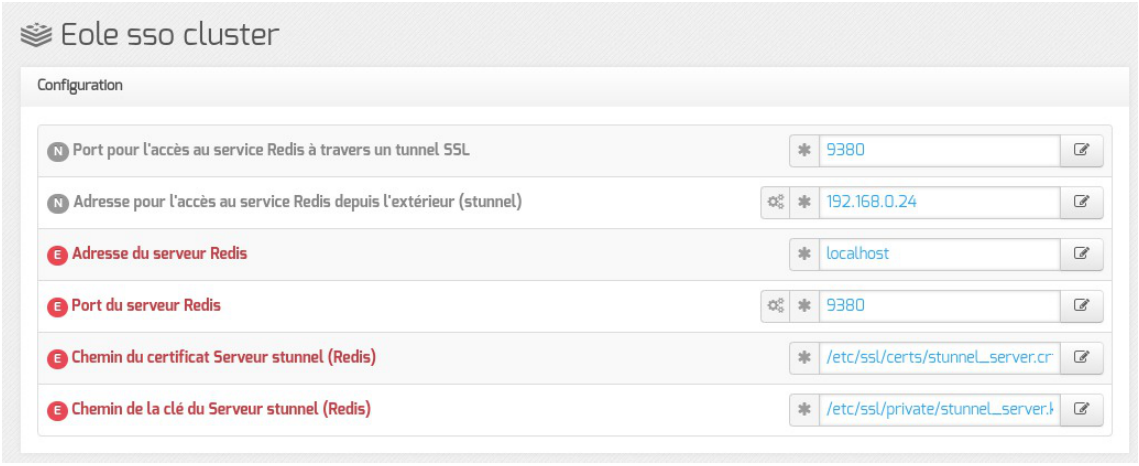
Installation et configuration en mode serveur

Sur un module Eole, il faut installer le paquet dédié à l'aide de la commande suivante :

```
# apt-eole install eole-sso-cluster-server
```

Celui-ci va installer un serveur Redis et configurer une instance spécifique sur le port `9380` (service redis-eolesso), ainsi qu'un service stunnel4 permettant de sécuriser l'accès à l'aide d'un tunnel SSL.

Dans l'interface de configuration du module apparaît le nouvel onglet `Eole sso cluster`.



Tous les paramètres sont renseignés pour une utilisation par défaut, mais il est possible d'effectuer les réglages suivants :

- `Port pour l'accès au service Redis à travers un tunnel SSL` : Permet de modifier le port sur lequel les clients se connecteront pour accéder à la base de données.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `Nom d'hôte ou adresse pour l'accès au service Redis depuis l'extérieur (stunnel)` : Permet de définir l'adresse sur laquelle le tunnel sera disponible. Par défaut, l'adresse IP de l'interface 0 est utilisée.
- `Chemin du certificat Serveur stunnel (Redis)` et `Chemin de la clé du Serveur stunnel (Redis)` : Permettent de renseigner un certificat serveur spécifique pour le tunnel SSL. Par défaut, un certificat est généré automatiquement (`/etc/ssl/certs/stunnel_client.crt`).
- `Nom d'hôte ou adresse IP du serveur Redis` et `Port du serveur Redis` : Permettent de modifier le port sur lequel l'instance de Redis écoute, ou d'accéder à un autre serveur Redis. Si le nom d'hôte est différent de 127.0.0.1 ou localhost, le service local redis-eolesso est désactivé.

Sur EOLE 2.7, `eole-sso-cluster-server` utilise partiellement le nouveau service `eole-redis`.

Afin d'éviter tout conflit, le port par défaut du service a été modifié de `6380` en `9380`.

À partir d'EOLE 2.7.1, il n'est plus possible d'installer les paquets `eole-sso-cluster-server` et `eole-sso-cluster-client` sur la même machine.

En cas d'utilisation d'un serveur Redis non local, il faut être conscient que les échanges circuleront en clair, ce qui est déconseillé en dehors d'un réseau sécurisé.

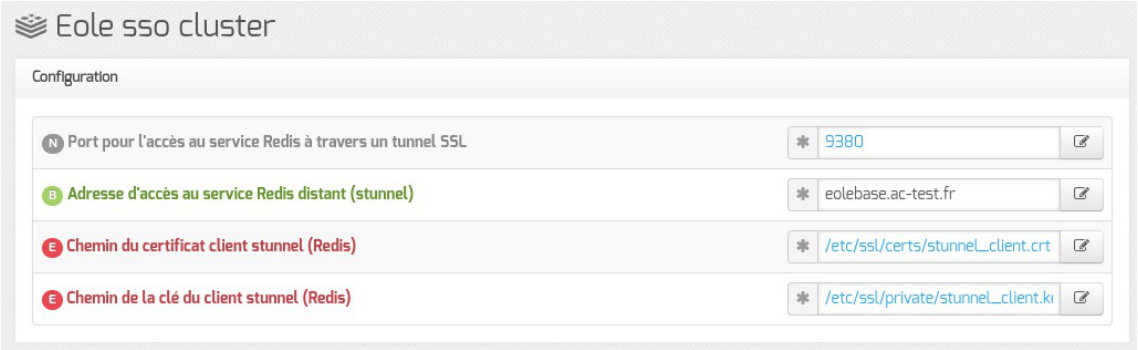
Installation et configuration en mode client

Sur un module Eole dont le service EoleSSO doit être utilisé en mode cluster il faut installer le paquet adéquat à l'aide de la commande suivante :

```
# apt-eole install eole-sso-cluster-client
```

Celui-ci va installer les librairies nécessaires à l'accès Redis par EoleSSO, ainsi qu'un service stunnel4 configuré en mode client.

Dans l'interface de configuration du module apparaît le nouvel onglet `Eole sso cluster`.



- `Port pour l'accès au service Redis à travers un tunnel SSL` : Permet de spécifier le port sur lequel le service stunnel4 va se connecter. Il doit correspondre à la valeur configurée sur la machine en mode serveur.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `Nom d'hôte ou adresse IP d'accès au service Redis distant (stunnel)` : Renseigner l'adresse choisie pour l'accès à Redis sur la machine en mode serveur.
- Les variables chemin du certificat et de la clé du client stunnel permettent d'utiliser un certificat spécifique pour le service stunnel local. Attention, ce certificat doit être un certificat client (nsCertType = client). par défaut, un certificat est généré automatiquement (`/etc/ssl/certs/stunnel_client.crt`)

> À partir d'EOLE 2.7.1, il n'est plus possible d'installer les paquets `eole-sso-cluster-server` et `eole-sso-cluster-client` sur la même machine.

Tunnel SSL

Échange des clés

Une fois la configuration renseignée, reconfigurer le serveur et générer les certificats à l'aide de la commande reconfigure sur chaque machine utilisée.

Il faut ensuite procéder à un échange des certificats entre le serveur et le client pour que la connexion par tunnel soit possible :

- Exécuter `reconfigure` sur chaque machine après avoir copié les fichiers.

Sur la machine en mode serveur il faut recopier dans le répertoire `/etc/stunnel/eole/` les fichiers `/etc/ssl/certs/ca_local.crt` et `/etc/ssl/certs/stunnel_client.crt` de chaque serveur en mode client. Il faut les renommer afin de ne pas les écraser au fur et à mesure de l'ajout de clients.

```
# scp root@<adresse_client> :/etc/ssl/certs/ca_local.crt /etc/stunnel/eole/ca_[adresse_client].crt
# scp root@<adresse_client> :/etc/ssl/certs/stunnel_client.crt /etc/stunnel/eole/stunnel_[nom_client].crt
```

Sur chaque machine en mode client il faut recopier dans le répertoire `/etc/stunnel/eole/` les fichiers `/etc/ssl/certs/ca_local.crt` et `/etc/ssl/certs/stunnel_server.crt` de chaque serveur en mode serveur.

```
# scp root@<adresse_client> :/etc/ssl/certs/ca_local.crt /etc/stunnel/eole/
# scp root@<adresse_client> :/etc/ssl/certs/stunnel_server.crt /etc/stunnel/eole/
```

> **Utilisation de certificats spécifiques**
>
> En cas d'utilisation d'un autre certificat que celui généré par défaut, les fichiers à échanger sont :
>
> - le fichier du certificat utilisé pour le service *stunnel* ;
> - toute les autorités de certification permettant de valider celui-ci (autorité racine et éventuels certificats intermédiaires).

> **Vérifier le bon fonctionnement du tunnel**
>
> Une fois les machines configurées, il faut se connecter sur un des serveurs en mode client, se placer dans le répertoire `/usr/share/sso/`, exécuter l'interpréteur `python` et saisir le code

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

suivant :

```
>>> import config, redis
>>> r = redis.Redis(host=config.REDIS_HOST, port=config.REDIS_PORT)
>>> r.ping()
```

La dernière commande doit retourner `True`.

Si la commande renvoie un message d'erreur se terminant par `Error while reading from socket: (104, 'Connection reset by peer')` , cela indique généralement un problème de validation des certificats (par le serveur ou le client), ou une interdiction d'accès au port du tunnel par le serveur (pare-feu, TCP Wrapper[p.86]...).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 8

Répartition de charge EoleSSO en mode cluster

Cette documentation a pour but de décrire la mise en place d'une configuration HAProxy afin de pouvoir mettre plusieurs services EoleSSO en cluster et de gérer la répartition de charge.

https://www.haproxy.com/fr/

Cette documentation décrit également la mise en place de 2 services pour suivre les métriques d'EoleSSO :

- Prometheus : https://prometheus.io/
- Grafana : https://grafana.net/

On suppose l'existence de 3 serveurs EoleSSO qui écoutent sur le port 443 dont les DNS sont les suivants :

- `sso-1.ac-academie.fr` ;
- `sso-2.ac-academie.fr` ;
- `sso-3.ac-academie.fr`.

Un quatrième serveur doit héberger le service ha-proxy avec pour nom DNS `sso-ha.ac-academie.fr`.

Le serveur hébergeant le service ha-proxy du cluster doit avoir un nom de domaine différent de celui du cluster de serveur web même si les 2 noms de domaine pointent sur la même adresse IP.

Pour maintenir et déployer la configuration (certificats pour stunnel, metadata, filtres, thèmes, CSS, attributs calculés) sur les différents serveurs EoleSSO il est possible d'utiliser Ansible.

Installation d'HAProxy

Sur le serveur `sso-ha.ac-academie.fr` :

```
# apt-eole install haproxy
```

Configuration d'HAProxy

Procéder à la configuration basique d'HAProxy (non détaillée ici).

Éditer le fichier de configuration /etc/haproxy/haproxy.cfg et ajouter les lignes suivantes :

```
1 global
2   ...
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
   # Les serveurs étant gérés par vous, la vérification ssl peut être désactivée
  ssl-server-verify none

frontend https-in
     bind <IP DU SERVEUR SSO-HA>:443 ssl crt <CHEMIN DU CERTIFICAT PEM>
     option   forwardfor
     redirect scheme https if !{ ssl_fc }
     default_backend    sso_servers

backend sso_servers
     balance         roundrobin
     cookie SSONAME  insert indirect nocache
     server sso-1.ac-academie.fr   sso-1.ac-academie.fr:443 ssl cookie sso1 check
     server sso-2.ac-academie.fr   sso-2.ac-academie.fr:443 ssl cookie sso2 check
     server sso-3.ac-academie.fr   sso-3.ac-academie.fr:443 ssl cookie sso3 check
```

<IP DU SERVEUR SSO-HA> : est à remplacer par l'adresse IP de votre serveur HAProxy

<CHEMIN DU CERTIFICAT PEM> : chemin du certificat + key

Penser à redémarrer le service haproxy :

```
# service haproxy restart
```

Mise en place de Prometheus et de Grafana

Il faut mettre en place un serveur Prometheus qui sera chargé de collecter les données fournies par nos serveurs EoleSSO et mettre en place Grafana pour avoir un visuel des métriques.

Pour des raisons de simplicité, des micro-services docker sont utilisés pour fournir ces deux applications, aussi il faut installer les paquets `docker` et `docker-compose`.

Il peut être intéressant de dissocier ces services du serveur HAPproxy, car il pourrait servir à d'autres serveurs, ce serveur de monitoring porte le nom DNS `monitoring.ac-academie.fr`.

Exemple de configuration de Prometheus

Exemple de configuration, contenu dans le fichier `/shared/prometheus/monitoring-compose.yml` :

```
prometheus:
  image: prom/prometheus
  ports:
    - 9090:9090
  volumes:
    - /shared/prometheus/etc/:/etc/prometheus/
    - /shared/prometheus/data/:/prometheus

grafana:
  image: grafana/grafana:4.1.1
  ports:
    - 3000:3000
  volumes:
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
    - /shared/prometheus/grafana/:/var/lib/grafana/
env_file:
    - /shared/prometheus/grafana.config.monitoring
```

Configuration de Prometheus

Le fichier de configuration de prometheus `/shared/prometheus/etc/prometheus.yml` contient :

```
global:
  scrape_interval: 60s

scrape_configs:
  - job_name: "eole_sso"
    metrics_path: /metrics
    scheme: https
    tls_config:
      insecure_skip_verify: true
    static_configs:
        - targets:
            - sso-1.ac-academie.fr
            - sso-2.ac-academie.fr
            - sso-3.ac-academie.fr
```

Configuration de Grafana

Configuration de Grafana dans le fichier `/shared/prometheus/grafana.config.monitoring`

```
GF_SECURITY_ADMIN_PASSWORD=VOTRE_MOT_DE_PASSE_ADMIN
GF_USERS_ALLOW_SIGN_UP=false
http_proxy=PROXY_HOST:PROXY_PORT
https_proxy=PROXY_HOST:PROXY_PORT
```

Modifier les valeurs de :

VOTRE_MOT_DE_PASSE_ADMIN

PROXY_HOST

PROXY_PORT

La documentation de Grafana décrit les paramètres possibles :

http://docs.grafana.org/installation/configuration/

JSON pour le tableau de bord Grafana

```
{
  "annotations": {
    "list": []
  },
  "editable": true,
  "gnetId": null,
  "graphTooltip": 0,
  "hideControls": false,
  "id": 16,
  "links": [],
  "refresh": "1m",
  "rows": [
    {
      "collapse": false,
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
      "height": 237,
      "panels": [
        {
          "aliasColors": {
            "sso-3": "#82B5D8",
            "sso-1": "#7EB26D",
            "sso-2": "#EAB839"
          },
          "bars": false,
          "datasource": null,
          "editable": true,
          "error": false,
          "fill": 7,
          "grid": {},
          "id": 9,
          "legend": {
            "avg": false,
            "current": false,
            "max": false,
            "min": false,
            "show": true,
            "total": false,
            "values": false
          },
          "lines": true,
          "linewidth": 0,
          "links": [],
          "nullPointMode": "connected",
          "percentage": false,
          "pointradius": 5,
          "points": false,
          "renderer": "flot",
          "seriesOverrides": [],
          "span": 4,
          "stack": true,
          "steppedLine": false,
          "targets": [
            {
              "expr": "eolesso_login_gauge",
              "intervalFactor": 2,
              "legendFormat": "{{host}}",
              "metric": "eolesso_login_gauge",
              "refId": "A",
              "step": 120
            }
          ],
          "thresholds": [],
          "timeFrom": null,
          "timeShift": null,
          "title": "Nombre de tickets de login (TicketCache)",
          "tooltip": {
            "msResolution": false,
            "shared": true,
            "sort": 0,
            "value_type": "cumulative"
          },
          "type": "graph",
          "xaxis": {
            "mode": "time",
            "name": null,
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
            "show": true,
            "values": []
          },
          "yaxes": [
            {
              "format": "short",
              "label": null,
              "logBase": 1,
              "max": null,
              "min": null,
              "show": true
            },
            {
              "format": "short",
              "label": null,
              "logBase": 1,
              "max": null,
              "min": null,
              "show": true
            }
          ]
        },
        {
          "bars": true,
          "datasource": null,
          "editable": true,
          "error": false,
          "fill": 10,
          "grid": {},
          "id": 4,
          "legend": {
            "avg": false,
            "current": false,
            "max": false,
            "min": false,
            "show": true,
            "total": false,
            "values": false
          },
          "lines": false,
          "linewidth": 0,
          "links": [],
          "nullPointMode": "null as zero",
          "percentage": false,
          "pointradius": 5,
          "points": false,
          "renderer": "flot",
          "seriesOverrides": [],
          "span": 4,
          "stack": true,
          "steppedLine": true,
          "targets": [
            {
              "expr": "(rate(eolesso_sessions_new_counter[10m]))*60*2",
              "intervalFactor": 2,
              "legendFormat": "{{host}} [{{authclass}}]",
              "metric": "eolesso_sessions_new_counter",
              "refId": "A",
              "step": 120
            }
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
        ],
        "thresholds": [],
        "timeFrom": null,
        "timeShift": null,
        "title": "Nb connexions/s",
        "tooltip": {
          "msResolution": false,
          "shared": true,
          "sort": 0,
          "value_type": "individual"
        },
        "type": "graph",
        "xaxis": {
          "mode": "time",
          "name": null,
          "show": true,
          "values": []
        },
        "yaxes": [
          {
            "format": "short",
            "label": null,
            "logBase": 1,
            "max": null,
            "min": null,
            "show": true
          },
          {
            "format": "short",
            "label": null,
            "logBase": 1,
            "max": null,
            "min": null,
            "show": true
          }
        ]
      },
      {
        "aliasColors": {
          "sso-3": "#82B5D8",
          "sso-1": "#7EB26D",
          "sso-2": "#EAB839"
        },
        "bars": false,
        "datasource": null,
        "editable": true,
        "error": false,
        "fill": 3,
        "grid": {},
        "id": 2,
        "legend": {
          "avg": false,
          "current": false,
          "max": false,
          "min": false,
          "show": true,
          "total": false,
          "values": false
        },
        "lines": true,
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
        "linewidth": 1,
        "links": [],
        "nullPointMode": "null",
        "percentage": false,
        "pointradius": 5,
        "points": false,
        "renderer": "flot",
        "seriesOverrides": [],
        "span": 4,
        "stack": true,
        "steppedLine": false,
        "targets": [
          {
            "expr": "eolesso_sessions_nb_gauge",
            "intervalFactor": 1,
            "legendFormat": "{{host}}",
            "metric": "eolesso_sessions_gauge",
            "refId": "A",
            "step": 60
          }
        ],
        "thresholds": [],
        "timeFrom": null,
        "timeShift": null,
        "title": "Nombre de tickets de sessions (auth)",
        "tooltip": {
          "msResolution": false,
          "shared": true,
          "sort": 0,
          "value_type": "cumulative"
        },
        "type": "graph",
        "xaxis": {
          "mode": "time",
          "name": null,
          "show": true,
          "values": []
        },
        "yaxes": [
          {
            "format": "short",
            "label": null,
            "logBase": 1,
            "max": null,
            "min": null,
            "show": true
          },
          {
            "format": "short",
            "label": null,
            "logBase": 1,
            "max": null,
            "min": null,
            "show": true
          }
        ]
      }
    ],
    "repeat": null,
    "repeatIteration": null,
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
      "repeatRowId": null,
      "showTitle": false,
      "title": "Row",
      "titleSize": "h6"
    },
    {
      "collapse": false,
      "height": "250px",
      "panels": [
        {
          "aliasColors": {
            "sso-3": "#82B5D8",
            "sso-1": "#7EB26D",
            "sso-2": "#EAB839"
          },
          "bars": false,
          "datasource": null,
          "editable": true,
          "error": false,
          "fill": 7,
          "grid": {},
          "id": 7,
          "legend": {
            "avg": false,
            "current": false,
            "max": false,
            "min": false,
            "show": true,
            "total": false,
            "values": false
          },
          "lines": true,
          "linewidth": 1,
          "links": [],
          "nullPointMode": "connected",
          "percentage": false,
          "pointradius": 5,
          "points": false,
          "renderer": "flot",
          "seriesOverrides": [],
          "span": 6,
          "stack": true,
          "steppedLine": true,
          "targets": [
            {
              "expr": "eolesso_calcdata_gauge",
              "intervalFactor": 2,
              "legendFormat": "{{host}}",
              "metric": "eolesso_calcdata_gauge",
              "refId": "A",
              "step": 60
            }
          ],
          "thresholds": [],
          "timeFrom": null,
          "timeShift": null,
          "title": "taille du cache des attributs calculés",
          "tooltip": {
            "msResolution": false,
            "shared": true,
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
            "sort": 0,
            "value_type": "cumulative"
          },
          "type": "graph",
          "xaxis": {
            "mode": "time",
            "name": null,
            "show": true,
            "values": []
          },
          "yaxes": [
            {
              "format": "decbytes",
              "label": "Octets",
              "logBase": 1,
              "max": null,
              "min": null,
              "show": true
            },
            {
              "format": "short",
              "label": null,
              "logBase": 1,
              "max": null,
              "min": null,
              "show": true
            }
          ]
        },
        {
          "aliasColors": {
            "sso-3": "#82B5D8",
            "sso-1": "#7EB26D",
            "sso-2": "#EAB839"
          },
          "bars": false,
          "datasource": null,
          "editable": true,
          "error": false,
          "fill": 5,
          "grid": {},
          "id": 8,
          "legend": {
            "avg": false,
            "current": false,
            "max": false,
            "min": false,
            "show": true,
            "total": false,
            "values": false
          },
          "lines": true,
          "linewidth": 1,
          "links": [],
          "nullPointMode": "connected",
          "percentage": false,
          "pointradius": 5,
          "points": false,
          "renderer": "flot",
          "seriesOverrides": [],
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
          "span": 6,
          "stack": true,
          "steppedLine": false,
          "targets": [
            {
              "expr": "eolesso_userdata_gauge",
              "intervalFactor": 2,
              "legendFormat": "{{host}}",
              "metric": "eolesso_userdata_gauge",
              "refId": "A",
              "step": 60
            }
          ],
          "thresholds": [],
          "timeFrom": null,
          "timeShift": null,
          "title": "taille du cache des attributs ldap",
          "tooltip": {
            "msResolution": false,
            "shared": true,
            "sort": 0,
            "value_type": "cumulative"
          },
          "type": "graph",
          "xaxis": {
            "mode": "time",
            "name": null,
            "show": true,
            "values": []
          },
          "yaxes": [
            {
              "format": "decbytes",
              "label": "Octets",
              "logBase": 1,
              "max": null,
              "min": null,
              "show": true
            },
            {
              "format": "short",
              "label": null,
              "logBase": 1,
              "max": null,
              "min": null,
              "show": true
            }
          ]
        }
      ],
      "repeat": null,
      "repeatIteration": null,
      "repeatRowId": null,
      "showTitle": false,
      "title": "New row",
      "titleSize": "h6"
    },
    {
      "collapse": false,
      "height": "250px",
```

```
    "panels": [
      {
        "aliasColors": {
          "sso.ac-reunion.fr:4430": "#82B5D8",
          "sso.ac-reunion.fr:4431": "#E5A8E2",
          "sso.ac-reunion.fr:4432": "#AEA2E0"
        },
        "bars": false,
        "datasource": null,
        "editable": true,
        "error": false,
        "fill": 0,
        "grid": {},
        "id": 3,
        "legend": {
          "alignAsTable": true,
          "avg": false,
          "current": true,
          "max": false,
          "min": false,
          "rightSide": true,
          "show": true,
          "total": false,
          "values": true
        },
        "lines": true,
        "linewidth": 1,
        "links": [],
        "nullPointMode": "null as zero",
        "percentage": false,
        "pointradius": 5,
        "points": false,
        "renderer": "flot",
        "seriesOverrides": [],
        "span": 6,
        "stack": false,
        "steppedLine": false,
        "targets": [
          {
            "expr": "process_virtual_memory_bytes{job='eole_sso'}",
            "intervalFactor": 2,
            "legendFormat": "{{instance}}",
            "refId": "A",
            "step": 60
          }
        ],
        "thresholds": [
          {
            "colorMode": "critical",
            "fill": true,
            "line": true,
            "op": "gt",
            "value": 1517522817
          }
        ],
        "timeFrom": null,
        "timeShift": null,
        "title": "Mémoire utilisée",
        "tooltip": {
          "msResolution": false,
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
            "shared": true,
            "sort": 0,
            "value_type": "individual"
          },
          "type": "graph",
          "xaxis": {
            "mode": "time",
            "name": null,
            "show": true,
            "values": []
          },
          "yaxes": [
            {
              "format": "bytes",
              "label": null,
              "logBase": 1,
              "max": null,
              "min": null,
              "show": true
            },
            {
              "format": "short",
              "label": null,
              "logBase": 1,
              "max": null,
              "min": null,
              "show": true
            }
          ]
        },
        {
          "aliasColors": {
            "sso-3": "#82B5D8",
            "sso-1": "#7EB26D",
            "sso-2": "#EAB839"
          },
          "bars": false,
          "datasource": null,
          "editable": true,
          "error": false,
          "fill": 4,
          "grid": {},
          "id": 1,
          "legend": {
            "avg": false,
            "current": false,
            "max": false,
            "min": false,
            "show": true,
            "total": false,
            "values": false
          },
          "lines": true,
          "linewidth": 1,
          "links": [],
          "nullPointMode": "connected",
          "percentage": false,
          "pointradius": 5,
          "points": false,
          "renderer": "flot",
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
        "seriesOverrides": [],
        "span": 6,
        "stack": true,
        "steppedLine": false,
        "targets": [
          {
            "expr": "eolesso_appticket_gauge{job='eole_sso'}",
            "intervalFactor": 2,
            "legendFormat": "{{host}}",
            "metric": "eolesso_appticket_gauge",
            "refId": "A",
            "step": 60
          }
        ],
        "thresholds": [],
        "timeFrom": null,
        "timeShift": null,
        "title": "Nombre de Tickets applicatifs (AppTicket)",
        "tooltip": {
          "msResolution": false,
          "shared": true,
          "sort": 0,
          "value_type": "cumulative"
        },
        "type": "graph",
        "xaxis": {
          "mode": "time",
          "name": null,
          "show": true,
          "values": []
        },
        "yaxes": [
          {
            "format": "short",
            "label": null,
            "logBase": 1,
            "max": null,
            "min": null,
            "show": true
          },
          {
            "format": "short",
            "label": null,
            "logBase": 1,
            "max": null,
            "min": null,
            "show": true
          }
        ]
      }
    ],
    "repeat": null,
    "repeatIteration": null,
    "repeatRowId": null,
    "showTitle": false,
    "title": "New row",
    "titleSize": "h6"
  }
],
"schemaVersion": 14,
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
  "style": "dark",
  "tags": [],
  "templating": {
    "list": []
  },
  "time": {
    "from": "now-12h",
    "to": "now"
  },
  "timepicker": {
    "refresh_intervals": [
      "5s",
      "10s",
      "30s",
      "1m",
      "5m",
      "15m",
      "30m",
      "1h",
      "2h",
      "1d"
    ],
    "time_options": [
      "5m",
      "15m",
      "1h",
      "6h",
      "12h",
      "24h",
      "2d",
      "7d",
      "30d"
    ]
  },
  "timezone": "browser",
  "title": "SSO Copy",
  "version": 0
}
```

Monitoring

Lancer l'environnement de monitoring

```
# cd /shared/prometheus/
```

```
# docker-compose -f prometheus-compose.yml start
```

Par défaut Grafana écoute sur le port 3000 et Prometheus sur le port 9090

Pour accéder à Grafana :

http://monitoring.ac-academie.fr:3000

Pour accéder à Prometheus :

http://monitoring.ac-academie.fr:9090

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 9
Compléments de configuration EoleSSO

1. Résumé des fichiers et liens

Fichiers de configuration

Fichiers de base

- `/usr/share/sso/config.py` : fichier de configuration principal de l'application (sur un module Eole, la configuration est gérée via Creole)
- `/usr/share/sso/app_filters/*_apps.ini` : définition des applications et spécification du filtre à utiliser
- `/usr/share/sso/app_filters/*.ini` : fichiers de description des filtres d'attributs
- `/usr/share/sso/user_infos/*.py` : fonctions de calcul d'attributs supplémentaires
- `/usr/share/sso/interface/theme` : répertoire pour personnalisation de la CSS des pages d'authentification

Fichiers spécifiques au fonctionnement en mode SAML

- `/usr/share/sso/metadata/*.xml` : fichiers metadata des entités partenaires (doit contenir le certificat utilisé pour la signature des requêtes)
- `/usr/share/sso/metadata/attributes.ini` : définition des attributs requis/optionnels en tant que fournisseur de service (obsolète)
- `/usr/share/sso/attribute_sets/*.ini` : description de jeux d'attributs pour la fédération via SAML
- `/usr/share/sso/attribute_sets/associations*.ini` : fichiers de configuration des associations avec des fournisseurs d'identité

URL principales

Toutes les URL du service EoleSSO décrites ci-dessous commencent par https://addresse_serveur:8443 (port par défaut, peut être différent suivant la configuration du service).

URL Générales

- `/ (sans paramètres)` : Page d'accueil, le formulaire d'authentification est présenté et une session SSO est créée après validation. Si l'utilisateur est déjà authentifié il est redirigé sur la page `/loggedin` ou une liste des fédérations établies et des applications ayant un ticket est affichée
- `/logout` : adresse de déconnexion de la session actuelle (gestion du Single Logout pour les protocoles le supportant)

URL spécifiques à CAS

- `/?service=X` : Adresse d'obtention d'un ticket CAS pour les applications clientes (à utiliser comme URI de base dans la configuration des clients CAS)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

  - `service` est l'URL de l'application désirant obtenir un ticket. Une fois la validité de la session SSO vérifiée, le service EoleSSO redirige l'utilisateur sur cette URL en passant le ticket en paramètre (nom du paramètre : `ticket`)
- `/validate?service=X&ticket=Y` (ou `/serviceValidate`) : adresse de validation des tickets d'application CAS ;
  - `service` est l'URL du service pour lequel le ticket a été délivré
  - `ticket` est le ticket a vérifier (de type ST)
- `/proxyValidate?service=X&ticket=Y&pgtUrl=Z`: adresse de validation des tickets d'application CAS en mode proxy
  - `ticket` est le ticket à vérifier (de type ST ou PT) ;
- `/samlValidate` : adresse de validation des tickets CAS au format SAML 1. Les paramètres doivent être passés par méthode POST (méthode supportée par les client CAS java 3.1.X, phpCAS 1.1.0 et .NET CAS Client). Pour plus de détail sur, se reporter à la page http://en.wikipedia.org/wiki/SAML_1.1
  - `TARGET` : URL à laquelle la réponse doit être envoyée
  - Le corps de la requête doit contenir la requête SAML dans une enveloppe SOAP. Le ticket à valider est fourni comme valeur de l'élément AssertionArtifact
- `/proxy?pgt=X?targetService=Y` : adresse d'obtention d'un ticket de type proxy

URL spécifiques à SAML 2

- `/saml/metadata` : adresse de récupération des méta-données SAML du serveur (fournisseur d'identité et fournisseur de services)
- `/saml?sp_ident=X&RelayState=Y&index=Z` : adresse à utiliser pour envoyer une assertion d'authentification SAML à un fournisseur de services
  - `sp_ident` est l'identifiant de ce partenaire (ou le nom de son fichier metadata sans l'extension .xml)
  - `RelayState` est une information (URL ou autre) indiquant au partenaire où l'utilisateur doit être redirigé après la validation de l'assertion ;
  - `index` permet de forcer l'utilisation d'un binding particulier (voir le fichier de méta données pour les valeurs possibles)
- `/saml/acs` : adresse de traitement des assertions reçues en tant que fournisseur de services
- `/discovery?idp_ident=X&return_url=Y` : adresse permettant d'envoyer un demande d'authentification à un fournisseur d'identité
  - `idp_ident` est l'identifiant de ce partenaire (ou le nom de son fichier metadata sans l'extension .xml)
  - `return_url` est le service de destination sur lequel rediriger après authentification

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2. Astuces d'exploitation

Journalisation du service

Le fichier de journalisation du service EoleSSO est `/var/log/rsyslog/local/eolesso/eolesso.info.log`.

Il est possible d'activer un mode `debug` affichant beaucoup plus d'informations dans le fichier de log.

Pour l'activer, ouvrez le fichier `/usr/share/sso/config.py` et remplacer la ligne

```
DEBUG_LOG = False
```

par

```
DEBUG_LOG = True
```

Cette option de debug est à utiliser temporairement pour éviter de rendre les logs illisibles (et limiter l'espace disque utilisé). En cas de mise à jour du paquet eole-sso, elle sera réinitialisée à sa valeur par défaut.

Quand ce mode est activé, il est également possible d'afficher certaines requêtes SAML dans le navigateur en ajoutant un paramètre `show=1` aux urls gérant leur envoi.

Cela est possible dans les cas suivants :

- envoi d'une assertion d'authentification (ex : `/saml?sp_ident=X&show=1`)
- envoi d'une requête d'authentification (ex : `/discovery?idp_ident=X&show=1`)

Rechargement de la configuration du service

Il est possible de recharger le service EoleSSO (au lieu de le redémarrer) afin de prendre en compte de nouvelles données de configuration. Pour cela utilisez la commande suivante :

```
CreoleService eole-sso reload
```

L'avantage de cette méthode par rapport à `CreoleService eole-sso restart` est que les sessions des utilisateurs en cours sont conservées.

Les données suivantes sont prises en compte lors du rechargement :

- filtres d'attributs et description d'applications (situés dans `/usr/share/sso/app_filters`) ;
- jeu d'attributs et fichier de configuration d'associations (situés dans `/usr/share/sso/attribute_sets`) ;
- fichiers metadata des entités partenaires (situés dans `/usr/share/sso/metadata`) ;
- définitions d'attributs calculés (situés dans `/usr/share/sso/user_infos`).

3. Exemple de Fédération avec RSA/FIM

Préparation de la configuration FIM

Les données suivantes sont nécessaires pour configurer l'association dans FIM :

- Les méta-données du serveur EoleSSO : `wget https://<ip_serveur_sso>:8443/saml/metadata --no-check-certificate --outputfile=eolesso.xml`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- le certificat du serveur EoleSSO : `/etc/ssl/certs/eole.crt` (fichier par défaut, peut varier selon la configuration)

Si le certificat est au format PEM (c'est le cas du certificat par défaut sur un module EOLE), il faut le convertir au format DER : `openssl x509 -inform PEM -outform DER -in eole.crt -out eole_der.crt`

Une fois converti, utiliser la commande keytool pour intégrer le certificat à un truststore du serveur RSA/FIM (ou créer un truststore spécifique à cette occasion). Sur notre serveur de test, ils sont situés dans `/appli/federation/rsa-fim-config/keystores`

Par exemple : `<chemin vers jdk>/bin/keytool -import -alias fs-ac-mon_acad-et-mon_etab-1.0 -keystore mon_truststore-trust.jks -file eole_der.crt`

Configuration du fournisseur d'identité :

- aller dans Quick Setup -> add New Partner ;
- importer le fichier de méta-données `eolesso.xml` et donner un nom d'entité ;
- sauver dans la page suivante (association), choisir le fournisseur de service (FIM) ;
- cliquer sur l'onglet `general settings` et choisir les réglages suivants :
  - Encrypting/Signature truststores : sélectionner le truststore créé ci dessus ;
  - cocher la case `Transient Plug-in` ;
  - le greffon 'dictao cleartrust transient plugin' doit être sélectionné ;
  - attribute plugin : ajouter DictaoDumbAttributePluginRP ;
  - laisser les autres valeurs par défaut et sauver.

Configuration du serveur EoleSSO

La première étape est de récupérer le fichier de méta-données du fournisseur de service dans FIMConfig :

- Entities -> local entities -> manage existing ;
- cliquer sur le fournisseur, puis sur 'Export' dans le menu déroulant ;
- valider avec les valeurs par défaut, et copier le contenu affiché dans un fichier sur votre machine locale.

Placer ce fichier dans le répertoire `/usr/share/sso/metadata` (dans cet exemple, `fim_sp.xml`) du serveur EoleSSO et redémarrer le service.

Le fichier de méta-données doit être un fichier XML valide. Si l'entête suivant n'est pas présent, ajoutez le au début du fichier :

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

Test du lien de fédération

Pour accéder à une ressource au moyen de la fédération, il faut utiliser une adresse de ce type :

https://<adresse_FI>:8443/saml?sp_ident=<id_FS>&RelayState=<adresse_service>

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

4. Fédération entre 2 serveurs EoleSSO

Synopsis

On considère la situation suivante :

Un serveur Scribe en établissement (adresse : `Scribe_FI`) propose l'accès à des ressources protégé par un serveur Seshat (adresse : `Seshat_FS`) à travers son portail local.

Une réplication d'annuaire est en place entre les 2 serveurs (le serveur Seshat répliquant les annuaires de plusieurs établissements).

On souhaite que l'utilisateur se connecte sur le portail établissement du serveur Scribe, et accès à un application web du serveur Seshat (en saisissant une seule fois ses identifiants lors de la connexion au portail).

Pour permettre de retrouver les utilisateurs sur le fournisseur de service, on décide d'utiliser comme clé de jointure le champ FederationKey de l'annuaire de Scribe. Ce champ étant unique au niveau national, il n'y aura pas de problème

Se reporter à la partie traitant de la gestion des identifiants ENT dans la documentation Scribe pour plus d'informations sur la mise en place de l'attribut FederationKey

Configuration du fournisseur d'identité (module Scribe)

La première étape est de définir un filtre pour définir les attributs à envoyer au fournisseur de service dans l'assertion SAML.

Par défaut, le serveur EoleSSO utilise le filtre défini dans le fichier `/usr/share/sso/app_filters/saml.ini` si aucun filtre n'est spécifié pour l'adresse du fournisseur de service (pour information, cette adresse est https://Seshat_FS:8443/saml/acs).

Il n'y a ici rien à modifier car ce filtre envoie l'attribut FederationKey.

Configuration du fournisseur de service (Seshat)

Sur le fournisseur de service, il faut indiquer le jeu d'attributs à utiliser pour établir la correspondance entre les attributs donnés dans l'assertion SAML et les attributs présents dans l'annuaire de Seshat.

Ici aussi, la configuration par défaut convient. Si aucun jeu d'attribut n'est défini pour l'identifiant du fournisseur d'identité, le jeu par défaut est `FederationKey=FederationKey`, ce qui correspond à notre cas d'utilisation.

Ce filtre est défini dans le fichier `/usr/share/sso/attribute_sets/default.ini`.

Mise en oeuvre du lien de fédération

Une fois les 2 serveurs configurés, on échange les fichiers de méta données pour établir le lien. Une méthode simple est de le faire par les commandes suivantes :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- sur le module Scribe : `wget --no-check-certificate -O /usr/share/sso/metadata/seshat.xml https://seshat_FS:8443/saml/metadata`
- sur le module Seshat : `wget --no-check-certificate -O /usr/share/sso/metadata/scribe.xml https://scribe_FI:8443/saml/metadata`
- redémarrer le service `eole-sso` sur les 2 serveurs : `CreoleService eole-sso restart`

Pour tester le fonctionnement de la fédération, taper l'URL suivante dans un navigateur :

https://scribe_FI:8443/saml?sp_ident=seshat

Après validation du formulaire pour confirmer l'accès, le navigateur doit être redirigé sur l'URL https://seshat_FS:8443/loggedin. Des informations sur la session établie par le serveur Seshat sont affichées sur cette page

une fois le lien de fédération fonctionnel, ajouter un lien dans le portail du serveur Scribe pour accéder à l'application sur Seshat:

https://scribe_FI:8443/saml?sp_ident=seshat&RelayState=https://seshat_FS/mon_application

5. Mise en place de l'authentification OTP

Le service EoleSSO est capable de valider une authentification par clé OTP auprès d'un serveur RSA Authentication Manager (protocole SecurID).

Pour permettre ce fonctionnement, il est nécessaire d'installer sur le serveur un module PAM fourni par EMC.

Ce module est disponible à l'adresse suivante :

http://france.emc.com/security/rsa-securid/rsa-authentication-agents/pam-7-1.htm

La dernière version testée est la version 7.1.0.1. elle nécessite au minimum un serveur RSA Authentication Manager version 6.1 ou 7.1

Ce client n'est pas certifié pour fonctionner sur le système GNU/Linux Ubuntu, il peut être nécessaire de modifier le script d'installation présent dans l'archive pour qu'il s'exécute correctement sur un serveur EOLE (voir ci-dessous).

Adaptation du fichier `install_pam.sh` pour une installation sur un serveur EOLE :

- Remplacer les occurrences de `chmod 755` par `chmod 644` pour appliquer les permissions préconisées par la distribution.
- Rechercher la section concernant le paramétrage pour Linux (ligne 362 dans la version testée) :

```
'Linux' ) LNX_VERS=`uname -i`
   if [ `getconf LONG_BIT` = "32" ] ; then
        ARCH=32bit
        MODULE_DIR_PRIMARY="/lib/security"
        MODULE_DIR_SECONDARY=""
   else
        ARCH=64bit
        MODULE_DIR_PRIMARY="/lib/security"
        MODULE_DIR_SECONDARY="/lib64/security/"
   fi
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> Dans le bloc `else` (serveur 64 bits), remplacer `MODULE_DIR_SECONDARY="/lib64/security/"` par `MODULE_DIR_SECONDARY="/lib/x86_64-linux-gnu/security/"`.
>
> La même modification doit être effectuée sur le fichier `uninstall_pam.sh` si vous souhaitez désinstaller l'agent.
>
> Cette modification concerne la dernière version testée du client (v7.1.0.1.16.05_06_13_02_04_01), si besoin voir la documentation EoleSSO 2.3 si vous utilisez des versions plus anciennes.

Un fichier de configuration est livré avec EoleSSO pour utiliser le module fourni (`/etc/pam.d/rsa_securid`)

Le module nécessite également les étapes suivantes :

- enregistrement du serveur hébergeant EoleSSO en tant qu'agent dans la configuration du serveur Authentication Manager ;
- copie du fichier `sdconf.rec` présent sur le serveur RSA dans le répertoire `/var/ace` (serveur EoleSSO) ;
- activer la gestion de l'authentification OTP dans EoleSSO (dans l'interface de configuration du module, onglet `Eole sso` puis redémarrer le service). Se reporter à la section Configuration pour le détail des options de configuration disponibles.

> Deux utilitaires sont livrés avec le module PAM pour tester le fonctionnement :
>
> - `/opt/pam/bin/32bit/acestatus` : affiche les informations sur le serveur présentes dans `sdconf.rec`
> - `/opt/pam/bin/32bit/acetest` : permet de valider l'authentification d'un utilisateur
>
> Sur un serveur 64 bits, les utilitaires livrés avec le module PAM se trouvent dans le répertoire `/opt/pam/bin/64bit`.

> **Versions 32 ou 64 bits**
>
> Les scripts d'installation fournis n'installent pas toujours correctement le module PAM. En cas de dysfonctionnement, vérifier que la version installée de la librairie correspond bien à l'architecture de la machine (voir complément ci dessus sur le script d'installation).
>
> Vous pouvez comparer le fichier `pam_securid.so` installé avec les version 32 ou 64 bits qui peuvent être trouvées dans l'archive `sd_pam_agent.tar` du répertoire `/lnx` du répertoire d'installation de l'agent.
>
> La librairie doit être installée dans le répertoire `/lib64/security/` dans le cas d'une version d'EOLE inférieure à 2.5.0 ou dans le répertoire `/lib/x86_64-linux-gnu/security/` dans le cas contraire.

6. Application de redirection : Eole-dispatcher

Dans le cadre de l'utilisation du module Seshat en tant que point d'entrée d'un ENT centralisé,

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

l'application Eole-dispatcher permet de rediriger les utilisateurs vers leur établissement d'origine. Elle se base sur les informations remontées lors de la mise en place de la réplication des serveurs Scribe.

Elle est également prévue pour gérer le cas de l'affectation multiple pour les enseignants et les responsables :

- un enseignant qui aurait des services sur plusieurs établissements se verrait proposer le choix de l'établissement sur lequel il souhaite se connecter ;
- un parent d'élève qui aurait plusieurs enfants dans des établissements différents se verrait également proposer le choix de l'établissement. Il est à noter que la problématique de la l'affectation multiple pour un élève ne se pose pas, puisque ce dernier ne peut pas être scolarisé dans deux établissements.

Eole-dispatcher est capable (au travers de ses filtres d'attributs) de gérer les sources d'authentification suivantes :

- LDAP Académique pour les agents de l'Éducation nationale ;
- LDAP Téléservices pour les parents et élèves ;
- LDAP local (réplicat des serveurs Scribe) pour l'authentification des élèves et parents (si les téléservices ne sont pas déployés).

Le terme affectation est à prendre au sens large, il désigne l'appartenance d'une personne à un établissement.

Pré-requis

Cette application nécessite :

- la mise en place de la réplication LDAP des serveurs Scribe sur le serveur Seshat ;
- l'alimentation des annuaires des serveurs Scribe avec des extractions AAF **EXCLUSIVEMENT** ;
- la bonne saisie des numéros et libellés établissement sur les serveurs Scribe et Zéphir ;
- la configuration d'une fédération entre chaque serveur Scribe et le serveur Seshat (voir documentation EoleSSO au chapitre : Fédération entre 2 serveurs EoleSSO).

Installation

Le dispatcher est à installer sur le module Seshat, afin d'utiliser son portail EoleSSO comme portail unique d'authentification vers les ENT (Envole).

L'application n'est pas installée par défaut. Via l'interface de configuration du module, configurer le serveur pour recevoir les applications web :

- en mode normal dans l'onglet `Services`, passer `Activer le serveur web Apache` à `oui` ;
- dans l'onglet `Applications web`, saisissez le nom de domaine des applications web dans `Nom de domaine des applications web (sans http://)` ;
- enregistrer la configuration et quitter l'interface de configuration du module.

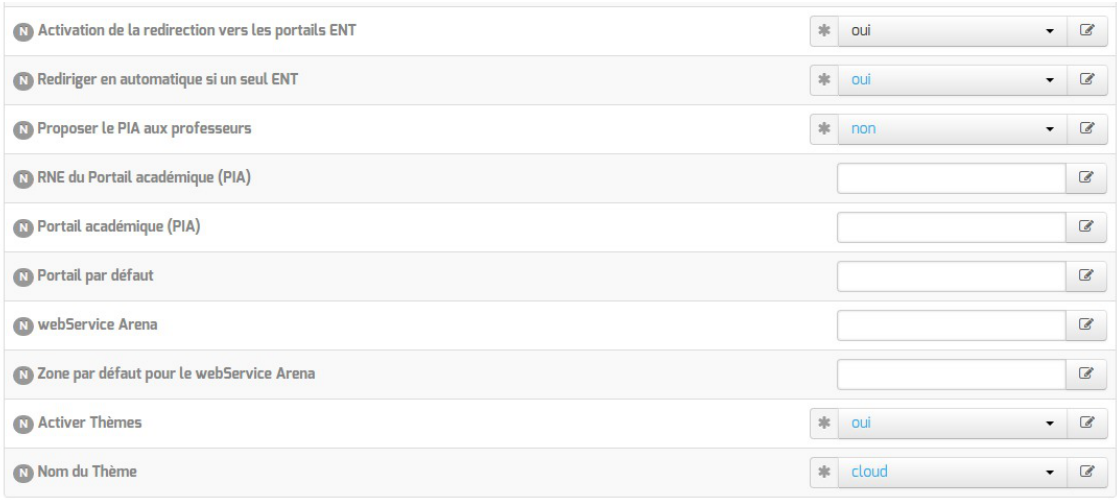
Puis saisir les commandes suivantes sur le module Seshat pour installer le paquet `eole-dispatcher` :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
# Query-Auto
# apt-eole install eole-dispatcher
```

Configuration

Une fois les paquets installés, il faut de nouveau se rendre dans l'onglet `Application web` de l'interface de configuration du module et passer `Activation de la redirection vers les portails ENT` à `oui`. Des paramètres supplémentaires s'affichent.



- `Rediriger en automatique si un seul ENT` ;
- `Proposer le PIA aux professeurs` : permet de proposer le portail académique aux enseignants ;
- `RNE du Portail académique (PIA)` : permet de saisir l'UAI du portail académique ;
- `Portail académique (PIA)` : portail sur lequel seront redirigés les personnels académiques ;
- `Portail par défaut` : adresse du site Internet dédié à l'ENT si aucun portail d'établissement n'est disponible pour l'utilisateur ;
- `webService Arena` : URL complète du webService ARENA pour la récupération des ressources ;
- `Zone par défaut pour le webService Arena` : zone par défaut du portail ARENA.

Il est possible de changer ou de désactiver le thème.

Une fois l'application paramétrée, il est nécessaire de reconfigurer le serveur à l'aide de la commande `reconfigure`.

Une fois le serveur reconfiguré, l'application est accessible à l'adresse : `http://<adresse_serveur>/edispatcher/`

> Il est possible de rendre l'application directement accessible depuis l'adresse `http://<adresse_serveur>/`, en renseignant `/edispatcher` en tant qu'`Application web par défaut (redirection)` dans la famille `Applications web`

Fonctionnement

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

L'installation du dispatcher va mettre en place sur le serveur SSO les filtres d'attributs nécessaires afin de rediriger correctement la personne.

Extrait du fichier `/usr/share/sso/app_filters/dispatcher.ini` :

```
[user]
rne=ecs_rne
user=uid
uid=uid
source=SourceAuth
FederationKey=DispatcherKey
displayName=displayName
profils=DispatcherProfils
auth=auth
```

L'attribut calculé `ecs_rne`, va permettre de récupérer les codes RNE en fonction des établissements d'affectation de l'utilisateur.

Lors de la connexion d'une personne, Eole-dispatcher va prendre tous les RNE reçus de EoleSSO et présenter tous les liens de fédération pour l'accès aux portails Envole le concernant.

Exemple d'URL de fédération

`https://<domaineSeshatSSO>/saml?sp_ident=<id_fs>&RelayState=https:/`
Cette URL effectue une fédération vers le fournisseur de service `<id_fs>` et redirige vers l'`<URL_du_portail_Établissement>` du client en fournissant un identifiant de session.

Eole-dispatcher et EoleSSO

RNE : `id_fs`

`id_fs` est :

- soit l'identifiant du fournisseur de service (entityID tel que défini dans son fichier de méta-données) ;
- soit le nom de son fichier de méta-données placé dans `/usr/share/sso/metadata/` (sans l'extension `.xml`).

Par simplicité il est possible de nommer le fichier metadata de nos entités partenaires (Serveur Scribe des établissements) par `<RNE>.xml` ; `id_fs` est alors le code RNE de l'établissement.

Libellé et adresse du portail des établissements : URL_du_portail_Établissement

EoleSSO va générer automatiquement, à chaque redémarrage du service `eole-sso`, un fichier dans `/var/www/html/edispatcher/utils/etabs.ini` qui va contenir les entrées nécessaires pour chaque établissement :

```
[9740091F]
libelle = COLLEGE LECONTE DE LISLE
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
portail = https://portail.college-lecontedelisle.re
```

...

Ces entrées sont récupérées depuis Zéphir, il est donc nécessaire que les serveurs Scribe soient enregistrés sur le serveur Zéphir. Dans le cas contraire, ou si des informations sont incorrectes ou manquantes, il faudra remplir ce fichier à la main (voir le chapitre : Gestion des sources d'authentification multiples).

Vous pouvez vous baser sur le fichier d'exemple : `/var/www/html/edispatcher/utils/etabs.ini.sample`.

Message d'erreur : `aucun portail trouvé`

Il manque une section pour le code RNE dans le fichier `/var/www/html/edispatcher/utils/etabs.ini`.

Description de liens vers des applications web ou vers des portails.

Fichier `/var/www/html/edispatcher/applications.ini` :

- Format des sections :

```
[<identifiant du lien>]
url="<adresse du lien>"
piwik=<identifiant piwik>
```

- Paramétrage des URLs : il est possible d'insérer des étiquettes dynamiques dans les URLs

```
[SSO] : adresse du serveur SSO de Seshat
[PORTAILHOST] : portail dépendant de la zone d'accès du client (configuré dans portails.ini)
[TICKET] : identifiant de session
```

Configuration de l'accès à un portail en fonction de la plage IP du client

Eole-dispatcher est également utilisé dans certaines académies comme portail d'authentification unique pour l'accès aux portails ARENA[p.83].

Il peut exister plusieurs portails en fonction de l'endroit où se trouve l'utilisateur. Par exemple, dans l'académie de la Réunion il existe au moins trois portails d'accès aux application ARENA :

- `portail.ac-reunion.fr` (accessible en externe) ;
- `scoens.ac-reunion.fr` (depuis le réseau pédagogique des établissements) ;
- `scoweb.ac-reunion.fr` (depuis le réseau administratif).

Chaque portail, en fonction de sa zone de confinement, ne présentera pas les mêmes ressources et l'utilisation d'une clé OTP[p.84] sera proposée ou non.

Il faut donc permettre à l'utilisateur d'obtenir le bon portail en fonction de la zone où il se trouve.

La fonction `GetPortailHost` du fichier `/var/www/html/edispatcher/inc.php` du dispatcher

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> permet, en fonction de l'adresse IP du client, de rediriger l'utilisateur vers le bon portail. La récupération de l'adresse IP du client se base sur le champ `HTTP_X_FORWARDED_FOR` des headers HTTP.

Les différentes associations réseau / portail sont définies dans le fichier `/var/www/html/edispatcher/utils/portails.ini`.

Créer le fichier `/var/www/html/edispatcher/utils/portails.ini` et ajouter des sections décrivant une plage IP et l'adresse du portail correspondant :

```
[<adresse IP>]
mask=<masque IP>
portail="<adresse du portail pour cette plage IP>"
```

Un exemple de fichier est présent dans : `/var/www/html/edispatcher/utils/portails.ini.sample`.

```
[172.16.0.0]
mask=13
portail="scoens.ac-reunion.fr"
arena="rev-proxy-peda"
[172.31.190.64]
mask=26
portail="portail.ac-reunion.fr"
arena="rev-proxy-id"
[172.31.16.0]
mask=16
portail="portail.ac-reunion.fr"
arena="rev-proxy-id"
[10.205.0.0]
mask=16
portail="scoweb.ac-reunion.fr"
arena="rev-proxy-agr"
```

Dans cet exemple, tout utilisateur se présentant avec une adresse IP du réseau 10.205.0.0/16, se verra renvoyé vers l'URL du portail académique https://scoweb.ac-reunion.fr.

La variable `arena`, permet de spécifier la zone ClearTrust associée au portail. Elle est utilisée si vous souhaitez intégrer les ressources ARENA dans le bureau Envole.

Plus d'informations : https://envole.ac-dijon.fr/wordpress/2014/02/19/integration-de-arena-dans-le-bureau-envole.

Voir aussi...

- Gestion des sources d'authentification multiples

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

7. Configuration du fournisseur d'identité France Connect

Pour mettre en place la relation de confiance entre EoleSSO et France Connect, il faut effectuer une demande d'enregistrement auprès de France Connect : https://franceconnect.gouv.fr/inscription

Le fournisseur d'identité France Connect renvoi un identifiant client (Client ID) et une clé privée secrète (Client secret) utilisé pour valider les échanges. Il met à disposition un certain nombre d'URLs nécessaires à la configuration du client.

Pour l'inscription il est demandé les informations suivantes:

- le nom du service ;
- une adresse électronique de contact ;
- un logo représentant le fournisseur de service (logo EOLE, logo de l'académie...) qui apparaîtra sur la page d'authentification de France Connect ;
- une adresse dite de callback : adresse sur laquelle est renvoyé l'utilisateur après authentification.

  Dans le cas d'EoleSSO cette adresse est :

  `https://<adresse_serveur_eolesso>:8443/oidcallback`

Les logos et bouton de connexion France Connect sont déjà fournis avec EoleSSO.

Pour plus d'informations sur le fonctionnement et la configuration, se reporter à : https://franceconnect.gouv.fr/fournisseur-service

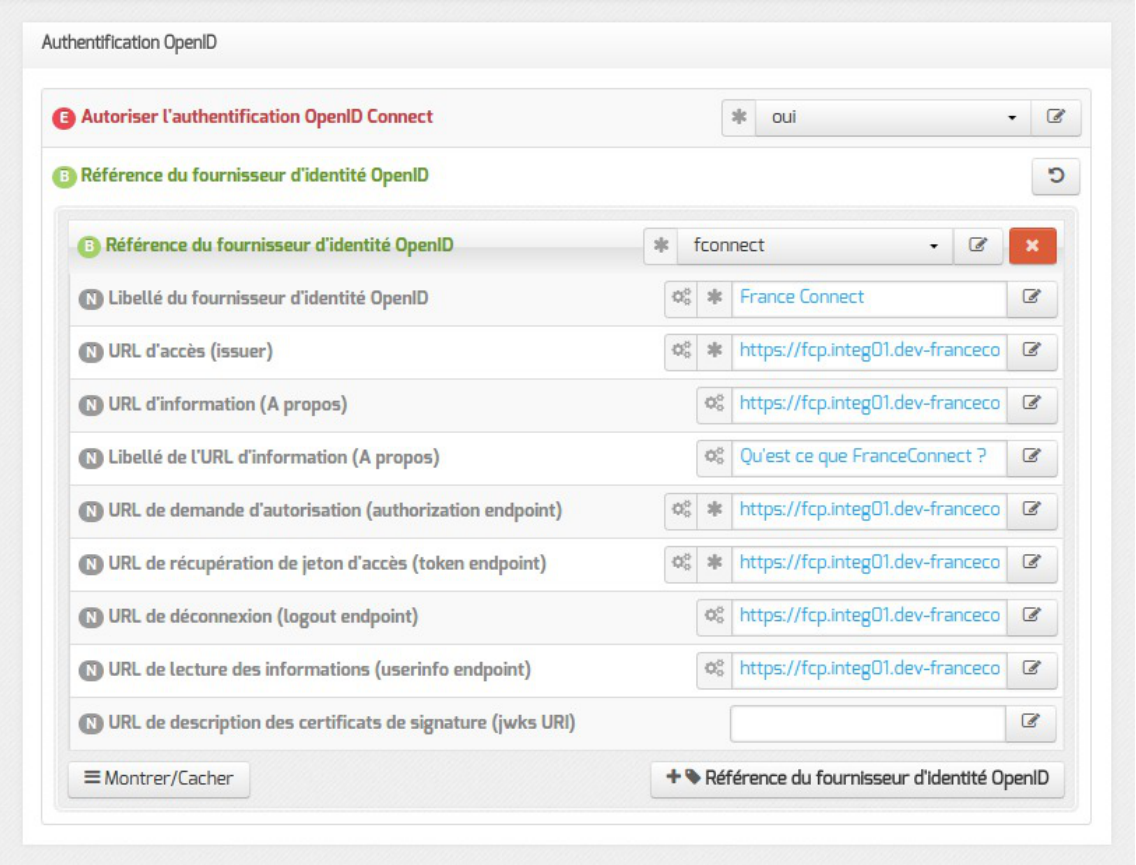
Les conditions d'utilisation de France Connect et le processus de raccordement sont décrites dans le document PDF suivant :

https://franceconnect.gouv.fr/files/CGU FS - Annexe Processus d'implementation de FC par FS V2.1.pdf [https://franceconnect.gouv.fr/files/CGU%20FS%20-%20Annexe%20Processus%20d'implementation%20de%20FC%20par%20FS%20V2.1.pdf]

À noter que parmi les conditions, une **déclaration CNIL** simplifiée est disponible et une **recette de la solution technique** mise en œuvre doit être effectuée par le SGMAP[p.86].

Une configuration prédéfinie est fournie pour France Connect.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Pour l'activer, choisissez `fconnect` dans la liste déroulante de la variable `Référence du fournisseur d'identité OpenID`, ne pas oublier de valider le choix pour faire apparaître les différentes variables.

L'identifiant client (Client ID) et la clé privée secrète (Client secret) renvoyés par le fournisseur d'identité utilisés pour valider les échanges doivent être, pour des raisons de sécurité, stockés dans un fichier à part avec des droits restreints.

Pour chaque fournisseur d'identité, ajouter une ligne dans le fichier `/etc/eole/eolesso_openid.conf` :

```
<nom_fournisseur> = "<client id> :<client secret>"
```

Le `nom fournisseur` doit correspondre au paramètre `Référence du fournisseur d'identité OpenID` renseigné dans l'interface de configuration du module.

Si ces informations ne sont pas renseignées pour l'un des fournisseurs déclarés, un message l'indiquera au lancement de la commande `diagnose`.

Voir aussi...

Onglet Eole sso : Configuration du service SSO pour l'authentification unique

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

8. Configuration du fournisseur d'identité Google (Google APIs).

Déclaration d'EoleSSO comme fournisseur de service

Pour récupérer votre Client ID / Client Secret, vous devez créer un compte développeur depuis cette adresse : https://developers.google.com/

Rendez-vous dans la console développeur de Google afin de déclarer votre service EoleSSO comme application : https://console.developers.google.com

- Créez un nouveau projet (barre supérieure de la console -> `select a project` -> `create a project`) ;
- Une fois le projet créé, cliquez sur la barre de menu gauche (3 barres horizontales), puis sur `API Manager`. Cliquez ensuite sur `Credentials` (à gauche) ;
- Cliquer sur `Oauth Consent Screen` et renseigner au minimum le champ `Product name shown to users` (par exemple 'établissement xxx') ;
- Sauvegarder et dans Credentias, cliquer sur `Create credentials`, *Oauth Client ID" ;
- Choisir `Web application` et renseigner les champs suivants :
  - Name : au choix
  - Authorized JavaScript origins : https://[adresse_serveur_sso]:8443
  - Authorized redirect URIs : https://[adresse_serveur_sso]:8443/oidcallback
- Cliquer sur Create et recopier l'identifiant et la clé secrète fournis ;

Configuration du fournisseur d'identité (Google) dans l'interface de configuration du module

Une fois les identifiants récupérés, vous pouvez configurer les paramètres d'EoleSSO (gen_config, onglet Eole SSO en mode expert)

- Passer à `oui` la variable `Autoriser l'authentification OpenID Connect` ;
- ajouter un forunisseur en cliquant sur `+Référence du fournisseur d'identité OpenID` ;
- `Référence du fournisseur d'identité OpenID` : google (des logos sont présents et utilisés automatiquement en choisissant ce libellé) ;
- `Libellé du fournisseur d'identité OpenID` : Google (ou autre description de votre choix) ;
- `issuer` : https://accounts.google.com ;
- `authorization endpoint` : https://accounts.google.com/o/oauth2/v2/auth ;
- `token endpoint` : https://www.googleapis.com/oauth2/v4/token ;
- `userinfo endpoint` : https://www.googleapis.com/oauth2/v3/userinfo ;
- `jwks uri` : https://www.googleapis.com/oauth2/v3/certs .

En cas de problème, les paramètres en cours de validité sont décrits ici : https://accounts.google.com/.well-known/openid-configuration

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Pour plus d'informations sur le support d'OpenID de Google : https://developers.google.com/identity/protocols/OpenIDConnect

L'identifiant client (Client ID) et la clé privée secrète (Client secret) renvoyés par le fournisseur d'identité utilisés pour valider les échanges doivent être, pour des raisons de sécurité, stockés dans un fichier à part avec des droits restreints.

Pour chaque fournisseur d'identité, ajouter une ligne dans le fichier `/etc/eole/eolesso_openid.conf` :

```
<nom_fournisseur> = "<client id> :<client secret>"
```

Le `nom fournisseur` doit correspondre au paramètre `Référence du fournisseur d'identité OpenID` renseigné dans l'interface de configuration du module.

Si ces informations ne sont pas renseignées pour l'un des fournisseurs déclarés, un message l'indiquera au lancement de la commande `diagnose`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 10

Questions fréquentes

Certaines interrogations reviennent souvent et ont déjà trouvées une réponse ou des réponses.

1. Questions fréquentes propres à EoleSSO

Pas de question fréquente pour le moment.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Glossaire

ARENA *= Accès aux Ressources de l'Éducation Nationale et Académiques*	Les portails d'applications ARENA vous donnent accès aux applications en ligne du ministère de l'Éducation nationale et de l'Académie.
CAS *= Central Authentication Service*	CAS est un système d'authentification unique créé par l'université de Yale : on s'authentifie sur un site Web, et on est alors authentifié sur tous les sites Web qui utilisent le même serveur CAS. Il évite de s'authentifier à chaque fois qu'on accède à une application en mettant en place un système de ticket.
DN *= Distinguished Name*	Identifiant unique dans le cadre des annuaires LDAP.
Fichiers métadata	Les fichier métadata sont des fichiers au format XML contenant les informations nécessaires à la définition des entités partenaires en vue d'échange de message SAML. Ces fichiers contiennent la plupart du temps : • le nom de l'entité ; • les différentes urls sur lesquelles envoyer les différentes requêtes et réponse au format SAML; • la description des certificats utilisés pour signer ses messages; • des informations sur les attributs nécessaires pour identifier les utilisateurs ; • .... La description complète du format de ces fichiers et des éléments possibles est disponible sur le site du consortium OASIS.
FranceConnect	FranceConnect est un dispositif permettant de garantir l'identité d'un utilisateur en s'appuyant sur des comptes existants pour lesquels son identité a déjà été vérifiée. Ce dispositif est un bien commun mis à la disposition de toutes les autorités administratives. Il est mis en œuvre par la DINSIC, dépendante du SGMAP2, un service du premier ministre. Certains acteurs du secteur privé peuvent aussi en bénéficier s'ils contribuent à l'action publique (banques et assurances par exemple). Source : http://fr.wikipedia.org/wiki/FranceConnect
instance *= instanciation, instancier*	Instancier un serveur correspond à la troisième étape de mise ne œuvre d'un module EOLE. Cette phase permet d'écrire les fichiers de configuration et de lancer ou de redémarrer les services d'après les valeurs renseignées lors de l'étape de configuration. L'instanciation prépare le système en vue de sa mise en production et s'exécute à l'aide de la commande `instance`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Keycloak	Keycloak est un outil libre et moderne de gestion d'identité et des accès (IAM).
LDAP *= Lightweight Directory Access Protocol*	À l'origine un protocole permettant l'interrogation et la modification des services d'annuaire, LDAP a évolué pour représenter une norme pour les systèmes d'annuaires.
LemonLDAP *= LemonLDAP::NG*	LemonLDAP::NG est une infrastructure d'authentification unique distribuée (SSO – Single Sign On) avec gestion centralisée des droits. Il se présente sous la forme d'une suite logicielle libre reposant sur le serveur web Apache. Source : http://www.starxpert.fr/lemon-ldap/
man in the middle *= homme du milieu*	L'attaque de l'homme du milieu (HDM) ou man in the middle attack (MITM) est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. Le canal le plus courant est une connexion à Internet de l'internaute lambda. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre. Source Wikipédia : http://fr.wikipedia.org/wiki/Attaque_de_l'homme_du_milieu
MD5 *= Message Digest 5*	L'algorithme MD5 est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier. Il a été inventé par Ronald Rivest en 1991. Source : https://fr.wikipedia.org/wiki/MD5
OAuth	OAuth est un protocole libre qui permet d'autoriser un site web, un logiciel ou une application (dit « consommateur ») à utiliser l'API sécurisée d'un autre site web (dit « fournisseur ») pour le compte d'un utilisateur. OAuth n'est pas un protocole d'authentification, mais un protocole de "délégation d'autorisation". Source Wikipédia : http://fr.wikipedia.org/wiki/OAuth
OpenID Connect *= OIDC*	OpenID Connect est un système d'authentification décentralisé qui permet l'authentification unique, ainsi que le partage d'attributs. Il permet à un utilisateur de s'authentifier auprès de plusieurs sites sans avoir à retenir un identifiant pour chacun d'eux mais en utilisant à chaque fois un unique identifiant OpenID Connect. Cette couche d'identification simple est basée sur le protocole OAuth 2.0. Ce standard est géré par la fondation OpenID. Plusieurs entreprises utilisent OpenID Connect tel Google, Microsoft, Ping Identity, Deutsche Telekom, salesforce.com, Trustelem. L'état Français l'utilise également dans son dispositif d'authentification et d'identification universel FranceConnect. Source Wikipédia : http://fr.wikipedia.org/wiki/OpenID_Connect

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

OTP *= One-time password*	Un Mot de passe unique (OTP) est un mot de passe qui n'est valable que pour une session ou une transaction. Les OTP permettent de combler certaines lacunes associées aux traditionnels mots de passe statiques, comme la vulnérabilité aux attaques par rejeu. Cela signifie que, si un intrus potentiel parvient à enregistrer un OTP qui était déjà utilisé pour se connecter à un service ou pour effectuer une opération, il ne sera pas en mesure de l'utiliser car il ne sera plus valide. En revanche, les OTP ne peuvent pas être mémorisé par les êtres humains, par conséquent, ils nécessitent des technologies complémentaires afin de s'en servir. Source : http://fr.wikipedia.org/wiki/Mot_de_passe_unique
PAM *= Pluggable Authentication Modules*	PAM est un mécanisme permettant d'intégrer différents schémas d'authentification de bas niveau dans une API de haut niveau, permettant de ce fait de rendre indépendants du schéma les logiciels réclamant une authentification. PAM est une création de Sun Microsystems et est supporté en 2006 sur les architectures Solaris, Linux, FreeBSD, NetBSD, AIX et HP-UX. L'administrateur système peut alors définir une stratégie d'authentification sans devoir recompiler des programmes d'authentification. PAM permet de contrôler la manière dont les modules sont enfichés dans les programmes en modifiant un fichier de configuration. Les programmes qui donnent aux utilisateurs un accès à des privilèges doivent être capables de les authentifier. Lorsque vous vous connectez sur le système, vous indiquez votre nom et votre mot de passe. Le processus de connexion vérifie que vous êtes bien la personne que vous prétendez être. Il existe d'autres formes d'authentification que l'utilisation des mots de passe, qui peuvent d'ailleurs êtres stockés sous différentes formes.
Redis *= REmote DIctionary Server*	Le nom Redis vient de l'anglais REmote DIctionary Server qui peut être traduit par « serveur de dictionnaire distant » et qui est un jeu de mot avec le mot Redistribute. Redis est un système de gestion de base de données clef-valeur scalable, très hautes performances, écrit avec le langage de programmation C ANSI et distribué sous licence BSD. Il fait partie de la mouvance NoSQL et vise à fournir les performances les plus élevées possibles. Source Wikipédia : http://fr.wikipedia.org/wiki/Redis
SAML *= Security assertion markup language*	SAML est un standard informatique définissant un protocole pour échanger des informations liées à la sécurité. Il est basé sur le langage XML. SAML suppose un fournisseur d'identité et répond à la problématique de l'authentification au-delà d'un intranet.
SecurID	

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	SecurID est un système de token, ou authentifieur, produit par la société RSA Security et destiné à proposer une authentification forte à son utilisateur dans le cadre de l'accès à un système d'information. Source : http://fr.wikipedia.org/wiki/SecurID
SGMAP *= Secrétariat Général pour la Modernisation de l'Action Publique*	Le secrétariat général pour la modernisation de l'action publique est une administration française placée sous l'autorité du Premier ministre et rattachée au secrétaire général du Gouvernement. http://www.modernisation.gouv.fr/
SSO *= Single Sign On, Authentification unique*	SSO est une méthode permettant de centraliser l'authentification afin de permettre à l'utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications informatiques. Les objectifs sont : • simplifier pour l'utilisateur la gestion de ses mots de passe : plus l'utilisateur doit gérer de mots de passe, plus il aura tendance à utiliser des mots de passe similaires ou simples à mémoriser, abaissant par la même occasion le niveau de sécurité que ces mots de passe offrent ; • simplifier la gestion des données personnelles détenues par les différents services en ligne, en les coordonnant par des mécanismes de type méta-annuaire ; • simplifier la définition et la mise en œuvre de politiques de sécurité.
TCP Wrapper *= tcpd*	TCP Wrapper est une technique, propre à Unix, permettant de contrôler les accès à un service (ou démon) suivant la source. Il se configure grâce au deux fichiers /etc/hosts.allow et /etc/hosts.deny. Tous les démons ne supportent pas la technique TCP Wrapper.
Twisted	Twisted est un framework d'application réseau écrit en Python et sous licence MIT. Twisted supporte TCP, UDP, SSL/TLS, multicast, Unix domain sockets, un grand nombre de protocoles dont HTTP, NNTP, IMAP, SSH, IRC, FTP, et beaucoup d'autres. Twisted se base sur un paradigme événementiel, ce qui signifie que les utilisateurs écrivent de courtes fonctions de rappel (callbacks) qui sont appelées par le framework. http://twistedmatrix.com
XML-RPC *= XML Remote procedure call*	XML-RPC est un protocole RPC (Remote procedure call), une spécification simple et un ensemble de codes qui permettent à des processus s'exécutant dans des environnements différents de faire des appels de méthodes à travers un réseau. XML-RPC permet d'appeler une fonction sur un serveur distant à partir de n'importe quel système (Windows, Mac OS X, GNU/Linux) et

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	avec n'importe quel langage de programmation. Le serveur est lui même sur n'importe quel système et est programmé dans n'importe quel langage. Cela permet de fournir un Service web utilisable par tout le monde sans restriction de système ou de langage. Source : http://fr.wikipedia.org/wiki/XML-RPC

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)