EoleSSO - Demande #14807

Authentification OTP sur eole-sso 2.4.2

25/01/2016 18:28 - Académie Grenoble Ac-Grenoble

Statut:	Fermé	**Début:**	25/01/2016
Priorité:	Normal	**Echéance:**	
Assigné à:	Bruno Boiget	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:		**Temps passé:**	0.00 heure

Description

Bonjour,

Nous avons un eole-sso 2.4.2 installé sur un eole-base (et non sur un seshat). Lorsqu'on essaie de s'authentifier avec sa clé OTP sur pia.ac-grenoble.fr, le navigateur affiche l'erreur suivante :

> Echec de l'authentification OTP, veuillez recommencez

Ceci se traduit par les messages ci-dessous dans les journaux pia-sso1:/var/log/rsyslog/local/eolesso/eolesso.info.log :

> Jan 25 11:55:21 pia-sso1 eolesso: [-] ! Session non valide :
> TMP-pia-sso1.ac-grenoble.fr-100ea400706ce7519625f26cbde44c8b43934cbd1616bd7f74b64a87 !
> Jan 25 11:55:21 pia-sso1 eolesso: [-] Session utilisateur non reconnue :
> TMP-pia-sso1.ac-grenoble.fr-100ea400706ce7519625f26cbde44c8b43934cbd1616bd7f74b64a87
> Jan 25 11:55:21 pia-sso1 eolesso: [-] !
> TMP-pia-sso1.ac-grenoble.fr-100ea400706ce7519625f26cbde44c8b43934cbd1616bd7f74b64a87 -- Echec de création de session pour le service https://pia.ac-grenoble.fr/envole/portal/login.php !
> Jan 25 11:55:21 pia-sso1 eolesso: [-]
> TMP-pia-sso1.ac-grenoble.fr-100ea400706ce7519625f26cbde44c8b43934cbd1616bd7f74b64a87 -- Redirection vers l'application appelante avec le ticket : https://pia.ac-grenoble.fr/envole/portal/login.php

Nous avons activé l'authentification OTP dans gen_config, ce qui est d'ailleurs requis pour pouvoir interroger à la fois le LDAP local (utilisé uniquement pour le compte admin) et le LDAP académique (pour l'authentification des agents). Nous croyons nous souvenir que des dépendances supplémentaires étaient requises pour permettre l'authentification OTP, et qu'elles n'étaient résolues que sur le Seshat ?

En décembre 2015, au cours d'une réunion entre le Pôle Identité et l'académie de Grenoble, on avait évoqué l'idée d'un rapprochement entre les pôles de compétences Eole et Identité. Ceci notamment dans l'optique de permettre à toutes les académies d'installer un PIA selon une procédure standardisée. Est-ce pertinent à vos yeux pour résoudre ce présent ticket ?

Bien à vous,
--
Mathieu Jourdan

Demandes liées:

Lié à EoleSSO - Tâche #15028: EoleSSO : fichier /etc/pam.d/rsa_securid non in...	**Fermé**	**11/02/2016**

Historique

#1 - 27/01/2016 15:26 - Bruno Boiget

- Statut changé de Nouveau à En attente d'informations

- Assigné à mis à Bruno Boiget

Les principaux éléments à mettre en oeuvre sont décrits dans l'annexe de la documentation EoleSSO :

http://eole.ac-dijon.fr/documentations/2.5/beta/partielles/EoleSSO/co/06_install_otp.html

- activation dans gen_config (plus d'infos sur les paramêtres ici http://eole.ac-dijon.fr/documentations/2.5/beta/partielles/EoleSSO/co/02-configurationModeExpert.html)
- installer le plugin PAM/securid fourni par EMC (voir lien dans la doc)
- ajouter le serveur hébergeant EoleSSO comme agent d'authentification dans la console du serveur 'RSA Authentication manager'
- mettre en place le fichier sdconf.rec correspondant à ce serveur

Quelques écueils que j'ai rencontré lors de la mise en place de nos maquettes et dans plusieurs académies :

- Le script d'installation du client PAM doit être modifié pour 'exécuter correctement (voir le bloc complément dans la page de documentation).
- il faut faire attention à ce que la librairie installée corresponde bien à l'architecture du serveur (i386/amd64). En principe le script doit le détecter
- un jeton unique est stocké dans le fichier /var/ace/securid pour identifier l'agent PAM auprès du serveur RSA. En cas de réinstallation sur une nouvelle adresse ip, il faut dans certains cas supprimer ce fichier et demander la génération d'un nouveau jeton depuis la page de gestion des agents dans la console RSA. (rechercher "node secret" dans ce document https://www.emc.com/collateral/15-min-guide/h12276-am8-administrators-guide.pdf)

Est ce que ces informations sont suffisantes pour vous débloquer votre problème ?

Nous n'avons pas vraiment d'expertise sur la partie configuration FIM, il pourrait effectivement être intéressant d'avoir un document validé/écrit par le pôle Identité concernant cet aspect. La documentation de mise en oeuvre d'un PIA complet me semble dépasser le cadre de cette demande.

#2 - 11/02/2016 11:14 - Bruno Boiget

- Statut changé de En attente d'informations à Fermé

Vu avec Mathieu sur IRC, les informations fournies devraient permettre d'avancer sur le sujet (ouvrir une nouvelle demande en cas de problème).