

Cassification d'un serveur SFTP

Quelques notes sur la Cassification d'un serveur SFTP en vue de son utilisation avec Esup-FileManager :

Accès aux Homedir par sftp cassifié

Afin de permettre d'accéder aux HomeDir des utilisateurs au travers de l'ENT, on propose d'utiliser pour cela du SFTP cassifié.

Côté serveur, cela drevient donc à cassifier un espace de stockage accessible en SSH.

Pour ce faire, on peut utiliser le module pam_cas proposé et documenté par EsupPortail ici :

[Module PAM pour CAS](#)

* on installe le module cas dans /usr/local/esup-pam-cas-2.0.11-esup-2.0.7/

* on le compile dans sources, on récupère le pam_cas.so pour le mettre dans /usr/local/esup-pam-cas-2.0.11-esup-2.0.7/

- pour debian, on peut faire une copie de Makefile.redhat en Makefile

- quelques paquets sont requis pour la compilation également:

apt-get install make gcc libpam0g-dev libssl-dev

* on configure le /usr/local/esup-pam-cas-2.0.11-esup-2.0.7/pam_cas.conf directement (paramètres du serveur cas + certificat ssl/https)

Enfin on modifie /etc/pam.d/sshd, on lui ajoute la ligne

auth sufficient /usr/local/esup-pam-cas-2.0.11-esup-2.0.7/sources/pam_cas.so -ssftp://stock-2.mon-univ.fr -f/usr/local/esup-pam-cas-2.0.11-esup-2.0.7/pam_cas.conf

avant la ligne (exemple pour debian squeeze)

@include common-auth

Et on redémarre sshd :

/etc/init.d/sshd restart

Test

On peut ensuite tester cela avec un Service Ticket (ST).

Pour l'obtenir, il faut demander à CAS une authentification (ST donc) pour un service nommé ici **sftp://stock-2.mon-univ.fr**.

Pour ce faire on construit une url comme ceci : <https://cas.mon-univ.fr/login?service=sftp%3A%2F%2Fstock-2.mon-univ.fr>

En l'appellant depuis un navigateur, CAS vous demande de vous authentifier et tente ensuite de vous forwarder sur une url de ce type :

sftp://stock-2.mon-univ.fr?ticket=ST-231347-YgbLHGau6MRaduvdHjC2-cas

* Vous pouvez voir cela en sniffant le réseau avec wireshark par exemple ou simplement en utilisant un module Firefox : [Firebug](#) ou encore [LiveHttp Headers](#)

* Vous pouvez également récupérer le ticket ST-231347-YgbLHGau6MRaduvdHjC2-cas en consultant le logs cas (si celui-ci est configuré pour logger les tickets générés).

Vous pouvez alors tenter une connection sur votre sftp en utilisant le même username que pour l'authentification CAS, et le ST pour password !