

SaMBa4, retour d'expérience

Jérôme COLOMBET

Centre National de la Recherche Scientifique

Laboratoire de Chimie de Coordination

jerome.colombet@lcc-toulouse.fr

17 oct. 2019, RDV des Adminsys



- Laboratoire de 250 personnes, composé de chercheurs, d'enseignants chercheurs, **I**ngénieurs **T**echniciens **A**ministratifs et de non permanents (doctorants, étudiants,...).
- Le LCC unité propre de recherche situé au campus 205. Financement direct par le CNRS et des contrats (CPER, FEDER, ...).
- 15 équipes de recherche, 11 services scientifiques communs et 7 services administratifs et techniques.
- **R**essources **I**nformatiques et **C**alcul **S**cientifique.
- Service RICS composé de 2,7 ETP pour une structure de 11000m².
- Responsable de mon clavier/souris mais aussi ...



Du datacenter qui revient vers le futur (2013 - 2019)



- Réseau backbone 10G HP IRF réparti sur 3 bâtiments (20 SWs, 20 APs, 2 FWs, 1 LOGs). 600 prises réseaux.
- Parc utilisateurs en majorité sous Microsoft, mais avec des résistants sous Linux et Mac.
- Parc scientifique = problématique vieux systèmes (XP, 7, Redhat).
- Parc serveurs, 60 machines physiques.
- Parc de 32 VMs mixé entre KVM et LXC (performance vs windows).
- 3 clusters PCA-HA Proxmox v6.
- 2 clusters HPC-OAR (centos, debian), 492 cores et 4To ram.
- 2 stockages centralisés ZFS (data, VMs, mails, ...)
- Volumétrie 0,5 Po

- Centraliser et sécuriser les identifiants de l'utilisateur (2FA).
- Garantir l'identité de l'utilisateur dans la structure d'accueil, et propager ses habilitations dans le SI.
- Déployer une politique globale commune à l'ensemble des utilisateurs (rôle, complexité, historique, ...).
- Fédérer les identités pour offrir des services à l'extérieur de la structure. (nomade : vpn, wifi).
- Séquestrer (pas les utilisateurs), le mot de passe « Administrateur local », les clés de recouvrement.
- Simplifier la gestion des données de l'utilisateur via un GUI web (mot de passe, bureau, téléphone, ...).



Oui mais attention ...

Inconvénients

- Un accès unique = accès à de nombreuses ressources une fois l'utilisateur authentifié.
- les pertes peuvent être lourdes si une personne mal intentionnée accède au SI.
- il faut ajouter un second facteur ; cartes à puce, certificat, clé de sécurité physique.
- il faut garantir et sécuriser le système assurant ce rôle.

Avantages

- centralisation des systèmes d'authentification.
- gain de temps considérable, un seul mot de passe pour l'ensemble du SI.
- renforcement de la sécurité des applications SI en évitant la multiplication des sources d'authentification (bdd dans le apps web, contrôle d'accès, mfp).

Nous avons retenu le couple SaMBa et LDAP.

- 2012 - Migration de /etc/password à OpenLDAP
(cf : <https://homepages.lcc-toulouse.fr/colombet/samba-deployer-une-infrastructure-active-director/#chapitre2-1-6>)
- 2013 - Migration de OpenLDAP à SaMBA 4 version compilé 4.x.x.
(cf : <https://homepages.lcc-toulouse.fr/colombet/samba-deployer-une-infrastructure-active-director/#chapitre2-2-3-1>)
- 2013 - Intégration des solutions SOGo et Guacamole dans les schémas
(Agenda type ressources : <https://sogo.nu/> & SSH, VNC, RDP par users : <https://guacamole.apache.org/>)
- 2013 - Réplication des ADs vers OpenLDAP via LSCProject.
(cf : <https://lsc-project.org/documentation/howto/activedirectory>)
- 2014 - Migration sur SaMBa package Debian 8 - Jessie.
(cf : <https://homepages.lcc-toulouse.fr/colombet/samba-deployer-une-infrastructure-active-director/#chapitre3-2-2>)
- 2016 - Migration sur SaMBA package Debian 9 - Stretch.
- 2019 - Bugs Debian 10 - Buster, migration en attente.



LSC est un connecteur libre permettant de synchroniser les identités entre un annuaire LDAP et n'importe quelle source de données, y compris toute base de données avec un connecteur JDBC, un autre serveur LDAP, des fichiers plats, ... Depuis debian 9, lsc est disponible en 2.1.4 via apt-get install lsc

cf : <https://lsc-project.org/>

Les connexions SRC / DST

```
<?xml version="1.0" ?>
<lsc xmlns="http://lsc-project.org/XSD/lsc-core-2.1.\
xsd" revision="0">
  <connections>
    <ldapConnection>
      <name>ad-src-conn</name>
      <url>ldap://x.x.x.x:389/DC=formation,DC=fr</url>
      <username>CN=admin,CN=Users,DC=formation,DC=fr\
</username>
      <password>mypassword</password>
      ...
    <name>ldap-dst-conn</name>
    <url>ldap://x.x.x.x:389/DC=formation,DC=fr</url>
  </ldapConnection>
</connections>
```


Projet n°1 : SaMBa4 & LSC Project - Part2

Les taches

```
<tasks><task>
<name>ADSyncTask</name>
<bean>org.lsc.beans.SimpleBean</bean>
<ldapSourceService>
  <name>ad-src-service</name>
  <connection reference="ad-src-conn" />
  <baseDn>CN=Users,DC=formation,DC=fr</baseDn>
  <pivotAttributes><string>sAMAccountName</string></pivotAttributes>
  <fetchedExceptions>
    <string>sAMAccountName</string>
    <string>jpegPhoto</string>
  </fetchedExceptions>
  <getAllFilter>(&!(objectClass=user)!(sAMAccountName=admin))</getAllFilter>
  <getOneFilter>(&(objectClass=user)(sAMAccountName={sAMAccountName}))</getOneFilter>
</ldapSourceService>
<ldapDestinationService>
  <name>ldap-dst-service</name>
  <connection reference="ldap-dst-conn" />
  <baseDn>ou=users,dc=formation,dc=fr</baseDn>
  <pivotAttributes><string>uid</string></pivotAttributes>
  <fetchedExceptions>
    <string>uid</string>
    <string>jpegPhoto</string>
  </fetchedExceptions>
  <getAllFilter>(objectClass=inetOrgPerson)</getAllFilter>
  <getOneFilter>(&(objectClass=inetOrgPerson)(uid={sAMAccountName}))</getOneFilter>
</ldapDestinationService>
</task></tasks>
```

Projet n°2 : SaMBa4 & Bitlocker

```
Administrateur : Invite de commandes

C:\>manage-bde -status
Chiffrement de lecteur BitLocker : outil de configuration version 2.0
Copyright (C) 2013 Microsoft Corporation. Tous droits réservés.

Volumes de disques pouvant être protégés avec le
Chiffrement de lecteur BitLocker :
Volume C: [ ]
[Volume du système d'exploitation]

Taille : 231,01 Go
Version de BitLocker : 2.0
État de la conversion : Espace utilisé uniquement chiffré
Pourcentage chiffré : 100,0%
Méthode de chiffrement : XTS-AES 256
État de la protection : Protection activée
État du verrouillage : Déverrouillé
Champ d'identification : Inconnu
Protecteurs de clés :
    TPM
    Mot de passe numérique

C:\>manage-bde -on C: -RecoveryPassword -RecoveryKey F:\
```

Vérification depuis DCs

```
# ldbsearch -H /var/lib/samba/private/sam.ldb \
'(objectclass=msFVE-RecoveryInformation)' \
msFVE-RecoveryPassword

# record 1
dn: CN=2019-07-17T10:23:09\+01:00{B71A5BB7-5DD9-\
558C-7685-91213799BD55},CN=MON-MACOS,OU=monserv\
ice,DC=formation,DC=fr
msFVE-RecoveryPassword: 123456-7891011-121314-15\
1617-181920-212223-242526-27282

# Referral
ref: ldap://formation.fr/CN=Configuration,DC=for\
mation,DC=fr
# returned 999 records
# 998 entries
# 1 referrals
```

cf : <https://homepages.lcc-toulouse.fr/colombet/bitlocker>



Projet n°3 : SaMBa4 & OpenSSH

L'authentification par clé publique a longtemps été considérée comme l'une des méthodes les plus sûres. Cependant, l'utilisation de la même paire de clés pour plus d'une machine peut poser des risques de sécurité, surtout si cette clé n'est pas sécurisée par une phrase de chiffrement. Pour cette raison, il est possible d'utiliser Samba4 comme magasin de clés publiques SSH.

cf : <https://homepages.lcc-toulouse.fr/colombet/ad-keypub-ssh>

Création dans le schéma AD de :

- l'attribut `sshPublicKeys`
- la classe `ldapPublicKey`

Fichier `/etc/ssh/sshd_config`

```
PubkeyAuthentication yes
#AuthorizedKeysCommand fetchSSHKeysFromLDAP
AuthorizedKeysCommand ssh-ldap-publickey-wrapper
AuthorizedKeysCommandUser nobody
```

Script `fetchSSHKeysFromLDAP`

```
ldapsearch -h dclad.formation.fr -b 'CN=Users,DC=formation,DC=fr' '(sAMAccountName='${1%*}')' -D 'CN=Administrateur,CN=Users,DC=formation,DC=fr' -w 'Pa$$w0rd' 'sshPublicKey' | sed -n '/^/{H;d}; sshPublicKey:/x;$g;s/\n *///g;s/sshPublicKey: //g'
```



Projet n°4 : SaMBa4 & LAPS

LAPS (Local Administrator Password Support)

- Déploiement du client LAPS via WAPT
- Création d'une GPO pour LAPS

Modification du schema pour LAPS

```
# ldapadd -D "CN=Administrator,CN=Users,DC=formation,\
DC=fr" -W -p 389 -h 127.0.0.1 -x -ZZ -f laps.ldif
Enter LDAP Password:
adding new entry "CN=ms-MCS-AdmPwd,CN=Schema,cn=confi\
guration,DC=formation,DC=fr"
ldap_add: Server is unwilling to perform (53)
additional info: 00002035: schema_data_add: updates \
are not allowed: reject request

# ldbmodify -H /var/lib/samba/private/sam.ldb \
/root/laps.ldif --option="dsdb:schema update \
allowed=true"
```

cf : <https://homepages.lcc-toulouse.fr/colombet/laps>

LAPS UI

ComputerName
clientwin10

Password
0vp0]D9FQec#73

Password expires
11/11/2019 15:15:17

New expiration time
samedi 12 octobre 2019 16:22:33



Projet n°5 : SaMBa4 & Annuaire dynamique

SECURITE

WEBMAIL

- Accès international
- Formation

• Campus :

- Accès internet Remip 2000
- Contrôle d'accès
- Sauvegarde externe (PRA)
- Monitoring DR14

• Services applicatifs :

- Authentification unique SSO
- Wifi LCC, Invités et Eduroam
- Accès extérieur VPN
- Hébergements web institutionnel
- Applications métiers
- Solutions collaboratives

• **Responsable/Manager**

Jérôme COLOMBET
ITA

• **Membres/Members**

Fabrice CANDAU
ITA

Philippe MANFRE
ITA

David PNYL
ITA

PHPimport JPEGPhoto

```
//conversion image -> binaire
function encode_image($img,$taille)
...
//connexion base LDAP
$ds = @ldap_connect($ldap_host, $ldap_port)
$ldap_bind = @ldap_bind($ds,$ldap_filter,$pwd)
$base = 'CN=Users,DC=formation,DC=fr';
$search = ldap_search($ds,$base,$filter) or die('recher
$res = ldap_get_entries($ds,$search) or die('resultat no
...
//ajout au ldif de l'image
$f = fopen("/tmp/ldap-jpegphoto.ldif","w");
$img = "jpegphoto/silhouette.jpg";
$ing = "jpegPhoto/membres/".$nom."".$prenom.".jpg";
fputs($f,get_string_modify($res,$i,jpegphoto) . $champs.
fputs($f,$champs . ":: " . encode_image($img,strlen($cha
fputs($f,"-\n");
...
//integration du fichier ldif à AD
/usr/bin/ldbmodify -H /var/lib/samba/private/sam.ldb
/tmp/ldap-jpegphoto.ldif && rm /tmp/ldap-jpegphoto.ldif
```

SaMBA4 en production au LCC

● SYSTÈMES D'EXPLOITATIONS

- G4D webGUI personnel
- Authentification LCC
- OpenSSH pubkey
- Push contrôle d'accès
- Guacamole RDP
- CAS Jasig
- Openldap LSCProject
- Messagerie collaborative SOGo
- Organigramme dynamique
- Sympa listes de diffusion imbriquées

● RÉSEAUX

- Freeradius Eduroam, LCC
- Gespape impression unifié
- Packetfence
- VPN IPsec, OpenVPN

● STOCKAGES

- Nexenta – ZFS
- Nextcloud
- Borg+Samba ReadOnly





jerome.colombet@lcc-toulouse.fr

<https://homepages.lcc-toulouse.fr/colombet/>

