Matthias Leclair

Tutoriel

Mise en œuvre d'ALCASAR en relation avec un serveur Active Directory

Sommaire

Infrastructure utilisée:

Durant ce tutoriel, l'infrastructure utilisée est la suivante :

L'infrastructure physique est composée :

- 1 PC connecté en Ethernet à une box ADSL.

L'infrastructure virtuelle est composée :

- 1 VM ALCASAR.
- 1VM Windows serveur 2012 R2.
- 1VM Client Windows.
- 1VM Client Linux.

Représentation de la topologie du réseau :

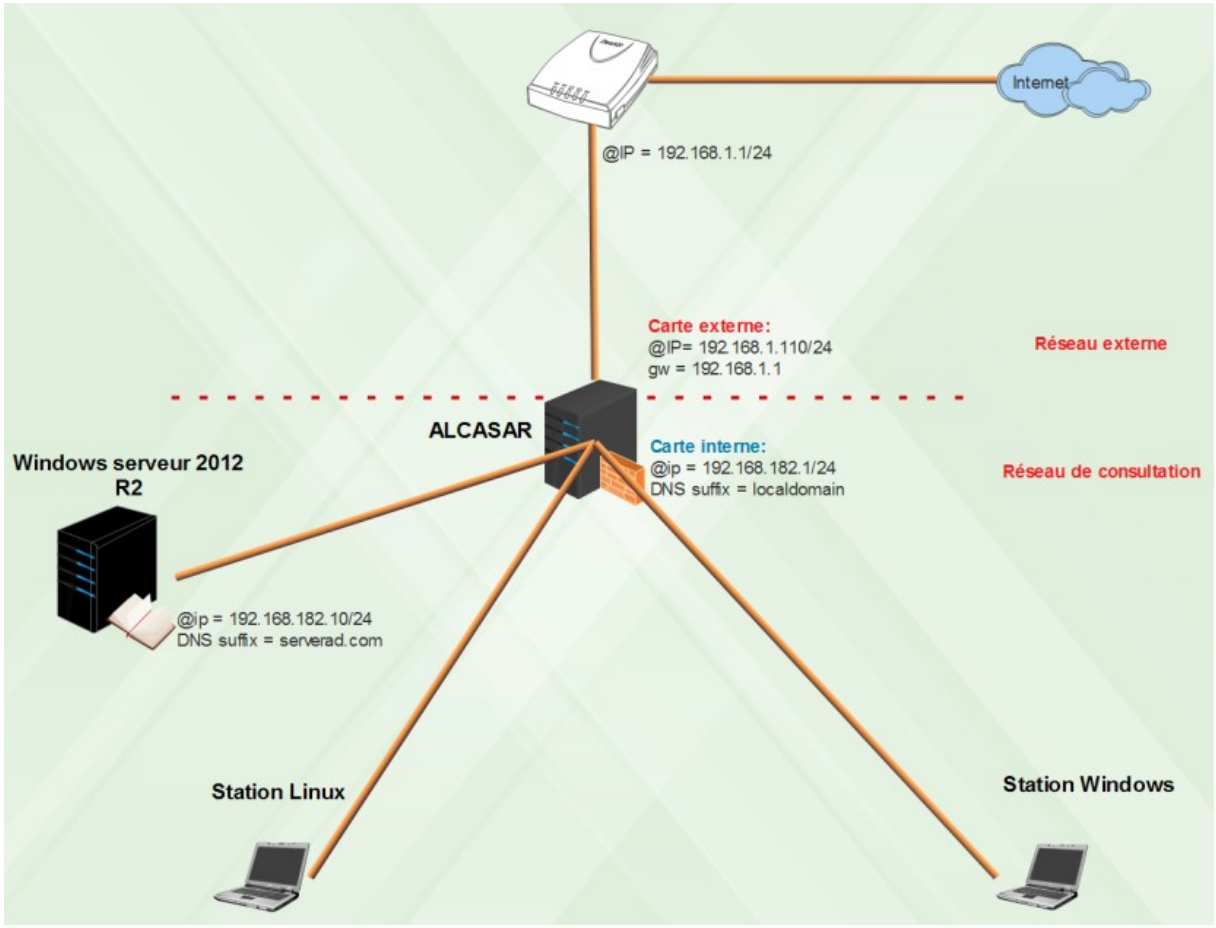

Figure 1 : Topologie réseau

Différentes étapes de mise en œuvre :

Installation d'ALCASAR :

La première étape fut l'installation d'une VM avec le système Mageia 4. La version d'ALCASAR utilisée est la 2.9.1. Pour cela, suivre la documentation d'installation.

Durant l'installation j'ai nommé l'organisme « protiste ».
Le plan d'adressage est le suivant :

Carte externe :
- @IP : 192.168.1.110/24
- GW : 192.168.1.1

Carte internet (réseau de consultation) :
- @IP : 192.168.182.1

Figure 2 : Page d'accueil pour identification

Installation de Windows serveur 2012 R2 :

Une fois l'installation du système effectuée, on accède aux différents services via l'interface de gestion. La capture ci-dessous correspond à cette interface.

C'est ici qu'on ajoutera les serveurs DNS, A.D et DHCP. Pour cela il suffit de sélectionner l'onglet « Manage », puis « Add Roles and Features », choisir le service à ajouter, et se laisser guider.

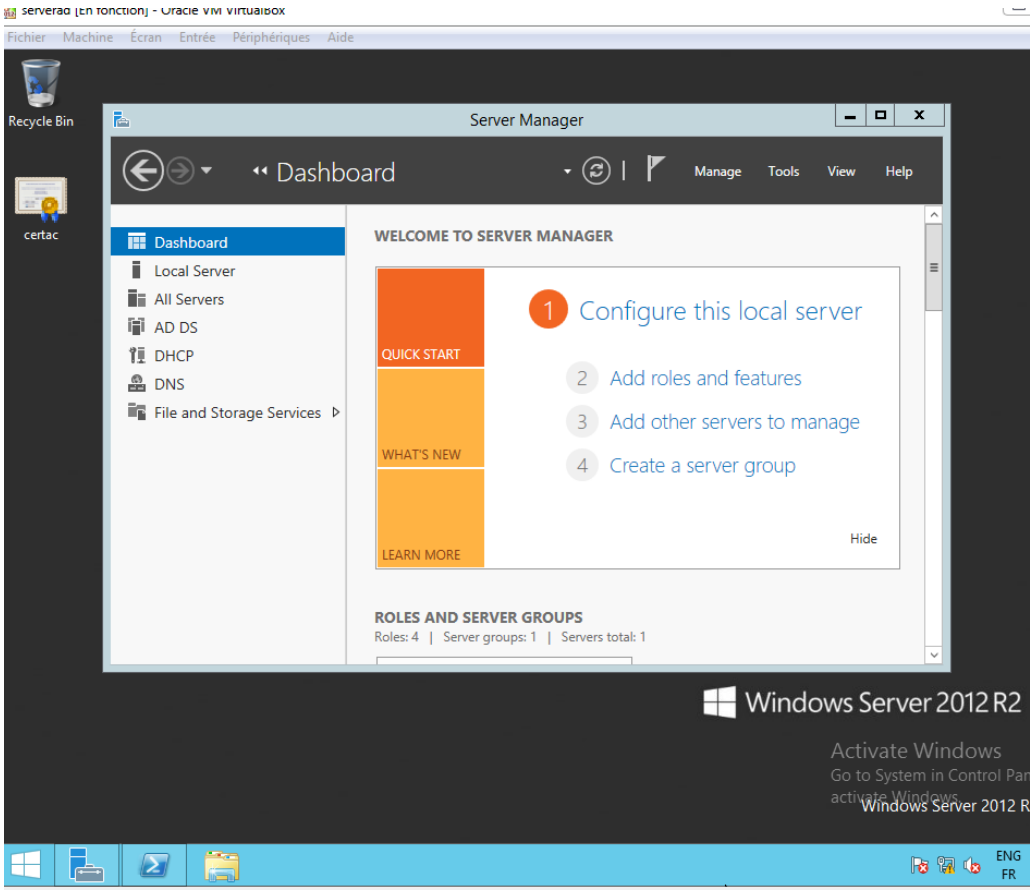

Figure 3 : Server Manager Windows 2012

Création de serveur DNS :

Le nom de domaine que j'ai choisi est « *serverad.com* ». Une fois créé, j'ai rajouté l'hôte alcasar en précisant son adresse IP *192.168.182.1* comme on peut le voir sur la capture ci-dessous.

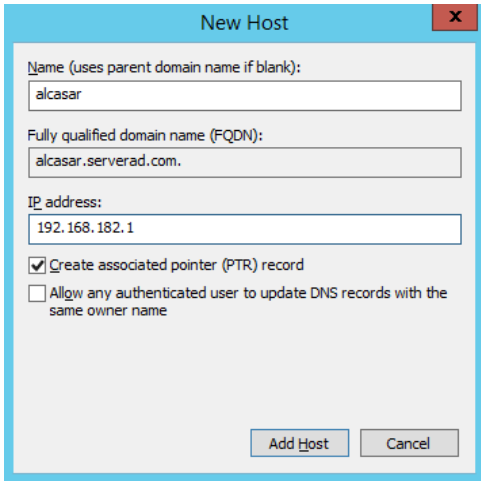

Figure 4: Création d'un nouvel hôte

Lorsque les utilisateurs consulteront Internet, le serveur DNS requêté sera celui d'ALCASAR, par conséquent il est nécessaire d'effectuer une redirection vers le serveur DNS d'ALCASAR.

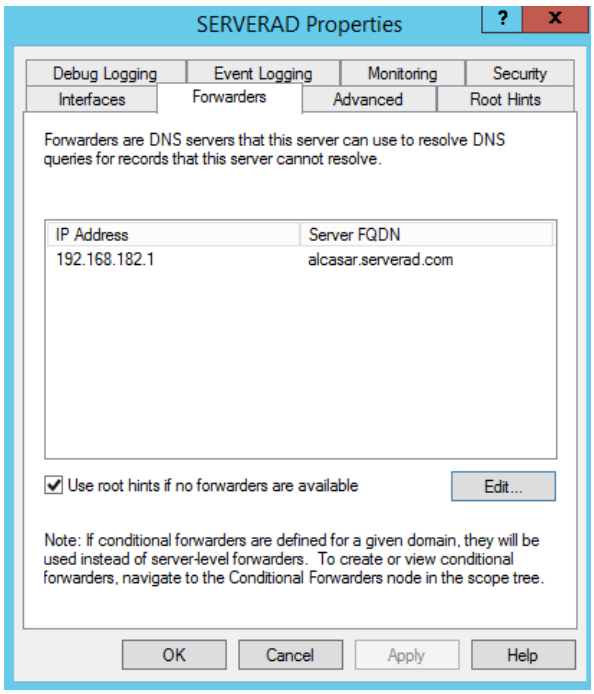

Figure 6 : DNS Forward

Comme expliqué dans la documentation d'exploitation d'ALCASAR, dans une architecture A.D, les stations Windows sont liées à leur contrôleur de domaine et doivent s'adresser à la fois au DNS Windows pour les services Windows, et aux DNS d'ALCASAR pour l'accès Internet.
Il faut donc configurer le DNS d'ALCASAR pour rediriger vers le contrôleur de domaine les requêtes liées aux services Windows.

Il faut donc renseigner les paramètres suivants dans le fichier /usr/local/etc/alcasar.conf :
INT_DNS_DOMAIN=serverad.com
INT_DNS_IP=192.168.182.10
INT_DNS_ACTIVE=on

Puis appliquer la configuration : alcasar-conf.sh --apply
Les différentes instances de DNSMASQ (serveurs DNS utilisés par ALCASAR) seront redémarrées à l'issue.
Il est possible de vérifier que les paramètres DNS ont été pris en compte :

- dans le fichier /usr/local/etc/alcasar-dns-name, on doit retrouver la directive server=/serverad.com/192.168.182.10
- dans les fichiers /etc/dnsmasq.conf{dnsmasq-blacklist.conf, dnsmasq-whitelist.conf et dnsmasq-blackhole.conf}, on doit avoir le paramètre *filterwin2k* commenté par un #

Changement de serveur DHCP :

Le changement de serveur DHCP consiste en deux étapes. La première est de désactiver le service DHCP d'ALCASAR, la seconde est d'activer et de configurer le service DHCP du serveur Windows.

Désactivation du service DHCP d'ALCASAR :

Le serveur Windows gérant les utilisateurs, il peut être intéressant de désactiver le service DHCP d'ALCASAR au profit de celui du serveur Windows.

Le service DHCP d'ALCASAR se désactive depuis l'interface de gestion, comme le montre la capture ci-dessous. L'interface de gestion est accessible à l'adresse https://alcasar/acc depuis une station de consultation. Le login utilisé étant celui créé lors de la dernière étape de l'installation d'ALCASAR.
La capture ci-dessous correspond à cette interface.

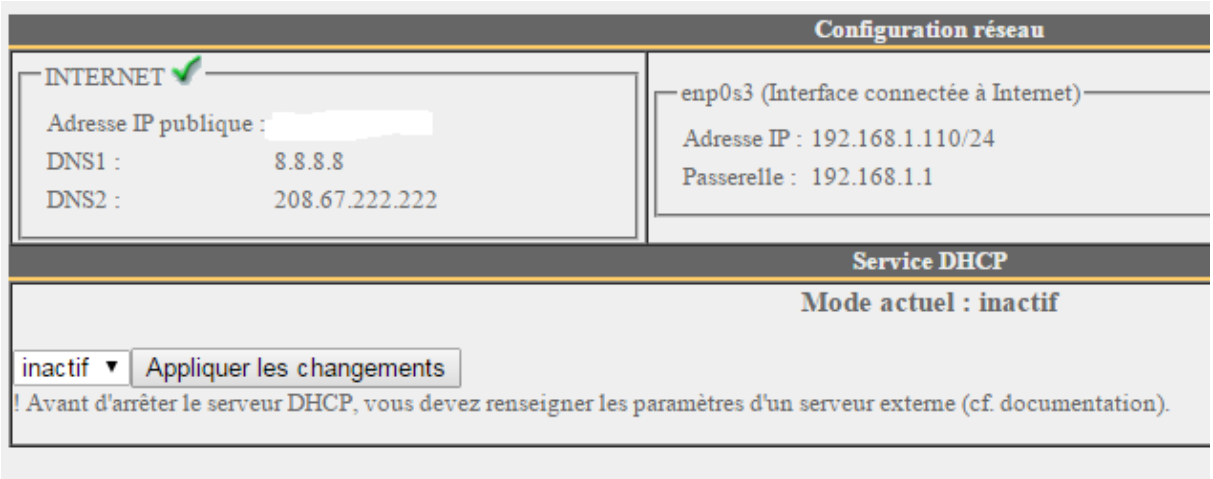

Figure 7 : Désactivation du service DHCP d'ALCASAR

Il faut ensuite modifier le fichier de conf d'ALCASAR se trouvant à */usr/local/etc/alcasar.conf*. Les 3 lignes à modifier sont :

EXT_DHCP= < @IP serveur DHCP externe>
RELAY_DHCP= < @IP ALCASAR de la carte réseau du côté du serveur DHCP externe>
RELAY_DHCP_PORT= < port à utiliser, 67 par défaut>

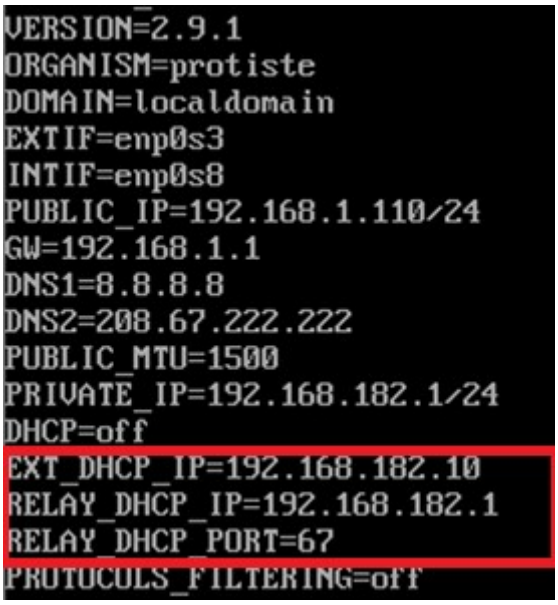

Figure 8 : Fichier de configuration d'ALCASAR

Mise en service du serveur DHCP Windows :

L'installation du service consiste à configurer différents paramètres. Le premier est la plage d'adresses pouvant être affectées aux différentes machines. Cette dernière correspond au plan d'adressage choisi préalablement pour lors de l'installation d'ALCASAR.

- Adresses IP : Elles doivent commencer au minimum par *192.168.182.3*, deux premières étant réservées par ALCASAR.
- Route par défaut : ALCASAR *192.168.182.1*
- DNS : *192.168.182.1, 192.168.182.10*
- Suffixe DNS d'ALCASAR et Windows: *localdomain, serverad.com*

La capture d'écran ci-dessous résume les différentes options affectées aux utilisateurs.

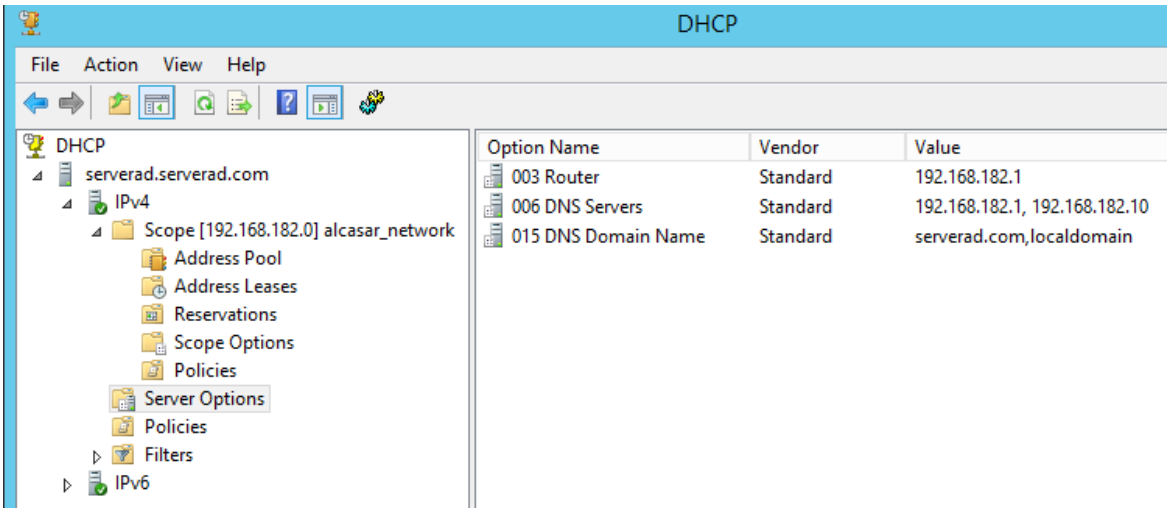

Figure 9 : Serveur DHCP et options

Gestion des utilisateurs Windows et configuration d'ALCASAR pour se connecter au serveur Active Directory :

Afin qu'ALCASAR puisse authentifier les utilisateurs du serveur Active Directory, il est nécessaire qu'il puisse consulter l'annuaire des utilisateurs. Pour cela, on va créer un utilisateur auquel on délègue le droit « *All read properties* » comment on peut le voir sur les deux captures ci-dessous.

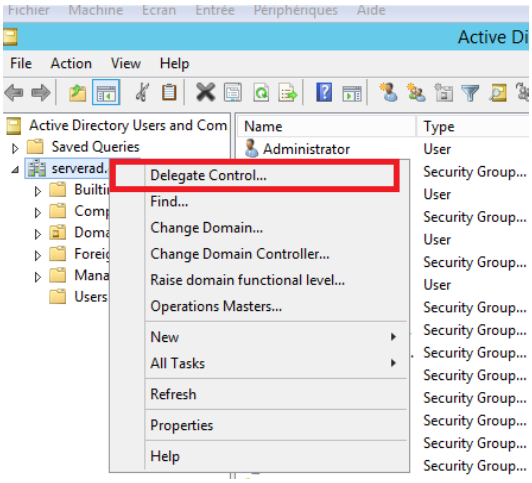

Figure 10: Délégation de contrôle 1

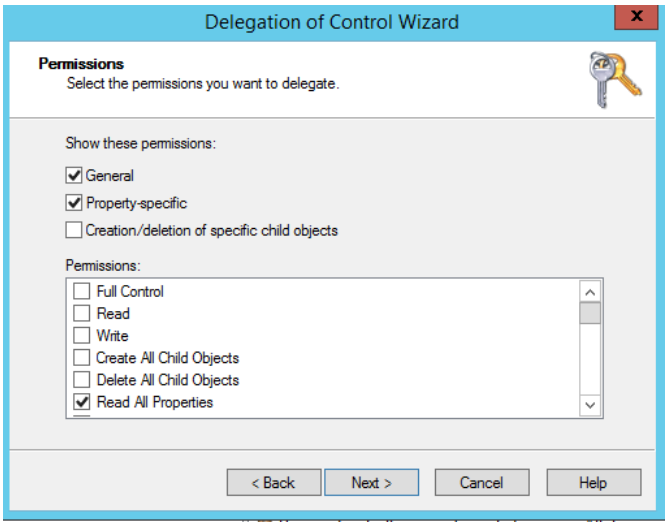

Figure 11: Délégation de contrôle 2

Par la suite, on va remplir un formulaire sur la page de gestion d'ALCASAR afin de renseigner les différents paramètres nécessaire l'authentification A.D des utilisateurs.
Ces paramètres sont :

- L'adresse du serveur A.D.
- Le DN (Distinguished Name) de la base de recherche contenant la localisation des informations des utilisateurs dans l'annuaire.
- L'identifiant LDAP, correspondant au mot clé d'identification de connexion qu'on va rechercher (sAMAcountName pour un A.D.)
- on peut rajouter des filtres de recherche pour affiner les objets utilisateurs
- Le FQDN du compte qu'utilisera ALCASAR afin de se connecter au serveur A.D.
- Le mot de passe de ce compte.

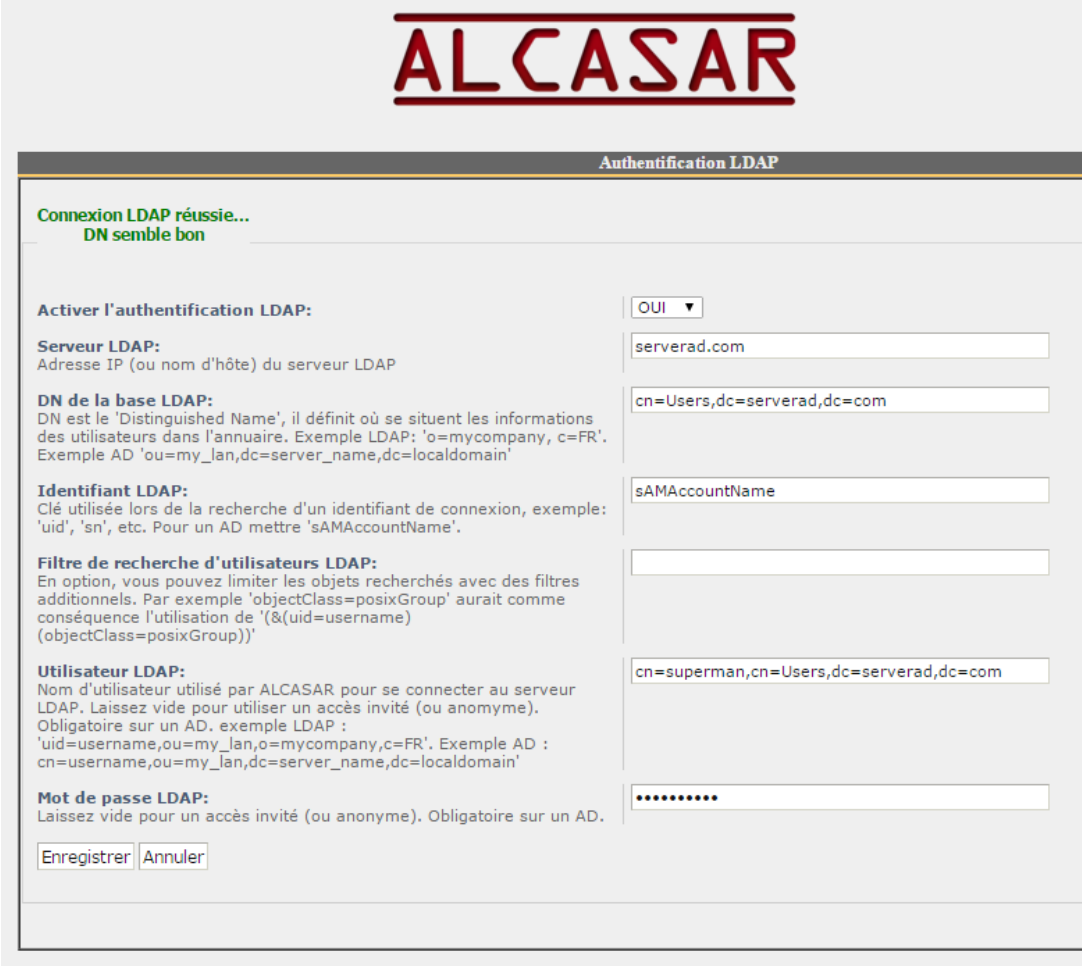

Figure 12 : Formulaire de connexion LDAP

NB : Il est très facile d'obtenir ces informations en utilisant la commande *dsquery*, comme la montre la capture ci-dessous :

```
PS C:\Users\Administrator> dsquery group -name Users
"CN=Users,CN=Builtin,DC=serverad,DC=com"
PS C:\Users\Administrator> dsquery user -name superman
"CN=superman,CN=Users,DC=serverad,DC=com"
```

Figure 10 : Commande dsquery

Résultats :

Il est possible de vérifier le bon fonctionnement de l'authentification d'un utilisateur en utilisant Wireshark. Comme le montre la capture ci-dessous, ALCASAR va se connecter au serveur A.D avec le compte spécifiquement créé sur le serveur Windows (superman).

Une fois l'authentification de ce dernier réussie, il va faire une recherche de l'utilisateur renseigné dans l'annuaire A.D pour déterminer si le couple *login/password* de l'utilisateur est correct. Le serveur renvoie ensuite *success* ou *fail*.

```
14 0.045920   192.168.182.1    192.168.182.10   LDAP   129 bindRequest(1) "cn=superman,cn=Users,dc=serverad,dc=com" simple
15 0.046792   192.168.182.10   192.168.182.1    LDAP    88 bindResponse(1) success
16 0.047081   192.168.182.1    192.168.182.10   TCP     66 59564 → 389 [ACK] Seq=64 Ack=23 Win=29312 Len=0 TSval=33278229 TSecr…
17 0.047179   192.168.182.1    192.168.182.10   LDAP  10…  searchRequest(2) "cn=Users,dc=serverad,dc=com" wholeSubtree
18 0.047462   192.168.182.10   192.168.182.1    LDAP   146 searchResEntry(2) "CN=john,CN=Users,DC=serverad,DC=com"  | searchRes…
19 0.048003   192.168.182.1    192.168.182.10   TCP     74 59565 → 389 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3…
20 0.048034   192.168.182.10   192.168.182.1    TCP     74 389 → 59565 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SA…
21 0.048344   192.168.182.1    192.168.182.10   TCP     66 59565 → 389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=33278230 TSecr=3…
22 0.048481   192.168.182.1    192.168.182.10   LDAP   130 bindRequest(1) "CN=john,CN=Users,DC=serverad,DC=com" simple
23 0.049159   192.168.182.10   192.168.182.1    LDAP    88 bindResponse(1) success
```

Figure 13 : Capture de trafic Wireshark de l'authentification d'un utilisateur.

L'utilisateur est alors correctement authentifié :

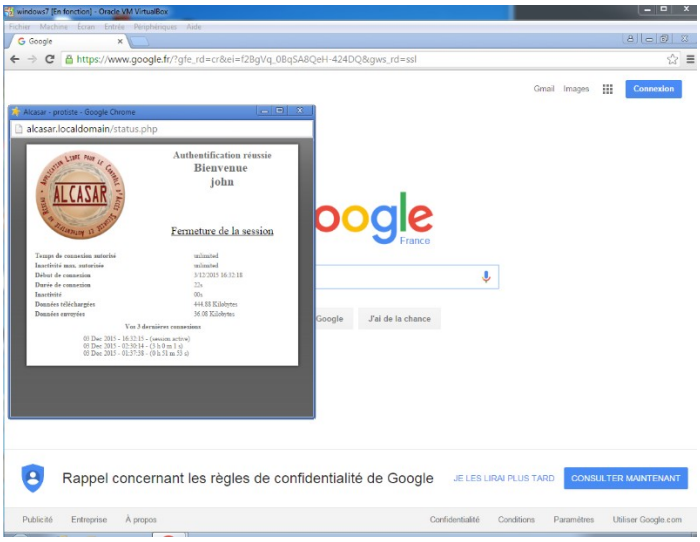

Figure 14 : Authentification réussie

L'authentification via un annuaire externe est correctement prise en charge par ALCASAR. Il est alors possible d'appliquer des règles similaires à celles proposées par ALCASAR concernant les utilisateurs. Sur Windows Server cela correspond à la mise en place de GPO (Group Policies), et notamment la QoS policy, permettant le contrôle de trafic réseau.

Attention ! Par défaut, un utilisateur authentifié sans groupe dispose du profil des attributs du groupe ldap (à créer dans ALCASAR). Un utilisateur authentifié par un annuaire est donc lié à ce profil 'ldap'. Pour attribuer des profils différents à des utilisateurs d'un annuaire, il faut également créer ces utilisateurs au login identique (et avec génération de mot de passe aléatoire pour ne pas laisser un utilisateur à l'identifiant prédictif sans mot de passe) et les associer à des groupes par le biais de l'interface de gestion d'ALCASAR.

Une évolution du produit permettra de récupérer les groupes gérés directement dans l'annuaire afin de supprimer cette double saisies.

Bibliographie

Documantation d’installation d’ALCASAR :
http://www.alcasar.net/fr/telechargement?func=fileinfo&id=39

Documentation d’exploitation d’ALCASAR :
http://www.alcasar.net/fr/telechargement?func=fileinfo&id=40

Tutoriel pour Dsquery :
https://www.youtube.com/watch?v=3p28KG7sBeQ

Diverses documentations pour windows server 2012 :
https://technet.microsoft.com/en-us/library/dd448614.aspx