



Tutoriel ALCASAR

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

Table des matières

Intégration dans une architecture complexe (A.D., DHCP externe, LDAP).....	2
Gestion du DNS Windows.....	2
Utilisation d'un serveur DHCP Externe.....	3
Integration in a complex architecture (AD, external DHCP, LDAP).....	4
Managing Windows DNS.....	4
Using an External DHCP Server.....	5
Installation d'ALCASAR.....	7
Installation d'une machine de consultation Linux.....	7
Installation de Windows serveur 2016.....	8
Création du serveur DNS.....	8
Changement de serveur DHCP.....	9
Désactivation du service DHCP d'ALCASAR.....	10
Mise en service du serveur DHCP Windows.....	11
Gestion des utilisateurs Windows et configuration d'ALCASAR pour se connecter au serveur Active Directory.....	12
Bibliographie.....	14

Projet : ALCASAR	Auteur : Alcasar Team
Objet : Installation	Version : 4
Mots clés : portail captif, contrôle d'accès au réseau (Network Acces Control - NAC), imputabilité, traçabilité, authentification, contrôle parental, filtrage	Date : février 2022

Intégration dans une architecture complexe (A.D., DHCP externe, LDAP)

ALCASAR peut s'intégrer dans une architecture existante comportant un domaine Windows, un serveur DHCP et un serveur d'annuaire LDAP ou A.D..

Gestion du DNS Windows

Dans une architecture A.D. les stations Windows sont liées à leur contrôleur de domaine. Celles-ci doivent s'adresser à la fois au DNS de leur contrôleur (le serveur AD) pour les résolutions propres aux services Windows (résolution de services) et au DNS d'ALCASAR pour l'accès à Internet (résolution de noms de domaine Internet). Une solution consiste à configurer le DNS d'ALCASAR afin qu'il redirige vers le contrôleur de domaine les requêtes le concernant. De cette manière, les équipements de consultation sont configurés avec ALCASAR comme unique DNS.

Sur ALCASAR, deux solutions sont possibles.

La première consiste à modifier les lignes suivantes dans le fichier `/usr/local/etc/alcasar.conf` :

```
INT_DNS_DOMAIN=<your_domain>
INT_DNS_IP=<@IP_domain_server>
INT_DNS_ACTIVE=on
```

Par exemple :

```
INT_DNS_DOMAIN=serverad.com
INT_DNS_IP=192.168.182.10
INT_DNS_ACTIVE=on
```

Puis de relancer le script pour que vos modifications soient appliquées (« `alcasar-conf.sh --apply` »)


La deuxième méthode consiste à créer un fichier de forwarder DNS `/etc/unbound/conf.d/common/local-forward` puis d'ajouter les informations suivantes (se baser sur le modèle du fichier `custom.conf`).

```
server:
  local-zone: "<your_domain>." transparent
forward-zone:
  name: "<your_domain>."
  forward-addr: <@IP_domain_server>
```

Par exemple :

```
server:
  local-zone: "serverad.com." transparent
forward-zone:
  name: "serverad.com."
  forward-addr: 192.168.182.10
```

Relancer le service unbound pour que vos modifications soient appliquées (« `service unbound restart` »).

 **Rappel** : Les stations de consultation (en adressage fixe ou en DHCP) intégrées dans un domaine Windows doivent disposer du suffixe principal lié au domaine Windows ainsi que du suffixe '.localdomain'.

Utilisation d'un serveur DHCP Externe

L'utilisation d'un serveur DHCP externe nécessite d'une part qu'ALCASAR ne fournisse plus les paramètres réseau, mais que ces derniers soient fournis par un serveur DHCP répondant aux besoins impérieux d'ALCASAR.

Pour forcer l'offre d'adresses IP par un serveur DHCP externe, ALCASAR va agir comme agent relais vers celui-ci. Il faut alors arrêter le serveur DHCP d'ALCASAR (via l'interface de gestion/Système/Réseau : Mode Sans DHCP) et renseigner les variables pour gérer le serveur externe (fichier de configuration `/usr/local/etc/alcasar.conf`) :

```
EXT_DHCP_IP=<@IP_srv_externe>
RELAY_DHCP_IP=<@IP_interne_ALCASAR>
RELAY_DHCP_PORT=<port de relais vers le serveur DHCP externe> : (par défaut 67)
```

Le serveur DHCP externe doit être configuré pour fournir aux stations :

- une plage d'@IP correspondant à la plage autorisée par ALCASAR (par défaut 192.168.182.3-254/24) ;
Attention : depuis la version 2.7, le portail réserve l'adresse suivante celle à sa patte interne : 192.168.182.1 ---> [l'@IP](#) 192.168.182.2 est également réservée pour le portail, mais non visible ;
- une adresse de passerelle correspondant à l'adresse IP interne d'ALCASAR (par défaut 192.168.182.1) ;
- le suffixe DNS « localdomain » ;
- l'@IP du serveur DNS --> l'adresse IP interne d'ALCASAR (par défaut 192.168.182.1) ;
- l'@IP du serveur de temps (NTP) --> l'adresse IP interne d'ALCASAR (par défaut 192.168.182.1) ou celle du contrôleur de domaine (pour éviter les dérives temporelles, veiller d'ailleurs à positionner la mise à l'heure automatique de celui-ci sur un serveur identifié de l'Internet ou plus simplement sur le portail ALCASAR).

Integration in a complex architecture (AD, external DHCP, LDAP)

ALCASAR can be installed in an existing network with a Windows domain, a DHCP server and an external directory for the authentication process (LDAP or AD).

Managing Windows DNS

If your existing environment already has Active Directory enabled, then, Windows computers of your domain controller must request the DNS of this controller for specific resolutions of the domain and they must request ALCASAR for Internet access. One solution is to configure the ALCASAR DNS so it redirects to the domain controller the DNS queries concerning resolution of the domain. In this way, devices are configured with a unique DNS : ALCASAR.

On ALCASAR, there are two solutions.

The first one is to modify the following lines in the file `/usr/local/etc/alcasar.conf` :

```
INT_DNS_DOMAIN=<your_domain>
INT_DNS_IP=<@IP_domain_server>
INT_DNS_ACTIVE=on
```

For example :

```
INT_DNS_DOMAIN=serverad.com
INT_DNS_IP=192.168.182.10
INT_DNS_ACTIVE=on
```

Don't forget to run the script to apply the changes (« `alcasar-conf.sh -apply` »)


The second one is to create a new file in `/etc/unbound/conf.d/common/local-forward` and then fill it in based on `custom.conf`

```
server:
  local-zone: "<your_domain>." transparent
forward-zone:
  name: "<your_domain>."
  forward-addr: <@IP_domain_server>
```

For example :

```
server:
  local-zone: "serverad.com." transparent
forward-zone:
  name: "serverad.com."
  forward-addr: 192.168.182.10
```

Don't forget to restart unbound to apply de changes (« `service unbound restart` »).

 **Reminder** : The computers (whether in static IP address mode or in DHCP mode) integrated into a Windows domain must have their primary DNS suffix configured with the Windows domain name and in addition with the suffix `'.localdomain'`.

Using an External DHCP Server

With an external DHCP server, ALCASAR must not assign network settings anymore, but this task must be is carried out by the external DHCP server.

In order to do this, ALCASAR will act as a relay agent to enable assignment of IP addresses by the DHCP server.

It is necessary to stop the ALCASAR DHCP server (in the ACC: System/Network: No DHCP mode) and to modify the following variables to manage the external server (configuration file «[usr/local/etc/alcasar.conf](#) »):

```
EXT_DHCP_IP=<@IP_srv_external>  
RELAY_DHCP_IP=<@IP_internal_ALCASAR>  
RELAY_DHCP_PORT=<relay port to the external DHCP server> : (default 67)
```

The external DHCP server must be configured to provide to devices:

- a range of IP @ corresponding to the range allowed by ALCASAR (default 192.168.182.3 to 254/24)
Warning: ALCASAR keep for itself the following address for its internal interface: 192.168.182.1 and 192.168.182.2.
- a gateway address corresponding to the internal IP address of ALCASAR (by default 192.168.182.1);
- the DNS suffix "localdomain";
- the IP address of the DNS server -> the internal IP address of ALCASAR (default 192.168.182.1);
- the IP address of the time server (NTP) -> the internal IP address of ALCASAR (default 192.168.182.1) or the domain controller (to avoid temporal drifts, synchronise the server clock with a trusted NTP server on the internet or with the ALCASAR server).

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

- Une partie physique composée d'un PC connecté à Internet
- Une partie virtuelle composée des éléments suivants :
 - 1 VM ALCASAR.
 - 1VM Windows serveur 2012 R2.
 - 1VM Client Windows.
 - 1VM Client Linux.

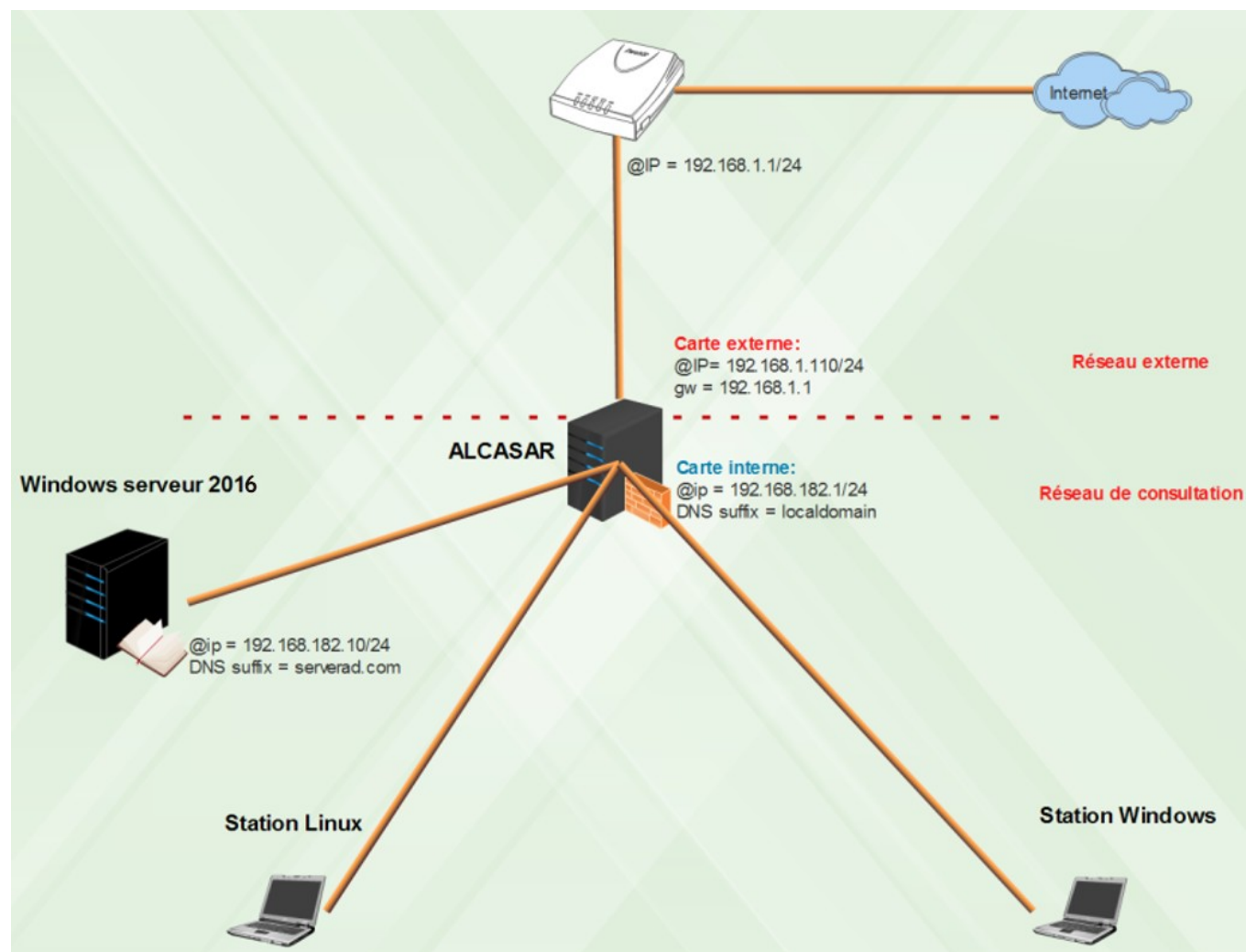


Figure 1 : Topologie réseau

Référez-vous au tutoriel « Création d'un environnement virtuel » pour l'installation de cette partie.

Rappel : les cartes réseau virtualbox des stations, du serveur A.D. et la deuxième carte ALCASAR sont en mode « réseau interne ».

Installation d'ALCASAR

La première étape est l'installation d'une VM avec ALCASAR (version utilisée : 3.1.4). Pour cela, suivre la documentation d'installation

Rappel : lors de la création de la VM, la taille du disque dur doit être supérieur à 30G.

L'organisme a été nommé « 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 : 192.168.182.1/24

Installation d'une machine de consultation Linux

Version minimaliste avec environnement LXDE et réseau en mode DHCP.

Test d'interception + connexion au centre de contrôle d'ALCASAR (l'ACC) + création d'un premier utilisateur + test de connexion



Figure 2 : Page d'interception

Installation de Windows serveur 2016

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.

Vous pouvez changer le nom du serveur (« w2016 » dans notre cas) et configurez le réseau en mode statique (normal pour un serveur). Pour être cohérent, vous pouvez ajouter l'adresse MAC et l'adresse IP de ce serveur dans la réservation DHCP d'ALCASAR (onglet « Réseau » de l'ACC).

Sur le serveur Windows, ajouter 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.

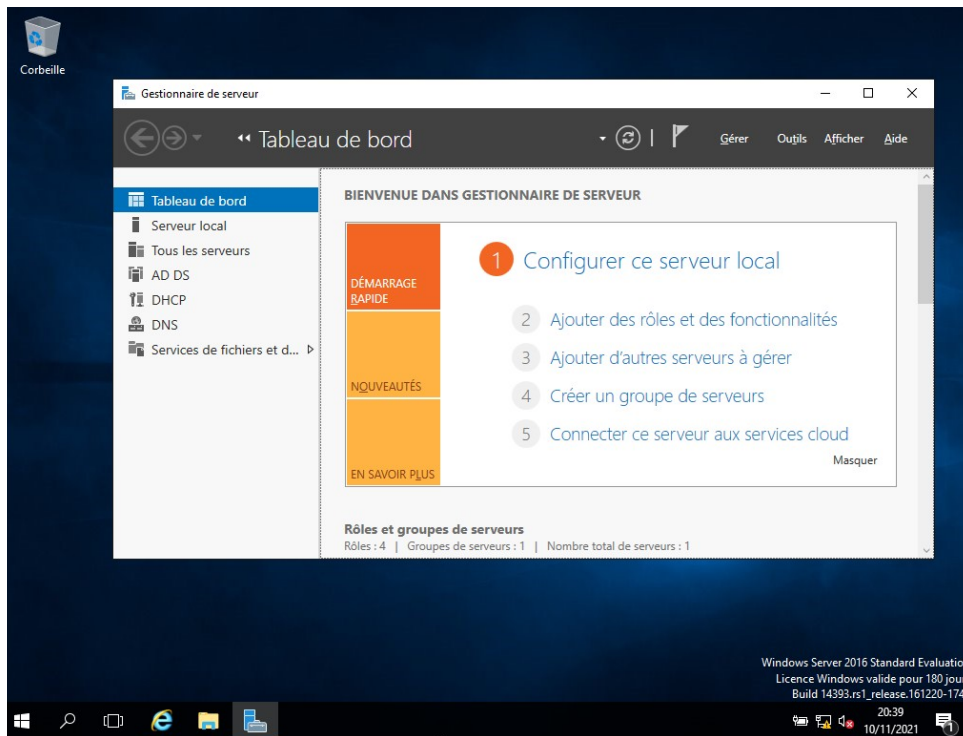


Figure 3 : Server Manager Windows 2016

Création du serveur DNS

Le nom de domaine choisi est « serverad.com ». Une fois créé, j'ai rajouté l'hôte alcasar en précisant son adresse IP 192.168.182.1 :

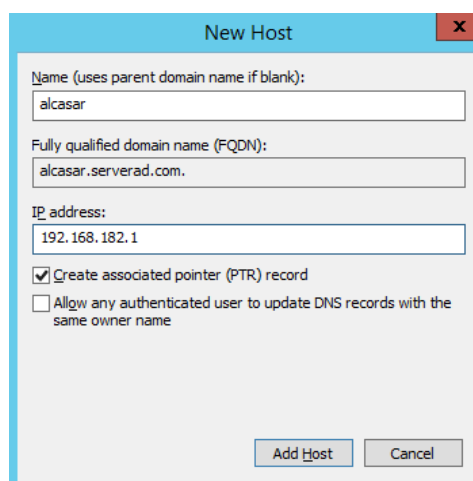


Figure 4 : Création de l'hôte ALCASAR

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.

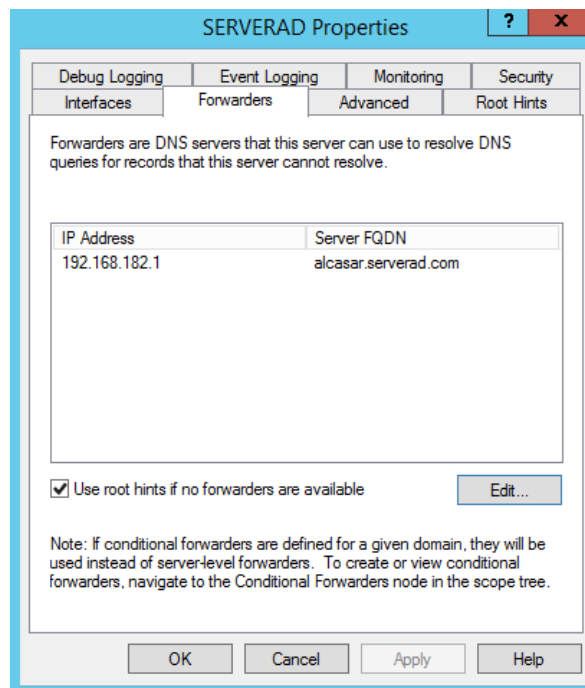


Figure 6 : DNS Forward

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. Pour réaliser cela, renseignez 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 alors redémarrées.

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 '#'. Ce '#' est très important pour ne pas bloquer les requêtes de type Service de Windows
- un ping « w2012.serverad.com » (ou tout autre nom de machine résolu par l'A.D.) doit fonctionner.

Changement de serveur DHCP

Le service DHCP est géré par ALCASAR. Mais pour des besoins d'intégrations dans une architecture donnée, il peut être opportun de s'appuyer sur un serveur DHCP externe au portail.

Ce changement de serveur DHCP comprend deux étapes :

- La première consiste à désactiver le service DHCP d'ALCASAR
- La seconde consiste à activer et 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 d'ALCASAR (ACC), comme le montre la capture ci-dessous.

The screenshot shows the 'Configuration réseau' section of the ALCASAR interface. It is divided into two main panels. The left panel, titled 'INTERNET' with a green checkmark, displays public IP settings: 'Adresse IP publique' (blurred), 'DNS1 : 8.8.8.8', and 'DNS2 : 208.67.222.222'. The right panel, titled 'enp0s3 (Interface connectée à Internet)', shows 'Adresse IP : 192.168.1.110/24' and 'Passerelle : 192.168.1.1'. Below these panels is the 'Service DHCP' section, where the 'Mode actuel' is set to 'inactif'. A dropdown menu is currently set to 'inactif', and there is an 'Appliquer les changements' button. A warning message at the bottom reads: '! Avant d'arrêter le serveur DHCP, vous devez renseigner les paramètres d'un serveur externe (cf. documentation).'

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=<@IP_srv_external>
RELAY_DHCP_IP=<@IP_internal_ALCASAR>
RELAY_DHCP_PORT=<relay port to the external DHCP server> : (default 67)
```

```

VERSION=2.9.1
ORGANISM=protiste
DOMAIN=localdomain
EXTIF=enp0s3
INTIF=enp0s8
PUBLIC_IP=192.168.1.110/24
GW=192.168.1.1
DNS1=8.8.8.8
DNS2=208.67.222.222
PUBLIC_MTU=1500
PRIVATE_IP=192.168.182.1/24
DHCP=off
EXT_DHCP_IP=192.168.182.10
RELAY_DHCP_IP=192.168.182.1
RELAY_DHCP_PORT=67
PRUTOCULS_FILTERING=off

```

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 lors de l'installation d'ALCASAR.

- Adresses IP : Elles doivent commencer au minimum par 192.168.182.3, les 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 de Windows : localdomain, serverad.com

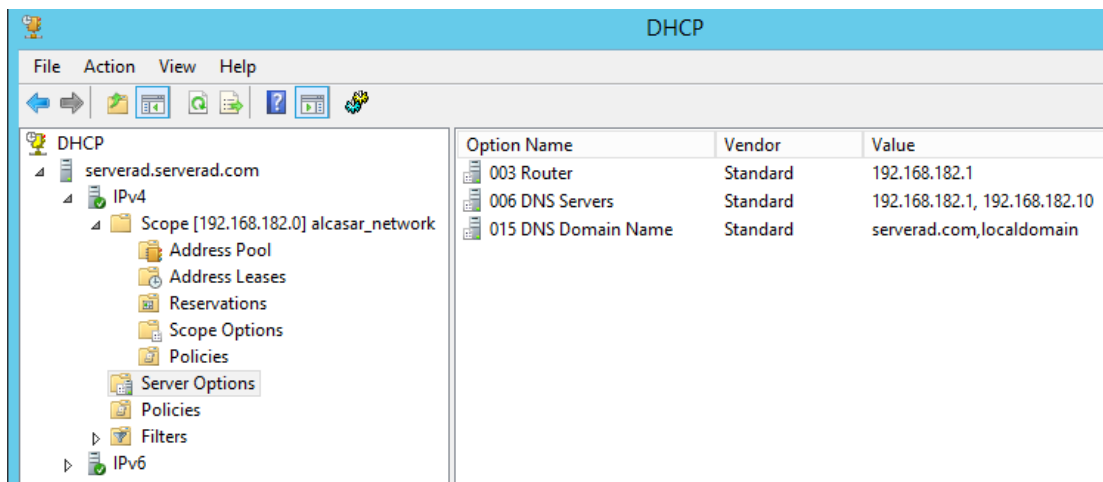


Figure 9 : Serveur DHCP et options

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

Afin qu'ALCASAR puisse authentifier les utilisateurs gérés par le serveur Active Directory, il faut créer un compte utilisateur qui puisse se consulter cet annuaire. Pour cela, créer un utilisateur (« superman » dans notre cas) avec une délégation le droit de type « All read properties » ou (« read all user information ») :

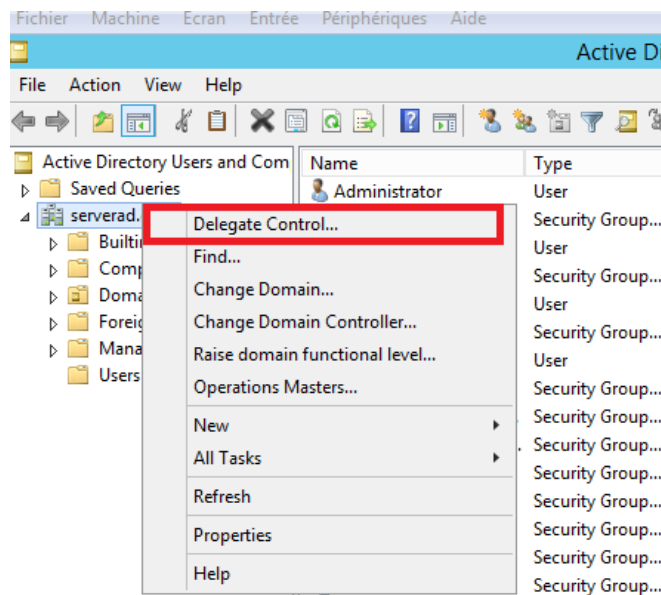


Figure 10 : Délégation de contrôle 1

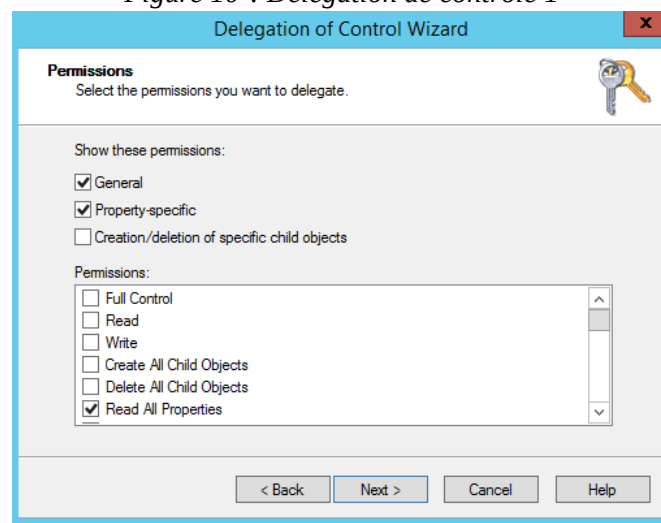


Figure 11 : Délégation de contrôle 2

Important : le mot de passe de cet utilisateur ne doit pas expirer

Enfin, on renseigne le formulaire de l'ACC relatif aux paramètres de l'A.D.

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 (sAMAccountName 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 sur Windows en utilisant la commande « dsquery », comme le 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 13 : Commande « dsquery »

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 se connecte au serveur A.D avec le compte spécifiquement créé sur le serveur Windows (superman).

Une fois l'authentification de ce dernier réussie, il va réaliser 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 14 : Capture de trafic Wireshark de l'authentification d'un utilisateur.

L'utilisateur est alors correctement authentifié :

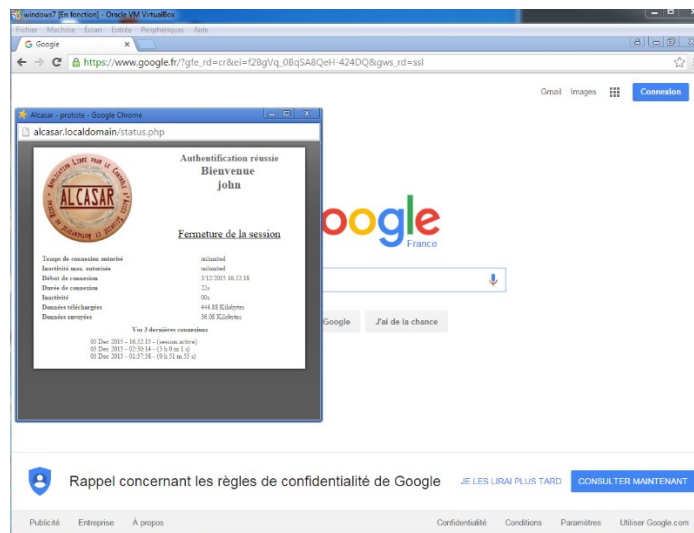


Figure 15 : Authentification réussie

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 aux 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.

Bibliographie

- Documentation 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>