Tutoriel ALCASAR

Mise en œuvre d'ALCASAR en relation avec un serveur AD©

Table des matières

Projet : ALCASAR	Auteur : Alcasar Team
Objet : Installation	Version : 4
Mots clés : portail captif, contrôle d'accès au réseau (Network Access Control - NAC), imputabilité, traçabilité, authentification, contrôle parental, filtrage	Date : octobre 2025

1) Architecture

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

- 1 VM ALCASAR
- 1VM Windows serveur 2019
- 1VM Client Windows
- 1VM Client Linux

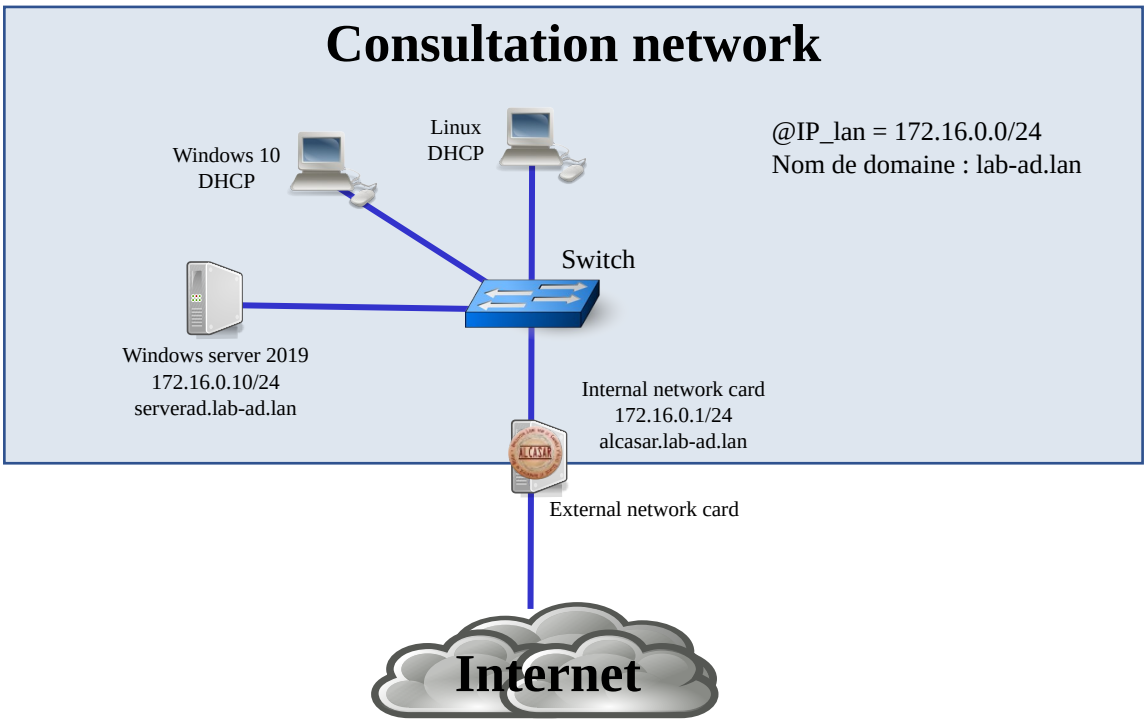


Figure 1 : Topologie réseau

Les cartes réseau virtualbox des stations, du serveur A.D. et la carte interne d'ALCASAR sont en mode « réseau interne ».

Le nom de domaine utilisé pour ce tutoriel est : « lab-ad.lan »

2) Installation des systèmes

- ## Installation d'ALCASAR

La première étape est l'installation d'une VM avec ALCASAR (version utilisée : 3.7.0). Pour cela, suivre la documentation d'installation.

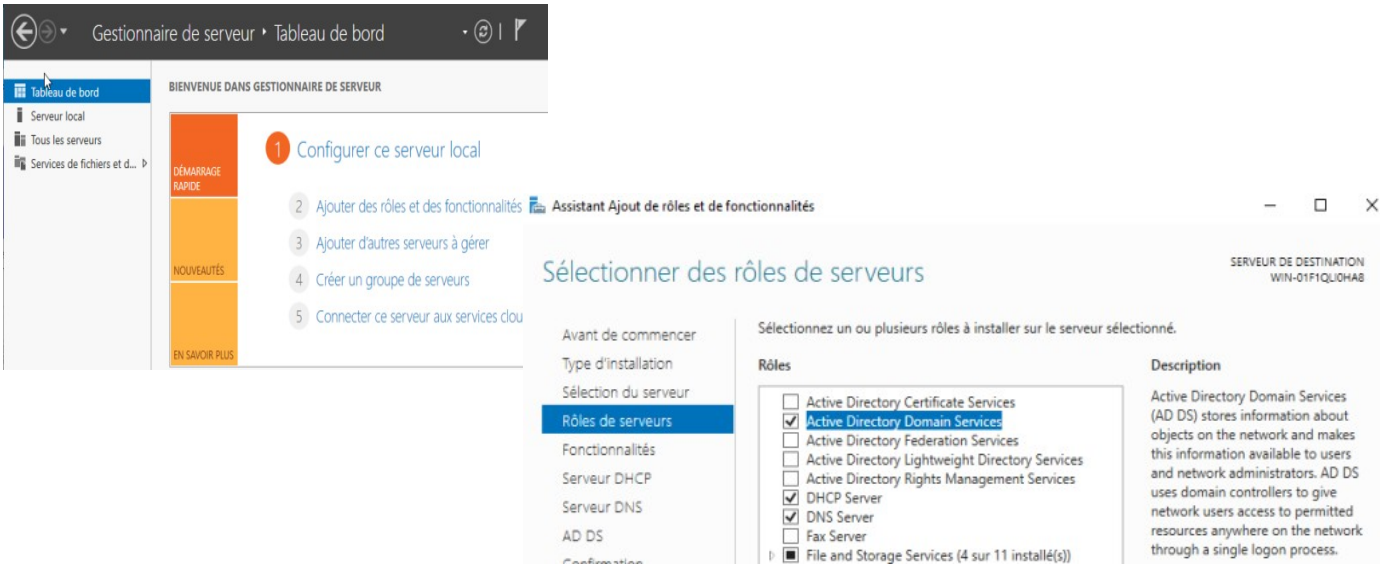
- ## Installation de deux machines de consultation Linux/Windows

Une fois installée, effectuez un test d'interception, une connexion au centre de contrôle d'ALCASAR (ACC), la création d'un premier compte utilisateur. Testez la connexion avec cet utilisateur.

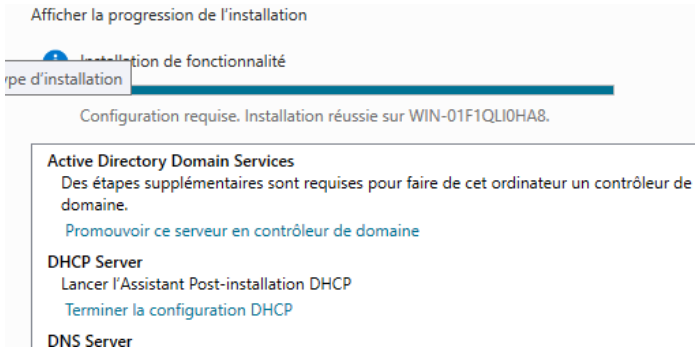
- ## Installation de Windows serveur 2019 et de l'A.D.

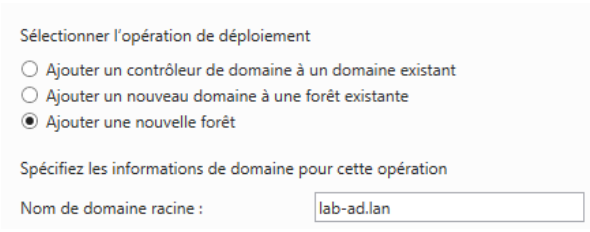
Une fois l'installation terminée, configurez le réseau en mode statique (logique pour un serveur). Lancez le navigateur et connectez-vous à l'ACC. Ajoutez l'adresse MAC et l'adresse IP de ce serveur dans la réservation DHCP d'ALCASAR (onglet « Réseau » de l'ACC). Créez un compte utilisateur qui vous permet de vous connecter à Internet. Réalisez la mise à jour du système. Pour votre confort, vous pouvez installer les drivers Virtualbox via les Guest-additions (https://download.virtualbox.org/virtualbox).

Lancez l'interface de gestion du serveur (cf. capture ci-dessous). Ajouter les rôles DHCP, DNS et Active Directory Domain Services « AD-DS »). Pour cela, sélectionnez l'onglet « Manage », puis « Add Roles and Features ». Installer dans un premier temps le service « Service AD DS » (il installera automatiquement le serveur DNS). Le nom de domaine « lab-ad.lan » a été choisi pour ce tutoriel.

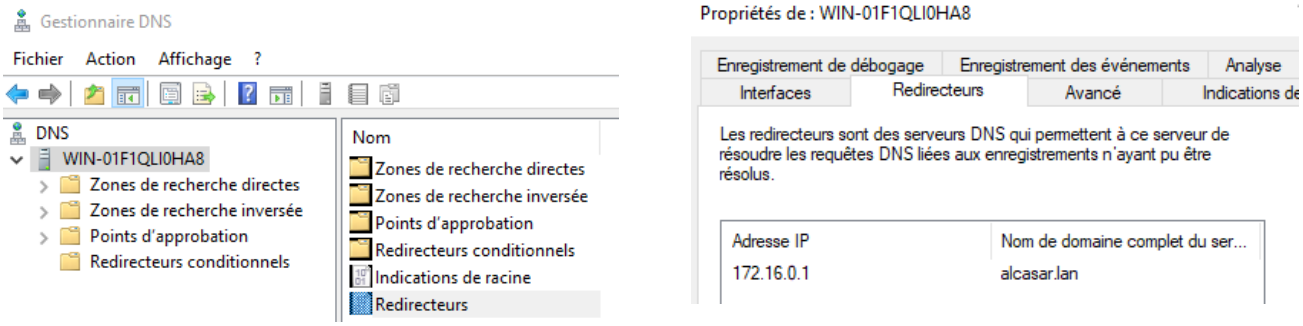


Une fois les rôles installés, cliquez sur « promouvoir ce serveur en contrôleur de domaine », puis « ajouter une nouvelle forêt ». Entrez le nom de domaine (« lab-ad.lan » pour notre tutoriel) :

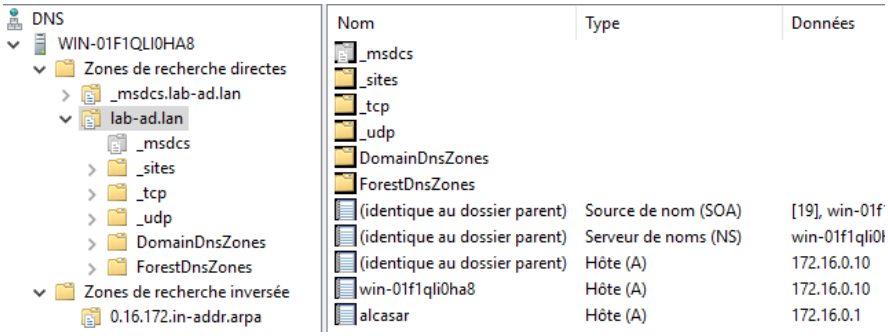




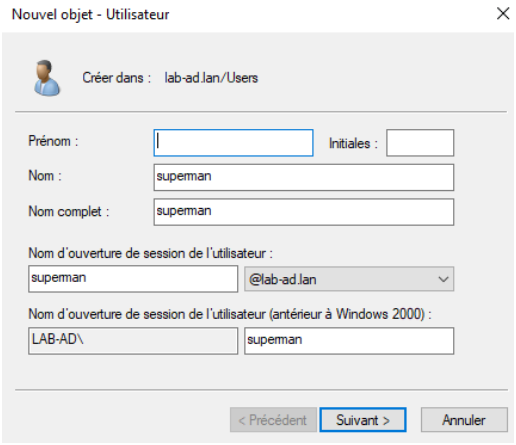
Le serveur DNS de l'A.D. résout uniquement le domaine « lab-ad.lan ». Vérifiez qu'il va bien rediriger les autres requêtes de résolution vers l'@IP d'ALCASAR : « outils d'administration » + « DNS » + sélectionnez le nom du serveur A.D. + sélectionnez « Redirecteurs » :

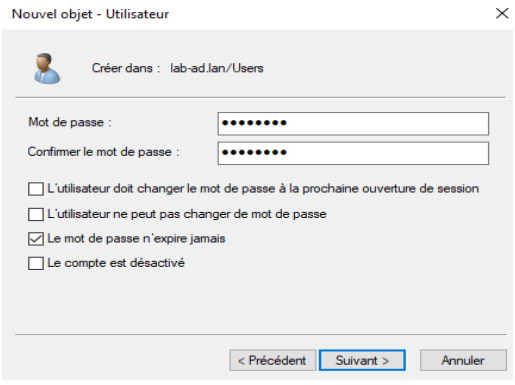


Dans ce gestionnaire DNS, vérifiez aussi que l'hôte « alcasar » est bien résolu dans la zone directe et inverse du serveur DNS. Ajoutez-le le cas échéant.

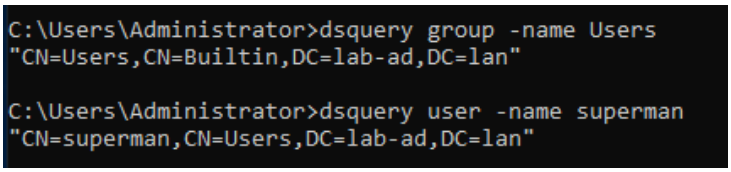


Afin qu'ALCASAR puisse authentifier les utilisateurs gérés par l'A.D., il faut créer sur l'A.D. un compte utilisateur qui sera exploité par ALCASAR pour consulter l'annuaire. Créer cet utilisateur (« superman » dans notre exemple). Affectez-lui un mot de passe avec l'attribut « Le mot de passe n'expire jamais ».

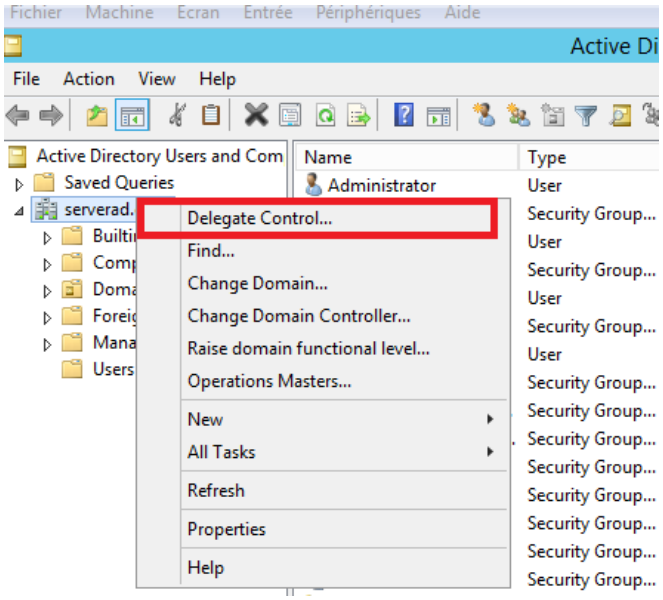


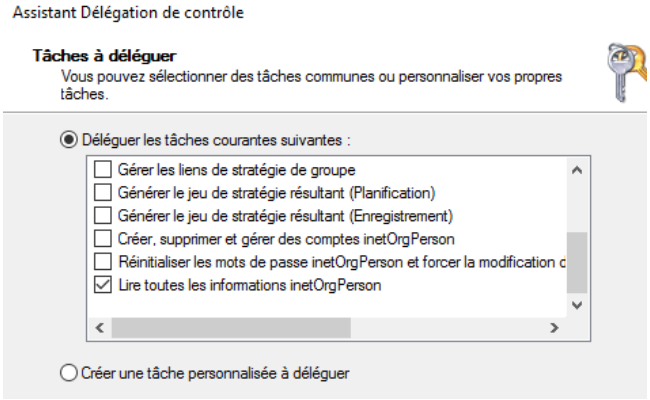


Gardez en mémoire le DN (Distinguish Name) de cet utilisateur : « CN=superman,CN=Users,DC=lab-ad,DC=lan ». Il est possible d'obtenir ces informations sur l'A.D. en utilisant la commande « dsquery » dans un terminal, comme le montre la capture ci-dessous :



Attribuez une délégation le droit à cet utilisateur de type « Lire toutes les informations inetOrgPerson ». Pour cela, allez dans le « gestionnaire de serveur », sélectionnez « outils » puis « Utilisateur et ordinateurs AD », puis « clic droit » sur le nom du serveur.





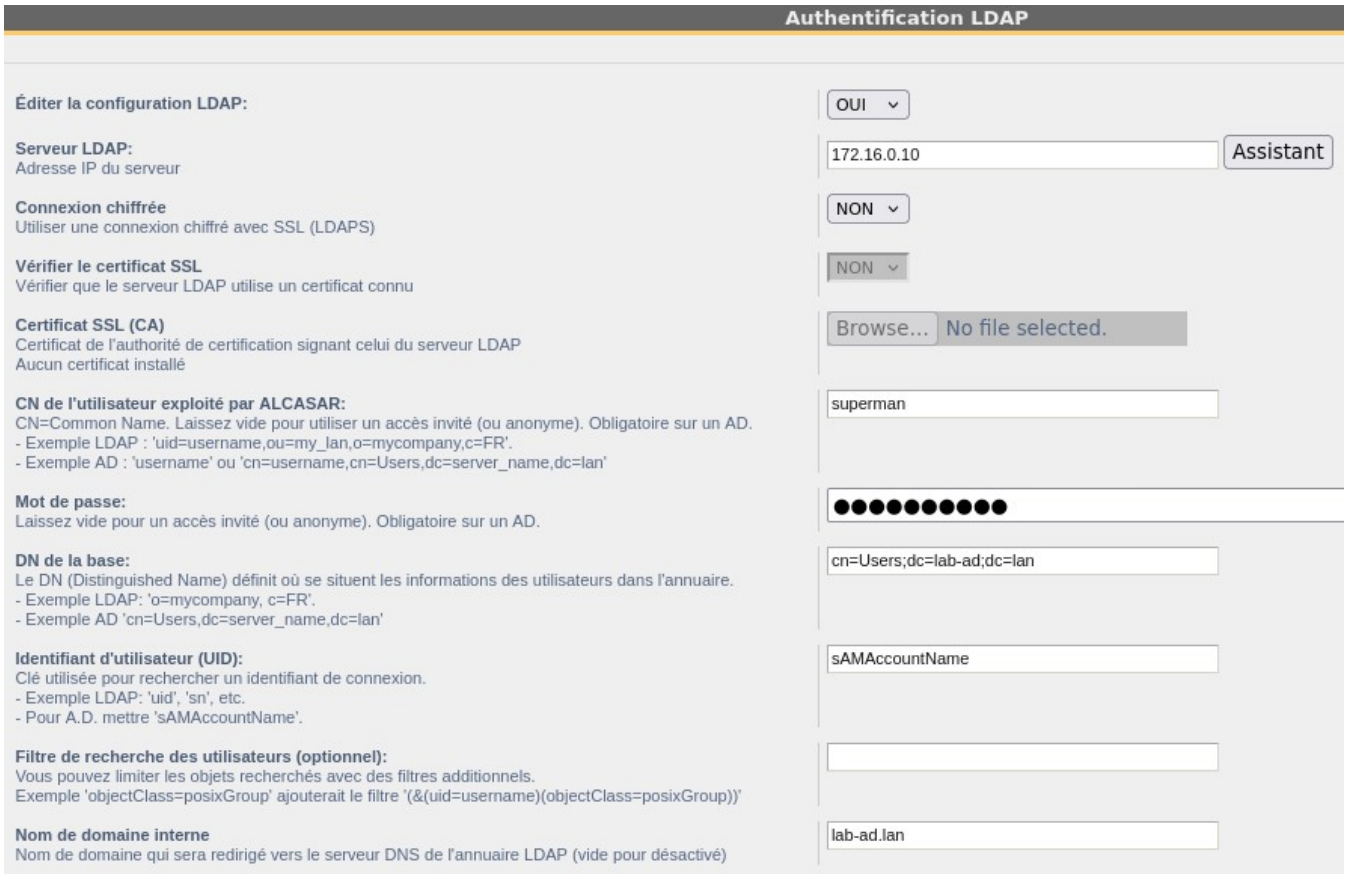
3) Configuration d'ALCASAR

- Connexion à l'A.D.

Les informations nécessaires pour connecter ALCASAR à l'A.D sont :

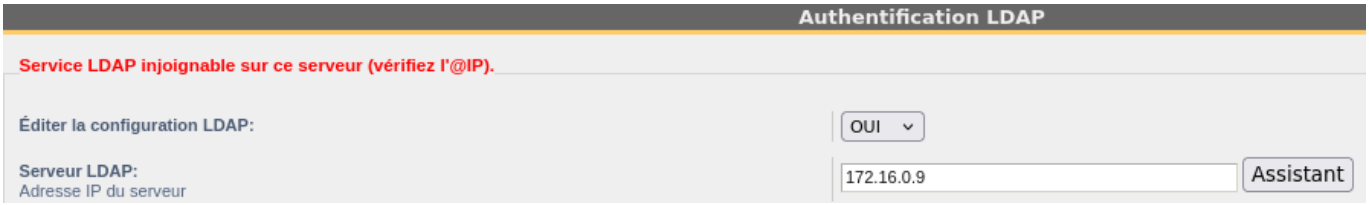
- L'adresse IP du serveur A.D.
  - « 172.16.0.10 » dans notre exemple
- Le DN (Distinguished Name) et le mot de passe de l'utilisateur de l'A.D. exploité par ALCASAR pour consulter l'annuaire :
  - « CN=superman,CN=Users,DC=lab-ad,DC=lan » dans notre exemple
- Le DN de la base contenant les informations des utilisateurs dans l'annuaire :
  - « CN=Users,DC=lab-ad,DC=lan » dans notre exemple
- Le nom de l'attribut unique identifiant les utilisateurs qu'ALCASAR va rechercher dans l'annuaire :
  - « sAMAcountName » dans le cas générique d'un A.D. ;
- Il est possible d'ajouter des filtres pour affiner (et accélérer) la recherche des utilisateurs :
  - rien dans notre cas.

Renseignez les différents champs.

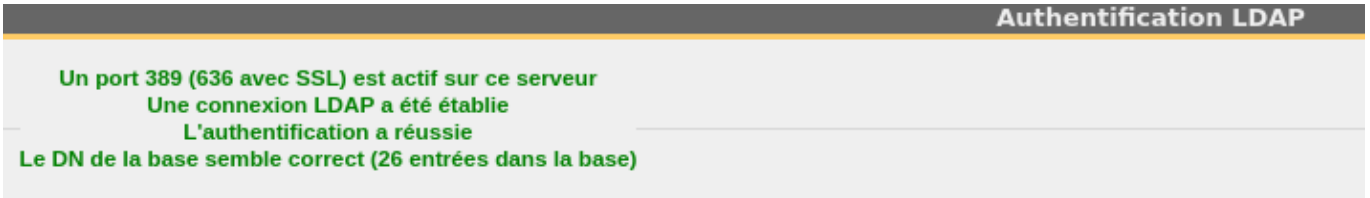


L'ACC vous propose deux assistants qui permettent de tester les paramètres de configurations :

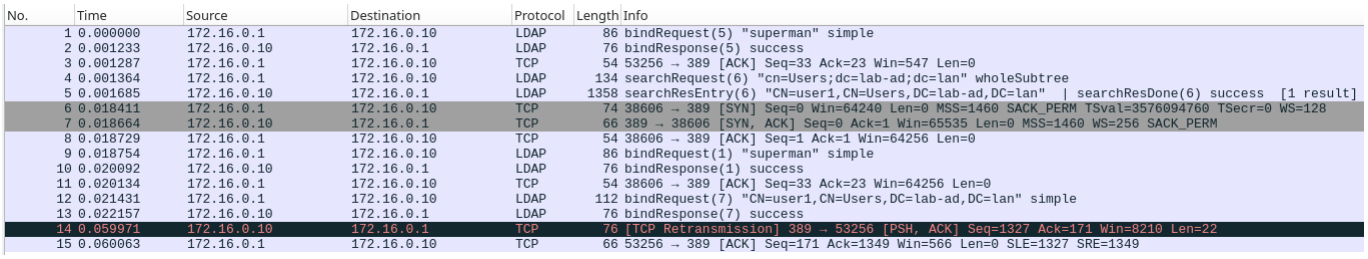
- validation de la connexion à l'@IP du serveur :



- validation d'une requête sur l'annuaire du serveur :



À titre pédagogique, voici l'analyse des flux réseau entre ALCASAR et le serveur A.D.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.0.1	172.16.0.10	LDAP	86	bindRequest(5) "superman" simple
2	0.001233	172.16.0.10	172.16.0.1	LDAP	76	bindResponse(5) success
3	0.001287	172.16.0.1	172.16.0.10	TCP	54	53256 → 389 [ACK] Seq=33 Ack=23 Win=547 Len=0
4	0.001364	172.16.0.1	172.16.0.10	LDAP	134	searchRequest(6) "cn=Users;dc=lab-ad;dc=lan" wholeSubtree
5	0.001685	172.16.0.10	172.16.0.1	LDAP	1358	searchResEntry(6) "CN=user1,CN=Users,DC=lab-ad,DC=lan" | searchResDone(6) success [1 result]
6	0.018411	172.16.0.1	172.16.0.10	TCP	74	38606 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3576094760 TSecr=0 WS=128
7	0.018664	172.16.0.10	172.16.0.1	TCP	66	389 → 38606 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
8	0.018729	172.16.0.1	172.16.0.10	TCP	54	38606 → 389 [ACK] Seq=1 Ack=1 Win=64256 Len=0
9	0.018754	172.16.0.1	172.16.0.10	LDAP	86	bindRequest(1) "superman" simple
10	0.020092	172.16.0.10	172.16.0.1	LDAP	76	bindResponse(1) success
11	0.020134	172.16.0.1	172.16.0.10	TCP	54	38606 → 389 [ACK] Seq=33 Ack=23 Win=64256 Len=0
12	0.021431	172.16.0.1	172.16.0.10	LDAP	112	bindRequest(7) "CN=user1,CN=Users,DC=lab-ad,DC=lan" simple
13	0.022157	172.16.0.10	172.16.0.1	LDAP	76	bindResponse(7) success
14	0.059971	172.16.0.10	172.16.0.1	TCP	76	[TCP Retransmission] 389 → 53256 [PSH, ACK] Seq=1327 Ack=171 Win=8210 Len=22
15	0.060063	172.16.0.1	172.16.0.10	TCP	66	53256 → 389 [ACK] Seq=171 Ack=1349 Win=566 Len=0 SLE=1327 SRE=1349

Explication :

- Trame 1+2 et trames 9+10 : Chaque requête dans l'annuaire commence par une demande de connexion sur le serveur A.D en utilisant le compte spécifiquement créé pour consulter l'annuaire (« superman » dans notre cas).
- La trame 4 est une requête demandant si l'utilisateur « user1 » existe. La trame 5 valide la présence de l'utilisateur « user1 ».
- La trame 12 est une demande de validation d'authentification pour l'utilisateur « user1 ». La trame 10 valide l'authentification.

Il est possible d'appliquer des attributs ALCASAR aux utilisateurs authentifiés via un annuaire externe. Pour cela il faut créer le groupe « default ». Ce groupe accueille tous les utilisateurs qu'ils soient internes ou authentifiés par un serveur LDAP/A.D. externe. Il est alors possible de laisser les utilisateurs LDAP/A.D. hériter des attributs du groupe « default » et créer un autre groupe pour les utilisateurs gérés localement par ALCASAR.

Il est aussi possible d'affecter des attributs ALCASAR à un utilisateur particulier authentifié par un annuaire externe. Pour cela, il faut créer un utilisateur ALCASAR ayant le même « nom de login » que celui de l'annuaire externe (attention, ALCASAR respecte la casse, contrairement aux annuaires externes). Particularité : ne laissez surtout pas son mot de passe vide (générez-en un de manière aléatoirement) afin qu'en cas d'échec de l'authentification LDAP, ALCASAR ne l'authentifie pas automatiquement.

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

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, 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 »)

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 defaut 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 x.y.z.3-254/24) ; **Attention :** depuis la version 2.7, le portail réserve les adresses x.y.z.1 et x.y.z.2 pour son usage interne ;
- une adresse de passerelle correspondant à l’adresse IP interne d’ALCASAR (par défaut x.y.z.1) ;
- le suffixe DNS « localdomain » ;
- l’@IP du serveur DNS --> l’adresse IP interne d’ALCASAR (par défaut x.y.z.1.1) ;
- l’@IP du serveur de temps (NTP) --> l’adresse IP interne d’ALCASAR (par défaut x.y.z.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).