Utilisation des serveurs DNS Linux BIND pour les domaines Active Directory

Lien : https://www.serverlab.ca/tutorials/linux/network-services/using-linux-bind-dns-servers-for-active-directory-domains/

Présentation

Active Directory s'appuie sur le DNS pour fonctionner correctement. Si votre environnement dispose déjà d'un serveur DNS BIND basé sur Linux, il est possible que les zones DNS Active Directory soient hébergées sur le serveur DNS existant.

Les avantages :

- Un serveur Linux BIND est un serveur DNS très léger et rapide.
- Linux peut être plus sûr car il y a moins de vulnérabilités connues.

Les inconvénients :

- perte de certaines fonctionnalités d'Active Directory.
- les zones de domaine BIND ne peuvent avoir qu'un seul maître, contrairement à Windows DNS. Un serveur de noms Windows dans un environnement Active Directory est capable d'être multimaître, ce qui vous donne une disponibilité beaucoup plus élevée.

Enregistrements nécessaires

Un domaine Active Directory a besoin d'enregistrements de ressources du localisateur SRV (Service Location) pour fonctionner. Ces enregistrements permettent aux clients et aux contrôleurs de domaine de localiser les services AD comme les contrôleurs de domaine, les serveurs LDAP, Kerberos, etc.

Les enregistrement SRV doivent alors exister pour les services suivants :

- _kerberos
- _ldap
- _gc

Enregistrements A (Address Records)

Ces enregistrements associent un nom d'hôte à l'adresse IP des contrôleurs de domaine AD.

Ces enregistrements seront utilisés pour que les clients puissent résoudre le nom du contrôleur de domaine AD en adresse IP.

Exemple : agence-dc.agence.cub.fr qui a l'adresse IP 172.16.50.70

```
agence-dc   IN      A       172.16.50.70
```

Enregistrements SRV (Service Resource Records)

Les enregistrements SRV sont nécessaires pour localiser les services AD. Ces enregistrements ont le format suivants :

_service._protocol.domain

Voici les principaux enregistrements SRV adapté au contexte CUB:

. Enregistrement	Description
_ldap._tcp.dc._msdcs.agence.cub.fr	Localise les contrôleurs de domaine via LDAP.
_kerberos._tcp.dc._msdcs.agence.cub.fr	Localise les serveurs Kerberos pour l'authentification.
_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.agence.cub.fr	Localise les DCs dans le site AD créé par défaut.
_kerberos._tcp.Default-First-Site-Name._sites.dc._msdcs.agence.cub.fr	Localise les serveurs Kerberos dans un site créé par défaut.
_gc._tcp.agence.cub.fr	Localise les serveurs de catalogue global (Global Catalog).
_ldap._tcp.pdc._msdcs.agence.cub.fr	Localise le contrôleur de domaine principal (PDC Emulator).

Pour vérifier les enregistrements SRV avec Nslookup :

- Tapez nslookup et appuyez sur Entrée.

- Tapez set type=all et appuyez sur Entrée.
- Tapez _ldap._tcp.dc._msdcs.agence.cub.fr puis appuyez sur Entrée.

Exemple de configuration pour l'AD CUB

```
; enregistrement Active directory du  domaine cub.fr
cub-dc                                      IN  A   172.16.x.y
_ldap._tcp                                  IN  SRV  0 0 389 cub-dc
_ldap._tcp.pdc._msdcs                       IN  SRV  0 0 389 cub-dc
_ldap._tcp.default-First-Site-Name._sites     IN  SRV  0 0 389 DC-01
_ldap._tcp.dc._msdcs                        IN  SRV  0 0 389 cub-dc
_ldap._tcp.gc._msdcs                        IN  SRV  0 0 389 cub-dc
_kerberos._tcp                              IN  SRV  0 0 88  cub-dc
_kerberos._tcp.dc._msdcs                    IN  SRV  0 0 88  cub-dc
_ldap._tcp.default-First-Site-Name._sites     IN  SRV  0 0 389 cub-dc
_kerberos._tcp.Default-First-Site-Name._sites IN  SRV  0 0 88  cub-dc
```

Tester

- Utilisation de dcdiag sur le contrôleur de domaine pour avoir un diagnostic complet des enregistrements DNS liés à AD.

```
dcdiag /test:DNS /v /s:NomDuDC
```

- les enregistrements sont manquants, Vérifier que le service Netlogon est démarré.
- Forcer la régénération des enregistrements SRV avec :

```
ipconfig /registerdns
net stop netlogon
net start netlogon
```

Cela recréera les enregistrements SRV dans DNS si le DC est bien configuré.

Promouvoir le serveur Windows en contrôleur de domaine

- Configurez au préalable votre seveur Windows pour utiliser comme résolveur DNS dans sa configuration IP, le résolveur du réseau de votre agence qui renvoie vers le serveur DNS NS0 de votre agence.
- installez le rôle **Service de domaine Active Directory**
- Faites ensuite la **promotion** de votre serveur Windows en **contrôleur de domaine** avec les paramètres suivants :
    - créer une nouvelle forêt
    - décocher l'installation du serveur DNS de Windows

Configurer la mise à jour dynamique de BIND9 (Attendre - documentation non mise à jour)

Synchronisation de l'heure

Kerberos exige une synchronisation stricte (±5 minutes). Si l'horloge dérive, l'authentification échoue :

- Debian utilsie openntpd
- Active Directory utilise Windows Time Service (W32Time) basé sur NTP.

Configurer NTP sur ns0n

```
apt install openntpd
```

Intégrer le serveur BIND dans le domaine AD

- installer les prérequis

```
apt install packagekit samba-common-bin sssd-tools sssd libnss-sss libpam-sss sssd realmd

sudo apt install  adcli  oddjob oddjob-mkhomedir packagekit
```

- Visualiser les informations AD

```
realm discover agence.cub.fr
```

- faire adhérer le serveur BIND au domaine agence.cub.local

```
realm join --user=Administrator@agence.cub.fr agence.cub.fr
```

La configuration d'un proxy GSS-TSIG (Generic Security Service Algorithm for TSIG) va permettre au contrôleur de domaine Active Directory (Windows Server) de faire des mises à jour DNS dynamiques sécurisées vers le serveur BIND9, en utilisant Kerberos comme mécanisme d'authentification.

C'est la méthode native utilisée par Windows Server pour sécuriser les mises à jour DNS.

GSS-TSIG est une extension de TSIG.

Une clé TSIG (Transaction SIGnature) est une clé cryptographique partagée utilisée pour sécuriser les mises à jour dynamiques DNS entre le client contrôleur de domaine Active Directory et le serveur DNS BIND9.

La a clé TSIG permet :

- d'authentifier les requêtes de mise à jour DNS envoyer par le contrôleur de domaine AD ;
- d'empêcher les mises à jour non autorisées par d'autres clients qui pourraient modifier les enregistrements DNS ;
- d'assurer l'intégrité des données échangées (protection contre les modifications en transit).

Avantages de GSS-TSIG :

- Authentification forte via Kerberos.
- Intégration native avec Active Directory.
- Pas besoin de gérer manuellement des clés TSIG.

Création d'un utilisateur spécifique pour les mises à jour

Créez dans votre annuaire AD un utilisateur nommé **dnsbind** avec le mot de passe de votre choix (exemple **Sio1234***) dédié à la mise à jour du serveur BIND. Le mot de passe de ce compte ne doit pas être changé et ne doit pas expirer.

Ce compte représentera le serveur BIND dans le domaine.

Installation du client Kerberos sur le serveur BIND

L'installation du client Kerberos est nécessaire pour que Bind9 puisse authentifier les requêtes venant d'AD via GSSAPI.

- installer les paquets

```
apt update
apt install krb5-user libkrb5-dev libgssapi-krb5-2
```

Lors de l'installation, renseignez les informations suivantes :

- Le nom du domaine Kerberos : AGENCE.CUB.FR
- Le serveur KDC : agence-cub.agence.cub.fr
- Le serveur d'administration, qui est le même que le KDC : agence-cub.agence.cub.fr

Configurer /etc/krb5.conf

Modifiez / complétez le fichier /etc/krb5.conf

```
[libdefaults]
 default_realm = AGENCE.CUB.FR
 permitted_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96
 dns_lookup_realm = true
 dns_lookup_kdc = true
 ticket_lifetime = 24h
 forwardable = yes
[realms]
 AGENCE.CUB.FR = {
  kdc = agence-dc.age,ce.cub.fr
  admin_server = agence-dc.agence.cub.fr
[domain_realm]
```

```
 .agence.cub.fr = AGENCE.CUB.FR
 agence.cub.fr = AGENCE.CUB.FR
```

Tester la connexion Kerberos

Depuis une invite de commande de votre serveur BIND, testez une authentification avec le compte dnsbind :

```
kinit dnsbind@AGENCE.CUB.FR
```

Le mot de passe sera demandé et la commande suivant permet de lister le ticket Kerberos créé :

```
klist
```

Création du principal dnsbind

Pour permettre au serveur Windows AD de s'authentifier automatiquement auprès du service BIND, un principal va être créé.

En Kerberos, un principal est une identité unique utilisée pour l'authentification. C'est l'équivalent d'un "utilisateur" ou "service" dans le système Kerberos.

Un principal est généralement composé de trois parties : nom_utilisateur/nom_service@REALM

Dans l'invite de commande Windows, utilisez la commande suivante pour créer un principal pour dnsbind qui sera enregistré dans le fichier dnsbind.keytab

```
ktpass -princ DNS/ns0.agence.cub.fr@AGENCE.CUB.FR -mapuser dnsbind -pass Sio1234* -out dnsbind.keytab -
ptype KRB5_NT_PRINCIPAL -crypto AES256-SHA1
```

Le principal Kerberos doit correspondre au FQDN du serveur BIND

Vérifier la création du principal du compte dnsbind

> **SPN** : ServicePrincipalName

- Visualiser le ou les SPN du compte (setspn -L NomDuCompte)

```
setspn -L dnsbind
```

- Ajouter un SPN au compte (setspn -A HTTP/serveur.domaine.local NomDuCompte)

```
setspn -A DNS/ns0.agence.cub.fr dnsbind
```

- Supprimer un SPN au compte (setspn -D HTTP/serveur.domaine.local NomDuCompt)

```
setspn -D DNS/ns0.agence.cub.fr dnsbind
```

- Vérifier s'il n'y a pas de doublon ce qui peut faire échouer l'authentification Kerberos

```
setspn -X
```

Copier avec scp de fichier dnsbind.keytab dasn le dossier /etc du serveur BIND avec le nom krb5.keytab

```
scp dnsbind.keytab sio@ipDebian:/home/sio/
```

Dans l'invite de commandes du serveur BIND

```
cp /home/sio/dbsbind.keytab /etc/krb5.keytab
chown bind:bind /etc/krb5.keytab
chmod 600 /etc/krb5.keytab
```

Tester l'authentification Kerberos

```
kinit -k -t /etc/krb5.keytab DNS/ns0.oslo.cub.fr@OSLO.CUB.FR
```

Visualiser le ticket

```
klist
```

Un ticket valide doit être affiché

```
root@NS0:/etc/bind# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: DNS/ns0.oslo.cub.fr@OSLO.CUB.FR

Valid starting     Expires            Service principal
11/17/25 16:10:03  11/18/25 02:10:03  krbtgt/OSLO.CUB.FR@OSLO.CUB.FR
        renew until 11/18/25 16:10:03
```

Utiliser le fichier keytab dans BIND pour les mises à jour dynamiques

Les lignes de configuration **tkey-gssapi-credential** et **tkey-domain** doivent être ajoutées dans le fichier **named.conf.options** de BIND9, dans le bloc options.

```
options {
    directory "/var/cache/bind";

    // Autoriser les mises à jour dynamiques sécurisées via GSS-TSIG
    tkey-gssapi-credential "DNS/dnsbind.agence.cub.fr@AGENCE.CUB.FR";
    tkey-domain "AGENCE.CUB.FR";
    tkey-gssapi-keytab "/etc/krb5.keytab";

    ...
};
```

Dans la zone DNS du fichier **named.conf.local** :

```
zone "agence.cub.fr" {
    type master;
        file "/etc/bind/db.agence.cub.fr";
        update-policy {
           grant DNS/ns0.oslo.cub.fr@OSLO.CUB.FR zonesub ANY;
        };
};
```

> Le mot-clé **zonesub** :
>
> zonesub autorise les mises à jour dans la zone et ses sous-domaines.
>
> Pour limiter les mises à jour à la zone principale, utilisez **zone ANY** à la place de **zonesub ANY**.

Relancer BIND9

```
systemctl restart bind9
```

Vérification de la création des enregistrements

- utilisez la commande suivante en invite de commande de votre serveur windows pour forcer la création des enregisterments DNS :

```
ipconfig /registerdns
```

Retour Configurer le service DNS

- Configurer le service DNS