Red Stack
eArticle

Intégration Oracle 12.2 avec Active Directory Windows 2016

Mouhamadou Diaw, dbi services

Introduction

Les utilisateurs des bases de données devenant de plus en plus nombreux, leur gestion devient une problématique de plus en plus importante. Et la question qui se pose de plus en plus est de savoir comment simplifier cette gestion.

Dans cet article nous allons voir comment il est possible d'intégrer une Active Directory (AD) Windows avec une base de données oracle. L'idée étant de laisser la gestion des mots de passe à Windows.

Cela veut dire que l'utilisateur une fois connecté sur un client du domaine, pourra se connecter directement sur la base sans fournir de mot de passe en utilisant le ticket fourni par le KDC.

Environnements

Nous commencerons par décrire les éléments qui composent notre environnement.

Environnement Windows

- un contrôleur de domaine Windows 2016 : **192.168.168.101**
- un client Windows 2016 intégré dans le domaine
- un client 11.2 installé sur le client Windows
- un client oracle 12.2 installé sur le client
- un domaine ayant pour nom : **SUMADOMAIN.COM**
- un utilisateur du domaine : **activediroracle@SUMADOMAIN.COM**

Environnement Linux

- serveur Oracle linux OEL7 :
- Nom du serveur : standbyserver1.loacaldomain (192.168.168.10)
- Une base de données oracle 12.2

Vérification de la présence d'Oracle Advanced Security

L'intégration nécessitant l'option Oracle Advanced Security (ASO), il convient dans un premier temps de vérifier son installation sur le serveur de base de données. En effet les librairies nécessaires pour la configuration avec Kerberos sont fournies par ASO.
Dans la documentation Oracle (http://docs.oracle.com/database/121/DBLIC/options.htm#DBLIC143) on peut lire ces lignes ci-dessous :
Network encryption (native network encryption and SSL/TLS) and strong authentication services (Kerberos, PKI, and RADIUS) are no longer part of Oracle Advanced Security and are available in all licensed editions of all supported releases of the Oracle database.
L'option est donc gratuite pour l'authentification Kerberos.

```
[oracle@standbyserver1 ~]$ adapters

Installed Oracle Net transport protocols are:

    IPC
    BEQ
    TCP/IP
    SSL
    RAW
    SDP/IB
    ExaDirect

Installed Oracle Net naming methods are:

    Local Naming (tnsnames.ora)
    Oracle Directory Naming
```

```
    Oracle Host Naming

Installed Oracle Advanced Security options are:

    RC4 40-bit encryption
    RC4 56-bit encryption
    RC4 128-bit encryption
    RC4 256-bit encryption
    DES40 40-bit encryption
    DES 56-bit encryption
    3DES 112-bit encryption
    3DES 168-bit encryption
    AES 128-bit encryption
    AES 192-bit encryption
    AES 256-bit encryption
    MD5 crypto-checksumming
    SHA-1 crypto-checksumming
    Kerberos v5 authentication
    RADIUS authentication
[oracle@standbyserver1 ~]$
```

Listing 1

La ligne “Installed Oracle Advanced Security options are:” confirme la présence de l’option.

Création de l’utilisateur de domaine

On créera un utilisateur dans le domaine. Nous l’appellerons activediroracle@SUMADOMAIN.COM

Génération d’un fichier de mappage des utilisateurs

La première étape est de générer, avec un utilisateur privilégié, un fichier qui va servir à mapper les utilisateurs. Mais avant Il faut d’abord mettre à jour le Service Principal Name (SPN) de l’utilisateur avec la commande setspn.
Il faut juste remarquer le domaine SUMADOMAIN.COM est toujours référencé en majuscules.

```
C:\Windows\system32>setspn -A
oracle/standbyserver1.localdomain@SUMADOMAIN.COM activediroracle
Checking domain DC=sumadomain,DC=com

Registering ServicePrincipalNames for CN=Active Directory
Oracle,CN=Users,DC=sumadomain,DC=com
        oracle/standbyserver1.localdomain@SUMADOMAIN.COM
Updated object
```

Listing 2

Dans la commande précédente

- le mot oracle est un nom de service que nous indiquerons dans nos fichiers de configuration plus loin.
- standbyserver1.localdomain est le nom du serveur Linux hébergeant la base

- SUMADOMAIN.COM est le domaine Windows
- activediroracle est l'utilisateur de domaine

On peut visualiser le SPN par la commande

```
C:\Windows\system32>SETSPN -L activediroracle
Registered ServicePrincipalNames for CN=Active Directory
Oracle,CN=Users,DC=sumadomain,DC=com:
        oracle/standbyserver1.localdomain@SUMADOMAIN.COM
```

Listing 3

Il faut ensuite utiliser la commande ktpass.exe pour générer le fichier keytab qui devra par la suite être transféré sur le serveur linux hébergeant la base de données.

```
C:\Windows\system32>ktpass.exe -princ
oracle/standbyserver1.localdomain@SUMADOMAIN.COM -target
192.168.168.101 -ptype KRB5_NT_PRINCIPAL -mapuser activediroracle -
crypto RC4-HMAC-NT -pass Root2017* -out c:\temp\keytab
Using legacy password setting method
Successfully mapped oracle/standbyserver1.localdomain to
activediroracle.
Key created.
Output keytab to c:\temp\keytab:
Keytab version: 0x502
keysize 83 oracle/standbyserver1.localdomain@SUMADOMAIN.COM ptype 1
(KRB5_NT_PRINCIPAL) vno 6 etype 0x17 (RC4-HMAC) keylength 16
(0xbdeeeb464c67ce85827553d997f48e1b)
```

Listing 4

Création de l'utilisateur dans la base de données

Dans la base de données il faudra créer l'utilisateur en EXTERNALLY (attention aux majuscules pour le login)

```
[oracle@standserver1 ~]$ rlwrap sqlplus / as sysdba

SQL*Plus: Release 12.2.0.1.0 Production on Sat Jun 3 15:44:41 2017

Copyright (c) 1982, 2016, Oracle.  All rights reserved.


Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit
Production

SQL> create user "ACTIVEDIRORACLE@SUMADOMAIN.COM" identified
externally;

User created.
```

```
SQL> grant create session, create table to
"ACTIVEDIRORACLE@SUMADOMAIN.COM";

Grant succeeded.

SQL>
```

Listing 5

Et ajuster aussi les paramètres ci-dessous dans la base de données.

```
SQL> alter system set os_authent_prefix='' scope=spfile;

System altered.

SQL> shut immediate;

SQL > startup
```

Listing 6

```
SQL> show parameter authen

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------
-----------
os_authent_prefix                    string
remote_os_authent                    boolean     FALSE
SQL>
```

Listing 7

Configuration de Kerberos sur le serveur Linux

Il nous faut d'abord vérifier la présence des services Kerberos.

```
[root@standbyserver1 ~]# grep kerberos /etc/services
kerberos        88/tcp          kerberos5 krb5  # Kerberos v5
kerberos        88/udp          kerberos5 krb5  # Kerberos v5
kerberos-adm    749/tcp                         # Kerberos `kadmin'
(v5)
kerberos-adm    749/udp                         # kerberos
administration
kerberos-iv     750/udp         kerberos4 kerberos-sec kdc loadav
kerberos-iv     750/tcp         kerberos4 kerberos-sec kdc rfile
kerberos_master 751/udp         pump            # Kerberos
authentication
kerberos_master 751/tcp         pump            # Kerberos
authentication
[root@standbyserver1 ~]#
```

Listing 8

Et ensuite créer un fichier krb5.conf. Ci-dessous le contenu de notre fichier krb5.conf

```
[oracle@standbyserver1 ~]$ cat /u01/app/kerberos/krb5.conf
[libdefaults]
default_realm = SUMADOMAIN.COM

[realms]
SUMADOMAIN.COM= {
  kdc = 192.168.168.101:88
}

[domain_realm]
.localdomain = SUMADOMAIN.COM
localdomain = SUMADOMAIN.COM
```

Listing 9

Configuration de Kerberos sur le client Windows

Le même fichier krb5.conf est aussi créé sur le client Windows. Dans notre cas le fichier est placé dans c:\kerberos\krb5.conf

Configuration des fichiers sqlnet.ora

Sur le serveur Linux, il faut ajouter ces lignes dans le fichier sqlnet.ora. Le fichier keytab référencé ici est celui qui a été créé précédemment sur le client Windows et transféré sur le serveur Linux.

```
SQLNET.KERBEROS5_KEYTAB=/u01/app/kerberos/keytab
SQLNET.KERBEROS5_CONF=/u01/app/kerberos/krb5.conf
SQLNET.KERBEROS5_CONF_MIT=TRUE
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE=oracle
SQLNET.AUTHENTICATION_SERVICES=(BEQ,KERBEROS5)
```

Listing 10

Il faudra juste noter le nom de service oracle dont on a parlé plus haut

SQLNET.AUTHENTICATION_KERBEROS5_SERVICE=oracle

Pareil sur le sqlnet.ora de la machine cliente Windows

```
SQLNET.KERBEROS5_CC_NAME=c:\kerberos\cc
SQLNET.AUTHENTICATION_SERVICES= (beq,kerberos5)
SQLNET.KERBEROS5_CONF =c:\kerberos\krb5.conf
SQLNET.KERBEROS5_CONF_MIT = true
```

Listing 11

Initialisation manuelle du ticket Kerberos

Pour la connexion, le ticket Kerberos peut être initialisé manuellement. Pour cela il faut se loguer avec l'utilisateur SUMADOMAIN\activediroracle et exécuter la commande okinit.

```
C:\Users\activediroracle>okinit

Kerberos Utilities for 64-bit Windows: Version 12.2.0.1.0 -
Production on 03-JUN-2017 07:47:07

Copyright (c) 1996, 2016 Oracle.  All rights reserved.

Configuration file : c:\kerberos\krb5.conf.
Password for activediroracle@SUMADOMAIN.COM:
```

Listing 12

On peut par la suite visualiser

```
C:\Users\activediroracle>oklist

Kerberos Utilities for 64-bit Windows: Version 12.2.0.1.0 -
Production on 03-JUN-2017 07:50:24

Copyright (c) 1996, 2016 Oracle.  All rights reserved.

Configuration file : c:\kerberos\krb5.conf.
Ticket cache: FILE:c:\kerberos\cc
Default principal: activediroracle@SUMADOMAIN.COM

Valid starting     Expires            Service principal
06/03/17 07:47:29  06/03/17 17:47:29
krbtgt/SUMADOMAIN.COM@SUMADOMAIN.COM
        renew until 06/04/17 07:47:07
```

Listing 13

Une fois le ticket obtenu, on pourra se connecter à partir du client Windows utilisant la syntaxe.

```
C:\Users\activediroracle>sqlplus /@ORCL

SQL*Plus: Release 12.2.0.1.0 Production on Wed May 31 16:24:46 2017

Copyright (c) 1982, 2016, Oracle.  All rights reserved.

Last Successful login time: Wed May 31 2017 16:24:19 +01:00

Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit
Production

SQL> show user;
```

```
USER is "ACTIVEDIRORACLE@SUMADOMAIN.COM"
```

Listing 14

Obtention automatique du ticket Kerberos

Quand l'utilisateur de domaine se connecte sur un poste client, Oracle est capable d'utiliser la cache interne de Windows pour les informations de connexions.
Cette cache est un ticket Kerberos et élimine la nécessité d'obtenir manuellement un ticket avec la commande okinit.

Pour l'utilisation du ticket automatiquement il faut une ligne dans le sqlnet.ora de la forme sur la machine cliente Windows

SQLNET.KERBEROS5_CC_NAME=OSMSFT://

```
SQLNET.KERBEROS5_CC_NAME= OSMSFT://
SQLNET.AUTHENTICATION_SERVICES= (beq,kerberos5)
SQLNET.KERBEROS5_CONF =c:\kerberos\krb5.conf
SQLNET.KERBEROS5_CONF_MIT = true
```

Listing 15

Il faut juste noter, dans mon cas, que le ticket automatique ne marche bien avec le client 12c. D'ailleurs il y'a un bug référencé par oracle dans le document ci-dessous.
Bug 17471371 : 12C CLIENT USING OSMSFT TO CONNECT WITH KERBEROS FAILS WITH ORA-12641

Avec le client 12c la commande oklist retourne une erreur

```
C:\Users\activediroracle>
C:\app\oracle\product\12.2.0\client_1\bin\oklist

Kerberos Utilities for 64-bit Windows: Version 12.2.0.1.0 -
Production on 03-JUN-2017 15:33:20

Copyright (c) 1996, 2016 Oracle.  All rights reserved.

Configuration file : c:\kerberos\krb5.conf.
oklist: Unknown credential cache type resolving ccache OSMSFT://.
```

Listing 16

Ce qui fait quand on essaie de se connecter on a le message suivant

```
C:\Users\activediroracle>
C:\app\oracle\product\12.2.0\client_1\bin\sqlplus /@PROD

SQL*Plus: Release 12.2.0.1.0 Production on Sat Jun 3 15:42:56 2017

Copyright (c) 1982, 2016, Oracle.  All rights reserved.
```

```
ERROR:
ORA-12641: Authentication service failed to initialize
```

Listing 17

Alors que pour le client 11.2, la connexion marche très bien

```
C:\Users\activediroracle>
C:\app\oacle\product\11.2.0\client_1\bin\oklist

Kerberos Utilities for 64-bit Windows: Version 11.2.0.1.0 -
Production on 03-JUN-2017 15:33:39

Copyright (c) 1996, 2010 Oracle.  All rights reserved.

Ticket cache: win2kcc
Default principal: activediroracle@SUMADOMAIN.COM

   Valid Starting           Expires            Principal
03-Jun-2017 14:44:15  04-Jun-2017 00:44:15
krbtgt/SUMADOMAIN.COM@SUMADOMAIN.COM        renew until 10-Jun-2017
14:44:15
03-Jun-2017 15:26:06  04-Jun-2017 00:44:15
oracle/standbyserver1.localdomain@SUMADOMAIN.COM    renew until 10-
Jun-2017 14:44:15
03-Jun-2017 14:44:32  04-Jun-2017 00:44:15
LDAP/bourdjoloff.sumadomain.com/sumadomain.com@SUMADOMAIN.COM
renew until 10-Jun-2017 14:44:15
03-Jun-2017 14:44:15  04-Jun-2017 00:44:15
host/djoloffclient.sumadomain.com@SUMADOMAIN.COM    renew until 10-
Jun-2017 14:44:15
```

Listing 18

```
C:\Users\activediroracle>
C:\app\oacle\product\11.2.0\client_1\bin\sqlplus.exe /@PROD

SQL*Plus: Release 11.2.0.1.0 Production on Sat Jun 3 15:44:26 2017

Copyright (c) 1982, 2010, Oracle.  All rights reserved.

Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit
Production

SQL> show user
USER is "ACTIVEDIRORACLE@SUMADOMAIN.COM"
SQL>
```

Listing 19

Conclusion

Dans cet article, nous avons essayé d'expliquer pas à pas la configuration d'une authentification des utilisateurs d'une Active Directory Windows dans une base oracle. Nous avons montré comment il est possible d'utiliser le ticket Kerberos de l'AD, manuellement ou directement à partir de la cache Windows, pour ensuite utiliser ce ticket et se connecter ainsi dans la base de données

Références :

- oracle official documentation
- support.oracle.com (218275.1, 158599.1)
- http://mit.edu/kerberos