Configuring ASO Kerberos Authentication with a Microsoft Windows 2008 R2 Active Directory KDC (Doc ID 1304004.1)

In this Document

APPLIES TO:

Advanced Networking Option - Version 11.2.0.2 and later
Information in this document applies to any platform.

PURPOSE

The purpose of this article is to describe how to configure an Oracle database with Advanced Security Option (ASO) for Kerberos authentication against Microsoft Windows 2008 R2 Active Directory, and how to configure the Oracle clients.

SCOPE

This article is primarily intended for System and Database Administrators wishing to implement Kerberos authentication of Oracle Database users against a Windows Server 2008 R2 Active Directory Server.

The article discusses aspects of configuring Microsoft Windows Server 2008 R2 Active Directory, as well as Kerberos and Oracle Advanced Security Option.

The article is intended to supplement the Oracle Advanced Security Administrator's Guide. This article has a minimum version requirement of 11.2.0.2 for both the client and database server.

The article assumes the existence of an already fully functional Microsoft Windows 2008 R2 Active Directory server and an Oracle Database server with Advanced Security Option (ASO) installed.

DETAILS

NOTE: In the images and/or the document content below, the user information and data used represents fictitious data from the Oracle sample schema(s) or Public Documentation delivered with an Oracle database product. Any similarity to actual persons, living or dead, is purely coincidental and not intended in any manner.

Overview

Kerberos is a network authentication protocol originally developed by MIT that authenticates users to network resources, such as an Oracle database. Through the use of service tickets and symmetric-key cryptography, Kerberos eliminates the need to transmit passwords over the network. Oracle Advanced Security Option (ASO) provides authentication adapters for most common external authentication schemes, including Kerberos.

An Oracle database server typically services many Oracle clients. When configured for Kerberos authentication, the database server becomes a client of the Kerberos Key Distribution Centre (KDC).

Topology

The configuration referred to throughout the article is based on the following topology.

Kerberos Server (Microsoft KDC):

* Host name:<hostname1>.<domain>
* Microsoft Windows Server 2008 R2 Enterprise Edition with Service Pack 1
* Active Directory (incorporating Kerberos Key Distribution Centre (KDC))
* Realm name: <HOST1>.<LOCAL>

Oracle Database:

* Host name: oraclebox1.<domain>
* Oracle Enterprise Linux 5
* Oracle11g R2 Server Enterprise Edition

Oracle Client:

* Microsoft Windows XP
* Oracle11g R2 Client installation full version

Part 1: Create Users in Windows 2008 R2 Active Directory

Within Microsoft Active Directory a minimum of two 'users' must be created. Using Kerberos terminology these would be considered to be principals, one for the Oracle server and one for an Oracle user.

In this example the domain for the Microsoft server is <HOST1>.<LOCAL> which would also be the Kerberos realm.

First within 'Active Directory Users and Computers' create a new user for the user for the principal for the Oracle server,

The ‘First Name’ is the fully qualified domain name of the machine the Oracle server is running on.

The ‘Full Name’ will automatically be filled in.

The dialogue box for ‘User logon name’ is of limited width and will not necessarily fit a fully qualified domain name, so a shorter name such as hostname should be used.

After clicking next enter a password twice,

Finally clicking ‘Next’ followed by ‘Finish’ will create the user.

The next step is to create an Active Directory user for an Oracle database user. In this example the user ‘Testuser’ is being created,

Part 2: Create Key Table in Windows 2008 R2

The final step on the Windows 2008 R2 server is to extract a key table for the database server principal. This is done using the KTPASS.EXE tool.

```
C:\>ktpass.exe -princ oracle/oraclebox1.<domain>@<HOST1>.<LOCAL> -mapuser oraclebox1.<domain>
-crypto all -pass password -out c:\keytab
```

The resulting keytab file should then be transferred to the machine running Oracle.

Part 3: Configuring the Oracle Database

It is assumed an Oracle database has been created on this server. First user(s) must be created within the database. In this example user 'TESTUSER' is created who will represent the user TESTUSER create with Active Directory,

```
SQL> create user "TESTUSER@<HOST1>.<LOCAL>" identified externally;
SQL> grant create session to "TESTUSER@<HOST1>.<LOCAL>";
```

This username must be created in uppercase and must have the realm (Active Directory domain) specified.

Next confirm that the system settings remote_os_authent=false and os_authent_prefix="" are configured correctly,

```
SQL> select value from v$parameter where name = 'os_authent_prefix';

VALUE
-----------------------------------------------------------------


SQL> select value from v$parameter where name = 'remote_os_authent';

VALUE
-----------------------------------------------------------------
FALSE
```

Part 4: Configuring SQLNET for Kerberos on the Oracle Server

> Note: One has to check whether the kerberos5 adapter is enabled at OS level. For this open /etc/services file and check if kerberos5 is present as follows:
>
> kerberos 88/tcp kerberos5 krb5 # Kerberos v5
>
> kerberos 88/udp kerberos5 krb5 # Kerberos v5

The Oracle server sqlnet.ora file needs to be configured for Kerberos authentication.

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

The SQLNET.KERBEROS5_KEYTAB setting should point to the keytab file that was transferred from the Active Directory machine.

The SQLNET.KERBEROS5_CONF setting refers to a Kerberos configuration file that doesn't exist on Microsoft Kerberos, so it will be created manually.

The SQLNET.AUTHENTICATION_KERBEROS5_SERVICE refers to the 'oracle/' part added to the server principal name when ktpass.exe was run.

The krb5.conf file is a standard MIT Kerberos configuration file that stores information regarding the machine Kerberos is running on. This file will need entries similar with:

```
[libdefaults]
default_realm = <HOST1>.<LOCAL>
[realms]
<HOST1>.<LOCAL> = {
kdc = <host1>.<domain>:88
}
[domain_realm]
.<domain> = <HOST1>.<LOCAL>
<domain> = <HOST1>.<LOCAL>
```

Part 5: Configuring SQLNET for Kerberos on the Oracle Client for a manual ticket

Note: One has to check whether the kerberos5 adapter is enabled at OS level. For this open C:\Windows\system32\etc\drivers\services file and check if kerberos5 is present as follows:

kerberos 88/tcp kerberos5 krb5 # Kerberos v5

kerberos 88/udp kerberos5 krb5 # Kerberos v5

There are 2 mechanisms an Oracle client running on Windows can use to get a Kerberos ticket from Active Directory - Either get a manual ticket from the command line using okinit, or use the Windows internal credentials cache where the client machine is a member of the Active Directory domain.

This section covers the manual ticket, and the next section will cover the internal credential cache method.

On the 11.2.0.2 client ensure that Oracle Advanced Security is installed, and then in the client sqlnet.ora configure kerberos authentication with,

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

The krb5.conf file that was created on the Oracle server should also be created on the client - in this example it was created as c:\kerberos\krb5.conf

This client can then get a manual ticket using the command line tool okinit - For example,

```
C:\>okinit -e 23 Testuser

Kerberos Utilities for 32-bit Windows: Version 11.2.0.2.0 - Production on 15-MAR
```

```
-2011 xx:xx:xx

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

Password for testuser@<HOST1>.<LOCAL>:
```

The ticket can be seen using the command line tool oklist,

```
C:\>oklist

Kerberos Utilities for 32-bit Windows: Version 11.2.0.2.0 - Production on 15-MAR-2011
11:36:14

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

Ticket cache: c:\kerberos\cc
Default principal: testuser@<HOST1>.<LOCAL>

Valid Starting Expires Principal
15-Apr-20xx xx:xx:xx 15-Mar-20xx xx:xx:xx krbtgt/<HOST1>.<LOCAL>@<HOST1>.<LOCAL>
```

Finally the connection to the Oracle database can be made using sqlplus,

```
sqlplus /@orcl ### Here orcl is the database name which you want to connect using kerberos
authentication
```

Part 6: Configuring SQLNET for Kerberos on the Oracle Client using the internal credential cache

Where the client Windows Pc is a member of Active Directory Domain, and the user has logged into the Windows machine as a domain user, then Oracle is able to use the internal Windows credentials cache.

This cache is a Kerberos ticket and removes the need to get a ticket manually with okinit.

On the 11.2.0.2 client ensure that Oracle Advanced Security is installed, and then in the client sqlnet.ora configure kerberos authentication with,

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

The krb5.conf file that was created on the Oracle server should also be created on the client - in this example it was created as c:\kerberos\krb5.conf

As with a manual ticket you are able to see the ticket using oklist, and a connection can be made in the same manner using sqlplus.

Note:

####

For RAC systems as well need to add each node servername as the server principal in the active directory.

The kerberos 5 service should be already present in the /etc/service. If this is missing or not present please work with your system administrator to have it installed.