Overview and Configuration of ASO Encryption [ID 76629.1]

Modified 22-NOV-2011 *Type* BULLETIN *Status* PUBLISHED

In this Document

Applies to:

Advanced Networking Option - Version: 9.2 to 11.1 - Release: 9.2 to
Information in this document applies to any platform.
Checked for relevance on 22-Nov-2011

Purpose

This document explains about Encryption and Integrity solutions provided by Oracle, also configuring and troubleshooting the same.

Scope and Application

The readers of this document are expected to have a basic knowledge on Networks ,SQLNET and Network Security.

Overview and Configuration of ASO Encryption

What is Encryption ?

Encryption is a technique by which any information sent over a network is modified such that only authorized entities can understand the original information. For an unauthorized entity the information appears unintelligible.

Converting a plain text to cipher text based on a key is termed as Encryption and the vice versa is termed as Decryption.

What is Integrity [Check summing] ?

When a large piece of information is sent over a network , it is multi sected in to small packets . All these packets are transmitted in a sequence.

Rate this document

Integrity is a technique by which one verifies that all the packets which are transmitted by the source have reached the target in the same sequence and are not altered in between.

Why Encryption And Integrity ?

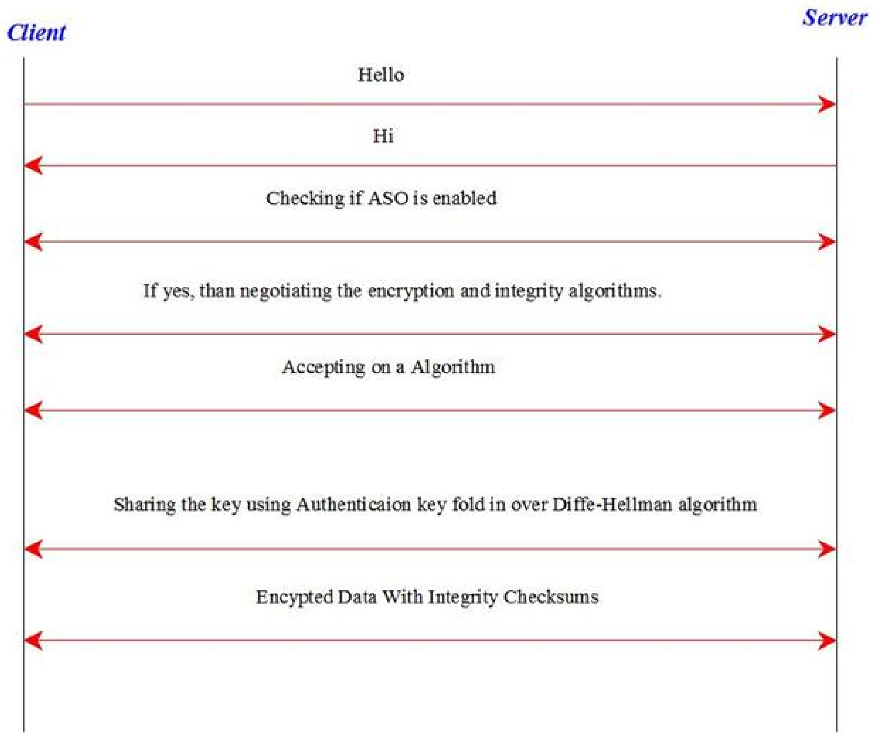
With the increased usage of internet and large corporate intranets, sensitive information in an Enterprise is transmitted over networks during day to day activities. Using Encryption and Integrity you can make sure only intended parties will have access to the information and also that it arrives unaltered, it allows you to communicate in a secure way end to end without the need to worry about the security of the intermediate network path either internal or over a public network.

For more information on security attacks and threats refer " Security Challenges in an Enterprise Environment " Section of Chapter 1 of Oracle Database Advanced Security Administratorâs Guide 11g Release 1 (11.1).

Oracle's Solution To The Security Challenges :

Oracle's Advanced Security Options addresses the security challenges with its implementation of Encryption and Integrity.

The following diagram briefly explains how encryption and integrity is implemented by Oracle's Advanced Security Options.


Client
Server
Hello
Hi
Checking if ASO is enabled
If yes, than negotiating the encryption and integrity algorithms.
Accepting on a Algorithm
Sharing the key using Authenticaion key fold in over Diffe-Hellman algorithm
Encypted Data With Integrity Checksums

Encryption Algorithms Supported By Oracle [11g] :

RC4 Encryption
DES Encryption
Triple-DES Encryption
Advanced Encryption Standard

Integrity Algorithms Supported By Oracle [11g] :

Message Digest 5(MD5) algorithm
Secure Hash Algorithm (SHA-1)

For more information on the above algorithms and " Authentication key fold in over Diffe-Hellman algorithm " refer Chapter 4 of Oracle Database Advanced Security Administratorâs Guide 11g Release 1 (11.1)

Configuring Encryption and Integrity

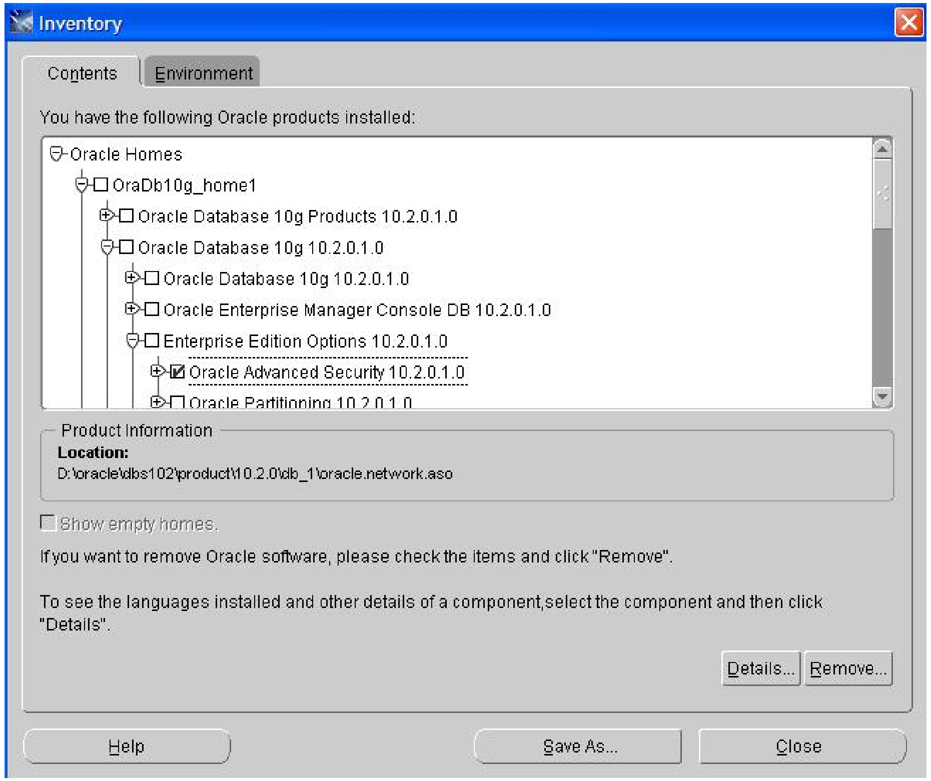
Where to configure Advanced Security Options ?

In general Encryption and Integrity can be configured between a database client and database server , for which Advanced Security Options has to be installed on both sides.

In order to configure Advanced Security Options over JDBC Thin Driver refer to Chapter 5 of Oracle Database Advanced Security Administratorâs Guide 11g Release 1 (11.1).

Check whether Advanced Security Options is installed.

Run Oracle Universal Installer from the installation home and select the installed products, Advanced Security Options has to be reflected as shown below :



Inventory

You have the following Oracle products installed:

```
⊖ Oracle Homes
  ⊖ □ OraDb10g_home1
    ⊕ □ Oracle Database 10g Products 10.2.0.1.0
    ⊖ □ Oracle Database 10g 10.2.0.1.0
      ⊕ □ Oracle Database 10g 10.2.0.1.0
      ⊕ □ Oracle Enterprise Manager Console DB 10.2.0.1.0
      ⊖ □ Enterprise Edition Options 10.2.0.1.0
        ⊕ ☑ Oracle Advanced Security 10.2.0.1.0
        ⊕ □ Oracle Partitioning 10.2.0.1.0
```

Product Information
Location:
D:\oracle\dbs102\product\10.2.0\db_1\oracle.network.aso

□ Show empty homes.

If you want to remove Oracle software, please check the items and click "Remove".

To see the languages installed and other details of a component,select the component and then click "Details".

If not than install the Advanced Security Options by doing a advanced installation over the required Oracle Home.

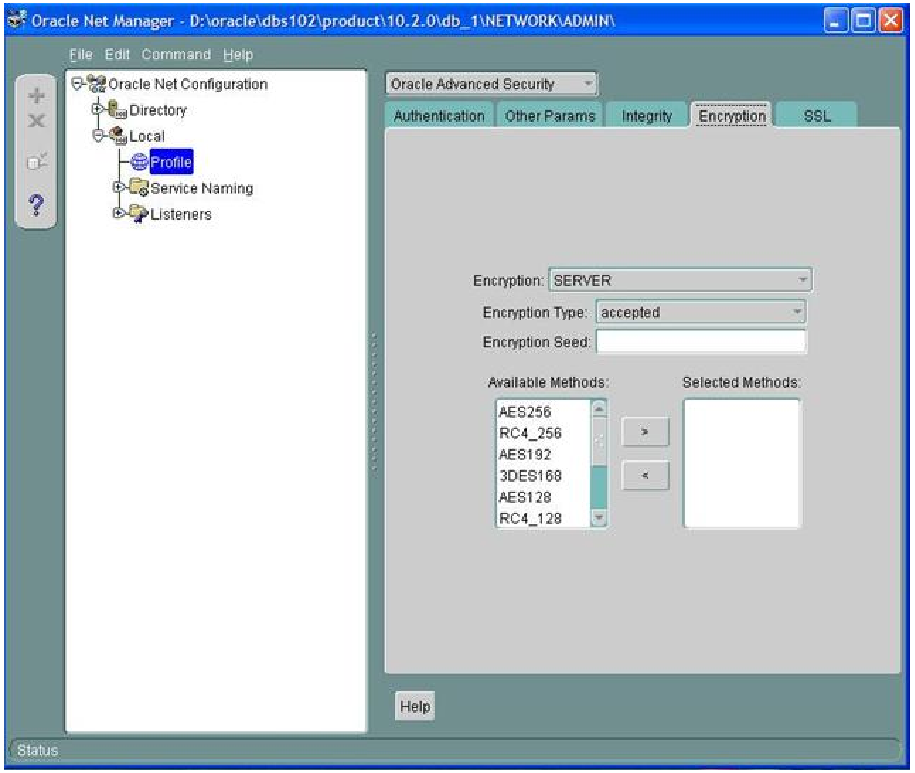
Configuring encryption on database client and database server :

a.) Launch NET MANAGER from the oracle home in which the encryption and integrity has to be configured.

b.) On the left pan expand "Local" and select "profile"

c.) On the Right pan from the drop down list select " Oracle Advanced Security "

d.) Select "Encryption" tab, the page should look as shown below :



Encryption: SERVER

Encryption Type: accepted

Encryption Seed:

Available Methods: AES256, RC4_256, AES192, 3DES168, AES128, RC4_128

e.)From the drop down list select CLIENT or SERVER appropriately.

f.)From the Encryption Type list, select one of the following :
REQUESTED - to enable the security service if the other side allows it
REQUIRED - to enable the security service and disallow the connection if the other side is not enabled for the security service
ACCEPTED - to enable the security service if required or requested by the other side
REJECTED - to disable the security service, even if the required by the other side

g.)Optionally in the Encryption Seed field, enter between 10 and 70 random characters.

> The encryption seed for the client should not be the same as that for the server.

h.)Select an encryption algorithm in the Available Methods list. Move it to the Selected Methods list by choosing the right arrow [>].

Repeat for each additional method you want to use.

i.)Save the configuration by selecting Choose File -> Save Network Configuration.
The respective changes should be reflected in the SQLNET.ORA.

j.)Repeat the same procedure to configure encryption on the server.

The SQLNET.ORA file on the two systems should contain the following entries :

On the server :

```
SQLNET.ENCRYPTION_SERVER = [accepted | rejected | requested | required]
SQLNET.ENCRYPTION_TYPES _SERVER = (encryption,[integrity])
SQLNET.CRYPTO_SEED = [crypto seed]
```

On the client :

```
SQLNET.ENCRYPTION_CLIENT = [accepted | rejected | requested | required]
SQLNET.ENCRYPTION_TYPES_CLIENT = (encryption,[integrity])
SQLNET.CRYPTO_SEED = [crypto seed]
```

The default value of SQLNET.ENCRYPTION_<CLIENT/SERVER> is ACCEPTED. Depending upon the value of this parameter at both the sides the encryption is activated or inactivated.

By default both the client and server supports All encryption algorithms. However you can specify specific list of encryption algorithms using SQLNET.ENCRYPTION_TYPES_<CLIENT/SERVER> parameter.

Configuring integrity on database client and database server :

a.) Launch NET MANAGER from the oracle home in which the encryption and integrity has to be configured.

b.) On the left pan expand "Local" and select "profile"

c.) On the Right pan from the drop down list select " Oracle Advanced Security "

d.) Select "Integrity" tab, this will open a tab similar to the encryption tab shown above

e.)From the drop down list select CLIENT or SERVER appropriately.

f.)From the Checksum Level list, select one of the checksum level values

g.)Select an integrity alorithm in the Available Methods list. Move it to the Selected Methods list by choosing the right arrow [>].

Repeat for each additional method you want to use.

i.)Save the configuration by selecting Choose File -> Save Network Configuration.
The respective changes should be reflected in the SQLNET.ORA.

j.)Repeat the same procedure to configure integrity on the server.

On the server:

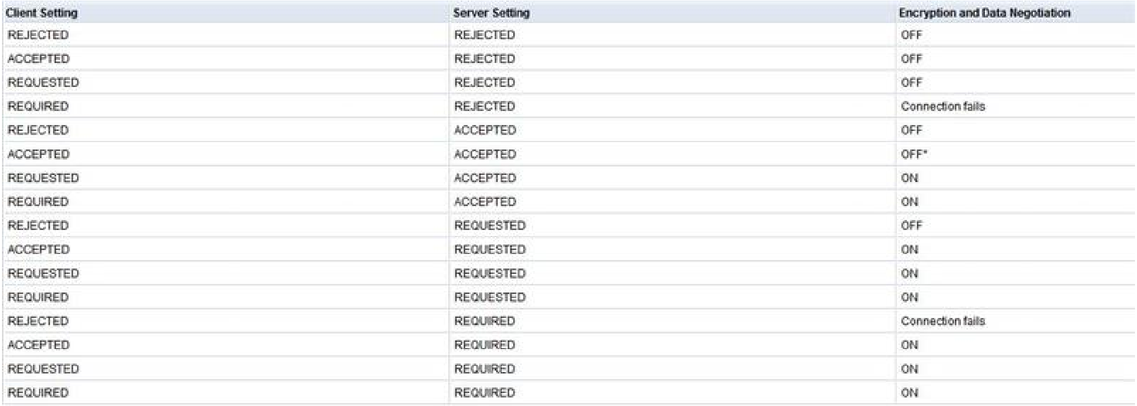
```
SQLNET.CRYPTO_CHECKSUM_SERVER = [accepted | rejected | requested | required]
SQLNET.CRYPTO_CHECKSUM_TYPE_SERVER = (encryption,[integrity])
```

On the client:

```
SQLNET.CRYPTO_CHECKSUM_CLIENT = [accepted | rejected | requested | required]
SQLNET.CRYPTO_CHECKSUM_TYPE_CLIENT = (encryption,[integrity])
```

The default value of SQLNET.CRYPTO_CHECKSUM_TYPE_<CLINET/SERVER> is MD5.

The Following table describes the outcome of negotiations on encryption and integrity levels :



Client Setting	Server Setting	Encryption and Data Negotiation
REJECTED	REJECTED	OFF
ACCEPTED	REJECTED	OFF
REQUESTED	REJECTED	OFF
REQUIRED	REJECTED	Connection fails
REJECTED	ACCEPTED	OFF
ACCEPTED	ACCEPTED	OFF*
REQUESTED	ACCEPTED	ON
REQUIRED	ACCEPTED	ON
REJECTED	REQUESTED	OFF
ACCEPTED	REQUESTED	ON
REQUESTED	REQUESTED	ON
REQUIRED	REQUESTED	ON
REJECTED	REQUIRED	Connection fails
ACCEPTED	REQUIRED	ON
REQUESTED	REQUIRED	ON
REQUIRED	REQUIRED	ON

How to Verify Whether Encryption and Integrity is working ?

The best method is to take a SQLNET client and server trace and verify whether the information in the trace is in cipher text[encrypted] or in plain text.

A part of the client trace before enabling the Encryption and Integrity will be as shown below :

```
nspsend: 00 00 00 00 00 24 46 65 |.....$Fe|
nspsend: 01 12 73 65 6C 65 63 74 |..select|
nspsend: 20 2A 20 66 72 6F 6D 20 |.*.from.|
nspsend: 64 75 61 6C 01 00 00 00 |dual....|
nspsend: 00 00 00 00 00 00 00 00 |........|
nspsend: 00 00 00 00 00 00 00 00 |........|
nspsend: 00 00 00 00 00 00 00 00 |........|
nspsend: 01 00 00 00 00 00 00 00 |........|
nspsend: 00 00 00 00 00 00 00 00 |........|
nspsend: 00 00 00 00 00 00 00 00 |........|
```

A part of the client trace after enabling the Encryption and Integrity will be as shown below :

```
nspsend: 1F C6 56 89 B0 5C 83 CA |..V..\..|
nspsend: 90 B4 B0 8E 45 0C 00 32 |....E..2|
nspsend: CE BC 9F 22 43 76 DD 84 |..."Cv..|
nspsend: EF 61 25 62 29 8A 0D A8 |.a%b)...|
nspsend: 2F DE 12 38 18 80 A8 56 |/..8...V|
nspsend: 44 AD A2 7E B6 7A 7D E1 |D..~.z}.|
nspsend: 28 76 9B D9 54 6F 2C 72 |(v..To,r|
nspsend: 6F 3F 45 17 DA 2D 93 CB |o?E..-..|
nspsend: EE C6 29 31 E1 BF 22 E5 |..)1..".|
nspsend: 02 32 0B F6 26 CA F4 4C |.2..&..L|
nspsend: B8 BC A0 5E C7 64 1D DC |...^.d..|
nspsend: 78 B3 D2 43 B5 1A D7 C4 |x..C....|
nspsend: 9A 79 1F 3C A8 EE DC 38 |.y.<...8|
nspsend: E2 5C 07 01 |.\.. |
```

The below My Oracle Support document contains the information on generating a client and server trace :

Note 395525.1 How to Enable Oracle SQLNet Client , Server , Listener , Kerberos and External procedure Tracing from Net Manager

References

NOTE:395525.1 - How to Enable Oracle SQLNet Client , Server , Listener , Kerberos and External procedure Tracing from Net Manager

Related

Products

- Oracle Database Products > Oracle Database > Net Services > Advanced Networking Option

Keywords

ADVANCED ENCRYPTION STANDARD; ADVANCED NETWORKING OPTION; DATA ENCRYPTION STANDARD; SQLNET.CRYPTO_CHECKSUM_CLIENT; SQLNET.CRYPTO_CHECKSUM_SERVER; SQLNET.ENCRYPTION_CLIENT; SQLNET.ENCRYPTION_SERVER; SQLNET.ENCRYPTION_TYPES_CLIENT

Back to top