Additional ENCRYPTION Option In 11g DATAPUMP [ID 1195013.1]

Modified 29-OCT-2010 *Type* HOWTO *Status* PUBLISHED

In this Document

Applies to:

Oracle Server - Enterprise Edition - Version: 11.1.0.7 to 11.2.0.1.0 - Release: 11.1 to 11.2
Information in this document applies to any platform.

Goal

To describe how to encrypt both data and metadata, only data, only metadata, no data, or only encrypted columns during a datapump export?

Solution

User can specify additional encryption options in the following areas:

1. You can choose to encrypt both data and metadata, only data, only metadata, no data, or only encrypted columns during a DataPump export using the ENCRYPTION parameter.

ENCRYPTION:

Default: The default value depends upon the combination of encryption-related parameters that are used. To enable encryption, either the ENCRYPTION or ENCRYPTION_PASSWORD parameter, or both, must be specified. If only the ENCRYPTION_PASSWORD parameter is specified, then the ENCRYPTION parameter defaults to ALL. If neither ENCRYPTION nor ENCRYPTION_PASSWORD is specified, then ENCRYPTION defaults to NONE.

Purpose :

Specifies whether or not to encrypt data before writing it to the dump file set.

Syntax and Description :

ENCRYPTION = {ALL | DATA_ONLY | ENCRYPTED_COLUMNS_ONLY | METADATA_ONLY | NONE}
ALL enables encryption for all data and metadata in the export operation.

* DATA_ONLY specifies that only data is written to the dump file set in encrypted format.

* ENCRYPTED_COLUMNS_ONLY specifies that only encrypted columns are written to the dump file set in encrypted format.

* METADATA_ONLY specifies that only metadata is written to the dump file set in encrypted format.

* NONE specifies that no data is written to the dump file set in encrypted format.

2. User can specify a specific encryption algorithm to use during a DataPump export using the parameter ENCRYPTION_ALGORITHM.

Users can specify the type of security to use for performing encryption and decryption during an export. For example, perhaps the dump file set will be imported into a different or remote database and it must remain secure in transit. Or perhaps the dump file set will be imported onsite using the Oracle Encryption Wallet but it may also need to be imported offsite where the Oracle Encryption Wallet is not available.

ENCRYPTION_ALGORITHM

Default: AES128

Purpose:

Specifies which cryptographic algorithm should be used to perform the encryption.

Syntax and Description :

ENCRYPTION_ALGORITHM = { AES128 | AES192 | AES256 }
See Oracle Database Advanced Security Administrator's Guide for information about encryption algorithms.

Restrictions :

***** To use this encryption feature, the COMPATIBLE initialization parameter must be set to at least 11.0.0.

***** The ENCRYPTION_ALGORITHM parameter requires that you also specify either the ENCRYPTION or ENCRYPTION_PASSWORD parameter; otherwise an error is returned.

***** This parameter is valid only in the Enterprise Edition of Oracle Database 11g.

3. Users can specify the type of security to use for performing encryption and decryption during the DataPump export. For example, perhaps the dump file set will be imported into a different or remote database and it must remain secure in transit. Or perhaps the dump file set will be imported onsite using the Oracle Encryption Wallet but it may also need to be imported offsite where the Oracle Encryption Wallet is not available. Please refer to the parameter ENCRYPTION_MODE.

ENCRYPTION_MODE

Default: The default mode depends on which other encryption-related parameters are used. If only the ENCRYPTION parameter is specified, then the default mode is TRANSPARENT. If the ENCRYPTION_PASSWORD parameter is specified and the Oracle Encryption Wallet is open, then the default is DUAL. If the ENCRYPTION_PASSWORD parameter is specified and the Oracle Encryption Wallet is closed, then the default is PASSWORD.

Purpose :

Specifies the type of security to use when encryption and decryption are performed.

Syntax and Description:

ENCRYPTION_MODE = { DUAL | PASSWORD | TRANSPARENT }
DUAL mode creates a dump file set that can later be imported either transparently or by specifying a password that was used when the dual-mode encrypted dump file set was created. When you later import the dump file set created in DUAL mode, you can use either the Oracle Encryption Wallet or the password that was specified with the ENCRYPTION_PASSWORD parameter. DUAL mode is best suited for cases in which the dump file set will be imported onsite using the Oracle Encryption Wallet, but which may also need to be imported offsite where the Oracle Encryption Wallet is not available.

***** **PASSWORD** mode requires that you provide a password when creating encrypted dump file sets. You will need to provide the same password when you import the dump file set. PASSWORD mode requires that you also specify the ENCRYPTION_PASSWORD parameter. The PASSWORD mode is best suited for cases in which the dump file set will be imported into a different or remote database, but which must remain secure in transit.

***** **TRANSPARENT** mode allows an encrypted dump file set to be created without any intervention from a database administrator (DBA), provided the required Oracle Encryption Wallet is available. Therefore, the ENCRYPTION_PASSWORD parameter is not required, and will in fact, cause an error if it is used in TRANSPARENT mode. This encryption mode is best suited for cases in which the dump file set will be imported into the same database from which it was exported.

Restrictions:

***** To use DUAL or TRANSPARENT mode, the COMPATIBLE initialization parameter must be set to at least 11.0.0.

***** When user use the ENCRYPTION_MODE parameter, user must also use either the ENCRYPTION or ENCRYPTION_PASSWORD parameter. Otherwise, an error is returned.

***** This parameter is valid only in the Enterprise Edition of Oracle Database 11g.

Example: (test case)

```
$ sqlplus

SQL*Plus: Release 11.1.0.7.0 - Production on Thu Sep 2 04:07:19 2010

Copyright (c) 1982, 2008, Oracle. All rights reserved.

Enter user-name: sys as sysdba
Enter password:

Connected to:
Oracle Database 11g Enterprise Edition Release 11.1.0.7.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options


SQL>
SQL>
-- Created directory to place the dumpfile------
SQL> create directory vi as '/tmp';

Directory created.

SQL> conn vishwa/vishwa
Connected.
SQL>
SQL>
SQL>
SQL> select * from tab;

no rows selected


--- Created table ----
SQL> create table emp (n number,name varchar2(23));

Table created.

-- Inserted rows in a table emp-----

SQL> insert into emp values(&n,'&name');
Enter value for n: 1
Enter value for name: mohan
old 1: insert into emp values(&n,'&name')
new 1: insert into emp values(1,'mohan')

1 row created.

SQL> /
Enter value for n: 3
Enter value for name: rajesh
old 1: insert into emp values(&n,'&name')
new 1: insert into emp values(3,'rajesh')

1 row created.

SQL> /
Enter value for n: 5
Enter value for name: mahesh
old 1: insert into emp values(&n,'&name')
new 1: insert into emp values(5,'mahesh')
```

```
1 row created.

SQL> /
Enter value for n: 9
Enter value for name: kapa
old 1: insert into emp values(&n,'&name')
new 1: insert into emp values(9,'kapa')

1 row created.

SQL> commit;

Commit complete.

SQL> select * from emp;

N NAME
---------- ----------
1 mohan
3 rajesh
5 mahesh
9 kapa
```

-- Export Schema "vishwa" by specifying password for dumpfile ----

```
$expdp system/manager directory=vi dumpfile=vishwa.dmp logfile=vishwa.log ENCRYPTION=data_only ENCRYPTION_PASSWORD=test schemas=vishwa

Export: Release 11.1.0.7.0 - Production on Thursday, 02 September, 2010 4:13:14

Copyright (c) 2003, 2007, Oracle. All rights reserved.

Connected to: Oracle Database 11g Enterprise Edition Release 11.1.0.7.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options
FLASHBACK automatically enabled to preserve database integrity.
Starting "SYSTEM"."SYS_EXPORT_SCHEMA_01": system/******** directory=vi dumpfile=vishwa.dmp logfile=vishwa.log ENCRYPTION=data_only ENCRYPTION_PASSWORD=******** schemas=vishwa
Estimate in progress using BLOCKS method...
Processing object type SCHEMA_EXPORT/TABLE/TABLE_DATA
Total estimation using BLOCKS method: 64 KB
Processing object type SCHEMA_EXPORT/USER
Processing object type SCHEMA_EXPORT/SYSTEM_GRANT
Processing object type SCHEMA_EXPORT/ROLE_GRANT
Processing object type SCHEMA_EXPORT/DEFAULT_ROLE
Processing object type SCHEMA_EXPORT/PRE_SCHEMA/PROCACT_SCHEMA
Processing object type SCHEMA_EXPORT/TABLE/TABLE
Processing object type SCHEMA_EXPORT/POST_SCHEMA/PROCACT_SCHEMA
. . exported "VISHWA"."EMP" 5.453 KB 4 rows
Master table "SYSTEM"."SYS_EXPORT_SCHEMA_01" successfully loaded/unloaded
******************************************************************************
Dump file set for SYSTEM.SYS_EXPORT_SCHEMA_01 is:
/tmp/vishwa.dmp
Job "SYSTEM"."SYS_EXPORT_SCHEMA_01" successfully completed at 04:14:35

$sqlplus sys as sysdba

SQL*Plus: Release 11.1.0.7.0 - Production on Thu Sep 2 04:15:23 2010
```

```
Copyright (c) 1982, 2008, Oracle. All rights reserved.

Enter password:

Connected to:
Oracle Database 11g Enterprise Edition Release 11.1.0.7.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options

SQL> conn vishwa/vishwa
Connected.

-- Dropped table emp ----
SQL> drop table emp;

Table dropped.

SQL> exit

$ impdp system/manager directory=vi dumpfile=vishwa.dmp logfile=vishwaimp.log remap_schema=vishwa:vishwa
Import: Release 11.1.0.7.0 - Production on Thursday, 02 September, 2010 4:16:25

Copyright (c) 2003, 2007, Oracle. All rights reserved.

Connected to: Oracle Database 11g Enterprise Edition Release 11.1.0.7.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options
ORA-39002: invalid operation
ORA-39174: Encryption password must be supplied. <<<<< ---- Failed, need to specify the password.
```

-- Import the same password protected dumpfile by specifying the password---

```
$ impdp system/manager directory=vi dumpfile=vishwa.dmp logfile=vishwaimp.log remap_schema=vishwa:vishwa ENCRYPTION_PASSWORD=test

Import: Release 11.1.0.7.0 - Production on Thursday, 02 September, 2010 4:17:40

Copyright (c) 2003, 2007, Oracle. All rights reserved.

Connected to: Oracle Database 11g Enterprise Edition Release 11.1.0.7.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options
Master table "SYSTEM"."SYS_IMPORT_FULL_01" successfully loaded/unloaded
Starting "SYSTEM"."SYS_IMPORT_FULL_01": system/******** directory=vi dumpfile=vishwa.dmp logfile=vishwaimp.log remap_schema=vishwa:vishwa ENCRYPTION_PASSWORD=********
Processing object type SCHEMA_EXPORT/USER
Processing object type SCHEMA_EXPORT/SYSTEM_GRANT
Processing object type SCHEMA_EXPORT/ROLE_GRANT
Processing object type SCHEMA_EXPORT/DEFAULT_ROLE
Processing object type SCHEMA_EXPORT/PRE_SCHEMA/PROCACT_SCHEMA
Processing object type SCHEMA_EXPORT/TABLE/TABLE
Processing object type SCHEMA_EXPORT/TABLE/TABLE_DATA
. . imported "VISHWA"."EMP" 5.453 KB 4 rows
Processing object type SCHEMA_EXPORT/POST_SCHEMA/PROCACT_SCHEMA
Job "SYSTEM"."SYS_IMPORT_FULL_01" completed without error(s) at 04:17:47
```

Related

Products

- Oracle Database Products > Oracle Database > Oracle Database > Oracle Server - Enterprise Edition

Keywords

SECURE; VAULT; DATAPUMP; ENCRYPTION; SECURITY ADMINISTRATOR; ALGORITHM

Errors

ORA-39174; ORA-39002

Back to top