TDE Configuration steps:

On Primary Server:

-- Step 1--- CREATE MASTER KEY ---

USE MASTER

GO

CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'mYC0mpl3XP@$$w0rd12'

GO

-- Step 2--- CREATE CERTIFICATE ---

CREATE CERTIFICATE TDECert

WITH SUBJECT = 'TDE Certificate for Qshare Encrypted DB'

-- Step 3-- create a database encryption key on the user database ---

use [Qshare Encrypted DB]

CREATE DATABASE ENCRYPTION KEY

WITH ALGORITHM = AES\_256

ENCRYPTION BY SERVER CERTIFICATE TDECert;

GO

-- Step 4--- Run the following command to turn on TDE on the database ---

ALTER DATABASE [Qshare Encrypted DB]

SET ENCRYPTION ON

-- Step 5--- Run the following command to backup the certificate to a file ---

USE MASTER

GO

BACKUP CERTIFICATE TDECert

TO FILE = 'E:\TDE\TDECert\_File.cer'

WITH PRIVATE KEY (FILE = 'E:\TDE\TDECert\_Key.pvk' ,

ENCRYPTION BY PASSWORD = 'mYC0mpl3XP@$$w0rd12' )

GO

On Secondary DB:

-- Step 1--- CREATE MASTER KEY ---

USE MASTER

GO

CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'mYC0mpl3XP@$$w0rd12'

GO

-- Step 2--- Run the following command to backup the certificate to a file (-- Restore the certificate ) ---

USE MASTER

GO

CREATE CERTIFICATE TDECert

FROM FILE = 'E:\TDE\TDECert\_File.cer'

WITH PRIVATE KEY (FILE = 'E:\TDE\TDECert\_Key.pvk',

DECRYPTION BY PASSWORD = 'mYC0mpl3XP@$$w0rd12');

References:

<https://www.mssqltips.com/sqlservertip/3146/configuring-transparent-data-encryption-with-sql-server-2012-alwayson-availability-groups/>

<https://www.mssqltips.com/sqlservertip/6316/configure-sql-server-transparent-data-encryption-with-powershell/>

Useful Scripts:

SELECT name, symmetric\_key\_id, algorithm\_desc, create\_date

FROM sys.symmetric\_keys

WHERE symmetric\_key\_id = 101

go

SELECT

d.name,

d.is\_encrypted,

dek.encryption\_state,

dek.percent\_complete,

dek.key\_algorithm,

dek.key\_length

FROM

sys.databases as d

INNER JOIN sys.dm\_database\_encryption\_keys AS dek

ON d.database\_id = dek.database\_id