

TDE - enable,disable,backup,export,certificate backup

Last updated by | Vitor Tomaz | May 17, 2022 at 10:17 AM PDT

Contents

- [Issue](#)
- [Investigation/Analysis](#)
- [More Information](#)
- [Classification](#)

Issue

Unable to backup certificate on the Azure SQL Managed Instance

```
BACKUP CERTIFICATE MyServerCert
TO FILE = 'https://tapanmaudit.file.core.windows.net/certificates/MyCert.cer'
WITH PRIVATE KEY (file='https://tapanmaudit.file.core.windows.net/certificates/MyCertKEY.pvk ',
ENCRYPTION BY PASSWORD='MyTestKey123!@# ')
```

Msg 40538, Level 16, State 3, Line 31
A valid URL beginning with 'https://' is required as value for any filepath specified.

```
BACKUP CERTIFICATE MyServerCert
TO FILE = 'https://wasd2prodeus1aprsmi423.blob.core.windows.net/managedserver-d60072b7-6e71-45e6-a2ef-0e3f5eb2'
WITH PRIVATE KEY (file='https://wasd2prodeus1aprsmi423.blob.core.windows.net/managedserver-d60072b7-6e71-45e6-
ENCRYPTION BY PASSWORD='MyTestKey123!@# ')
```

Msg 15151, Level 16, State 1, Line 24
Cannot find the certificate 'MyServerCert', because it does not exist or you do not have permission.

Investigation/Analysis

Certificate cannot be backed up on Azure SQL Managed Instance as MI uses service-managed encryption.

More Information

How to check if TDE enabled for a database?

```
select database_id, name, is_encrypted from sys.databases
```

Symmetric key query:

-- List symmetric keys in Database | Azure SQL DB uses symmetric key

```
select * from sys.symmetric_keys
```

-- List asymmetric keys in Database

```
select * from sys.asymmetric_keys
```

Check current connections and whether they're encrypted:


```
select session_id, auth_scheme, encrypt_option, net_packet_size, client_net_address, connect_time from sys.dm_
order by encrypt_option
```



In-transit encryption:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-security-overview>

Important

All connections to Azure SQL Database require encryption (SSL/TLS) at all times while data is "in transit" to and from the database. In your application's connection string, you must specify parameters to encrypt the connection and not to trust the server certificate (this is done for you if you copy your connection string out of the Azure portal), otherwise the connection does not verify the identity of the server and is susceptible to "man-in-the-middle" attacks. For the [ADO.NET](#)  driver, for instance, these connection string parameters are Encrypt=True and TrustServerCertificate=False.

Enable TDE on MI

```
ALTER DATABASE DBname SET ENCRYPTION ON;
```

This enables the TDE encryption on the DB in MI. There is already a symmetric encryption key named ##MS_ServiceMasterKey## and the database is encrypted with certificate that gets listed in the encryption keys table after enabling encryption.

Useful queries

```
use Customer_DBName

select * from sys.certificates

use master

select * from sys.certificates

select * from sys.master_key_passwords

select * from sys.dm_database_encryption_keys

select * from sys.symmetric_keys

select * from sys.asymmetric_keys

select * from sys.databases where name = 'Customer_DBName'
```

Disabling TDE is performed in the same way:

```
ALTER DATABASE DBname SET ENCRYPTION ON;
```

Backup TDE enabled DB in MI

You cannot backup a TDE enabled database in MI. The backup in MI has to be performed over a URL that points to the Azure blob storage. Having TDE enabled disables this capability since the certificate cannot be backed up along with encrypted DB.

Following error message shows up in this situation:

System.Data.SqlClient.SqlError: The backup operation for a database with service-managed transparent data encryption is not supported on SQL Database Managed Instance. (Microsoft.SqlServer.Smo)

Export TDE enabled DB in MI

BACPAC export of TDE enabled DB in MI is allowed since export operation to BACPAC is equivalent to decrypting from disk and reading through SELECT statements for this export.

Certificate rotation in MI

Certificate rotation works for Managed Instance just like in Azure SQL Database.

Microsoft automatically rotates these certificates at least every 90 days.

<https://docs.microsoft.com/en-us/azure/sql-database/transparent-data-encryption-azure-sql>

Classification

Root cause tree:

How good have you found this content?



-