Fortanix®

Integration Guide

USING DATA SECURITY MANAGER WITH MSSQL SERVER TDE – ADVANCED

VERSION 1.0

Fortanix, Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052| United States of America | +1 (650) 943-2484 |
info@fortanix.com | www.fortanix.com

TABLE OF CONTENTS

1.0 INTRODUCTION 2

2.0 BEST PRACTICES 2

2.1 Enable Startup Trace Flag 2
2.1.1 Trace Flag 15025 2
2.1.2 Trace Flag 5013 3

3.0 TROUBLESHOOTING 3

4.0 LOGGING 6

5.0 UPGRADING EKM CLIENT 6

6.0 DOCUMENT INFORMATION 8

6.1 Document Location 8

6.2 Document Updates 8

6.3 Revision History ..... Error! Bookmark not defined.

1.0 INTRODUCTION

This document describes the best practices for Microsoft SQL Transparent Data Encryption (TDE) operations integration.

2.0 BEST PRACTICES

It is recommended to follow the MSSQL TDE implementation best practices.

- Always take a full database backup before TDE implementation.
- Use a separate service account for the sysadmin DB credentials for key rotation.
- Use a nomenclature for the TDE master keys such as `hostname_dbName` to easily identify the key associated with database instance running on a specific host.
- It is strongly advised not to delete the old master keys from the Fortanix Data Security Manager (DSM) as they are required to restore the database from old backups. You can always disable the old keys if you do not want anyone to access them.

2.1 ENABLE STARTUP TRACE FLAG

2.1.1 TRACE FLAG 15025

Microsoft introduced a startup trace flag (TF) 15025 to disable the HSM access that is required for a newly created VLF. This allows high-volume customer workloads to continue without interruption. Once this trace flag is enabled, SQL Server that uses EKM for encryption and key generation doesn't contact HSM during the creation or rotation of VLF.

This trace flag applies to SQL Server 2019 (15.x) CU 19, SQL Server 2022 (16.x) CU 1, and later.

Hence, we recommend our customers upgrade the MSSQL Always On database to 2019 CU19 or 2022 CU1 and turn on the trace flag (TF) 15025.

NOTE: To enable this TF, please refer to the steps in the following URL: https://learn.microsoft.com/en-us/troubleshoot/sql/releases/sqlserver-2022/database-accessibility-issues-high-volume-customer-workloads

2.1.2 TRACE FLAG 5013

Microsoft also has a trace flag (TF) 5013 that is undocumented and works with SQL Server 2017 and above. In a high transitional database, SQL always tries to get a key from Fortanix DSM. If there is a connection problem between the SQL database and Fortanix DSM, this flag uses the cache key to avoid the database from crashing.

3.0 TROUBLESHOOTING

If your database has been encrypted previously, you may see errors at this point. If you are asked to take a pending log backup, then take the backup using the following methods:

- **Using command:**

```
BACKUP LOG employee TO DISK = 'C:\employee.TRN'
GO
```

This will create a transaction log backup of the employee database and write the backup contents to file `"C:\employee.TRN"`. The `.TRN` extension is commonly used to indicate that the backup is a transaction log backup.

- **Using SQL Server Management Studio:**
  1. Right-click the database name.
  2. Select **Tasks** > **Backup**.
  3. Select **Transaction Log** as the backup type.
  4. Select **Disk** as the destination.
     a) Click **Add...** to add a backup file and type "`C:\company.TRN`" and click **OK**.
     b) Click **OK** again to create the backup.

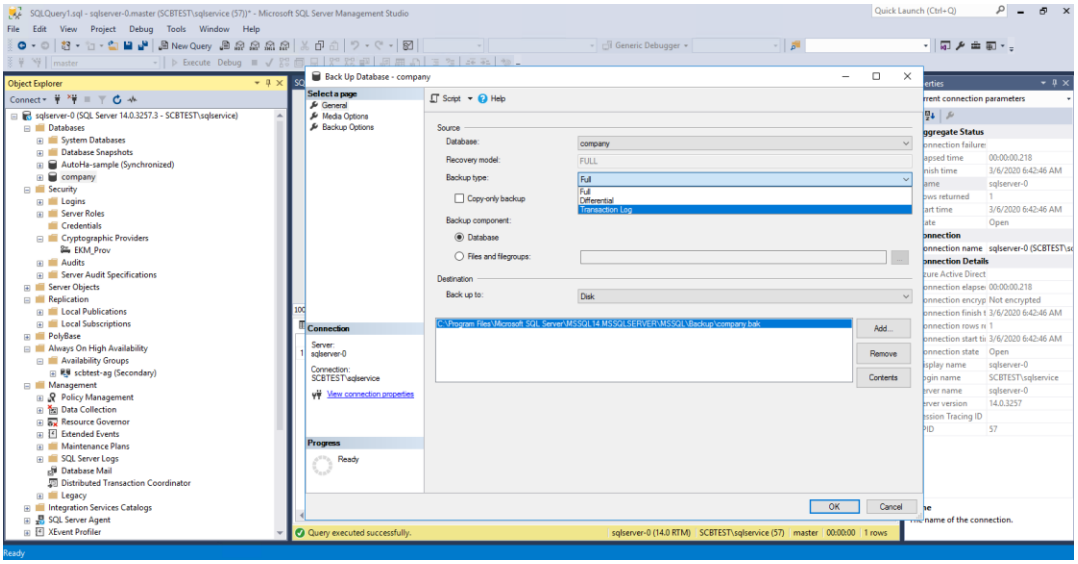

FIGURE 1: SQL SERVER MANAGEMENT STUDIO

If you get an error requesting that you take a log backup, then try the following commands to resolve the issue.

NOTE: Database administrators can try adapting the mentioned commands according to their requirements.

```
USE master;
GO
ALTER DATABASE <Name-of-your-database>
SET RECOVERY FULL;
GO
USE master;
GO
```

For example:

```
USE master;
GO
ALTER DATABASE SourceDatabase
SET RECOVERY FULL;
GO
USE master;
```

```
GO
EXEC sp_addumpdevice 'disk', 'EncryptedSourceDatabaseBackupLog',
'\\Server-2\NetWorkShareFolder\SourceDatabase_20160210122459';
GO
```

 **NOTE**: You should have provided a path to your backups when setting up your availability group.

```
EXEC sp_addumpdevice 'disk', '<Name-of-your-device>',
'<Path-to-your-backups>\<Name-of-your-log-backup-file>';
GO
```

Run the following command to take the back up of logs:

```
BACKUP LOG <Name-of-your-database> TO <Name-of-your-device>;
GO
```

For example:

```
BACKUP LOG SourceDatabase TO EncryptedSourceDatabaseBackupLog;
GO
```

Run the following command to drop the backup device:

```
EXEC sp_dropdevice '<Name-of-your-device>';
```

For example:

```
EXEC sp_dropdevice 'EncryptedSourceDatabaseBackupLog';
```

Run the following command to break any connection with the SourceDatabase so that encryption can commence:

```
USE [master];
GO
```

Run the following command to enable TDE (switch on encryption) on the SourceDatabase:

```
ALTER DATABASE SourceDatabase SET ENCRYPTION ON;
GO
```

4.0 LOGGING

Run the following command on the admin command prompt to find the External Key Manager (EKM) logs:

```
cd c:\
dir /s/a "EkmLog.txt"
```

The EKM log file is always located at the following path:
`C:\Windows\ServiceProfiles\MSSQLSERVER\AppData\Roaming\Fortanix\KmsClient`
Where, `MSSQLSERVER` will change according to your local setup.

5.0 UPGRADING EKM CLIENT

 **NOTE:** The upgrade from Fortanix CNG provider for Microsoft SQL Server EKM provider will uninstall the old CNG provider and install the latest downloaded version.

1. Download the latest CNG client from https://support.fortanix.com/hc/en-us/articles/360018084132-CNG-EKM
2. It is recommended to plan the downtime.
3. Ensure to take the latest database backup.
4. Install the updated client.

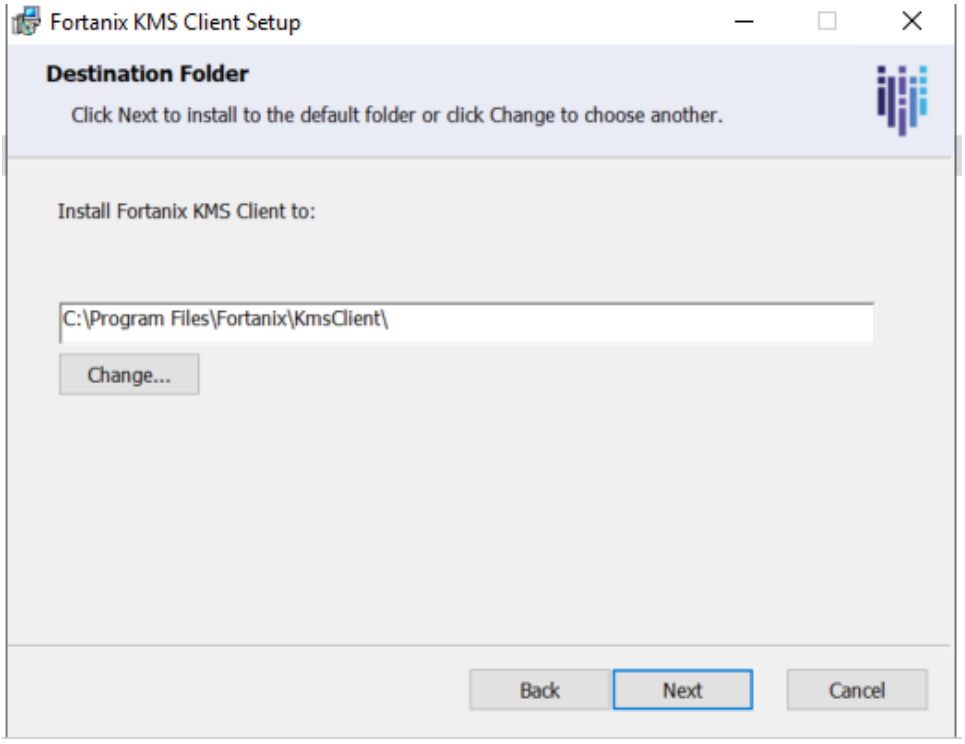

FIGURE 2: FORTANIX KMS CLIENT SETUP

5. Restart the Microsoft SQL Server service.

NOTE: For cluster setup, it is recommended to upgrade the secondary nodes before upgrading primary.

6.0 DOCUMENT INFORMATION

6.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

https://support.fortanix.com/hc/en-us/articles/13097103489556-Data-Security-Manager-with-Microsoft-SQL-Server-TDE-Guide-Advanced

6.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com