How to check TDE encryption status of MI DB

Last updated by | Radhika Shah | Jun 21, 2022 at 9:45 PM PDT

Contents

Issue

Customers complain that their databases on MI are not encrypted or have questions about DB encryption on MI.

Investigation/Analysis

By default, TDE is enabled at the instance level and newly created databases, with the following exceptions:

- Databases created through restore inherit encryption status from the source.
- Existing databases created before February 2019 are not encrypted by default.

For Azure SQL Managed Instance, the TDE protector is set at the instance level, and it is inherited by all encrypted databases on that instance.

TDE cannot be used to encrypt system databases, such as the master database, in Azure SQL Managed Instance. The master database contains objects that are needed to perform the TDE operations on the user databases. It is recommended to not store any sensitive data in the system databases.

The DMV *sys.dm_database_encryption_keys* returns information about the encryption state of a database and its associated database encryption keys.

Investigating from customer side

Customers can execute below T-SQL to check encryption status:

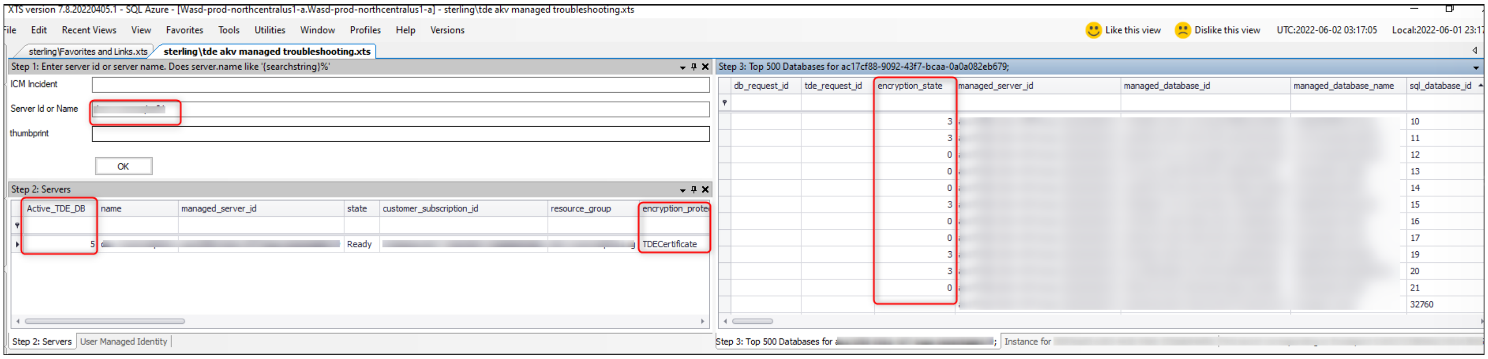
```
SELECT DB_NAME(database_id) AS [database],
encryption_state = CASE encryption_state
        WHEN '0'  THEN  'No database encryption key present, no encryption'
        WHEN '1'  THEN  'Unencrypted'
        WHEN '2'  THEN  'Encryption in progress'
        WHEN '3'  THEN  'Encrypted'
        WHEN '4'  THEN  'Key change in progress'
        WHEN '5'  THEN  'Decryption in progress'
        WHEN '6'  THEN  'Protection change in progress (The certificate or asymmetric key that is encrypting t
        ELSE 'No State'
        END,
encryption_scan_state = CASE encryption_scan_state
        WHEN '0'  THEN  'No scan has been initiated, TDE is not enabled'
        WHEN '1'  THEN  'Scan is in progress'
        WHEN '2'  THEN  'Scan is in progress but has been suspended, user can resume'
        WHEN '3'  THEN  'Scan was aborted for some reason, manual intervention is required. Contact Microsoft
        WHEN '4'  THEN  'Scan has been successfully completed, TDE is enabled and encryption is complete'
        ELSE 'No State'
        END,
percent_complete, encryptor_type, key_algorithm, key_length, modify_date
FROM sys.dm_database_encryption_keys
```

Note: When customer execute select * from sys.dm_database_encryption_keys, if there is row with encryption_state equals 3 that database with database_id is encrypted. If, for some database(s), corresponding row doesn't exists in this view, database is not encrypted.

Investigation from CSS side

For investigation from CSS side, encryption on MI DB can be verified via xts or Kusto.

XTS: sterling\tde akv managed troubleshooting.xts


XTS version 7.8.20220405.1 - SQL Azure - [Wasd-prod-northcentralus1-a.Wasd-prod-northcentralus1-a] - sterling\tde akv managed troubleshooting.xts
File Edit Recent Views View Favorites Tools Utilities Window Profiles Help Versions
Like this view
Dislike this view
UTC:2022-06-02 03:17:05
Local:2022-06-01 23:17
sterling\Favorites and Links.xts
sterling\tde akv managed troubleshooting.xts
OK
Step 2: Servers
User Managed Identity

Step 1: Enter server id or server name. Does server.name like '{searchstring}%'

ICM Incident:

Server Id or Name: [redacted]

thumbprint:

Step 2: Servers

Active_TDE_DB	name	managed_server_id	state	customer_subscription_id	resource_group	encryption_prote
5	[redacted]	[redacted]	Ready	[redacted]	[redacted]	TDECertificate

Step 3: Top 500 Databases for ac17cf88-9092-43f7-bcaa-0a0a082eb679;

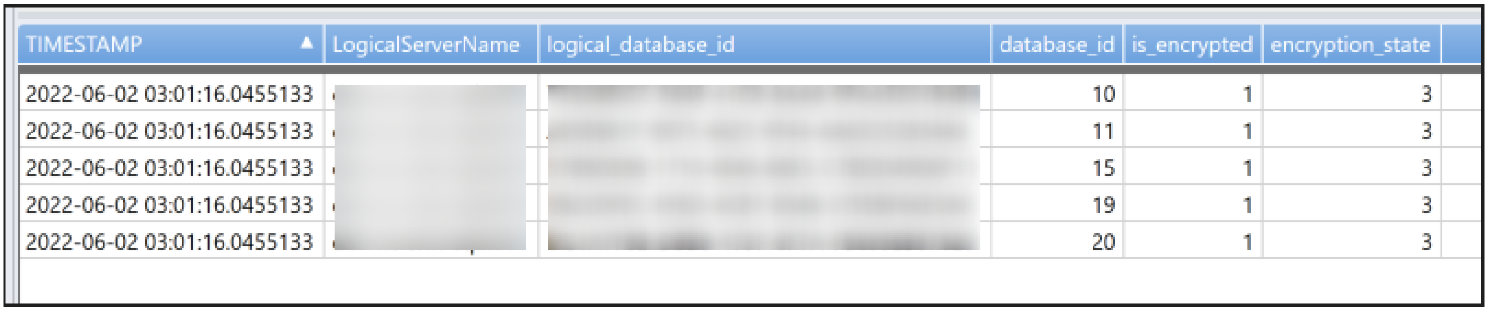
db_request_id	tde_request_id	encryption_state	managed_server_id	managed_database_id	managed_database_name	sql_database_id
		3	[redacted]	[redacted]	[redacted]	10
		3	[redacted]	[redacted]	[redacted]	11
		0	[redacted]	[redacted]	[redacted]	12
		0	[redacted]	[redacted]	[redacted]	13
		0	[redacted]	[redacted]	[redacted]	14
		3	[redacted]	[redacted]	[redacted]	15
		0	[redacted]	[redacted]	[redacted]	16
		0	[redacted]	[redacted]	[redacted]	17
		3	[redacted]	[redacted]	[redacted]	19
		3	[redacted]	[redacted]	[redacted]	20
		0	[redacted]	[redacted]	[redacted]	21
			[redacted]	[redacted]	[redacted]	32760

Step 3: Top 500 Databases for [redacted]; Instance for [redacted]

Kusto:

```
MonDatabaseEncryptionKeys
| where TIMESTAMP >= {StartDateTime} and TIMESTAMP <= {EndDateTime}
| where LogicalServerName == {MIName}
| where logical_database_id =~ {DB_guid}
| project TIMESTAMP, LogicalServerName, logical_database_id, database_id, is_encrypted, encryption_state
```

Sample Output:



TIMESTAMP	LogicalServerName	logical_database_id	database_id	is_encrypted	encryption_state
2022-06-02 03:01:16.0455133	[redacted]	[redacted]	10	1	3
2022-06-02 03:01:16.0455133	[redacted]	[redacted]	11	1	3
2022-06-02 03:01:16.0455133	[redacted]	[redacted]	15	1	3
2022-06-02 03:01:16.0455133	[redacted]	[redacted]	19	1	3
2022-06-02 03:01:16.0455133	[redacted]	[redacted]	20	1	3

Note: Kusto output will only show entries for encrypted databases. If database is not encrypted, kusto will not have an entry.

Internal Reference

ICM 305886457

How good have you found this content?