Always Encrypted v2 on a non enclave enabled SKU - Enclave not configured

Last updated by | Soma Jagadeesh | Jan 11, 2021 at 12:05 AM PST

Contents

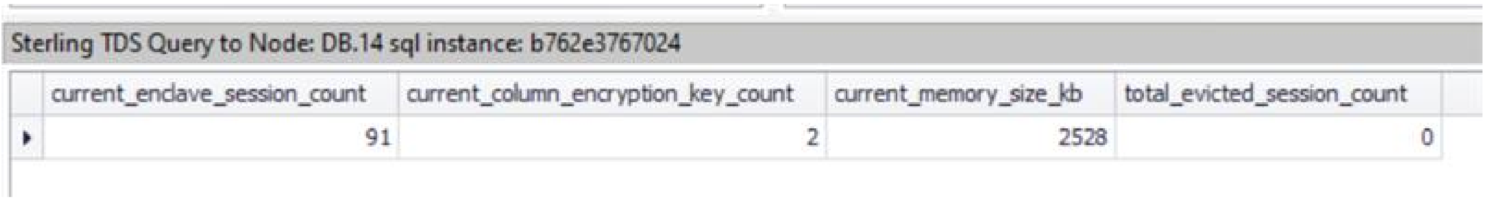
Check Machine Type

- Customers can only use Always Encrypted with secure enclaves on a DC series VM (which contains special hardware which allows enclave computation). You can check if db is on a DC series VM, by running the following CMS query (adhoccmsquery.xts when using xts). This info might be there in MonSqlSystemHealth
- SELECT service_level_objective FROM all_logical_databases WHERE logical_server_name = '<server_name>' and logical_database_name='<database_name>'
- The result of following query (in adhocquery.xts) contains 'DC'
- If this is not the case instruct the customer to move their DB to a DC series SKU.

Check Enclave Initialization

- After checking that the db is running on the correct hardware check to see if the enclave was loaded successfully:
- Use the adhocquerytobackendinstance.xts view to run the following query against the database: select * from sys.dm_column_encryption_enclave

  If this query returns rows the enclave is loaded.



Sterling TDS Query to Node: DB.14 sql instance: b762e3767024

	current_enclave_session_count	current_column_encryption_key_count	current_memory_size_kb	total_evicted_session_count
▸	91	2	2528	0

- If this is not the case, check for any enclave errors in the error log:

```
MonSQLSystemHealth
| where LogicalServerName == '<servername>'
| where message contains 'Internal enclave error'
```

Check Encryption Keys

- We can check on the backend if there are any enclave enabled CMKs or CEKs for a given instance.

```
MonTceMasterKeys
| where AppName == '<appname>'
| where AllowEnclaveComputations == 1
```

```
MonTceColEncryptionKey
| where AppName == '<appname>'
| where allow_enclave_computations_keys == 1
```

How good have you found this content?