

Always Encrypted: Attestation failures

Last updated by | Vitor Tomaz | Feb 18, 2021 at 3:29 AM PST

Contents

- [Step 1: Determine](#)
- [Step 2: \(Sanity check only\) DB placement logic:](#)
- [Step 3: Validate attestation URL format](#)
- [Step 4: Valid SGX Enclave load status](#)
- [Step 4: Attestation Failure error messages](#)
 - [Step 4.1 Error: Customer error message: Return code: '0x00...](#)
 - [Step 4.2 Error: Customer error message: Return code: '0x00...](#)
 - [Step 4.3 Error: Customer error message:](#)
 - [Step 4.4 Customer error message: Return code: '0x000001f4'](#)
 - [Step 4.5 Other error messages](#)

Step 1: Determine

Determine if the customer DB is running on DC series hardware, which only supports SGX enclave.

In sterling servers and databases.xts view, check the DB SLO name.

SGX supports SLO's are SQLDB_[GP|BC|HS]_DC_[2|4|6|8]
Such as SQLDB_GP_DC_2

The screenshot shows a table titled 'Databases for sgxtest2 (Double click to open DB Perf)'. The table has columns: logical_server_name, logical_database_name, logical_database_id, state, parent_state, sql_instance_name, logical_database_type, database_type, and service_level_objective. The data rows show various databases like contosoDB, elnataest2, epooltest, and jakub, all with a service_level_objective of SQLDB_GP_DC_2.

logical_server_name	logical_database_name	logical_database_id	state	parent_state	sql_instance_name	logical_database_type	database_type	service_level_objective
sgxtest2	contosoDB	9d93e5d2-559b-4197-82ba-1c89f4344d74	Ready	Ready	d8c6bc69faef	SterlingLogicalDatabase	SQLUserDb	SQLDB_GP_DC_2
sgxtest2	elnataest2	812a6fde-8854-40dd-b2fa-4f134613ee80	Ready	Ready	f0363adef42c	SterlingLogicalDatabase	SQLUserDb	SQLDB_GP_DC_2
sgxtest2	epooltest	ab9fe9e0-d0cb-4c74-9506-b2b4642e7061	Ready	Ready	fe25e8094f12	SterlingLogicalDatabase	SQLUserDb	SQLDB_GP_DC_2
sgxtest2	jakub	3c02c8f8-497e-4010-a2ef-ffdf90f8b24	Ready	Ready	a58e481b9c2a	SterlingLogicalDatabase	SQLUserDb	SQLDB_GP_DC_2

If DB's SLO is not DC series, then DB doesn't support SGX enclave, so customer will see attestation failure. Ask customer to create the DC series DB.

Step 2: (Sanity check only) DB placement logic:

Find the tenant ring Id by using the DB and Server name

Execute: [Web](#) [Desktop](#) [Web \(Lens\)](#) [Desktop \(SAW\)](#)

<https://sqlazureuk2.kustomfa.windows.net/sqlazure1>

```

MonSQLSystemHealth
| where LogicalServerName contains "sgxtestuksouthsrv" and logical_database_guid contains "79967fe5-dcfe-46a7-
| project ClusterName
| limit 1

```

ClusterName [tr1850.uksouth1-a.worker.database.windows.net](#) In capacity management (database move).xts, select the correct ring and validate the VM Size.

idow Profiles Help Versions Like this view

sterling\Favorites and Links.xts sterling\sterling servers and databases.xts **sterling\capacity management (database move).xts**

Target Tenant Ring Capacity

tr	target_tenant_ring	azure_cluster	weight	cap	idsu_cap	ob	sb	vm_size	nodes	fd	ud	cpu	disk	amu	acu	Idsu Mcu Ratio
1850	tr1850.uksouth1-a.worker.database.window...	lon22prdapp04	1	90	68	100	100	SQLDCGen6_2	25	5	10	14.81	0.81	3.40	0.38	0.05

How to Use | Local time | Target Tenant Ring Capacity | Placement Group | Placement Features in region | Disabling reason | Refreshing | Capacity Segments - Old Data Shown - |

For SGX DB, VM size should be SQLDCGen6_2.

If you VM size != SQLDCGen6_2, involve provisioning team to understand why DC series DB is placed on unsupported VM size

Step 3: Validate attestation URL format

Ask the customer to provide the full attestation URL which they are using to connect to the SQL DB.

- Attestation URL is the following format
 - <https://<attestation tenant name>.attest.azure.net/attest/SgxEnclave?api-version=2018-09-01-preview>
Or
 - <https://<attestation tenant name>.attest.azure.net/attest/SgxEnclave>

Note: Customer can drop the api-version number if needed. In case they are specifying the api-version, then they need to use the exact same version number as mentioned in above URL i.e. (2018-09-01-preview)

Such as (below is the sample URL, this is not work for customer DB)

<https://sqlcloudtestsgxattest.us.attest.azure.net/attest/SgxEnclave?api-version=2018-09-01-preview>

Note: We only support https protocol.

Attestation Url is not the above specified format, ask customer to fix it. (It's a customer error)

Step 4: Valid SGX Enclave load status

Option1: Using the below Kusto query, we can determine if SGX enclave

Execute: [Web](#) [Desktop](#) [Web \(Lens\)](#) [Desktop \(SAW\)](#)

<https://sqlazureuk2.kustomfa.windows.net/sqlazure1>

```

MonSQLSystemHealth
| where LogicalServerName contains "sgxtestuksouthsrv"
| where NodeName contains "DB.23"
| where error_id == 37308
| where TIMESTAMP > ago(30m)
| project TIMESTAMP, NodeName, AppName, error_id, message
| order by TIMESTAMP desc

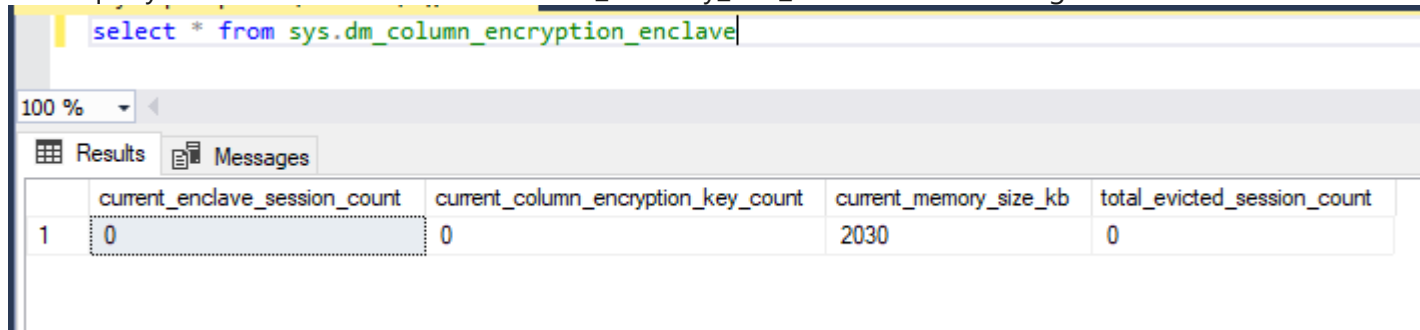
```

TIMESTAMP	NodeName	App name	Error_ID	Message
2021-01-04 22:30:44.3135540	DB.23	db6df7be41cd	37308	2021-01-04 22:28:48.26 Server Loaded SGX enclave for Always Encrypted.

Option 2: Customer can also validate if SGX enclave is loaded correctly or not by running the following query in SSMS.

```
select * from sys.dm_column_encryption_enclave
```

If the query returns a row and size of current_memory_size_kb > 0 then we are good.



	current_enclave_session_count	current_column_encryption_key_count	current_memory_size_kb	total_evicted_session_count
1	0	0	2030	0

If enclave fails to load due some reasons then we can do the failure over to mitigate the issue and send an email to Security team for follow-up

Procced to below steps once you validated all the above prerequisites.

Step 4: Attestation Failure error messages

Step 4.1 Error: Customer error message: Return code: '0x00000193'

In SSMS or client tool

Msg 37324, Level 16, State 57, Procedure sp_describe_parameter_encryption, Line 1 [Batch Start Line 11]

Enclave attestation failed. Attestation service returned Error code: 'Forbidden'. Error message: 'Access to /attest/SgxEnclave is denied'. Attestation URL: 'https://attestation_url.attest.azure.net/attest/SgxEnclave?api-version=2018-09-01-preview'. Return code: '0x00000193'. Verify the attestation policy. If the policy is correct, contact Customer Support Services.

An error occurred while executing batch. Error message is: Internal error. The result returned by 'sp_describe_parameter_encryption' is invalid. The attestation information resultset is missing for enclave type 'SGX'.

```
From Kusto query
MonSQLSystemHealth
| where LogicalServerName contains "sgxtestuksouthsrv"
| where error_id == 37324
| where TIMESTAMP > ago(3h)
| project TIMESTAMP, NodeName, AppName, error_id, message
| order by TIMESTAMP desc
```

TIMESTAMP	error_id	message
2021-01-04 23:24:44.4875839	37324	2021-01-04 23:23:46.94 spid90 Error: 37324, Severity: 16, State: 57. 2021-01-04 23:23:46.94 spid90 [Filtered Args] Enclave attestation failed. Attestation service returned Error code: '%1'. Error message: '%2'. Attestation URL: '%3'. Return code: '0x%4'. Verify the attestation policy. If the policy is correct, contact Customer Support Services.

It usually means customer haven't provided the RBAC permission to the attestation tenant. It's a customer error.

Mitigation (ask customer to run similar command)

```
New-AzRoleAssignment -ApplicationId $serverApplicationId -RoleDefinitionName "Attestation Reader" -
ResourceGroupName $attestationResourceGroupName
```

Where \$serverApplicationId - Is it application name \$attestationResourceGroupName - attestation resource group name

Example(how to find server application id)

```
$serverObj = Get-AzSqlServer -ResourceGroupName sgxtestuksouthrg -ServerName sgxtestuksouthsrv //
```

note: these are sample values \$sp = Get-AzADServicePrincipal -ObjectId *serverObj.Identity.PrincipalId*
serverApplicationId=\$sp.ApplicationId.Guid

Step 4.2 Error: Customer error message: Return code: '0x00002ee7'

In SSMS or client tool

Msg 37303, Level 16, State 21, Procedure sp_describe_parameter_encryption, Line 1 [Batch Start Line 11]

Internal error occurred while obtaining an authentication token for an attestation service. Authentication method: HttpConnectAndSendRequest, status: 0x00002ee7.

An error occurred while executing batch. Error message is: Internal error. The result returned by 'sp_describe_parameter_encryption' is invalid. The attestation information resultset is missing for enclave type

'SGX'.

```

From kusto query
MonSQLSystemHealth
| where LogicalServerName contains "sgxtestuksouthsrv"
| where TIMESTAMP > ago(3h)
| where error_id == 37303
| project TIMESTAMP, error_id, message
| order by TIMESTAMP desc

```

TIMESTAMP	error_id	message
2021-01-05 00:48:44.7470471	37303	2021-01-05 00:48:31.30 spid73 Error: 37303, Severity: 16, State: 21. 2021-01-05 00:48:31.30 spid73 Internal error occurred while obtaining an authentication token for an attestation service. Authentication method: HttpConnectAndSendRequest, status: 0x00002ee7

It usually means customer using the incorrect attestation url. It's a customer error

Mitigation: Ask customer to validate the attestation url and try again.

Step 4.3 Error: Customer error message:

PolicyEvaluationError - No Permit claim was issued in the authorizationrules section

In SSMS or client tool

Msg 37324, Level 16, State 57, Procedure sp_describe_parameter_encryption, Line 1 [Batch Start Line 13]

Enclave attestation failed. Attestation service returned Error code: 'PolicyEvaluationError'. Error message: 'Native operation failed with 65518: ..\NativePolicyWrapper\NativePolicyEngine.cpp(186)(null)!: (caller:) Exception(0) 83FFFFFFE Policy Evaluation Error has occurred Msg:[Policy Engine Exception: No Permit claim was issued in the authorizationrules section, authorization failed.]

..\Enclave\api.cpp(882)(null)!: (caller:) LogHr(0) 83FFFFFFE Policy Evaluation Error has occurred Msg:[Unhandled Enclave Exception: "Policy Evaluation Error has occurred"]

'. Attestation URL: '<https://sgxattest5pr.eus.attest.azure.net/attest/SgxEnclave?api-version=2018-09-01-preview>'. Return code: '0x00000190'. Verify the attestation policy. If the policy is correct, contact Customer Support Services. An error occurred while executing batch. Error message is: Internal error. The result returned by 'sp_describe_parameter_encryption' is invalid. The attestation information resultset is missing for enclave type 'SGX'.

```

In kusto
MonSQLSystemHealth
| where LogicalServerName contains "sgxtestuksouthsrv"
| where TIMESTAMP > ago(3h)
| where error_id == 37324
| project TIMESTAMP, error_id, message
| order by TIMESTAMP desc

```

TIMESTAMP	error_id	message
2021-01-04 23:24:44.4875839		
37324	2021-01-04 23:23:46.94 spid90 Error: 37324, Severity: 16, State: 57. 2021-01-04 23:23:46.94 spid90 [Filtered Args] Enclave attestation failed. Attestation service returned Error code: '%1'. Error message: '%2'. Attestation URL: '%3'. Return code: '0x%4'. Verify the attestation policy. If the policy is correct, contact Customer Support Services.	

It usually means customer specify wrong attestation policy. **It's a customer error**

Mitigation:

Ask customer to validate the attestation policy and try again.

Sample attestation policy: **(note: this is just a sample policy, customer might choose to provide a different one)**


```

version= 1.0;
authorizationrules
{
[ type=="x-ms-sgx-is-debuggable", value==false ]
&& [ type=="x-ms-sgx-product-id", value==4639 ]
&& [ type=="x-ms-sgx-svn", value>= 0]
&& [ type=="x-ms-sgx-mrsigner", value=="e31c9e505f37a58de09335075fc8591254313eb20bb1a27e5443cc450b6e33e5" ]
=> permit();
};

```

Step 4.4 Customer error message: Return code: '0x000001f4'

In SSMS

Attestation service returned Error code: 'InternalServerError'. Error message: 'An internal server error has occurred: Operation returned an invalid status code 'Unauthorized''. Attestation URL: <https://sgxattest5pr.eus.attest.azure.net/attest/SgxEnclave?api-version=2018-09-01-preview> . Return code: '0x000001f4'. Verify the attestation policy. If the policy is correct, contact Customer Support Services.

This is likely not a customer issue and we need to contact the MAA service owner.

Do escalate the issue to “Azure Security Engineering/Azure Attestation Service”

Step4.5 Other error messages

Below are the set of error messages which customer should never see. If customer is seeing these error it usually means deployment issue.

Error Code	Error Details
37325	Enclave attestation failed due to an error in Azure Data Center Attestation Primitives (DCAP) Client. Validate Azure DCAP Client is installed and configured properly
37309	Enclave attestation failed due to an error in Intel Data Center Attestation Primitives (DCAP)

How good have you found this content?

