Kusto Telemetry for troubleshooting common issues for SQL Ledger

Last updated by | Pooja Kamath | Jun 17, 2021 at 1:46 AM PDT

Kusto Telemetry for troubleshooting common issues for SQL Ledger

Contents

Customer reports verification taking too long

The query below reports events and duration of the different phases of verification: for the overall database ledger and the individual tables. It also reports if the user ran verification from storage or by explicitly providing digests and whether they requested to verify all tables or one.

```
MonSecurityEvents
| where LogicalServerName == "janderstestportal2server" and logical_database_name == "janderstestportal2"
| where event contains "verification"
| project PreciseTimeStamp, event, object_id, verify_all_tables, from_storage, is_successful, total_verificati
```

Customer reports verification failed (this could be user error as well)

The query below reports the reason verification failed. If we see input_error being true or digest_verification_failed (and especially if from_storage is false) this might indicate user error. If inter_block_verification_failed, intra_block_verification_failed are true, please escalate to PG.

```
MonSecurityEvents
| where LogicalServerName == "janderstestportal2server" and logical_database_name == "janderstestportal2"
| where event contains "verification"
| where is_successful == false
| project PreciseTimeStamp, event, object_id, verify_all_tables, from_storage, is_append_only, error_code, inp
```

Customer reports they don't see digests uploaded

(this could be user error as well if the right permissions are not granted. The Logical Server identity needs to be granted Data Contributor on the Storage account where digests are uploaded) The following queries look for upload success and failures and in the case of failures they report the error and description of it. For example if permissions are not properly granted error_description will say "NoPermissionsToContainer".

```
MonSecurityEvents
| where LogicalServerName == "janderstestportal2server" and logical_database_name == "janderstestportal2"
| where event startswith "ledger_digest_upload_" // Success or failure: ledger_digest_upload_success, ledger_d
| project PreciseTimeStamp, event, error, error_description, state, storage_type

MonSecurityEvents
| where LogicalServerName == "janderstestportal2server" and logical_database_name == "janderstestportal2"
| where event == "ledger_digest_upload_failed"
| project PreciseTimeStamp, event, error, error_description, state, storage_type
```

Issues with Azure Confidential Ledger

While our TSGs are specific to digest storage in Azure Storage rather than Azure Confidential ledger the troubleshooting flow remains similar (Example - we will troubleshoot container permissions if it is Azure Blob Storage . If it is ACL we will involve the ACL CSS POD to help troubleshoot) There are 2 scenarios where your team could reach out to ACL support team –

1. **Issues during saving digest to ACL**
2. **Issues during retrieving the digest**

Check here for collaboration details with ACL team

Generic information to view Ledger configuration

The queries below view generic information about a customer database and its ledger configuration.

Whether ledger has ever been used in the DB, whether the whole DB is marked as ledger and what is the storage configured for digests (if any)

```
MonSecurityEvents
| where LogicalServerName == "janderstestportal2server" and logical_database_name == "janderstestportal2"
| where event == "ledger_settings"
| project PreciseTimeStamp, is_ledger_enabled, is_ledger_database, storage_type
```

The number of transactions in the ledger since the last server restart.

```
MonSecurityEvents
| where LogicalServerName == "janderstestportal2server" and logical_database_name == "janderstestportal2"
| where event == "ledger_transaction_count"
| project PreciseTimeStamp, ledger_transaction_count = message
| order by PreciseTimeStamp asc
```

All the ledger tables in the database and whether they are updateable or append only

```
MonDatabaseMetadata
| where LogicalServerName == "janderstestportal2server" and logical_database_name == "janderstestportal2"
| extend is_ledger_updateable = binary_and(status2, 0x00040000) == 0x00040000, is_ledger_append_only = binary_
| where table_name == "sysschobjs" and (is_ledger_append_only == true or is_ledger_updateable == true)
| where nsid != 4 // Ignoring system tables
| project name, is_ledger_updateable, is_ledger_append_only
```

NOTE: The detailed telemetry is part of T59 which has not yet rolled out to any prod clusters yet (as of May 20th)

The majority of telemetry is captured in MonSecurityEvents and then we can join to MonDatabaseMetadata to get details about the schema of any ledger tables.

We are collecting the following metrics (or enough information to compute them after joining the above two tables in Kusto):

- Number of ledger tables and updatable vs. append-only
- Automated vs. manual digest upload and ACL vs. Azure Storage
- Number of generated digests/day and whether it was manual or not
- Number of verifications (database vs. table level) (explicit digests vs. from storage) (P2: append-only vs. updatable)
- Successful vs. failed verification (digest mismatch vs. internal inconsistency)
- Number of transactions on ledger tables
- Number of times ledger view is queried (append only vs. not)
- Number of digest uploads to Storage that succeeded or failed
- Number of dropped ledger tables (or potentially number of drops on ledger tables)

How good have you found this content?