Known issues

Last updated by | Sravani Saluru | Jul 20, 2022 at 9:44 AM PDT

Contents

Issues

Auditing

1.

- Http 0 error means that there is a network/Vpn/firewall problem in customer’s machine and the request never left the machine. This issue is not related to auditing and related to customers’ machine configuration.

2.

- Issue: When the Azure SQL Server name has upper case letter and we try to enable the audit we get the following error:
- Error: Failed to save server Auditing settings Failed to save Auditing settings for server: <server>. ErrorMessage: {'Code':'InternalServerError','Message':''}
- workaround is to create a new Azure SQL Server with no upper case letters and the move the databases to the new server.

3.

- Issue : customer is expecting server audit logs to be shown at datbaase diognostics settings (ICM 242820914)
- This is by design , server level audit logs will not be shown under database diognostic settings. server level audit logs are configured under master database for all databases

4.

- Issue : The customer can't update the retention period of the Azure SQL Auditing from the portal with the following error:

  “Failed to save Auditing settings for server “authprddbsv01”. The role assignment already exists” (ICM 274283589)

- Root cause : Issue with the storage account settings . The logs just say

```
2021-12-01 10:29:47.06 spid105 Audit: Server Audit: 65582, State changed from: START_FAILED to: TARGET_CREATION_FAILED

2021-12-01 10:29:47.06 spid105 Error: 37358, Severity: 17, State: 1. 2021-12-01 10:29:47.06 spid105 [Filtered Args] SQL Audit failed to create the audit file for the audit '%1' at '%2'. Make sure that SAS key is valid or Managed Identity has permissions to access the storage. This is an informative message. This error doesn't affect SQL availability.
```

- solution : time-based retention setting in the immutable BLOB storage settings for storage account.we have cases where removing this policy helped auditing to be enabled. if customer has it enabled , remove the time based retention setting and configure auditing.

5.

- Issue : Auditing log does not log AAD Server principal name for failed logins while (The successful connection of AAD auth include the name. And the SQL Server auth include this both for successful and failed situations.)
- Root cause : its by design
- solution : If the login fails in case token issue then we don't get server principal name... however if AAD profile is already added in Azure Active Directory admin and passes the token verification layer...and login fails because of firewall kind of issues.that time audit will show server principal name.

6.

- Issue : customer whose Azure SQL DB is currently exporting audits to a Storage Account, which is currently configured to allow access from all networks. Customer wants to change SA to a Private Endpoint, in order to block internet access to SA. Customer's questions is: while changing process is ongoing (SA going from public to private) will any audit events generated from SQL DB be lost? Or is there some kind buffer / retry mechanism on SQL side that will guarantee that absolutely no audit events are lost
- solution : during the resaving the audit the events will not be audited so there will be gap while changing the configuration

7.

- Issue : Customer tries to write audit logs to the event hub behind the firewall by allowing selected networks to bypass the firewall. The audit logs are not being recorded to the event hub.
- solution : First we have to resave the SQL audit setting after you move the Event hub behind the firewall and resaving the auditing will make that work . The other recommendations that we have to follow is not to create a hub manually in the namespace and allowing the SQL server to create a default hub for auditing manually to have better coordination.

8.

- Issue : customer subscription is not recieving emails “Azure SQL Server auditing failure on 'sql-xxxxxxxxxxx' server”.
- RCA : customer changed the email for the subscription owner

- Solution : this is by design as we cache the value of the email contact till the audit is restarted or when server is restarted during an upgrade/failover/update.

  If the email associated with the account is changed, then it is recommended to resave the audit.

9.

- Issue : Once SQL Server is deleted and on recreating trying to enable log analtics and eventhub audit returns error below

  ERROR: Multiple audit diagnostics settings are already enabled

  Portal does not show audit enabled for log analytics and EventHub.

- RCA : diagnostic settings for SQLSecurityAuditEvents and DevOpsOperationsAudit category set to "true"

- Solution : customer created the audit using powershell/CLI , when customer create using powershell/cli we dont create the diagnostic settings and customer has to manually perform that operation.so i so if customer disbale audit in future they need to manually delete the diagnostic settings delete the dignostic settings manually and reconfigure auditing resolves the problem

10.

- Issue : Unable to set auditing on few SQL Databases using Log Analytics and Storage , failing with below error

```
error : At least one data sink needs to be specified.
```

- Solution : The issue happened because earlier version of Diagnostic Settings page incorrectly allowed "SQLSecurityAuditEvents" category to be selected in user created Diagnostic settings. When database Audit is enabled with "Enable Auditing of Microsoft support operations" options enabled at server level, we try to create a diagnostic settings with "SQLSecurityAuditEvents" category and that was failing because it was already present in the other diagnostic settings for the same destination.

Classification

TBD

How good have you found this content?