Storage Firewall causing SQL DB Auditing failures

Last updated by | Rui Manuel Maia | Mar 6, 2023 at 6:53 AM PST

Issue

When users configure storage account firewall, SQL DB auditing may start failing, if SAS is being used. Users may receive an alert email with below information: "SQL Audit logs for server 'server' are not being recorded in storage account 'storageacc'". Vulnerability assessment can also be impacted and start failing.

Failed to set Auditing and Threat Detection Policy via PowerShell

- ```
  Set-AzSqlServerAudit -BlobStorageTargetState Enabled -ResourceGroupName $ResourceGroup -ServerName $ser
  ```

  Set-AzSqlServerAudit : Setting Auditing Settings failed.

- ```
  Update-AzSqlServerVulnerabilityAssessmentSetting -ResourceGroupName $ResourceGroup -ServerName $serverN
  ```

  Update-AzSqlServerVulnerabilityAssessmentSetting : The provided storage account shared access signature or account storage key is not valid.

Investigation/Analysis

Confirm with customer if firewall has been enabled on Storage Account.

Mitigation

Update settings on Azure Portal

Auditing: Edit settings on SQL Logical Server and change "Storage Authentication Type" to "Managed Identity".

Vulnerability Assessment: Edit settings on SQL Logical Server and save (no changes required).

RCA Template (optional)

n/a

More Information (optional)

n/a

Public Doc Reference (optional)

https://learn.microsoft.com/en-us/azure/azure-sql/database/audit-write-storage-account-behind-vnet-firewall?view=azuresql#prerequisites ↗ https://learn.microsoft.com/en-us/azure/azure-sql/database/sql-database-vulnerability-assessment-storage?view=azuresql ↗

Internal Reference (optional)

n/a

Root Cause Classification

Cases resolved by this TSG should be coded to the following root cause:
Azure SQL DB v2\Connectivity\Login Errors\Firewall errors and misconfigurations