Storage firewall and DB auditing

Last updated by | Balaji Barmavat | Nov 30, 2020 at 6:01 PM PST

Contents

Issue:

As soon as storage firewall is enabled, SQL DB auditing fails.

Workaround:

CSS Azure storage support team provided below info:

" I was able to reproduce the same in my subscription, so I went to our Product Group for confirmation on this as a known issue.

They confirmed they are aware of this and working with the SQL Auditing group to get this resolved. Currently there is no resolution for the failure to save. If Auditing is a Must-have, they have advised to not use Storage Firewalls."

Problem Scope

Failed to set Auditing and Threat Detection Policy via PowerShell

- Set-AzSqlServerAuditing -State Enabled -ResourceGroupName 'example_rg' -ServerName 'mssqlserver1e358' -StorageAccountName 'dbdiagnosticse9'

  > Set-AzSqlServerAuditing : One or more errors occurred. (Long running operation failed with status 'Failed'. Additional Info:'Insufficient read or write permissions on the provided storage account.') At line:1 char:1 + Set-AzSqlServerAuditing -State Enabled -ResourceGroupName 'example_rg ...

- Set-AzSqlServerThreatDetectionPolicy -ResourceGroupName 'example_rg' -ServerName 'mssqlserver1e358' -StorageAccountName 'dbdiagnosticse9' -NotificationRecipientsEmails 'lukasz.iwanicki@kroger.com;test@test.com' -RetentionInDays 30 -EmailAdmins $True

Set-AzSqlServerThreatDetectionPolicy : Long running operation failed with status 'Failed'. Additional Info:'An unexpected error occured while processing the request. Tracking ID: '3ca1b0f7-ee00-4331-94be-29d00c5d74fe'' At line:1 char:1 + Set-AzSqlServerThreatDetectionPolicy -ResourceGroupName 'example_rg' ...

- Received following error when you try to enable the threat policy on Azure SQL DB

az sql db threat-policy update -g example_rg -s mssqlserver1e358 -n testdbliwani --state Enabled --storage-endpoint https://dbdiagnosticse9.blob.core.windows.net/ --storage-key abc=my=key --email-addresses email@kroger.com --retention-days 30

Error occurred in request., RetryError: HTTPSConnectionPool(host='management.azure.com', port=443): Max retries exceeded with url: /subscriptions/Input SubscriptionId here/resourceGroups/example_rg/providers/Microsoft.Sql/servers/mssqlserver1e358/databases/testdbliwani/securityAlertPolicies/default?api-version=2014-04-01 (Caused by ResponseError('too many 500 error responses'))

Cause

Firewall setting in Azure Storage has to set to "allow access from all networks" as Azure SQL DB is not part of any VNET. I understand this is not the best security setting. However, this is the only option for Azure SQL DB to access storage account as of now.

Resolution

Changed the setup on the Storage Account to allow access from “All networks” and the command executed successfully now

Classification

Root cause Tree - Security/Service issue/Auditing

How good have you found this content?