

Error 18456, State 113 - DosGuard rejected the connection

Last updated by | Mustafa Ashour | Mar 7, 2023 at 8:10 AM PST

Contents

- [Issue](#)
 - [DosGuard](#)
 - [How does it work?](#)
- [Investigation/Analysis](#)
 - [Using Azure support center \(ASC\)](#)
 - [ASC Insight](#)
 - [SQL Troubleshooter](#)
 - [Using Kusto](#)
- [RCA Template](#)
- [Root Cause Classification](#)

Issue

DosGuard

Denial of service (DoS) attacks are reduced by a SQL Database gateway service called DoSGuard.

How does it work?

DoSGuard actively tracks failed logins from IP addresses. If there are multiple failed logins from a specific IP address within a period of time, the IP address is blocked from accessing any resources in the service for a pre-defined time period (5 minutes).

In addition, the Azure SQL Database gateway performs:

- Secure channel capability negotiations to implement TDS FIPS 140-2 validated encrypted connections when it connects to the database servers.
- Stateful TDS packet inspection while it accepts connections from clients. The gateway validates the connection information and passes on the TDS packets to the appropriate physical server based on the database name specified in the connection string.

The overarching principle for network security of the Azure SQL Database offering to allow only the connection and communication that is necessary to allow the service to operate. All other ports, protocols, and connections are blocked by default. Virtual local area networks (VLANs) and ACLs are used to restrict network communications by source and destination networks, protocols, and port numbers.

Mechanisms that are approved to implement network-based ACLs include ACLs on routers and load balancers. These mechanisms are managed by Azure networking, guest VM firewall, and Azure SQL Database gateway firewall rules, which are configured by the customer.

Investigation/Analysis

Using Azure support center (ASC)

We detect this issue in ASC tool, to generate insight with impact timeframe along with CSS & customer ready content to use and share with customer for handling this issue.

ASC Insight

SQL DATABASE

DoSGuard protection in effect

SQL SERVER DATABASE

Is this insight helpful?

Description

Between 2020-10-19 01:17:12 UTC and 2020-10-19 13:41:47 UTC we found that the DoS Guard protection was triggered on the databas: [redacted] on serve [redacted]. The other errors that happened during the timeframe are as below -

MinOccurredTime	MaxOccurredTime	PeerAddress	Error	State	SubState	ErrorCount	Description
10/19/2020 10:01:37 AM	10/19/2020 10:01:38 AM	52.240.143.x	18456	5	N/A	10	Login not found.
10/19/2020 10:01:38 AM	10/19/2020 10:01:38 AM	52.240.143.x	18456	113	N/A	3	The logins from this peer address were temporarily locked out due to repeating failed login attempts.

Impacted Resources

[redacted]

Recommended Action

Based on the other errors encountered during the DoS Guard timeframe, please advise the customer the next steps to be taken based on the error descriptions.

Customer Ready Content

Copy Content

New Email

Between 2020-10-19 01:17:12 UTC and 2020-10-19 13:41:47 UTC, the logins to databas: [redacted] on serve [redacted] were temporarily locked out due to multiple failed logins trying to connect to the server. The login failures occurred possibly due to one or more of the following reasons below.

Possible Reasons for Failure

First occurrence: 10/19/2020 10:01 UTC, Last occurrence: 10/19/2020 10:01 UTC, IP Address: 52.240.143.x Reason: Login not found.

Generated On

Oct 19, 2020 13:31:47 UTC

SQL Troubleshooter

After generating the SQL Troubleshooter report, choose Connectivity Tab, you will see the issue detected.

Summary

Connectivity

GeoDR

Downtime Reasons

Performance

Elastic Pools Performance

Read Scale Out

Recent Issues

Data Warehouse

Provisioning

Data Sync

Metrics

Hyperscale

Security

Backup/Restore

Import/Export

Troubleshooter

Data Explorer

Root Cause Analysis

User Outages

Diagnostic Checks

Root Cause Analysis

Drag a column header and drop it here to group by that column

Incident Start Time	Incident End Time	Root Cause	Property Name	Escalate To
2020-10-19T10:01:00	2020-10-19T10:02:00	No Match	LoginFailure/Error18456/State5	undefined
2020-10-19T10:01:00	2020-10-19T10:02:00	No Match	LoginFailure/Error18456/State113	undefined

Incident Start Time

Incident End Time

Root Cause

Property Name

Escalate To

10 10 Items per page

1 - 2 of 2 items

Using Kusto

Use standard MonLogin query (below) to find login failures (18456) with state 113 during the impacted timeframe.

MonLogin

where AppName == "DB Appname" and TIMESTAMP >= todatetime(datetime(00/00/2020 00:00:00)) and TIMESTA

project TIMESTAMP, event, error, state, login_time_ms

RCA Template

Summary of Impact: Between *<StartTime>* and *<EndTime>*, connection attempts to your database *<Database Name>* have failed with error 18456 and state 113.

Root Cause: This error is caused by too many failed logins from specific IP address, thus this IP address is blocked from accessing any resources in the service for a pre-defined time period (5 minutes)

Root Cause Classification

Cases resolved by this TSG should be coded to the following root cause:

Root Cause: Azure SQL DB v2\Connectivity>Login Errors\DOSGuard

How good have you found this content?

