Error 18456, State 113 - DosGuard rejected the connection

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

Contents

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.

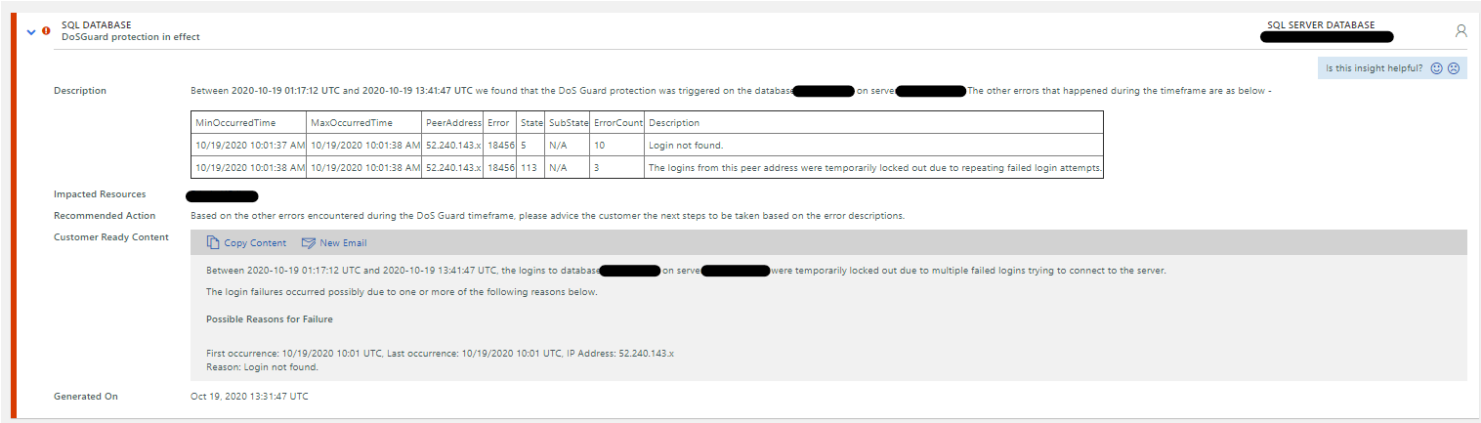
Mechanisms that are approved to implement network-based ACLs include ACLs on routers and load balancers. These mechanisms are managed by Azure networking, guest VM firewall, and Azure SQL Database gateway firewall rules, which are configured by the customer.

Investigation/Analysis

Using Azure support center (ASC)

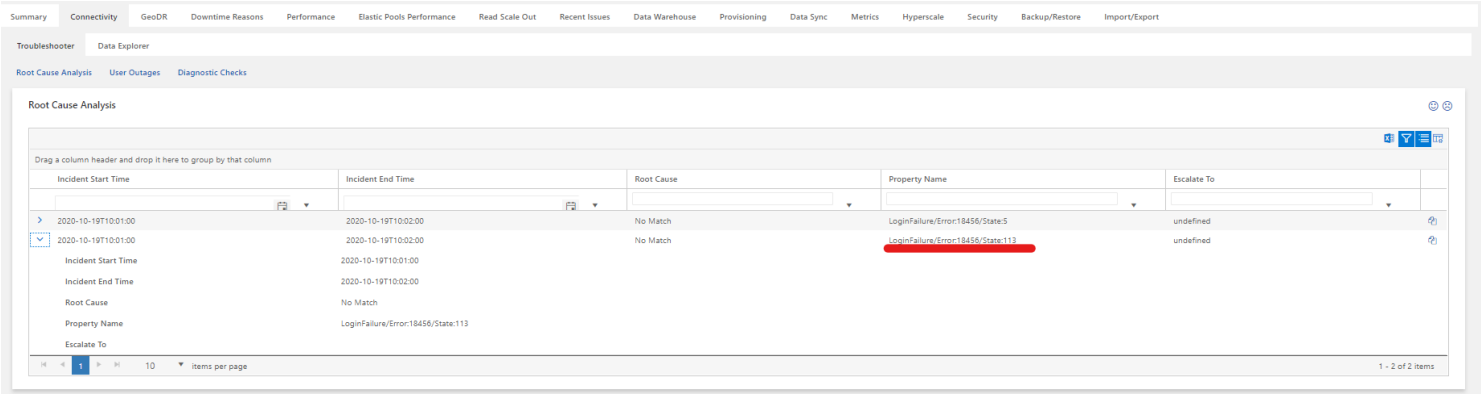
We detect this issue in ASC tool, to generate insight with impact timeframe along with CSS & customer ready content to use and share with customer for handling this issue.

ASC Insight



SQL Troubleshooter

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



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?