SNAT Port Exhaustion

Last updated by | Lisa Liu | Nov 6, 2020 at 10:34 AM PST

SNAT Port Exhaustion

Friday, August 9, 2019
2:57 PM

Problem:

Since Azure Postgres and MySQL services are PAAS applications, often a spike or abnormal hike in connection requests from some application instances could affect the others. I found that three to four instances of Azure Postgres instances had spiked their logins abnormally which caused our internal system to exhaust its Ports\resources. To resolve we these Azure Postgres instances to lesser used DNS servers

More Details:

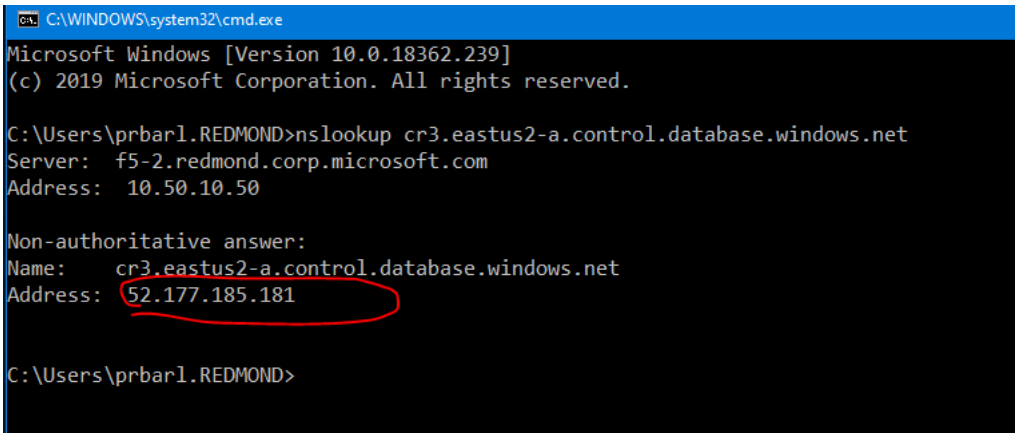
This issue is related to Network design with SNAT Public IP allocation.
https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections.

The IP flow during Postgres\MySQL connection is a 5-tuple (source IP Address, source port, protocol type, destination IP address, destination port). When all the v for source port are the same, which would happen when multiple VMs in a control ring attempt to connect to a tenant ring, then the SLB assigns a SNAT port to di separate connections. When this fixed number is exhausted, we get the result you see above with the failed connections

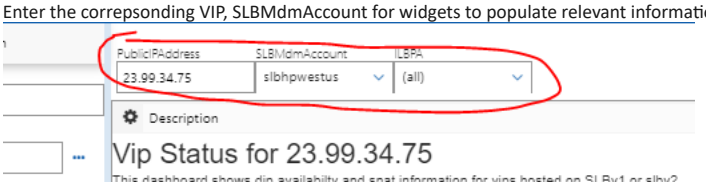
Related ICM: <https://icm.ad.msft.net/imp/v3/incidents/details/137617049/home>

How to Validate SNAT port exhaustion?

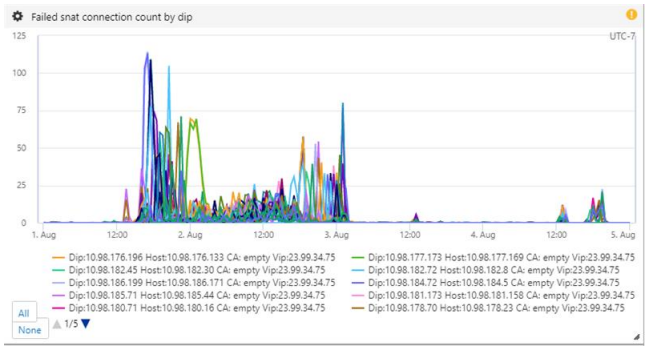
- From MonLogin check the Control Ring being used by the Server for connections. It's the clusterName column when NodeRole = GW
  Eg., cr3.eastus2-a.control.database.windows.net
- Check corresponding VIP of the Control Ring: ***nslookup cr3.eastus2-a.control.database.windows.net***



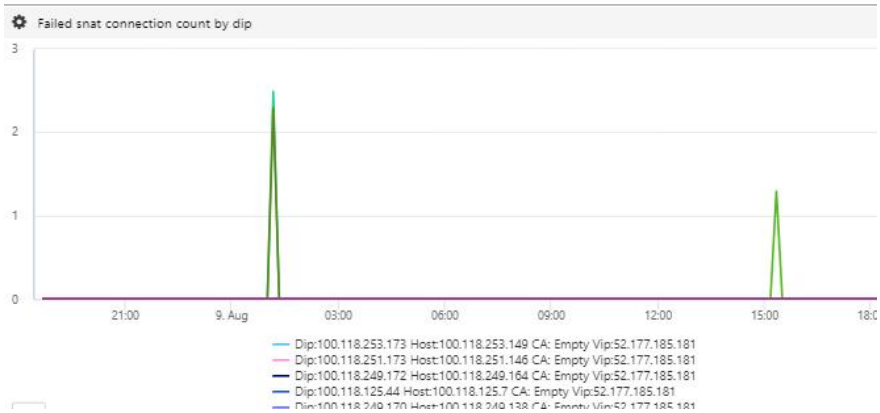
- Open SNAT Port Usage dashboard.
  - Enter the correpsonding VIP, SLBMdmAccount for widgets to populate relevant information.



  - Change the date range in the right upper corner
  - Check for "Failed SNAT connection count" widget.
    - Example: We had 3 intermittent connection issues on August 3; below is the corresponding Failed connection widget graph showing > 100 errors. Correspondingly we saw lot of MonLogin errors (error 18465, 4)



- Failed connection widget with less errors (<3)



- You can also check "NAT Ports in Use" widget:

The below widgets show that Nat Ports on all DIP's (~VM's) are using full capacity of allocated SNAT ports.
Note: About 800 ports are available per DIP but its not a hard limit as DIP's share ports.

- Mitigation:

Short term:

- Validate SNAT port exhaustion using above steps.
  - Note: Connections requests might not reach GW and in such scenarios there will not be any login telemetry.

- Check for servers with unusually high conneciton requests during the time range of connection failures.

Execute: [Web] [Desktop] [Web (Lens)] [Desktop (SAW)] https://sqlazurewus1.kusto.windows.net/sqlazure1

```
MonLogin
| where originalEventTimestamp > datetime(09/20/2019 15:11) and originalEventTimestamp  < datetime(09/20/2019 18:11)
| where event == 'process_login_finish'
| summarize  count() by logical_server_name,ClusterName, bin(originalEventTimestamp, 1h)
| where count_ > 1000
| render timechart
```

- Use this TSG - MSSOP0059: Managing Gateway slices and server bindings to move servers with spike in connection requests to use a different CR. These servers may not be the one who got affected. For example, to mitigate the ICM below we moved two to three servers which had spike in connection requests at the time of incident.

<https://icm.ad.msft.net/imp/v3/incidents/details/137617049/home>

The mitigation options are around load balancing:

- Reduce proxy load
  - Move proxy consumers between GW rings
  - Move proxy consumers to redirection
- Spread proxy consumers across more tenant rings

Long term:

- OSS needs to invest in supporting redirected connections.
- We need to take into account SNAT limits in our capacity planning and have some early detection on connectivity rings where we are approaching SNAT limits.

Need to discuss with NW team on longer-term solutions.

- Sources:
  - https://icm.ad.msft.net/imp/v3/incidents/details/130806493/home

Created with Microsoft OneNote 2016.

How good have you found this content?