RHC shows unavailable or unknown event

Last updated by | Abhijeet Survase | Mar 13, 2023 at 8:50 AM PDT

Contents

Overview

Resource Health is a Azure feature which customers leverage to diagnose health issues of their resources. If SQL DB is experiences problems due to a system error, Resource health on portal shows the resource to be Degraded/Not available for that time period.

SQL RHC is based on login failures data. Login failures can happen in one of the three hops:

1. Sqlserver
2. Xdbhost
3. Gateway

If login fails in one of the 3 hops due to system error, RHC reports it on portal. User errors like "wrong password" are not captured by Resource Health.

Degraded for cases where login failures due to system error are less than 25% total logins Not Available for cases where login failures due to system error are greater than 25% total logins Unknown is shown when there is an issue in the RHC telemetry pipeline. If customer can still connect to the database, they can ignore the unknown states.

Issue

If RHC shows unavailable or unknown events for customer's SQL databases, you can follow this TSG to troubleshoot.

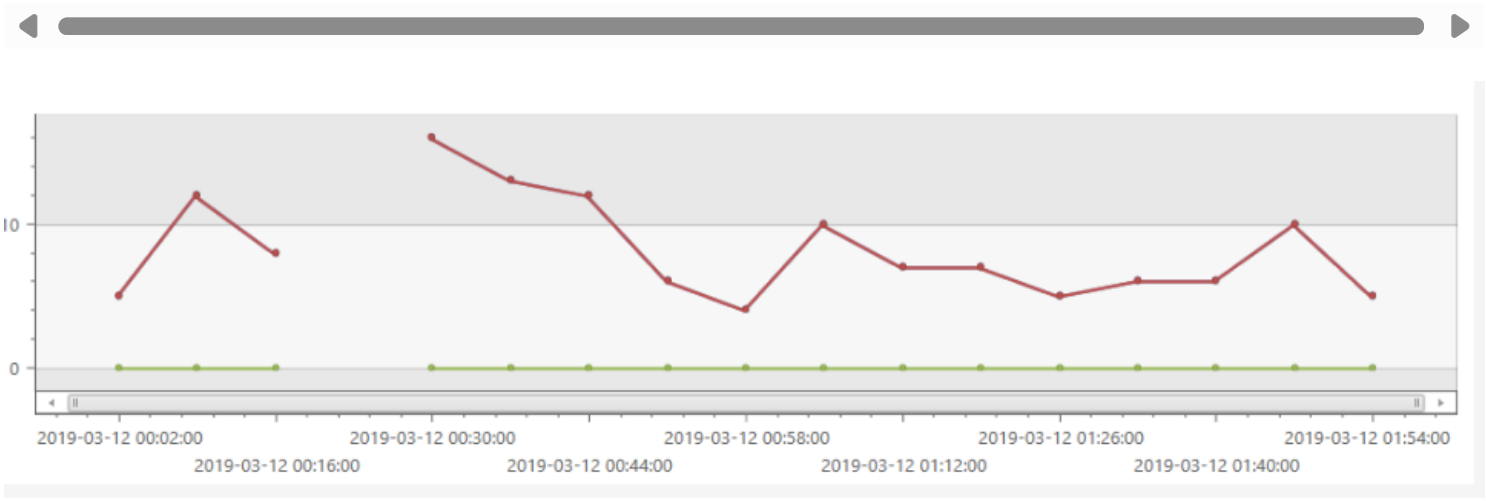
Troubleshoot

MDM retention is 90 days. Kusto retention is 7-10 days. When app fails over to another node, tail log might not be uploaded, so Kusto log might not match MDM. Hence it is good to check both Kusto and MDM to see if there are any login failures due to system error.

MDM upload is more reliable than Kusto. It is rare for both Kusto and MDM to have missing telemetry for the same resource at the same time.

Verify if there is tail telemetry loss

```
AlrMaQosEventFiveMinutes
| where TIMESTAMP > datetime(2019-03-12 00:00:00) and TIMESTAMP < datetime(2019-03-12 02:00:00)
| where ClusterName == "tr39.northeurope1-a.worker.database.windows.net"
| where AppName == 'd09df69f4047'
| where NodeName == "DB.137"or NodeName == "DB.195"
| where Operation == "MaRunTaskTransmitBond" and Object contains"_WASD2ProdMonLoginVer12v0_"
|project TIMESTAMP , DataItemReadCount , DataItemWriteCount ,  Diff = DataItemReadCount - DataItemWriteCount
|render timechart
```



Step 1: Verify data in Kusto

1. Confirm the data of downtime customer reported. If it is >7 days, Kusto query will not work as the data retention on Kusto is 7 days. You will need to check MDM as retention is 90 days.

2. Ensure the correct query is used and screenshot of RHC events correpsondes to the actual resource.

```
| where TIMESTAMP > datetime("08-29-2017") and  TIMESTAMP < datetime("08-30-2017")
| where event == "process_login_finish"
| where is_user_error == 0 and is_success == 0
| where logical_server_name =~ "advertiserbi20s" and database_name  =~ "AdvertiserBI_P808"
```

Step 2: Verify data in MDM

1. Plot data in Javis

    - Open Jarvis, click on Dashboard tab -> This will open up jarvis UI to chart metrics.

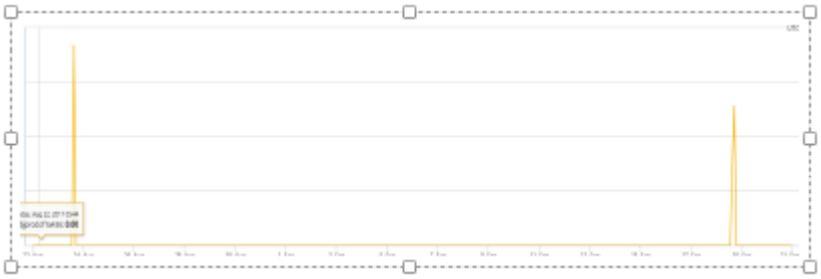
    - Click on the Gear button to the left, change the server and database name from the below templatized dashboard.

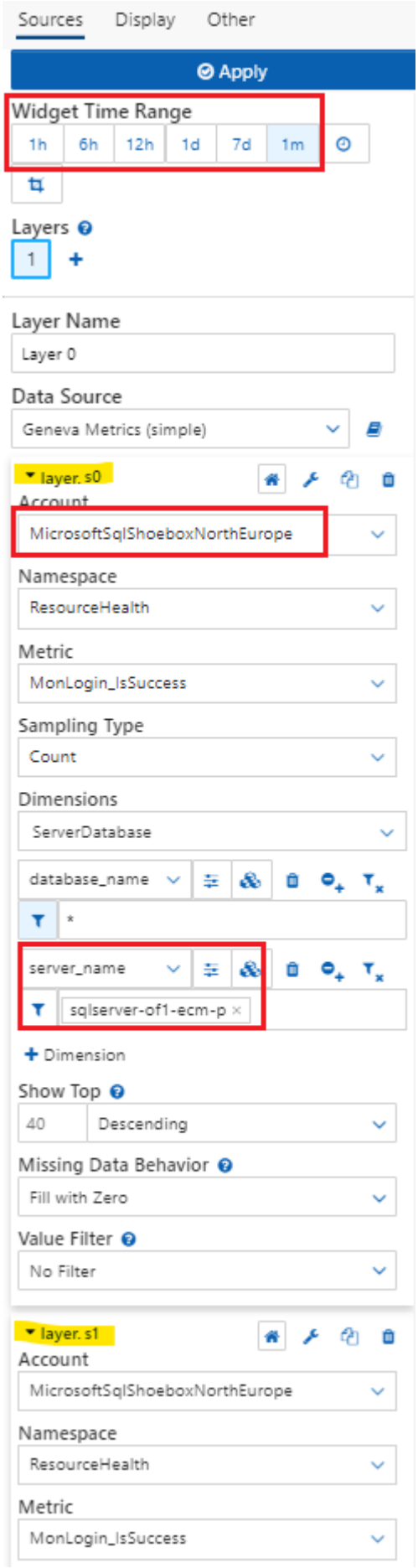
   If you see a spike, it means there happened to be a login failure during the timeframe due to system error. Please check/clarify the timezone in the incident reported by the customer/CSS engineer. There has been cases where there is confusion on PST vs UTC. Searching for a wrong time window would result in inaccurate results.

Example template to show login failures - https://jarvis-west.dc.ad.msft.net/dashboard/share/CEB88E77
TSG on how to chart MDM data on Jarvis -TSG - how to chart customer metrics

*** Make sure you are using the right MDM dashboard: it should have 2 layers. Login failure count = layer0 - Layer1. Layer0 is count of MonLogin_IsSuccess (total login count). Layer1 is sum of MonLogin_IsSuccess (total successful login count). ***

Example - Figure 1a shows a spike indicating login failure. Figure 1b shows the two layers (layer.s0 and layer.s1). Make sure you change server_name for both of these layers.





2. If you don't see any login failures in Kusto and MDM, check what was reported in RHC backend(health dashboard) using TSG - To check if RHC reported down for a resource. If backend shows green, there

hasn't been any failures and the issue seems to be in the UI. Raise ICM to **Azure Service Health/Resource Health Team**

3. If there are login failures in Step 1 & Step 2, follow other TSGs to troubleshoot login failures. If need help from PG, raise ICM to **Availability/Connectivity** team for RCA of login failure.

4. If there are no login failures in Step 1 & Step 2 but customer DB was indeed down and RHC showed available, check in MonLogin that the login failure is not due to user error (e.g. wrong password). If login failure is caused by system issue, this is likely due to the tail missing telemetry during failover.

5. If customer wants RCA for unknown state, check if there is login failure. If no login failure, tell customer that this is a transient issue in the RHC telemetry pipeline on reporting resource health, but the resource is healthy. If you see login failure from Kusto or MDM, then RCA login failure for customer. If cusotmer wants to RCA the unknown state without login failure in Kusto/MDM, open ICM with Azure Service Health / Resource Health.

Root Cause Classification Cases resolved by this TSG should be coded to the following root cause: Connectivity: Troubleshoot DB Availability and Connection Errors\Resource Health events

How good have you found this content?