Expired Certificates blocking logins for AAD users

Last updated by | Vitor Tomaz | Jun 8, 2022 at 5:23 AM PDT

Contents

Issue:

This is an ongoing issue (*as of 2/9/2022*) where expired certificates blocking logins for AAD SQL DB users. The mitigation involves Cert rotation, removing expired certs from nodes and restarting the node.

Please note- SQL Authentication is not impacted by this.

How to identify / classify issue:

- Failures when logging into database instances. Customer may receive login failure 18456 with state 109.
- The issue impacts AAD principals that are members of large number of groups (>200).
- Management operations to create new AAD logins/users may also have failed.

From ASC

- Check for ASC insight (No-code insight has been turned on for this to confirm the behavior)

Using Kusto

Use the below attached query which should return results for impacted users <server name>.

```
let srvr_name = 'replace server name';

MonLoginUserDDL
| where TIMESTAMP >= ago(lookback)
| where error_state == 113
| parse ClusterName with "tr" s1:string "." RegionName:string "." s2:string
| union (
MonFedAuthTicketService
| where originalEventTimestamp > ago(lookback)
| where error_message contains "AADSTS1000502: The provided certificate is not within its specified validity w
| union (
MonAzureActivDirService
| where originalEventTimestamp > ago(lookback)
| where error_state == 113)
| union (
MonSQLSystemHealth
| where originalEventTimestamp > ago(lookback)
| where event == "systemmetadata_written"
| where message contains "ADAL trace : Cannot find object or property")
| union (
MonLogin
| where TIMESTAMP >= ago(lookback)
| where event == "process_login_finish"
and (fedauth_adal_workflow > 0 or fedauth_library_type > 0)
and is_success != 1
and error == 18456 and (state == 133 or state == 109))
| summarize arg_max(originalEventTimestamp, ClusterName, AppTypeName, AppName, NodeName) by ClusterName, AppTy
| where AppTypeName !in ("Worker.DW","Worker.VDW.Frontend")
| project originalEventTimestamp, ClusterName, AppTypeName, AppName, NodeName, LogicalServerName
| extend cmd1 = strcat("Get-FabricNode -NodeName ", NodeName, " -NodeClusterName ", ClusterName, " | Kill-Proc
| extend Region = extract("(.*)\\.(.*)\\.(worker|control).(database|sqltest-eg1).(windows.net|chinacloudapi.cn
| where Region in ("southcentralus1-a","uksouth1-a","australiaeast1-a","northcentralus1-a","brazilsouth1-a","c
| extend ClusterCmd = strcat("Select-SqlAzureCluster Wasd-prod-", Region, "-CR2; ")
| project originalEventTimestamp, Region, ClusterName, AppTypeName, AppName, cmd1=strcat(ClusterCmd,cmd1), Nod
| extend Endpoint = strcat("wasd-prod-", extract("^[^.]*\\.([^.]*)\\.", 1, ClusterName))
| extend appUri=strcat("fabric:/",AppTypeName,"/",AppName)
| project AppName, ClusterName, NodeName, AppTypeName, Endpoint, appUri, LogicalServerName
| join kind=leftouter(
MonNonPiiAudit
| where TIMESTAMP > ago(lookback)
| where request_action contains "KillProcess"
| where request contains "sqlservr.exe"
| where request contains "Worker.ISO" or request contains "Worker.ISO.Premium" or request contains "Worker.Vld
| where request !contains "serviceManifestName"
| where username contains "GenevaAutomationConnector"
| summarize arg_max(TIMESTAMP, *) by ClusterName, request
| extend MitigatedAppUri = url_decode(extract(".*appUri=%27(.*)%27", 1, request))
| project TIMESTAMP, ClusterName, MitigatedAppUri
) on $left.appUri == $right.MitigatedAppUri
| where LogicalServerName =~ srvr_name
| where MitigatedAppUri == ''
```

Workaround or Mitigation:

PG implemented the fix on clusters with a high number of errors. Reviewing the telemetry engineering confirmed that the error rate has decreased drastically, and most customers would now see recovery within ~ 30min

However, if the issues persist for customers, then it requires escalation to Security team to restart the instance.

No recommended work around from customer side.

Root Cause for Customer: <PENDING>

We will share detail RCA once we complete the mitigation

Action from CSS: For SQLDB: Wait 30 mins for bot action to fix the issue. After 30 minutes, escalate to PG.

Reference

Parent ICM (LSI) to Link Support Cases: Master ICM link

How good have you found this content?

🙂 🙁