The Azure Key Vault client encountered an error with message

Last updated by | Vitor Tomaz | Jun 20, 2022 at 8:43 AM PDT

Contents

- Issue
- Investigation/Analysis
- Mitigation
- Root Cause Classification

Issue

MonSQLSystemHealth shows an message like '*The Azure Key Vault client encountered an error with message*' with multiple error code and info code like:

```
Error: 33183, Severity: 16, State: 1.
The Azure Key Vault client encountered an error with message '[error:106, info:12002, state:0] Cannot send a r
```

Investigation/Analysis

We ASC Insights for a few specific scenarios like:

- Inaccessible DB due to Deleted Key or key vault
- Inaccessible DB due to DNS issue or AKV Outage
- Inaccessible DB due to insufficient key permissions
- (and one generic called "Inaccessible Database")

Before proceeding with the investigation check if you can see any of these insights already.

If not, identify and check **info** code for more information:

```
MonSQLSystemHealth
| where originalEventTimestamp >= ago(1d)
| where LogicalServerName =~ 'abc'
| where event == "systemmetadata_written"
| where message has 'The Azure Key Vault client encountered an error with message'
| parse message with * "The Azure Key Vault client encountered an error with message '[error:" error ", info:"
| project originalEventTimestamp, ClusterName, AppName, LogicalServerName, error, info, msg
```

Info	Description	Outcome	ASC Insight
400	The request is invalid. This usually means the key name is invalid or contains invalid characters.'.	Database inaccessible is due to key vault been deleted	
401	Cannot get token due to incorrect credentials. Make sure the credential string or certificate is valid.'.		
403	The server responded 403, because the user does not have proper permission to perform the action. Please make sure you have the permission for the specified operation. At minimum,'get, wrapKey, unwrapKey' permissions are required.'.	Database inaccessible is due to insufficient key permissions	Inaccessible DB due to insufficient key permissions
404	The server responded 404, because the key name was not found. Please make sure the key name exists in your vault.'.	Database inaccessible is due to key been deleted or key vault been deleted	Inaccessible DB due to Deleted Key or key vault
12001	Network error		
12002	Network error, the operation timed out.	We don't make db inaccessible in this case, we just keep trying. For MI, the customer is in control of changing network configurations on the instance.	
12007	Network error, internet name not resolved.	Database inaccessible is due to AKV Outage or DNS resolution issue	Inaccessible DB due to DNS issue or AKV Outage
12029	Network error, cannot connect to AKV.	We don't make db inaccessible in this case, we just keep trying. For SQL MI, the customer is in control of changing network configurations on the instance.	

Mitigation

If customer is hitting 12002 or 12029 in SQL MI, the customer is in control of changing network configurations on the instance. This can be cause by multiple reasons, some are:

- Customer configure their instance with VNET/firewall rule that is very restrictive and the Managed Instance is not able to talk AKV due to that.
- Customer DNS resolution not working properly (custom DNS).
- Customer switched AKV to private link while forgetting to change NSG rule (**customer needs to set outbound NSG rule to allow traffic on port 443 to AKV private endpoint IP Address**).

Test connectivity using https://techcommunity.microsoft.com/t5/azure-sql-blog/how-to-test-tcp-connectivity-from-a-sql-managed-instance/ba-p/3058458 ↗

Root Cause Classification

Cases resolved by this TSG should be coded to the following root cause:
Root Cause: Azure SQL DB MI\Security\User Issue/Error

How good have you found this content?

😊 🙁