AKV Error while deleting Federated Client Id

Last updated by | Vitor Tomaz | Feb 24, 2023 at 3:29 AM PST

Contents

Issue

When a server is configured for only crooss tenant customer-managed keys, and if the federated client id is attempted to be deleted, the below error is most likely to be seen.

Investigation/Analysis

```
 The operation could not be completed because an Azure Active Directory error was encountered. Please ensure the
server '<SQl Server>' and key vault '<AKV>' belong to the same tenant. The error message from Active Directory
Authentication library is 'AADSTS700016: Application with identifier '<Guid>' was not found in the directory
'<AAD>'. This can happen if the application has not been installed by the administrator of the tenant or
consented to by any user in the tenant. You may have sent your authentication request to the wrong tenant.
```

When Federated Client id is tried to be removed, the check to validate id the server is able to reach the AKV will fail, as there wont be a way to federate the access to the AKV across tenants.

Mitigation

Configure the SQL Server to use System Managed Keys and then attempt to delete the federated client id.

RCA Template (optional)

TBD

Public Doc Reference (optional)

TBD

Internal Reference (optional)

PG is working on a backlog item to reference to the customer with accurate error details and solution

Root Cause Classification

Security/TDE and CMK, AKV/AKV/ Error Failure

How good have you found this content?

🙂 🙁