Failed to decrypt data

Last updated by | Soma Jagadeesh | Jan 10, 2021 at 9:46 PM PST

Contents

Issue

Failed to decrypt data with error ;   "Failed to decrypt a column encryption key using key store provider: 'AZURE_KEY_VAULT'. Verify the properties of the column encryption key and its column master key in your database."

Investigation/Analysis

Missing permission to the key vault

Mitigation

For application: • Grant permission to the application via the PowerShell: Set-AzureRmKeyVaultAccessPolicy -VaultName $vaultName -ResourceGroupName $resourceGroupName -ServicePrincipalName $clientId -PermissionsToKeys get,wrapKey,unwrapKey,sign,verify,list

• Or you can grant permission using the azure portal

• And register the Azure Key Vault provider with the ADO.NET ⧉ driver. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-always-encrypted-azure-key-vault ⧉ use application client id and client secret here clientCredential = new ClientCredential(clientId, clientSecret);

For user: • Also you grant permission to the user so that we can decrypt data in SSMS Set-AzureRmKeyVaultAccessPolicy -VaultName $vaultName -ResourceGroupName $resourceGroupName -PermissionsToKeys create,get,wrapKey,unwrapKey,sign,verify,list -UserPrincipalName $userPrincipalName

• Or you can grant permission using the azure portal

RCA (optional)

More Information (optional)

Detailed information/background that may be useful but isn't strictly required for troubleshooting. Often this is the "verbose" details that one usually doesn't need

Public Doc Reference (optional)

https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/create-and-store-column-master-keys-always-encrypted?view=sql-server-ver15#making-azure-key-vault-keys-available-to-applications-and-users ⧉

Internal Reference (optional)

Classification

Root cause tree: Security/User issue/error/Uncoded

How good have you found this content?

😊 🙁