Creating a Secret Scope in Databricks backed by Azure Key Vault fails

stackoverflow.com/questions/56537214/creating-a-secret-scope-in-databricks-backed-by-azure-key-vault-fails/56537215

Asked 3 years, 9 months ago

Modified 2 years, 7 months ago
Viewed 15k times

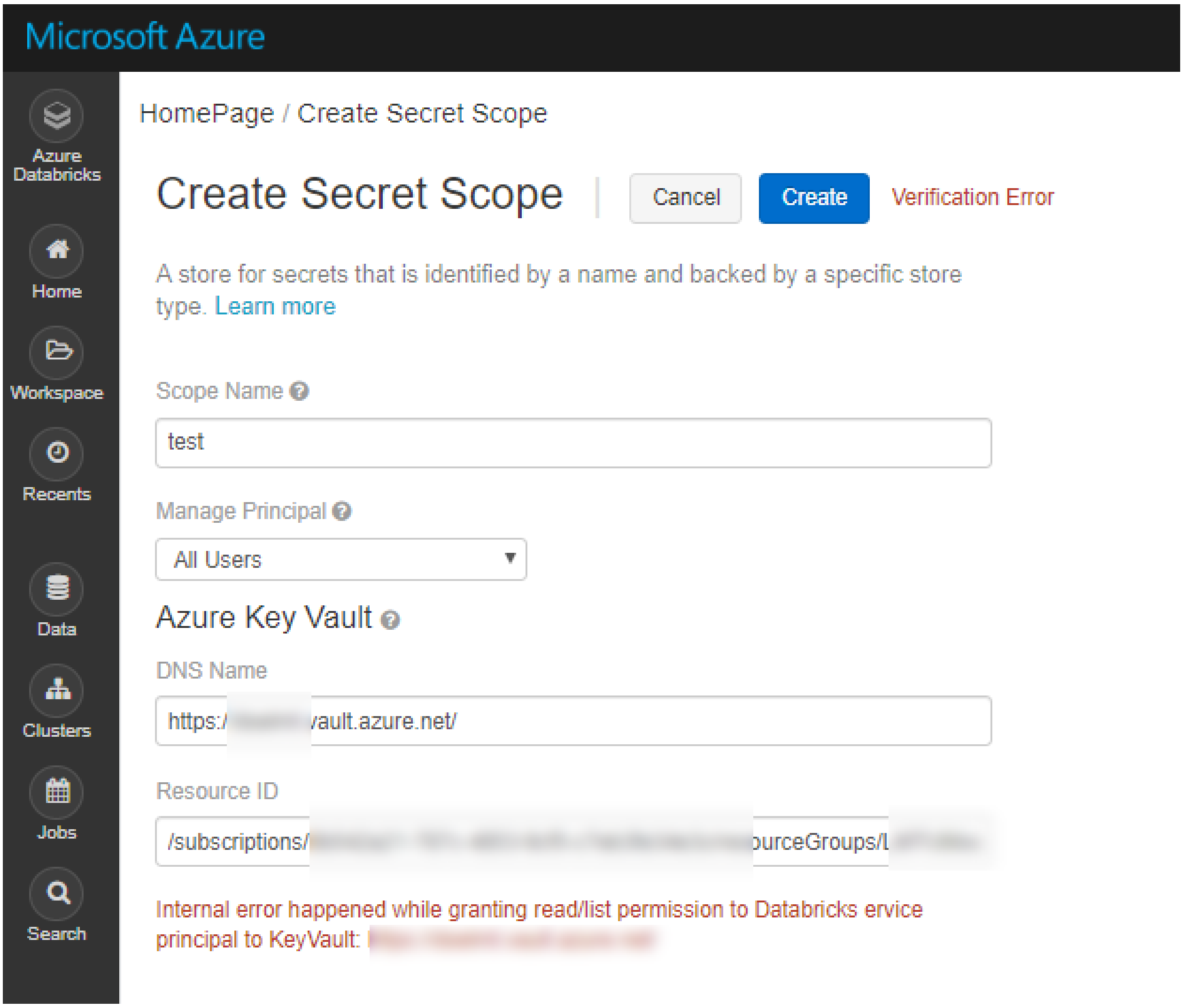
Part of Microsoft Azure Collective

10

You can create scopes in Databricks backed by Azure Keyvault instead of using the Databricks CLI. However, when you try to create a Scope, an obscure error message (with a spelling mistake!) is shown. It appears as not many people encounter this error:

"Internal error happened while granting read/list permission to Databricks ervice principal to KeyVault: XYZ"

Setting the Manage Principal to All Users does NOT help in this case.



HomePage / Create Secret Scope

Create Secret Scope | Cancel Create Verification Error

A store for secrets that is identified by a name and backed by a specific store type. Learn more

Scope Name: test

Manage Principal: All Users

Azure Key Vault

DNS Name: https:/[redacted]vault.azure.net/

Resource ID: /subscriptions/[redacted]ourceGroups/[redacted]

Internal error happened while granting read/list permission to Databricks ervice principal to KeyVault: [redacted]

edited Jun 11, 2019 at 5:54

Tony Ju

14.5k33 gold badges1616 silver badges2929 bronze badges

asked Jun 11, 2019 at 5:46

Rodney

5,31777 gold badges5555 silver badges9696 bronze badges

Add a comment

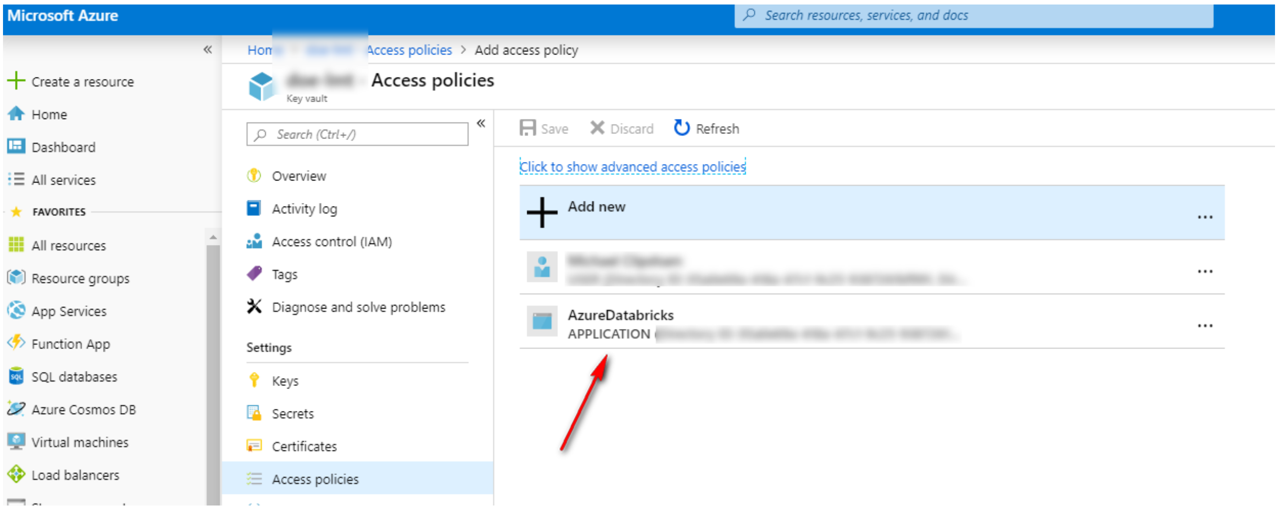
2 Answers

10

✓

I figured that this was a Service Principal issue in Azure AD. This particular user I was logged on to Databricks with was not an AD contributer and only had Contributer role on the Databricks and Keyvault service. I could not find any default Object ID in AD for Databricks so I assumed it was creating a service principal on the fly and connecting Databricks with Keyvault (I might be wrong here - it might already exist in AD when you enable the Databricks resource provider).

Logging in as an Admin with the rights to create service principals solved the problem. After that you can see in the Key Vault the DB service principal used in for the key retrieval:



answered Jun 11, 2019 at 5:46

Rodney

5,31777 gold badges5555 silver badges9696 bronze badges

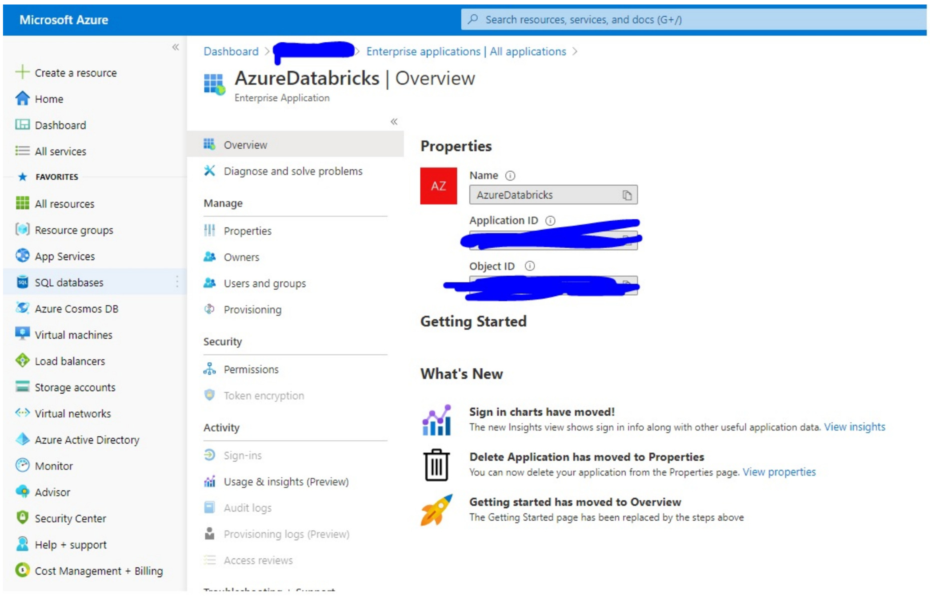
3

The 'AzureDatabricks' service principal already exists; it is in Azure Active Directory as an Enterprise Application (portal.azure.com/#blade/Microsoft_AAD_IAM/ManagedAppMenuBlade/...). You don't need permission to create service principals for this process to work, but you do need to have Owner permission on the Key Vault so that it can create an access policy for 'AzureDatabricks'. – rcabr Oct 28, 2019 at 19:47

Add a comment

2

As mentioned by @rcabr in his above comment there is already an SP by name 'AzureDatabricks' inside Enterprize Application, you need to get the object id details and add it in the access policy of the key vault. With this, the Databricks will be able to access the KeyVault



Dashboard > [redacted] > Enterprise applications | All applications >

AzureDatabricks | Overview

Enterprise Application

Properties

AZ

Name: AzureDatabricks

Application ID: [redacted]

Object ID: [redacted]

Getting Started

What's New

Sign in charts have moved!
The new Insights view shows sign in info along with other useful application data. View insights

Delete Application has moved to Properties
You can now delete your application from the Properties page. View properties

Getting started has moved to Overview
The Getting Started page has been replaced by the steps above

answered Aug 5, 2020 at 19:10

Yogesh_JavaJ2EE
6311 silver badge99 bronze badges

1

I tried to search this enterpirse app in ad enterprise app menu and not able to find. So I directly went to KV IAM and search for *AzureDataBricks* it appeard and I assigned – Jayendran Sep 16, 2021 at 9:07

Add a comment

Your Answer

Sign up or log in

Sign up using Google
Sign up using Facebook
Sign up using Email and Password

Post as a guest

Required, but never shown

Not the answer you're looking for? Browse other questions tagged azureazure-keyvaultazure-databricks or ask your own question.