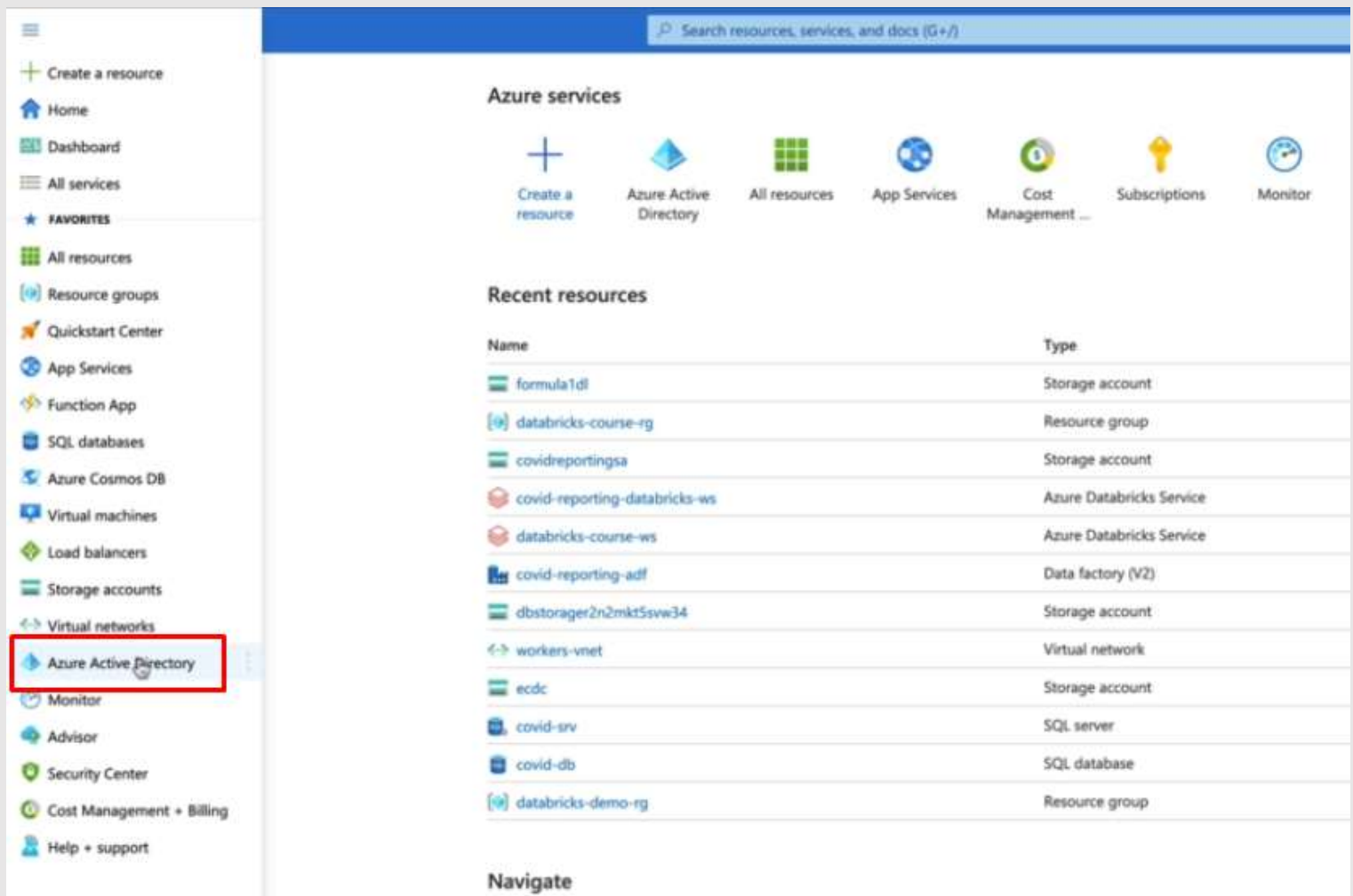


Azure Databricks Integracion con ADLS Usar Active Directory – Utilizar Service Principal / Databricks Scoped Secret

Creando un Azure Service Principal



The screenshot shows the Azure portal interface. On the left, the navigation pane lists various services, with 'Azure Active Directory' highlighted by a red box. The main content area displays 'Azure services' and 'Recent resources'.

Azure services

- Create a resource
- Azure Active Directory
- All resources
- App Services
- Cost Management ...
- Subscriptions
- Monitor

Recent resources

Name	Type
formula1dl	Storage account
databricks-course-rg	Resource group
covidreportingsa	Storage account
covid-reporting-databricks-ws	Azure Databricks Service
databricks-course-ws	Azure Databricks Service
covid-reporting-adf	Data factory (V2)
dbstorager2n2mkt5sve34	Storage account
workers-vnet	Virtual network
ecdc	Storage account
covid-srv	SQL server
covid-db	SQL database
databricks-demo-rg	Resource group

Navigate

Microsoft Azure

Search resources, services, and docs (G+/)

Home >

Default Directory | Overview

Azure Active Directory

Switch tenant Delete tenant + Create a tenant What's new Preview features Got feedback?

- Overview
- Getting started
- Preview features
- Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations**
- Identity Governance
- Application proxy
- Licenses

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Default Directory

Default Directory | App registrations

Azure Active Directory

+ New registration Endpoints Troubleshooting Download Preview features Got feedback?


Try out the new App registrations search preview! Click to enable the preview. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. Upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

All applications **Owned applications** Deleted applications (Preview) Applications from personal account

Start typing a name or Application ID to filter these results

Display name

	covid-reporting-app
---	---------------------

[Home](#) > [Default Directory](#) >

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

LE DAMOS UN NOMBRE

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Default Directory only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.



Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

Microsoft Azure

Search resources, services, and docs (G+)

Home > Default Directory >

databricks-service-app

Search (Cmd+/)

DeleteEndpointsPreview features

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Essentials

Display name : databricks-service-app

Application (client) ID : b9f0234a-70c9-44f6-a2a2-fff1d6939edc

Directory (tenant) ID : 65947afd-b0be-440f-b3d5-2ca66af0ef41

Object ID : adf28b97-79a0-4a80-a4f1-3373f39b9c5c

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD will be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get StartedDocumentation

COPIAR:
- Application (client) ID
- Directory (tenant) ID

Microsoft Azure

Search resources, services, and docs (G+)

Home > Default Directory > databricks-service-app

databricks-service-app | Certificates & secrets

Search (Cmd+/)

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	ID
No certificates have been added for this application.			

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
No client secrets have been created for this application.			

1

2

Microsoft Azure

Search resources, services, and docs (G+)

Home > Default Directory > databricks-service-app

databricks-service-app | Certificates & secrets

Search (Cmd+J) Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	ID
No certificates have been added for this application.			

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
No client secrets have been created for this application.			

Add a client secret

LE DAMOS UN NOMBRE

Description: databricks-access-secret

Expires: Recommended: 6 months

Microsoft Azure

Search resources, services, and docs (G+)

Home > Default Directory > databricks-service-app

databricks-service-app | Certificates & secrets

Search (Cmd+J) Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	ID
No certificates have been added for this application.			

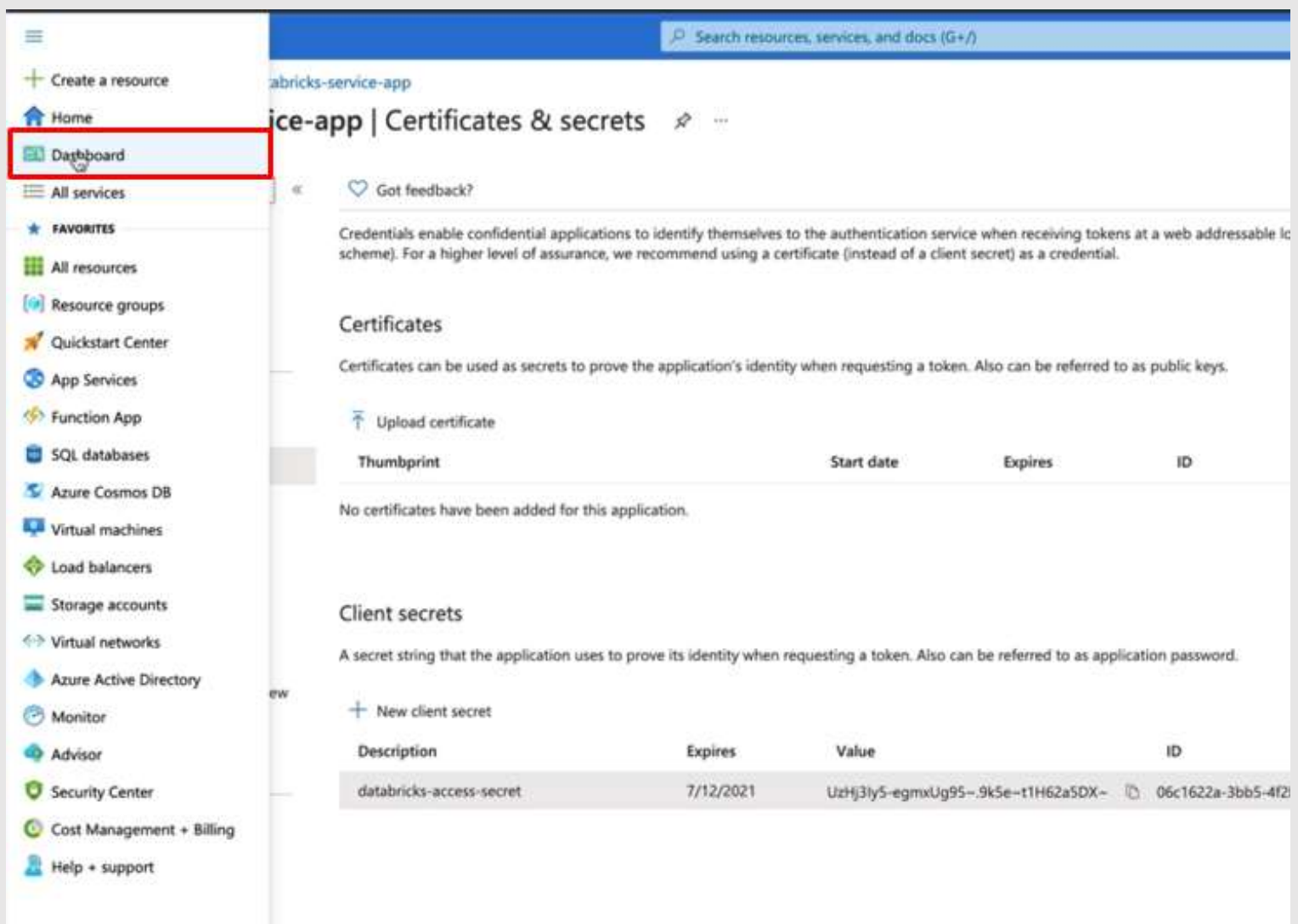
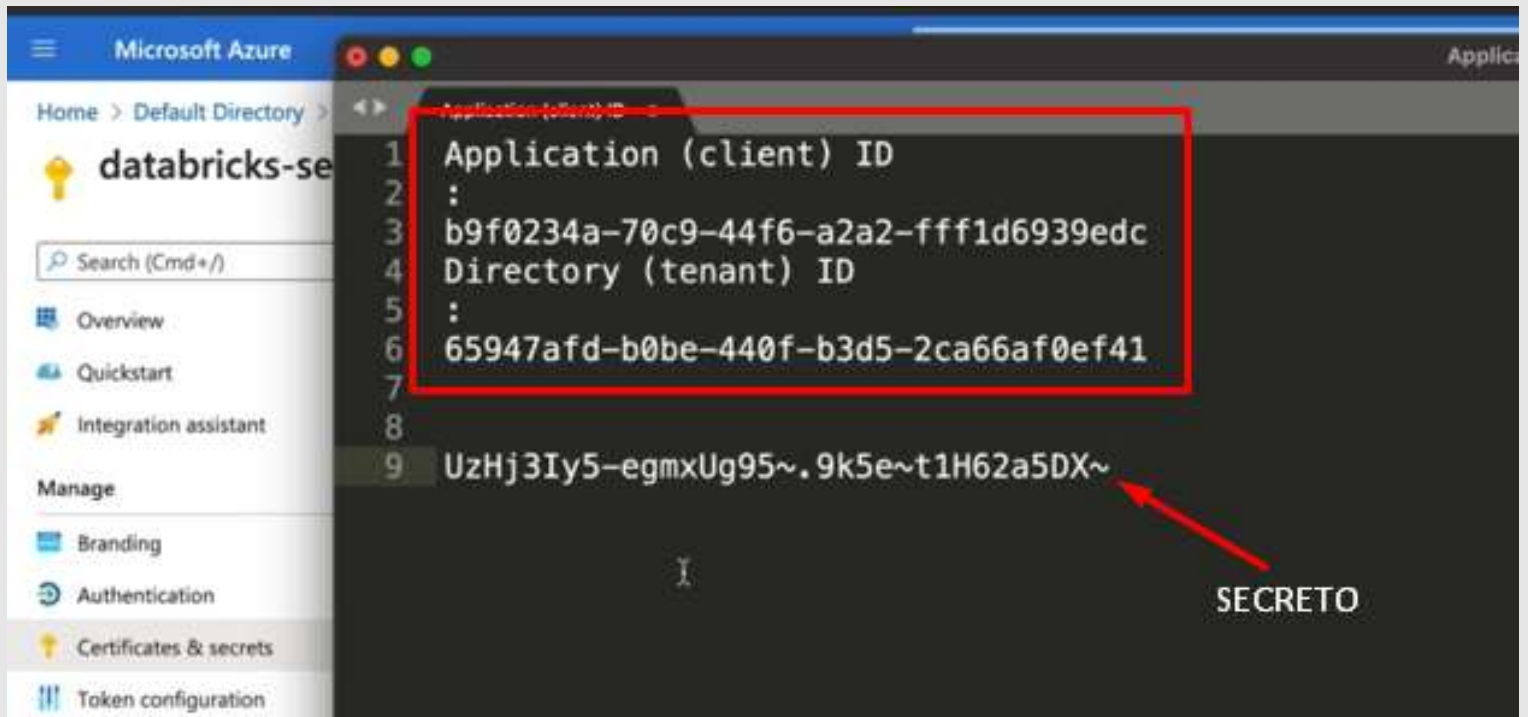
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
databricks-access-secret	7/12/2021	Uzhj3ly5-egmxUg95-.9k5e-t1H62a5DX-	06c1622a-3bb5-4f2b-ade6-19632a30bd8b

COPIAMOS EL SECRETO RECIÉN CREADO



Microsoft Azure

Search resources, services, and docs (G+)

Databricks Course Dashboard

Private dashboard

+ New dashboard ▾ Refresh Full screen Edit Share Download Clone Assign tags Delete Feedback

Auto refresh : Off

databricks-course-ws
Workspace

formula1dl
Storage account

Storage account: que corresponde a un ADLS

Microsoft Azure

Search resources, services, and docs (G+)

Dashboard > formula1dl

formula1dl | Access Control (IAM)

Storage account

Search (Cmd+/) « + Add Download role assignments Edit columns Refresh Remove Got feedback?

Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage Explorer (preview)
Settings
Access keys
Geo-replication
...

Add role assignment
Add co-administrator

My access
View my level of access to this resource.
[View my access](#)

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Find ○
User, group, or service principal ▾
Search by name or email address

Grant access to this resource
Grant access to resources by assigning a role.
[Add role assignments](#) [Learn more](#)

View deny assignments
View the role assignments that have been denied access to specific actions at this scope.

Microsoft Azure

Dashboard > formula1dl

formula1dl | Access Control (IAM)

Storage account

Search (Ctrl+Q)

+ Add Download role assignments Add columns Refresh Remove Get feedback?

Overview Activity log Tags Diagnose and solve problems Access Control (IAM) Data migration Events Storage Explorer (preview) Settings Access keys Geo replication CDAS Configuration Encryption Shared access signature Networking Security Static website

Check access Role assignments Roles Roles (Preview) Deny assignments Classic administrators

My access
View my level of access to this resource.
[View my access](#)

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Find

Grant access to this resource
Grant access to resources by assigning a role.
[Add role assignments](#) [Learn more](#)

View access to this resource
View the role assignments that grant access to this and other resources.
[View](#) [Learn more](#)

View deny assignments
View the role assignments that have been denied access to specific actions at this scope.
[View](#) [Learn more](#)

Add role assignment

Role

Assign access to

Select

Databricks Resource Provider

databricks-service-app

Selected members:
No members selected. Search for and add one or more members you want to assign to the role for this resource.
[Learn more about RBAC](#)

Azure Service Principal que acabamos de crear

Microsoft Azure

Dashboard > formula1dl

formula1dl | Access Control (IAM)

Storage account

Search (Ctrl+Q)

+ Add Download role assignments Add columns Refresh Remove Get feedback?

Overview Activity log Tags Diagnose and solve problems Access Control (IAM) Data migration Events Storage Explorer (preview) Settings Access keys Geo replication CDAS Configuration Encryption Shared access signature Networking Security Static website Properties Locks Data Lake Storage Containers Data protection Lifecycle management

Check access Role assignments Roles Roles (Preview) Deny assignments Classic administrators

My access
View my level of access to this resource.
[View my access](#)

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Find

Grant access to this resource
Grant access to resources by assigning a role.
[Add role assignments](#) [Learn more](#)

View access to this resource
View the role assignments that grant access to this and other resources.
[View](#) [Learn more](#)

View deny assignments
View the role assignments that have been denied access to specific actions at this scope.
[View](#) [Learn more](#)

Add role assignment

Role

Assign access to

Select

Databricks Resource Provider


databricks-service-app [Remove](#)

Selected members:

[Save](#) [Discard](#)

Mounting Azure Data Lake Storage Gen2

Antes que todo, vamos a utilizar Azure Key Vault para almacenar el Client ID, Tenant ID y el Client Secret.

 Microsoft Azure

Search resources, services, and docs (G+/f)

Home > New > Key Vault >

Create key vault

Validation passed

BasicsAccess policyNetworkingTagsReview + create

Review + create

Basics

Subscription	Pay-As-You-Go
Resource group	databricks-course-rg
Key vault name	formula1-key-vault
Region	UK South
Pricing tier	Standard
Soft-delete	Enabled
Purge protection during retention period	Disabled
Days to retain deleted vaults	90 days

Access policy

Azure Virtual Machines for deployment	Disabled
Azure Resource Manager for template deployment	Disabled
Azure Disk Encryption for volume encryption	Disabled
Permission model	Vault access policy
Access policies	1

Networking

Connectivity method	Public endpoint (all networks)
---------------------	--------------------------------

Create< PreviousNext >Download a template for automation

Así agregamos el servicio al dashboard

Microsoft Azure

Home > formula1-key-vault

formula1-key-vault

Search (Cmd+I)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Events

Settings

Keys

Secrets

Certificates

Access policies

Essentials

Resource group (changed) : datastudio-course-rg

Location : UK South

Subscription (changed) : Pay As You Go

Subscription ID : 38d7707a-1340-45c5-81e4-57af3d46111a

Tags (changed) : Click here to add tags

Get started

Monitoring

Tools + SDKs

Tutorials

Manage keys and secrets used by apps and services

Our recommendation is to use a vault per application per environment (Development, Pre-Production and Production). This helps you to not share secrets across environments and also reduces the threat in case of a breach.

Control access to key vault

Assign access policy and determine whether a given service principal, namely an application or user group, can perform different operations on key vault keys, secrets or certificates.

View access policies

Adding Access policy

How to authenticate to key vault

Enable logging and set up alerts

Enable logging to monitor how, when and by whom your key vaults are accessed. Monitor performance and configure alerts for key vault metrics e.g., service API latency, error code, throttling.

View diagnostic settings

How to enable key vault logging

How to configure monitoring and alerting

Turn on recovery options

For protection against accidental or malicious deletion, soft-delete is enabled. Turn on purge protection to guard against manual purging of deleted key vaults and items. Learn more

View properties

Key vault recovery options

Pin to dashboard

Existing

Create new

Type

Private

Shared

Dashboard

DataStudio Course Dashboard

Pin

Cancel

So that's done.

Microsoft Azure

Home > formula1-key-vault > formula1-key-vault

formula1-key-vault | Secrets

Key vault

Search (Cmd+I)

+ Generate/Import

Refresh

Restore Backup

Manage deleted secrets

Name

Type

There are no secrets available.

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Events

Settings

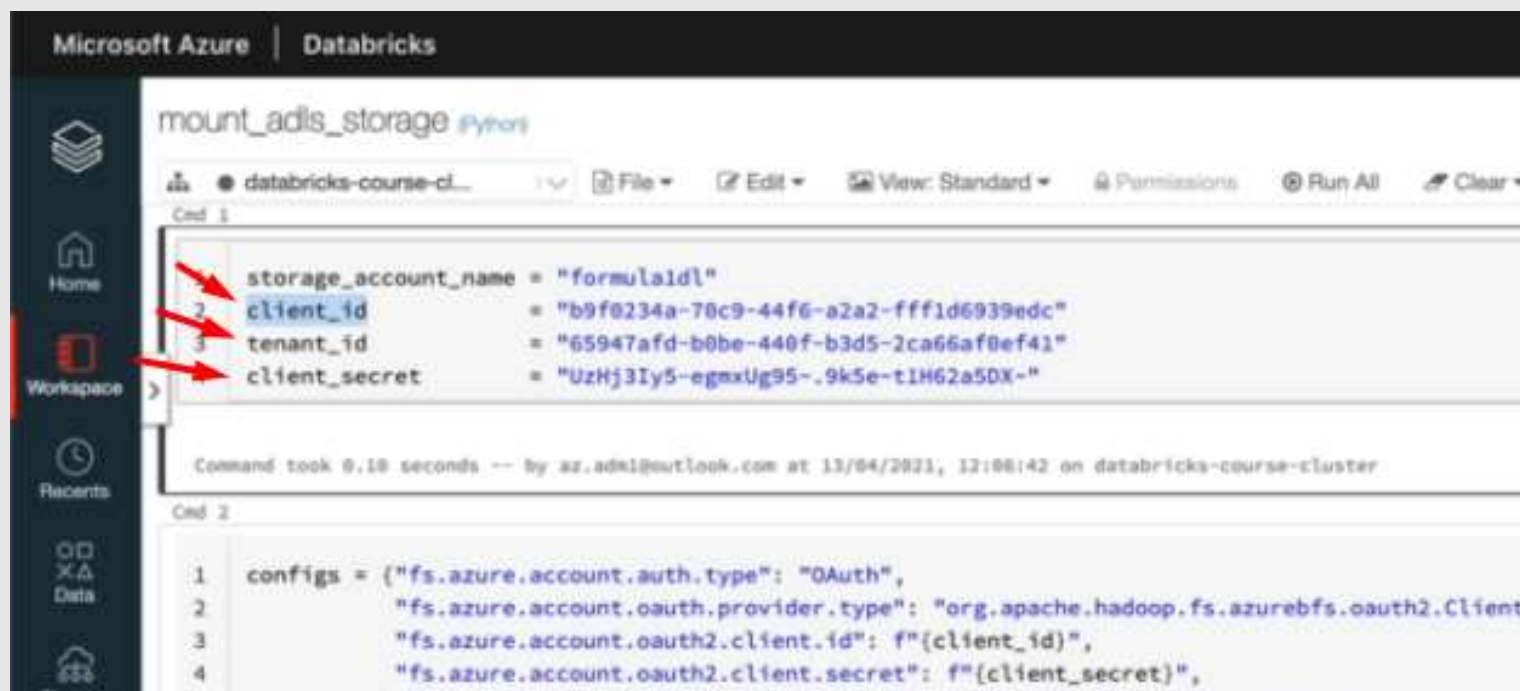
Keys

Secrets

Certificates

Access policies

Tenemos que generar 3 secretos en Azure Key Vault



Microsoft Azure | Databricks

mount_adls_storage *Python*

databricks-course-cl...

File Edit View: Standard Permissions Run All Clear

```
Cmd 1
1 storage_account_name = "formula1d1"
2 client_id = "b9f0234a-70c9-44f6-a2a2-fff1d6939edc"
3 tenant_id = "65947afd-b0be-440f-b3d5-2ca66af0ef41"
4 client_secret = "UzHj3Iy5-egmxUg95-.9k5e-tIH62a5DX-"

Command took 0.10 seconds -- by az.adml@outlook.com at 13/04/2021, 12:08:42 on databricks-course-cluster

Cmd 2
1 configs = {"fs.azure.account.auth.type": "OAuth",
2           "fs.azure.account.oauth.provider.type": "org.apache.hadoop.fs.azurebfs.oauth2.Client
3           "fs.azure.account.oauth2.client.id": f"{client_id}",
4           "fs.azure.account.oauth2.client.secret": f"{client_secret}",
```

Microsoft Azure

Search resources, services, and docs (G+)

Home > formula1-key-vault > formula1-key-vault

formula1-key-vault | Secrets

Key vault

Search (Cmd+/)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Events

Settings

Keys

Secrets

Certificates

+ Generate/import Refresh Restore Backup Manage deleted secrets

The secret 'databricks-app-client-id' has been successfully created.

Name	Type	Status
databricks-app-client-id		✓ Enabled

Repetimos el paso tanto para TENANT ID y el Client Secret

Se creó el secreto de Client ID en Azure Key Vault

Se han creado los 3 secretos

Microsoft Azure

Search resources, services, and docs (G+)

Home > formula1-key-vault > formula1-key-vault

formula1-key-vault | Secrets

Key vault

Search (Cmd+/)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Events

Settings

Keys

Secrets

Certificates

Access policies

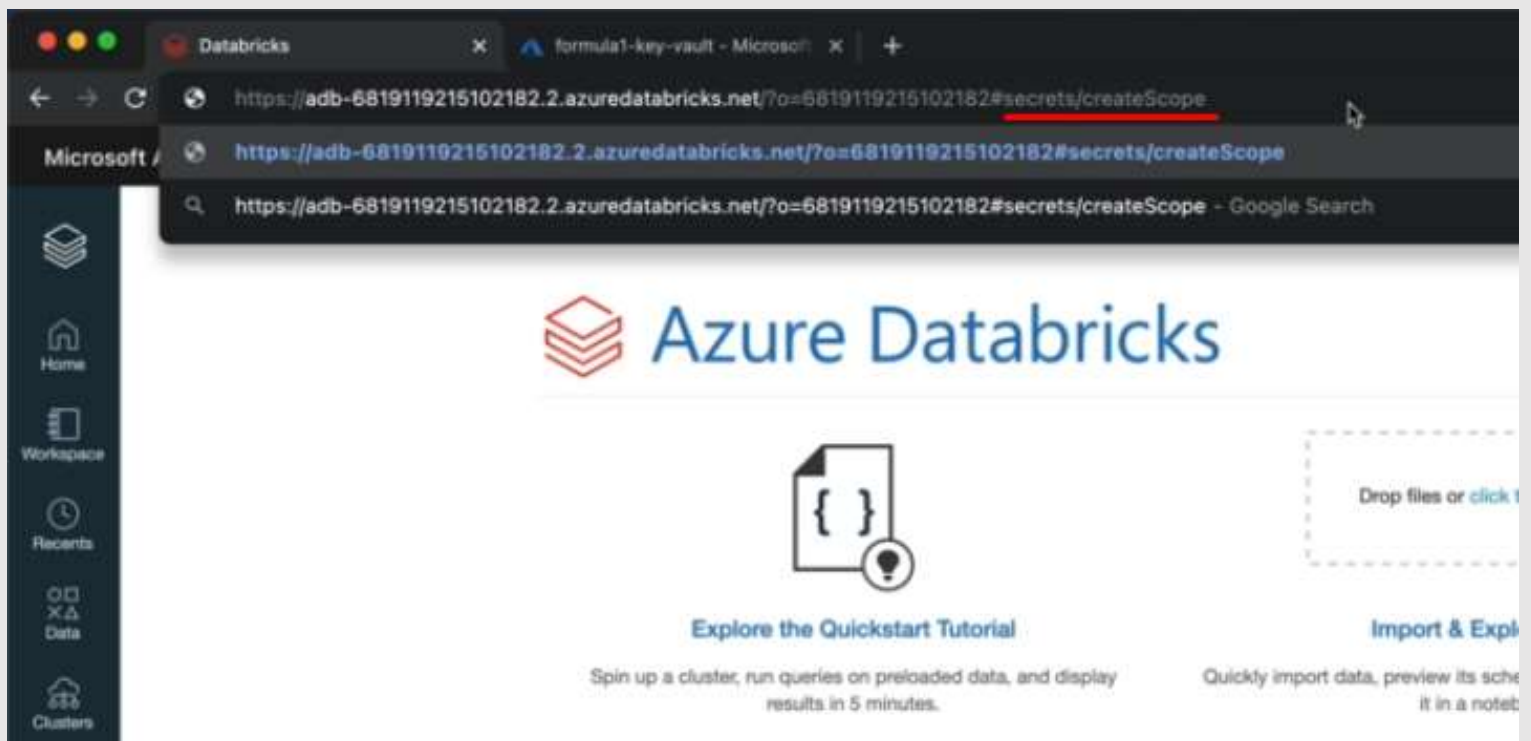
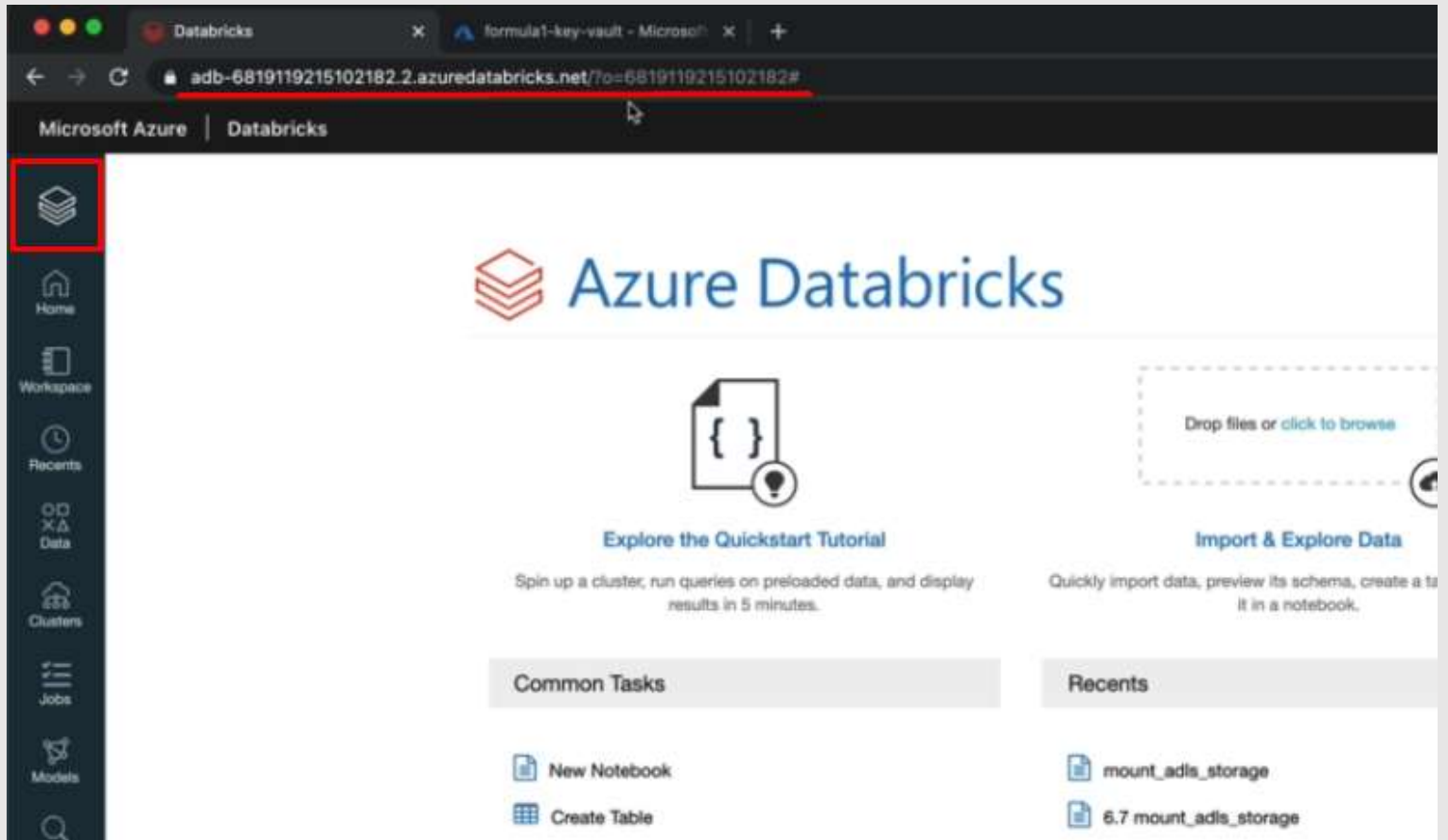
Networking

+ Generate/import Refresh Restore Backup Manage deleted secrets

The secret 'databricks-app-client-secret' has been successfully created.

Name	Type	Status
databricks-app-client-secret		✓ Enabled
databricks-app-tenant-id		✓ Enabled
databricks-app-client-id		✓ Enabled

Luego, damos clic en el símbolo de databricks y en la ruta web en el navegador agregaremos **#secrets/createScope**. Vamos a utilizar **Databricks Scoped Secret**



Regresamos al Azure Key Vault

Vault URI

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with the following items: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Events, Settings, Keys, Secrets, Certificates, Access policies, Networking, Security, Properties (highlighted with a red box), and Locks. The main content area displays the 'Properties' page for the 'formula1-key-vault' key vault. The 'Vault URI' field is highlighted with a red box, and a red arrow points to the 'Properties' tab in the left sidebar. The 'Vault URI' field contains the value: `https://formula1-key-vault.vault.azure.net/`. A 'Copy to clipboard' button is visible next to the 'Vault URI' field. The 'Resource ID' field contains the value: `/subscriptions/347767e-1340-40c5-81e4-5746544611e1/resourceGroups/Database-course-rg/providers/Microsoft.KeyVault/vaults/formula1-key-vault`. The 'Subscription ID' field contains the value: `347767e-1340-40c5-81e4-5746544611e1`. The 'Subscription Name' field contains the value: `Pay-As-You-Go`. The 'Directory ID' field contains the value: `629474d1-6d5e-4409-b3d5-b3ab4d4d4d11`. The 'Directory Name' field contains the value: `Default Directory`. The 'Soft delete' section indicates that soft delete has been enabled on this key vault. The 'Purge protection' section shows that the 'Disable purge protection' option is selected.

Property	Value
Name	formula1-key-vault
SKU (Pricing tier)	Standard
Location	uksouth
Vault URI	https://formula1-key-vault.vault.azure.net/
Resource ID	/subscriptions/347767e-1340-40c5-81e4-5746544611e1/resourceGroups/Database-course-rg/providers/Microsoft.KeyVault/vaults/formula1-key-vault
Subscription ID	347767e-1340-40c5-81e4-5746544611e1
Subscription Name	Pay-As-You-Go
Directory ID	629474d1-6d5e-4409-b3d5-b3ab4d4d4d11
Directory Name	Default Directory
Soft delete	Soft delete has been enabled on this key vault
Days to retain deleted vaults	30
Purge protection	<input checked="" type="radio"/> Disable purge protection (allow key vault and objects to be purged during retention period) <input type="radio"/> Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

Resource ID

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with the following items: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Events, Settings, Keys, Secrets, Certificates, Access policies, Networking, Security, Properties (highlighted with a red box), and Locks. The main content area displays the 'Properties' page for the 'formula1-key-vault' key vault. The 'Resource ID' field is highlighted with a red box, and a red arrow points to the 'Properties' tab in the left sidebar. The 'Resource ID' field contains the value: `/subscriptions/347767e-1340-40c5-81e4-5746544611e1/resourceGroups/Database-course-rg/providers/Microsoft.KeyVault/vaults/formula1-key-vault`. The 'Subscription ID' field contains the value: `347767e-1340-40c5-81e4-5746544611e1`. The 'Subscription Name' field contains the value: `Pay-As-You-Go`. The 'Directory ID' field contains the value: `629474d1-6d5e-4409-b3d5-b3ab4d4d4d11`. The 'Directory Name' field contains the value: `Default Directory`. The 'Soft delete' section indicates that soft delete has been enabled on this key vault. The 'Purge protection' section shows that the 'Disable purge protection' option is selected.

Property	Value
Name	formula1-key-vault
SKU (Pricing tier)	Standard
Location	uksouth
Vault URI	https://formula1-key-vault.vault.azure.net/
Resource ID	/subscriptions/347767e-1340-40c5-81e4-5746544611e1/resourceGroups/Database-course-rg/providers/Microsoft.KeyVault/vaults/formula1-key-vault
Subscription ID	347767e-1340-40c5-81e4-5746544611e1
Subscription Name	Pay-As-You-Go
Directory ID	629474d1-6d5e-4409-b3d5-b3ab4d4d4d11
Directory Name	Default Directory
Soft delete	Soft delete has been enabled on this key vault
Days to retain deleted vaults	30
Purge protection	<input checked="" type="radio"/> Disable purge protection (allow key vault and objects to be purged during retention period) <input type="radio"/> Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

Microsoft Azure | Databricks

HomePage / Create Secret Scope

Create Secret Scope

[Cancel](#) [Create](#)

A store for secrets that is identified by a name and backed by a specific store type. [Learn more](#)

Scope Name ⓘ

formula1-scope

Manage Principal ⓘ

Creator

Azure Key Vault ⓘ

DNS Name

https://formula1-key-vault.vault.azure.net/

Resource ID

oups/databricks-course-rg/providers/Microsoft.KeyVault/vaults/formula1-key-vault

Creamos un nombre

Vault URI

Resource ID

Nos generará un error

Microsoft Azure | Databricks

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 ⓘ

formula1-scope

Manage Principal ⓘ

Creator

Azure Key Vault ⓘ

DNS Name

https://formula1-key-vault.vault.azure.net/

Resource ID

/subscriptions/34cf7d7a-1340-43c5-81e4-57efa1d4b11a/resourceGroups/databric

Premium Tier is disabled in this workspace. Secret scopes can only be created with initial_manage_principal "users".

Modificamos el “Manage Principal” a “All Users”

Microsoft Azure | Databricks

HomePage / Create Secret Scope

Create Secret Scope

[Cancel](#) [Verifying...](#)

A store for secrets that is identified by a name and backed by a specific store type. [Learn more](#)

Scope Name ⓘ

Manage Principal ⓘ

All Users

Azure Key Vault ⓘ

DNS Name

Resource ID

Microsoft Azure | Databricks

HomePage / Create Secret Scope

Create Secret Scope

[Cancel](#) [Create](#)

A store for secrets that is identified by a name and backed by a specific store type. [Learn more](#)

Scope Name ⓘ

Manage Principal ⓘ

All Users

Azure Key Vault ⓘ

DNS Name

Resource ID

The secret scope named formula1-scope has been added.

Manage secrets in this scope in Azure KeyVault with [manage principal = users](#)

OK

Cmd 1

```
1 storage_account_name = "formuladl"
2 client_id             = dbutils.secrets.get(scope="formuladl-scope", key="databricks-app-client-id")
3 tenant_id             = dbutils.secrets.get(scope="formuladl-scope", key="databricks-app-tenant-id")
4 client_secret         = dbutils.secrets.get(scope="formuladl-scope", key="databricks-app-client-secret")
```

Cmd 2

```
1 configs = {"fs.azure.account.auth.type": "OAuth",
2           "fs.azure.account.oauth.provider.type": "org.apache.hadoop.fs.azurebfs.oauth2.ClientCredsTokenProvider",
3           "fs.azure.account.oauth2.client.id": f"{client_id}",
4           "fs.azure.account.oauth2.client.secret": f"{client_secret}",
5           "fs.azure.account.oauth2.client.endpoint": f"https://login.microsoftonline.com/{tenant_id}/oauth2/token"}
```

Cmd 3

```
1 def mount_adls(container_name):
2     dbutils.fs.mount(
3         source = f"abfss://{container_name}@{storage_account_name}.dfs.core.windows.net/",
4         mount_point = f"/mnt/{storage_account_name}/{container_name}",
5         extra_configs = configs)
```

Cmd 4

```
1 mount_adls("raw")
```

Cmd 5

```
1 mount_adls("processed")
```

Cmd 6

```
1 dbutils.fs.ls("/mnt/formuladl/raw")
```

Cmd 7

```
1 dbutils.fs.ls("/mnt/formuladl/processed")
```