Azure Databricks Architecture and Security

databricks

Quick Agenda

- Azure Databricks Platform Architecture
- Azure Databricks Security
    - Data Protection
    - IAM/Auth
    - Network Security
    - Compliance

Azure Databricks Platform Architecture

Azure Databricks

AZURE DATA SOURCES

Blob Storage

Data Lake Store

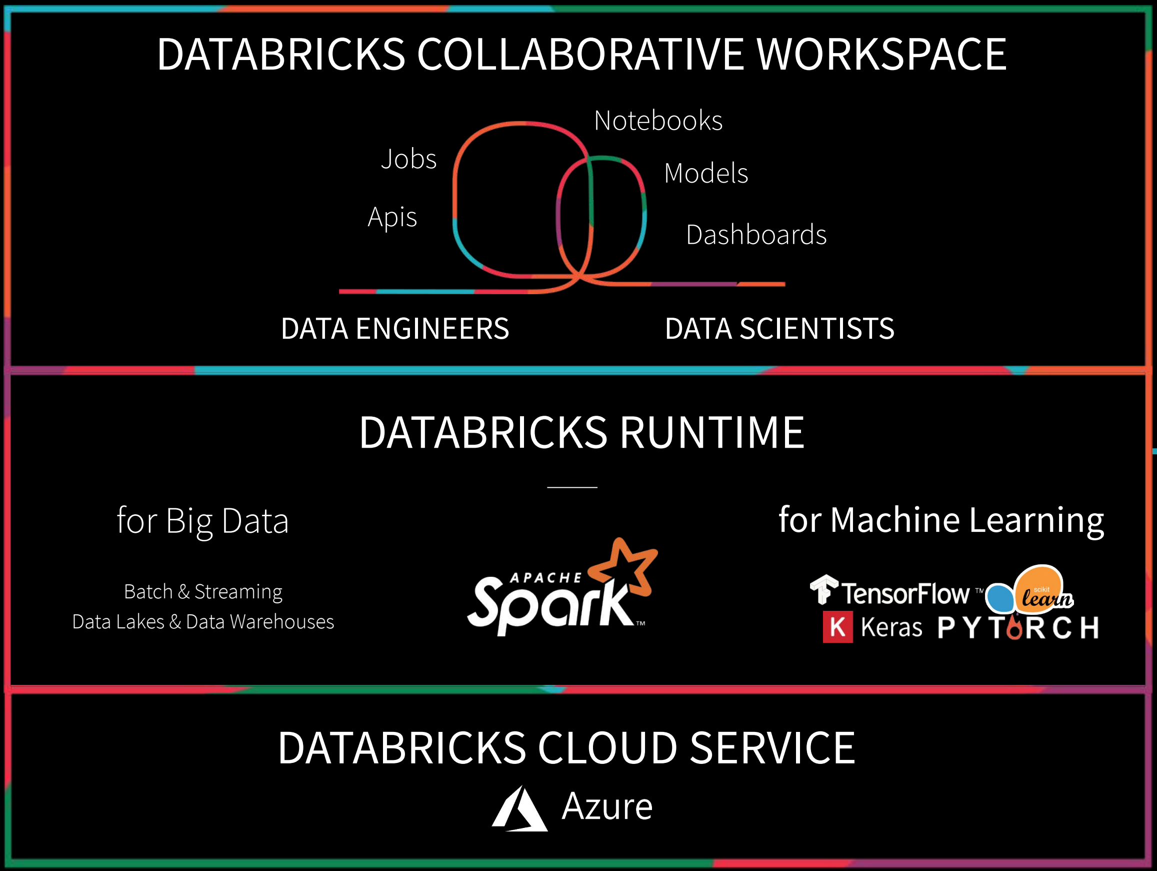
SQL Data Warehouse

Cosmos DB

Event Hub

IoT Hub

Azure Data Factory



DATABRICKS COLLABORATIVE WORKSPACE

DATA ENGINEERS

DATA SCIENTISTS

DATABRICKS RUNTIME

for Big Data

Batch & Streaming
Data Lakes & Data Warehouses

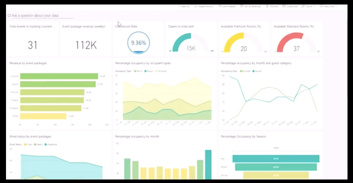
APACHE Spark™

for Machine Learning

TensorFlow™ scikit learn
Keras PYTORCH

DATABRICKS CLOUD SERVICE

Azure



Power BI

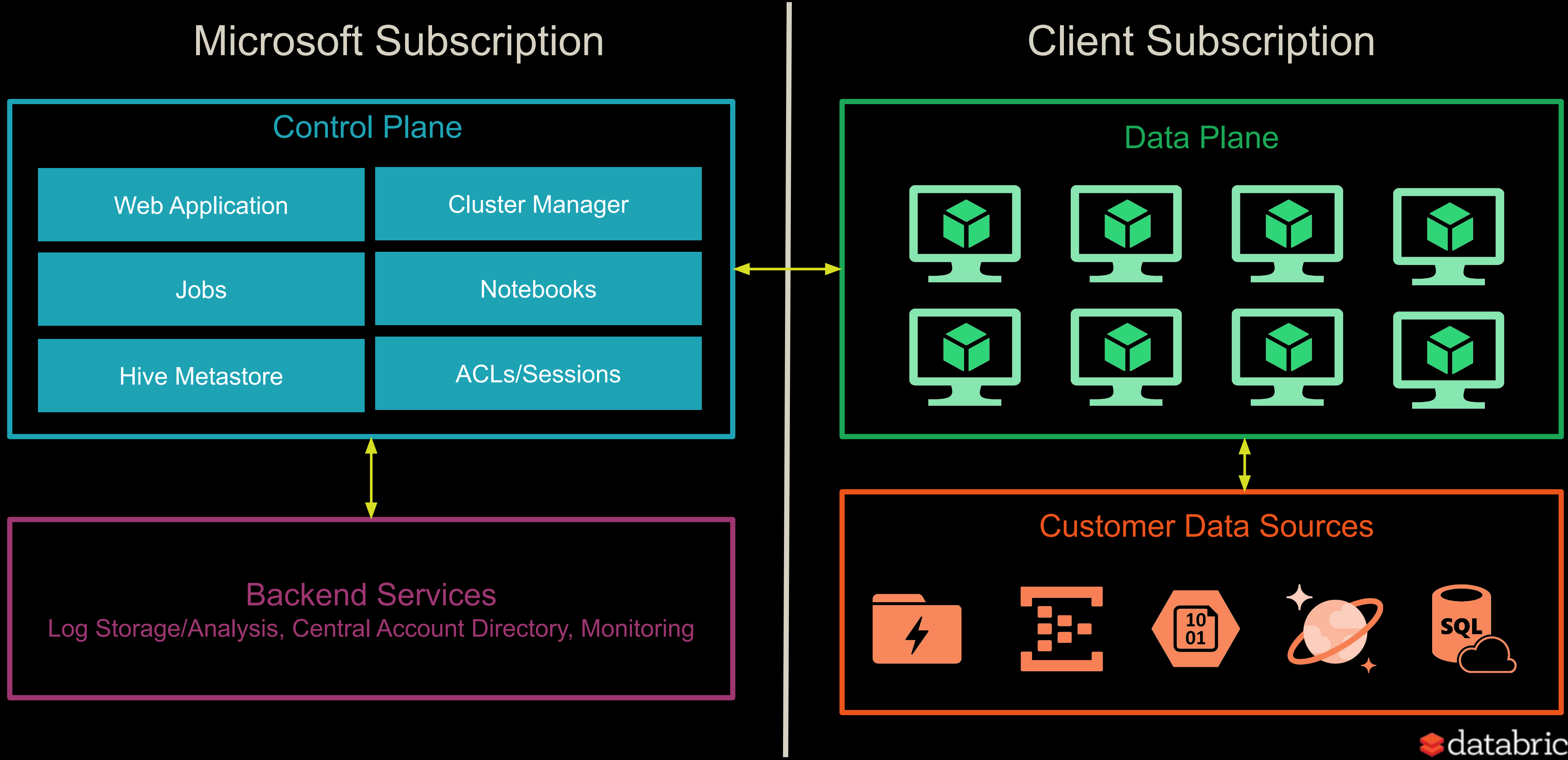
BI Reporting
Dashboards

Microsoft Active Directory

Security Integration

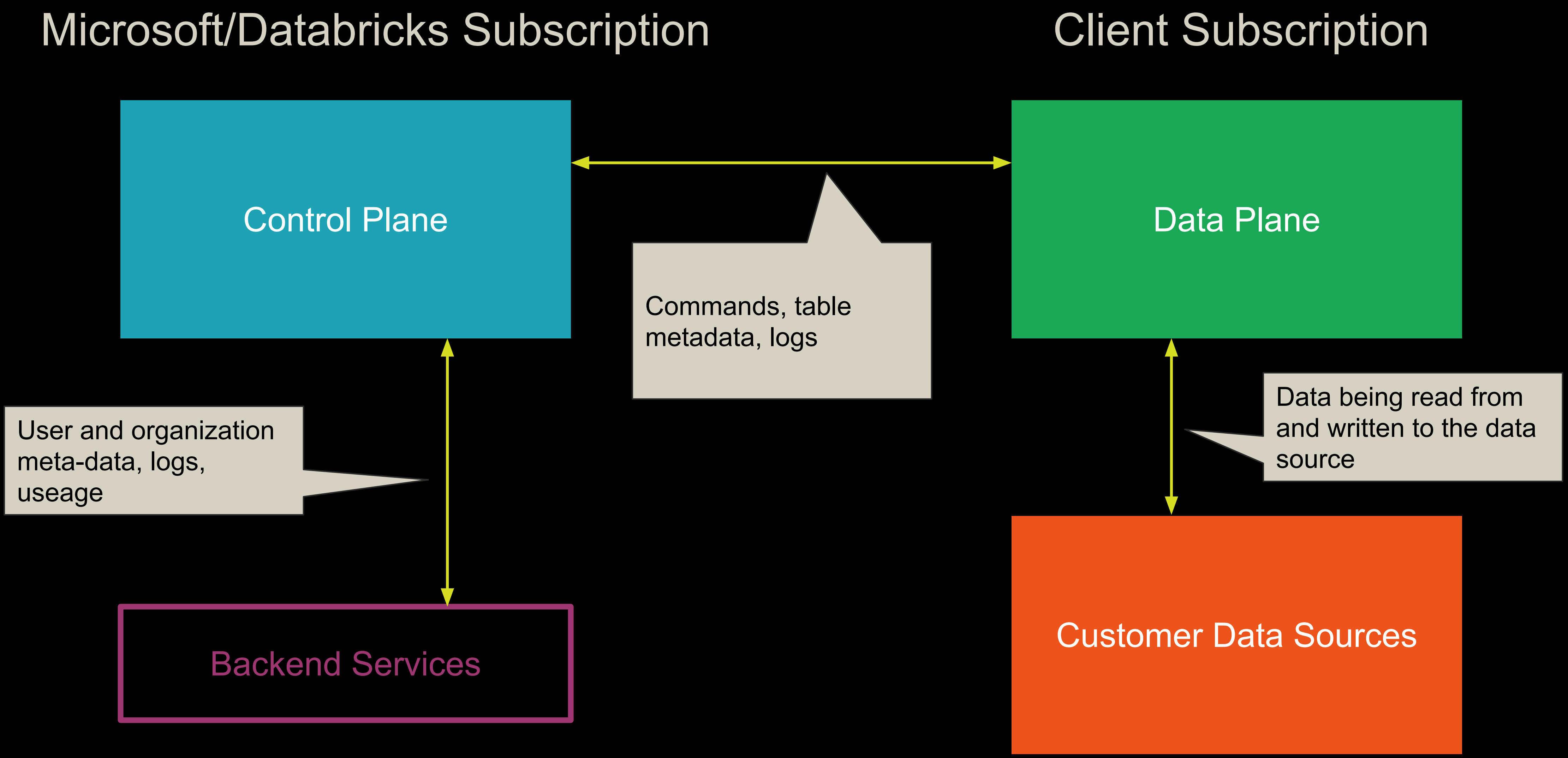
[Azure Portal]
One-Click setup
Unified Billing

Azure Databricks Platform Architecture



databricks

Azure Databricks Platform Architecture Cont’d



Microsoft/Databricks Subscription

Client Subscription

Control Plane

Data Plane

Commands, table metadata, logs

User and organization meta-data, logs, useage

Data being read from and written to the data source

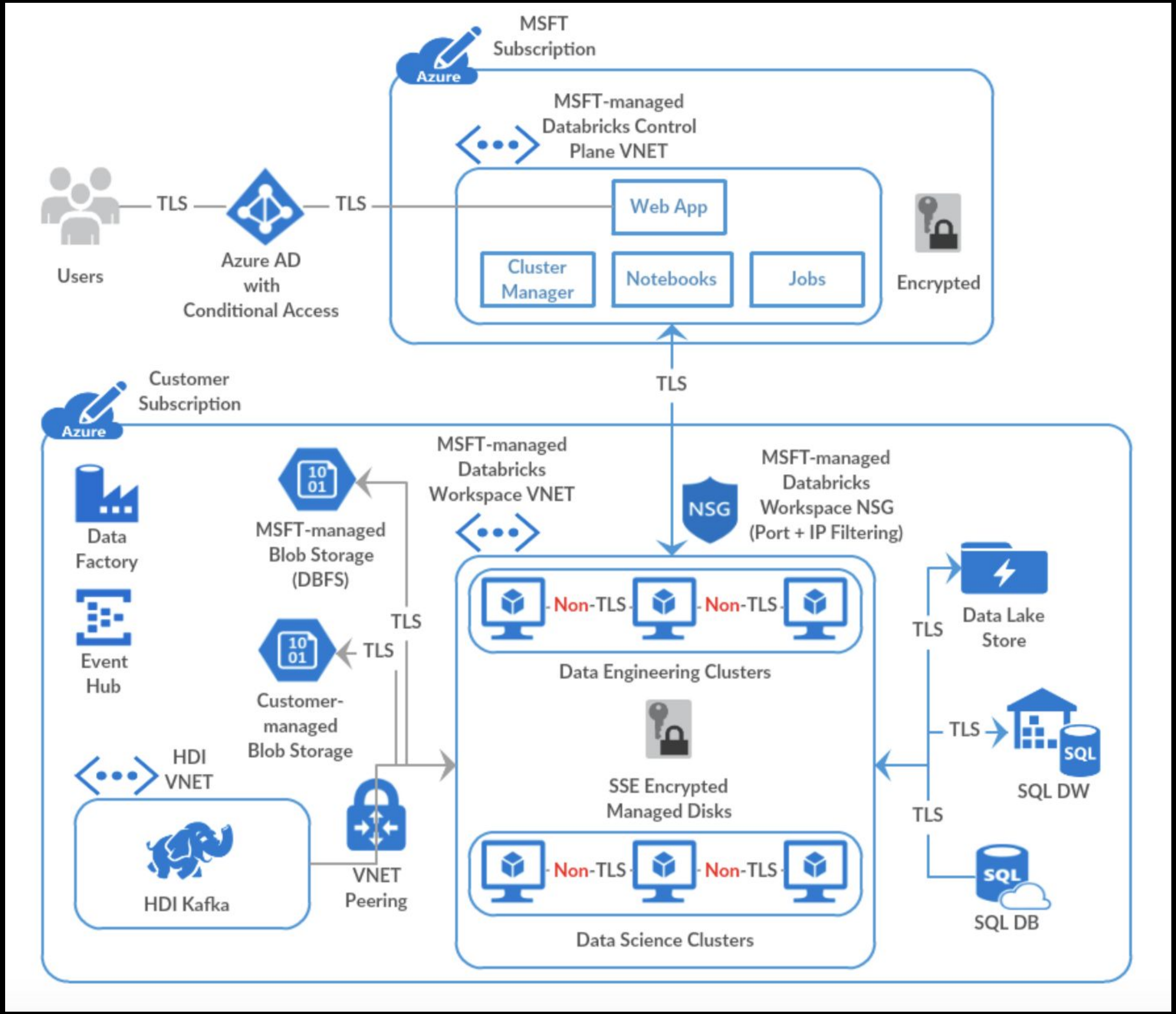
Backend Services

Customer Data Sources

databricks

Azure Databricks Platform Architecture

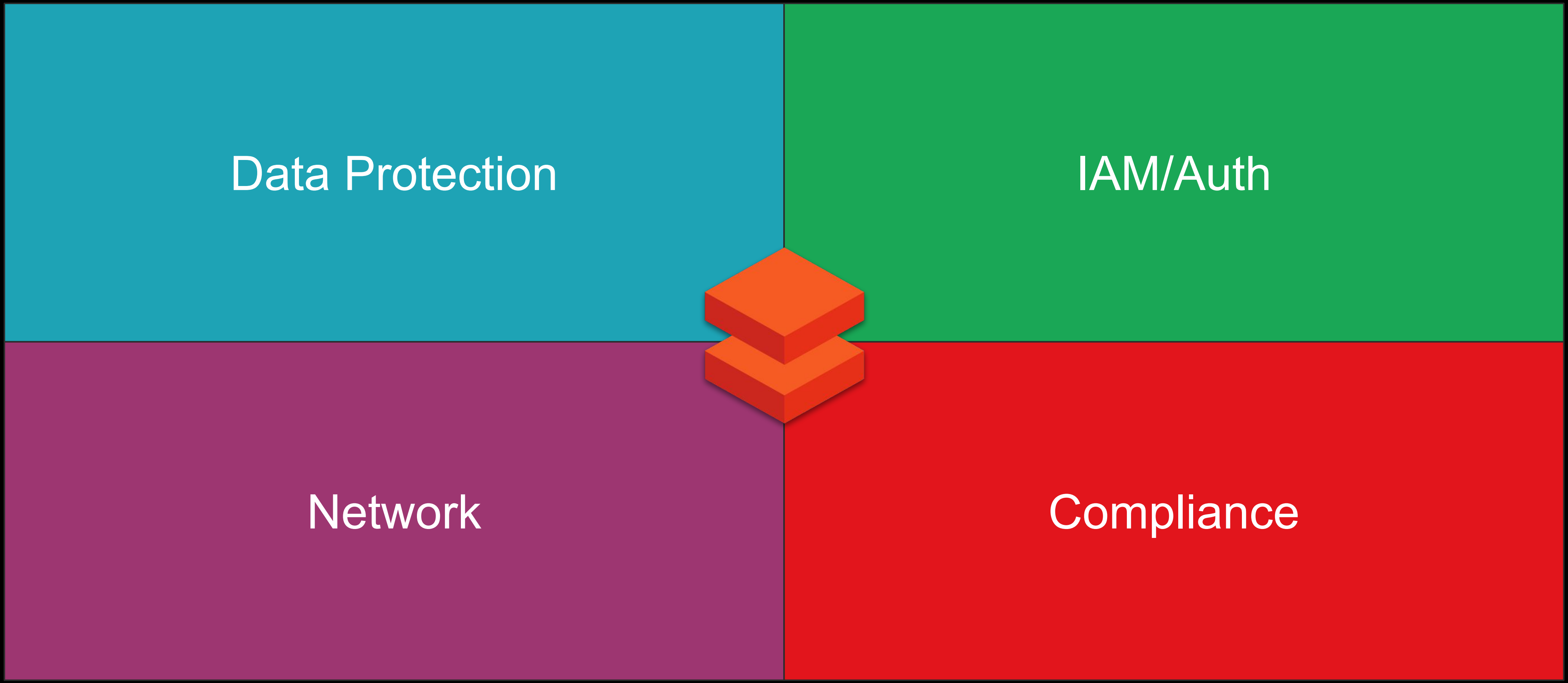
Standard Deployment View with no inter-node TLS



MSFT Subscription
Azure
MSFT-managed Databricks Control Plane VNET
Users
TLS
Azure AD with Conditional Access
TLS
Web App
Cluster Manager
Notebooks
Jobs
Encrypted
TLS
Customer Subscription
Azure
Data Factory
Event Hub
MSFT-managed Blob Storage (DBFS)
Customer-managed Blob Storage
TLS
TLS
MSFT-managed Databricks Workspace VNET
NSG
MSFT-managed Databricks Workspace NSG (Port + IP Filtering)
Non-TLS
Non-TLS
Data Engineering Clusters
SSE Encrypted Managed Disks
Non-TLS
Non-TLS
Data Science Clusters
HDI VNET
HDI Kafka
VNET Peering
TLS
Data Lake Store
TLS
SQL
SQL DW
TLS
SQL
SQL DB

Azure Databricks Security

Azure Databricks Security



Data Protection

IAM/Auth

Network

Compliance

Azure Databricks Security | Data Protection

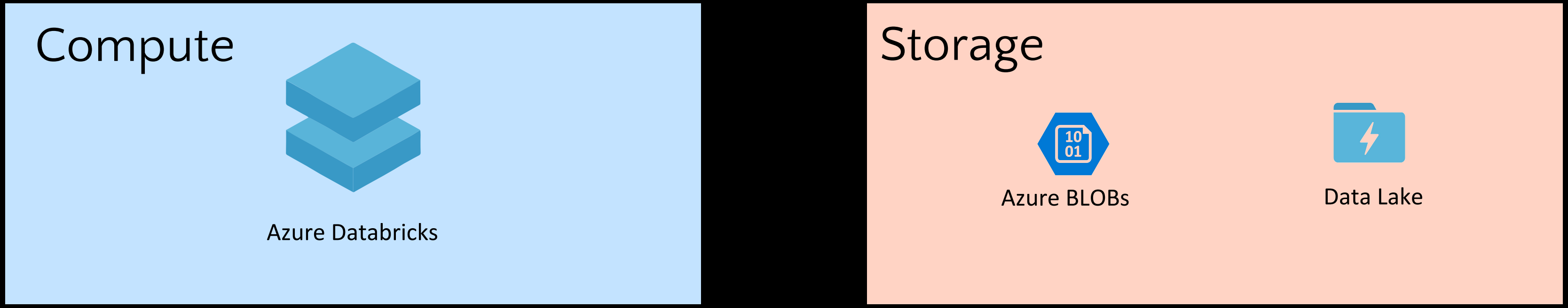
Data Protection

- Encryption-At-Rest – Service Managed Keys, User Managed Keys
- Encryption-in-flight (Transport Layer Security TLS)
- File/Folder Level ACLs for AAD Users, Groups, Service Principals
- ACLs for Clusters, Folders, Notebooks, Tables, Jobs
- Secrets with Azure Key Vault

* Preview feature

Data Protection | Encryption | At-Rest

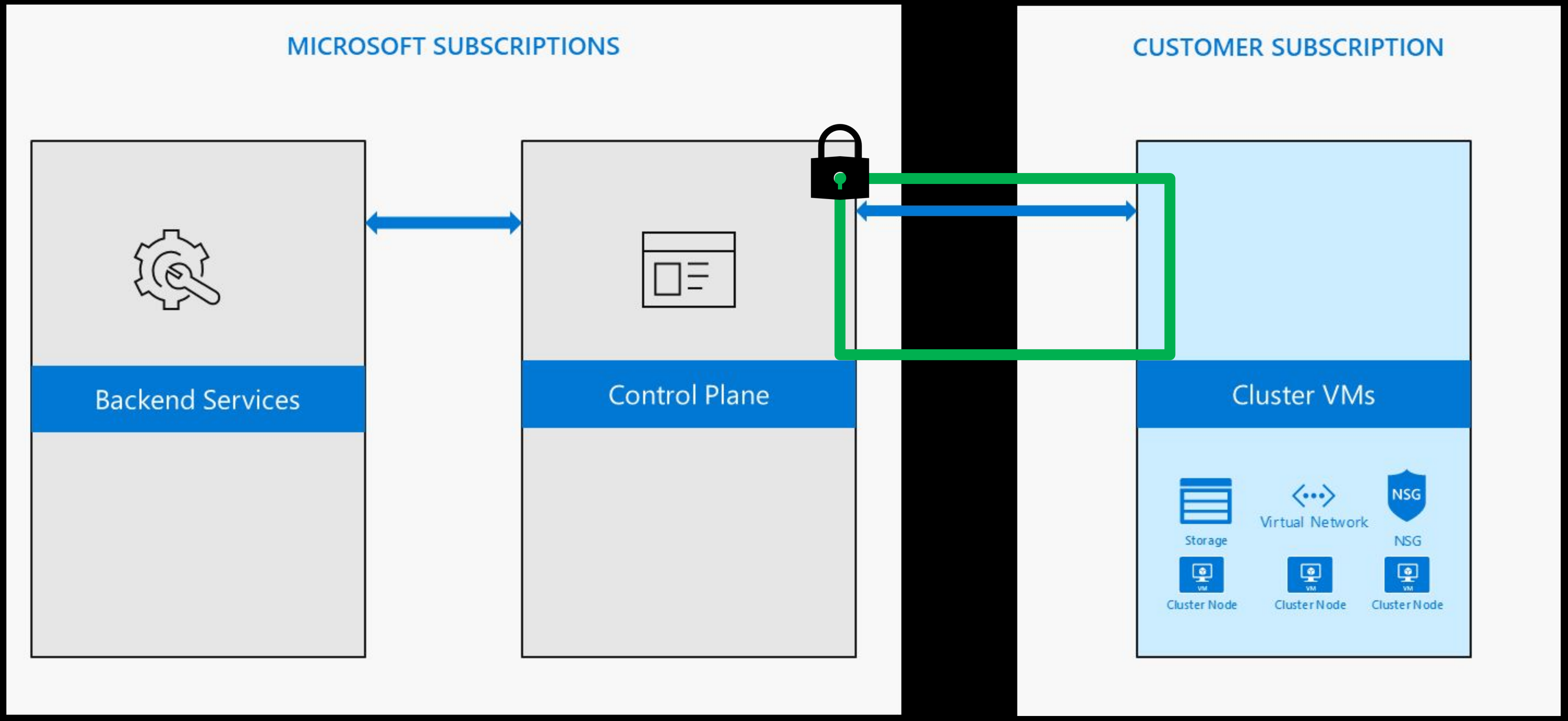
- Azure Databricks has separation of compute and storage



- Storage Services such as Azure Blob Store, Azure Data Lake Storage Provide
  - Encryption of Data
  - Customer Managed Keys
  - File/Folder Level ACLs (Azure Data Lake Storage)

Data Protection | Encryption | In-Transit

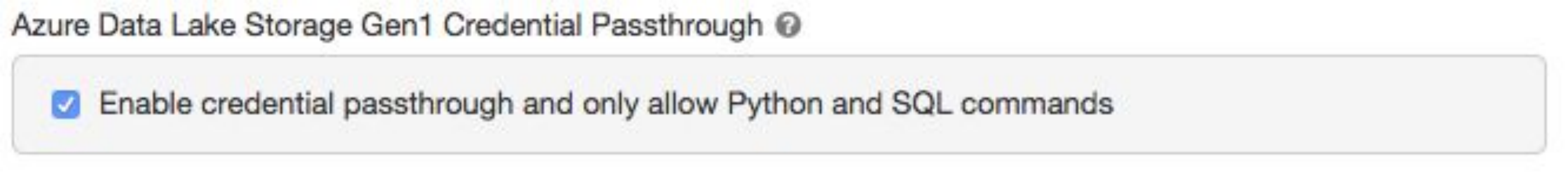
All the traffic from the Control Plane to the Clusters in the customer subscription is always encrypted with TLS.



databricks

Data Protection | Access Control | ADLS Passthru

- Authenticate automatically to Azure Data Lake Storage (ADLS) from Azure Databricks clusters using the same Azure Active Directory (Azure AD) identity that one uses to log into Azure Databricks.
- Commands running on a configured cluster will be able to read and write data in Azure Data Lake Storage without requiring one to configure service principal credentials.



Azure Data Lake Storage Gen1 Credential Passthrough

☑ Enable credential passthrough and only allow Python and SQL commands

Data Protection | Access Control | Folders

Ability	No Permissions	Read	Run	Edit	Manage
View items		x	x	x	x
Create, clone, import, export items		x	x	x	x
Run commands on notebooks			x	x	x
Attach/detach notebooks			x	x	x
Delete items				x	x
Move/rename items				x	x
Change permissions					x

Data Protection | Access Control | Notebooks

Ability	No Permissions	Read	Run	Edit	Manage
View cells		x	x	x	x
Comment		x	x	x	x
Run commands			x	x	x
Attach/detach notebooks			x	x	x
Edit cells				x	x
Change permissions					x

Data Protection | Access Control | Clusters

Ability	No Permissions	Can Attach To	Can Restart	Can Manage
Attach notebook to cluster		x	x	x
View Spark UI		x	x	x
View cluster metrics		x	x	x
Terminate cluster			x	x
Start cluster			x	x
Restart cluster			x	x
Edit cluster				x
Attach library to cluster				x
Resize cluster				x
Modify permissions				x

Data Protection | Access Control | Jobs

Ability	No Permissions	Can View	Can Manage Run	Is Owner	Can Manage (admin)
View job details and settings	x	x	x	x	x
View results, Spark UI, logs of a job run		x	x	x	x
Run now			x	x	x
Cancel run			x	x	x
Edit job settings				x	x
Modify permissions				x	x

Data Protection | Access Control | Tables

Objects

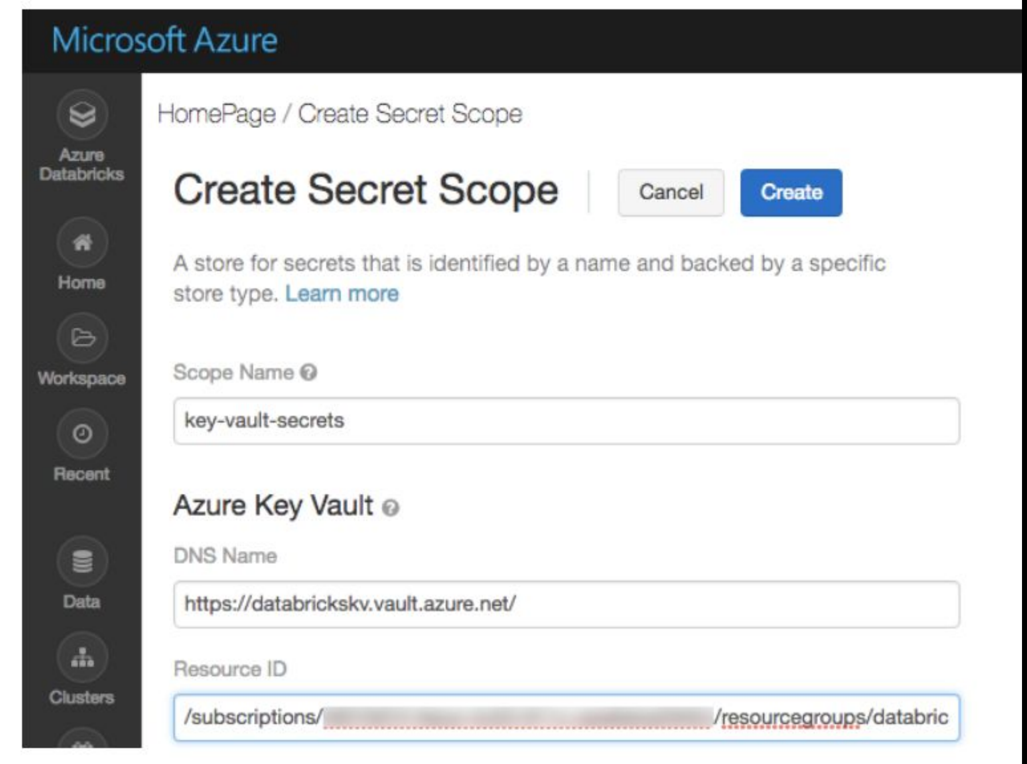
CATALOG | DATABASE | TABLE | VIEW | FUNCTION | ANONYMOUS FUNCTION | ANY FILE

Privileges

SELECT – read access to an object
CREATE – ability to create an object (eg. Table in a Database)
MODIFY – ability to add/delete/modify data in an Object
READ_METADATA – ability to read Metadata about an object
ALL_PRIVELEGES – all of the above

Data Protection | Secrets

- Using our Secrets APIs, Secrets can be securely stored including in a Azure Key Vault or Databricks backend
- Authorized users can consume the secrets to access services



HomePage / Create Secret Scope

Create Secret Scope

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

Scope Name: key-vault-secrets

Azure Key Vault

DNS Name: https://databrickskv.vault.azure.net/

Resource ID: /subscriptions/[redacted]/resourcegroups/databric

databricks

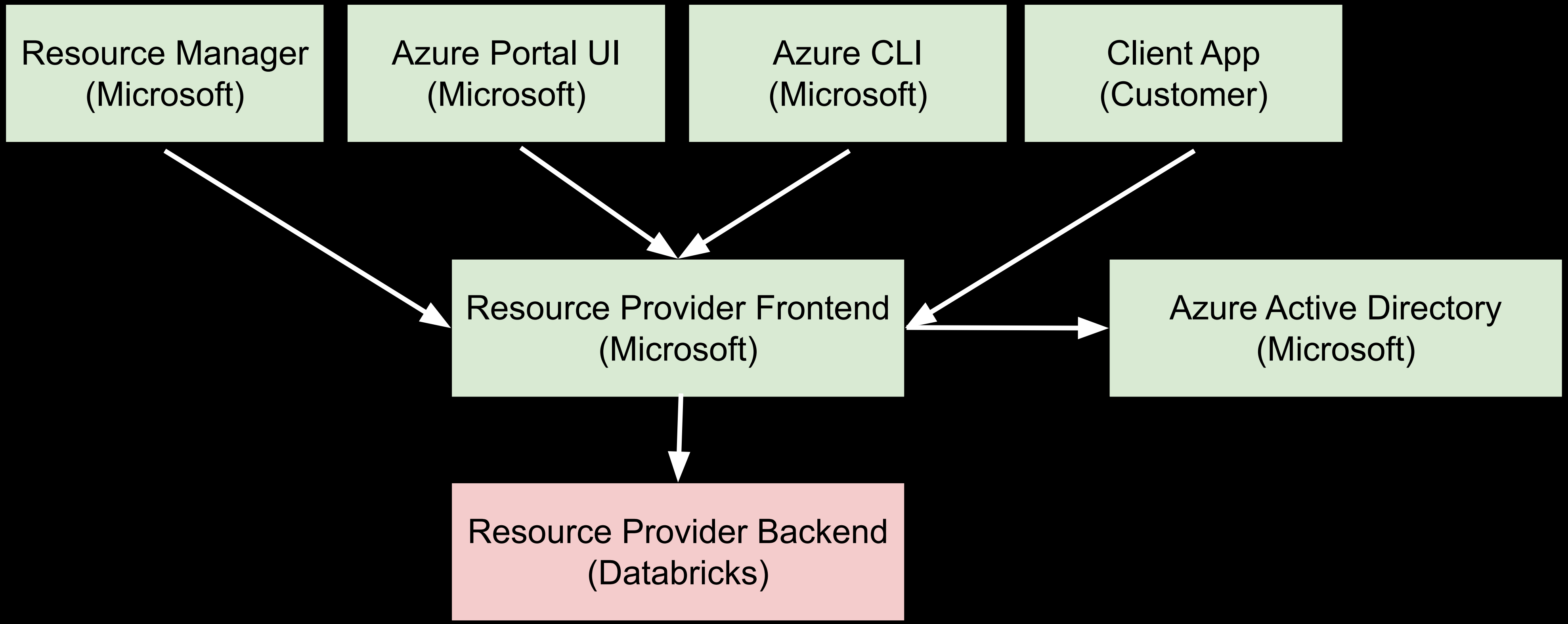
Azure Databricks Security | IAM/Auth

IAM/Auth

- Azure Active Directory (AAD) Authentication (w/ MFA)
- AAD Groups (using SCIM)
- AAD Conditional Access
- AAD Access Tokens

* Preview feature

IAM/Auth | First-party AAD Integration



Resource Manager (Microsoft)

Azure Portal UI (Microsoft)

Azure CLI (Microsoft)

Client App (Customer)

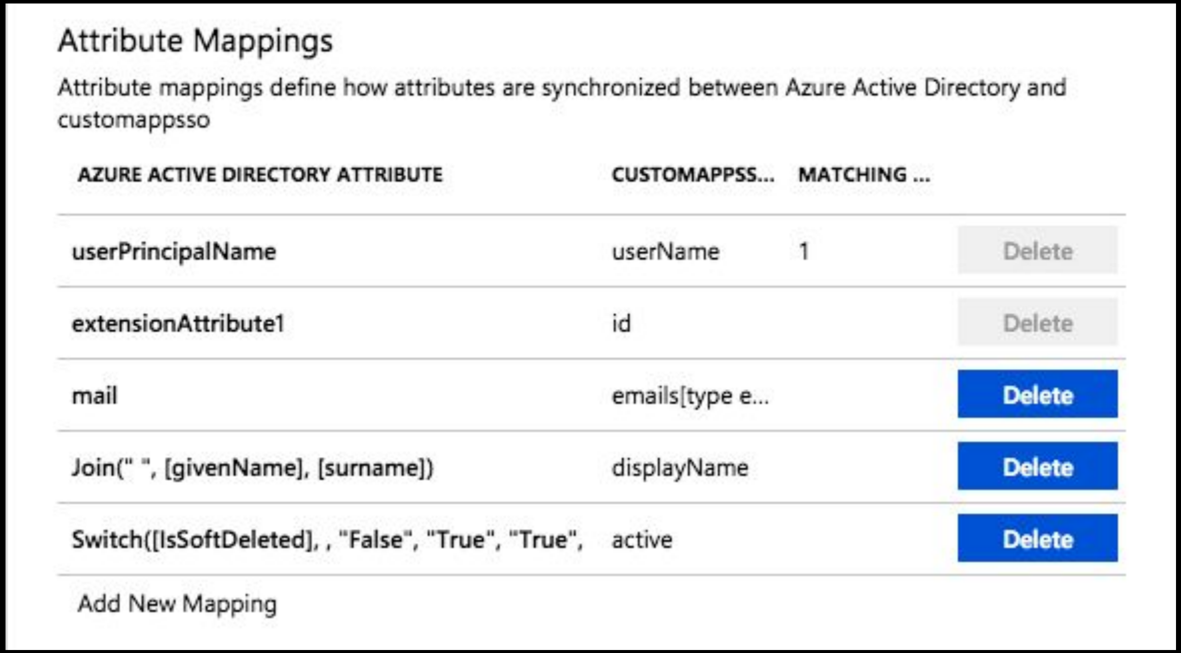
Resource Provider Frontend (Microsoft)

Azure Active Directory (Microsoft)

Resource Provider Backend (Databricks)

IAM/Auth | SCIM Integration

Azure Databricks supports SCIM, or System for Cross-domain Identity Management, an open standard that allows you to automate user provisioning. SCIM lets you use Azure Active Directory to create users in Azure Databricks and give them the proper level of access, as well as remove access for users (deprovision them) when they leave the organization or no longer need access to Azure Databricks.

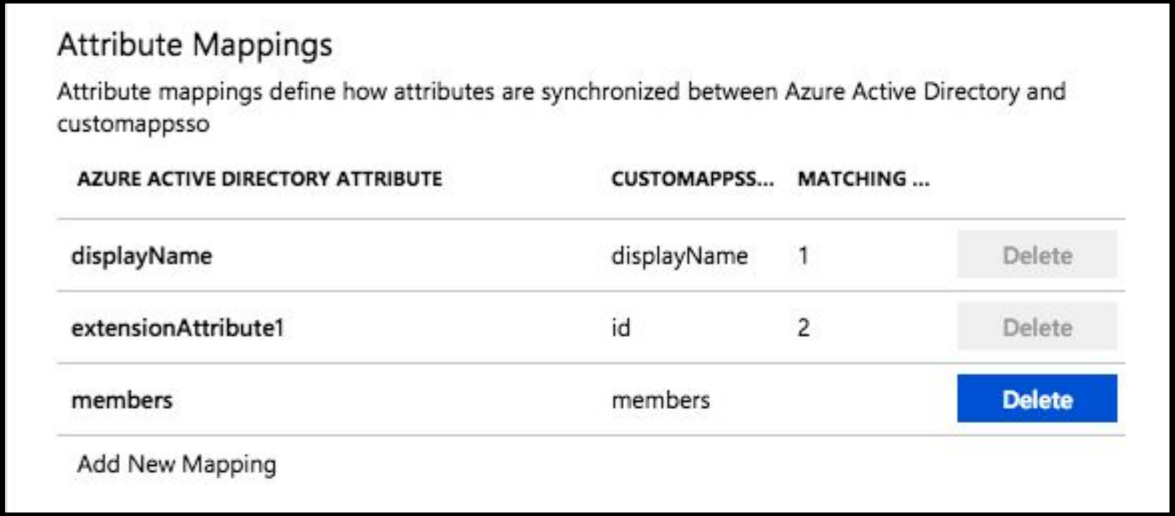


Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

AZURE ACTIVE DIRECTORY ATTRIBUTE	CUSTOMAPPSS...	MATCHING ...	
userPrincipalName	userName	1	Delete
extensionAttribute1	id		Delete
mail	emails[type e...		Delete
Join(" ", [givenName], [surname])	displayName		Delete
Switch([IsSoftDeleted], , "False", "True", "True",	active		Delete

Add New Mapping



Attribute Mappings

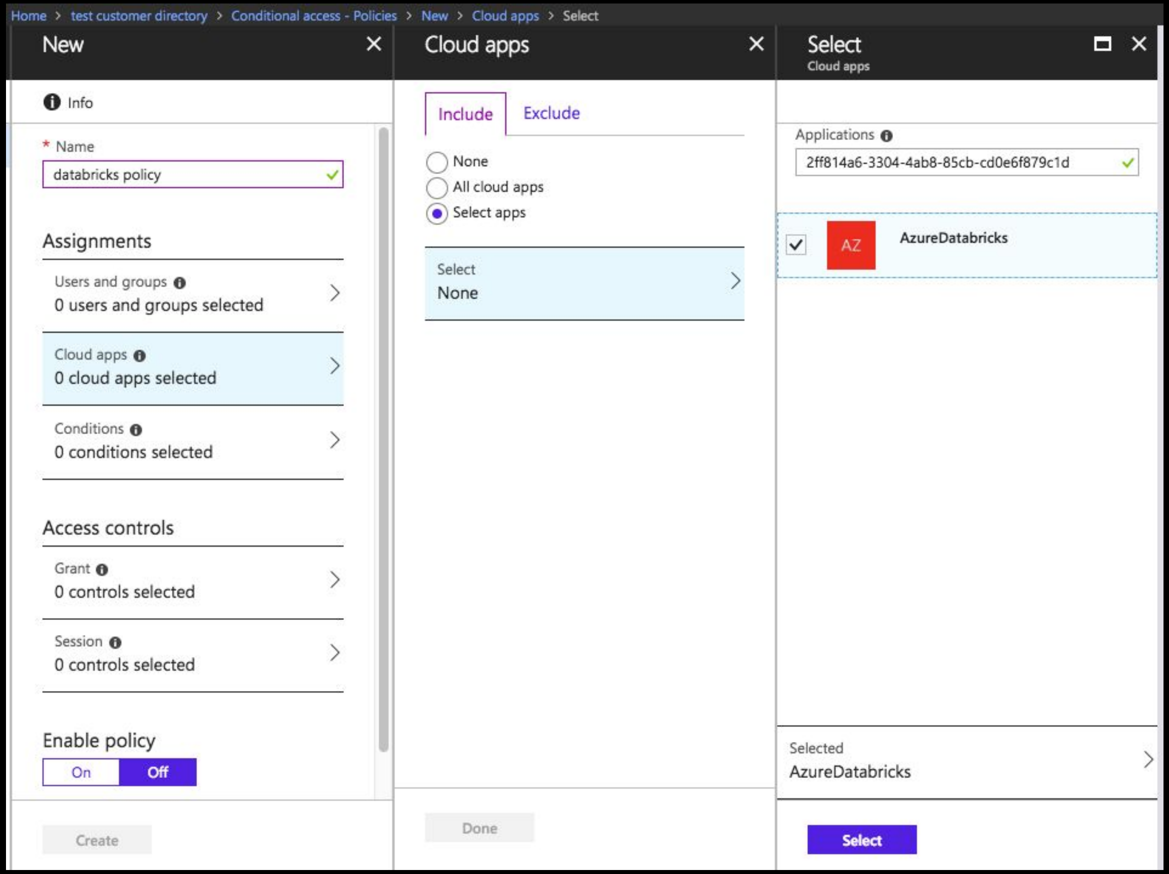
Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

AZURE ACTIVE DIRECTORY ATTRIBUTE	CUSTOMAPPSS...	MATCHING ...	
displayName	displayName	1	Delete
extensionAttribute1	id	2	Delete
members	members		Delete

Add New Mapping

IAM/Auth | Conditional Access

Azure Databricks supports Azure Active Directory conditional access, which allows administrators to control where and when users are permitted to sign in to Azure Databricks. For example, conditional access policies can restrict sign-in to your corporate network or can require multi-factor authentication.



Home > test customer directory > Conditional access - Policies > New > Cloud apps > Select

New

Info

* Name: databricks policy ✓

Assignments

- Users and groups: 0 users and groups selected
- Cloud apps: 0 cloud apps selected
- Conditions: 0 conditions selected

Access controls

- Grant: 0 controls selected
- Session: 0 controls selected

Enable policy: On [✓ Off]

Create

Cloud apps

Include | Exclude

○ None
○ All cloud apps
● Select apps

Select: None

Done

Select
Cloud apps

Applications: 2ff814a6-3304-4ab8-85cb-cd0e6f879c1d ✓

☑ AZ AzureDatabricks

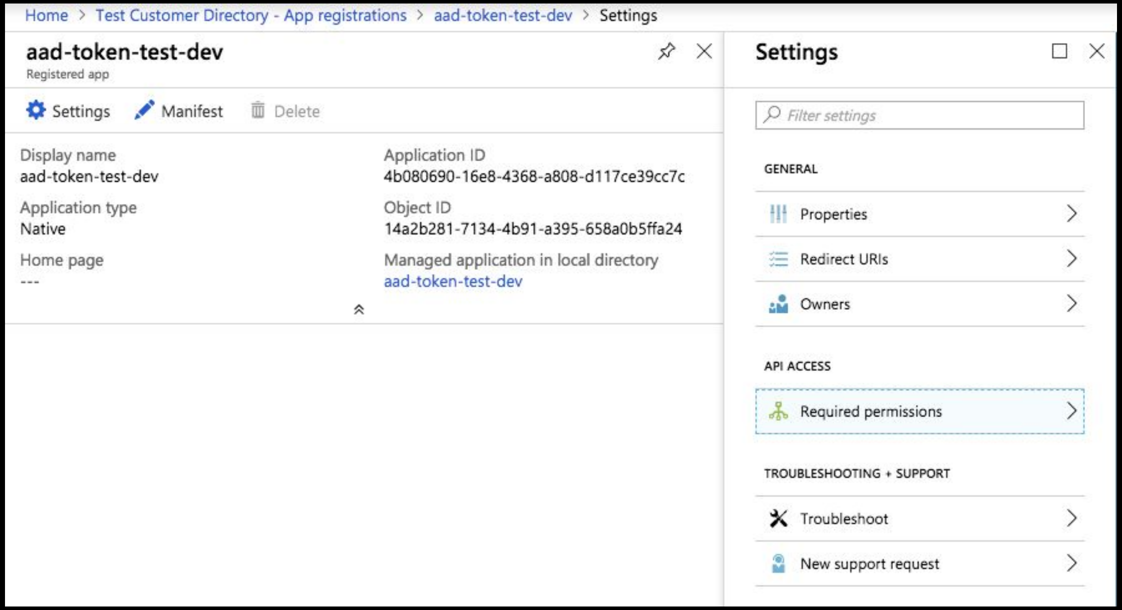
Selected: AzureDatabricks

Select

IAM/Auth | AAD Token Support

You could use AAD tokens to automate provisioning of Azure Databricks workspaces and access the Databricks REST API

****Private Preview Only****



Home > Test Customer Directory - App registrations > aad-token-test-dev > Settings

aad-token-test-dev
Registered app

Display name
aad-token-test-dev

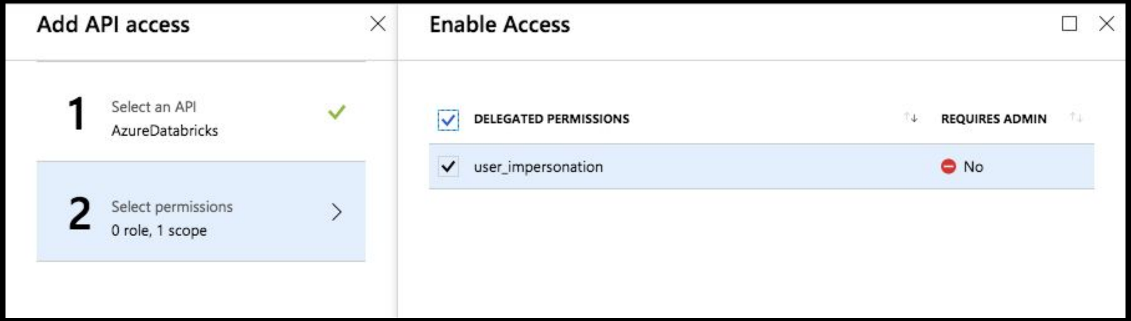
Application type
Native

Home page

Application ID
4b080690-16e8-4368-a808-d117ce39cc7c

Object ID
14a2b281-7134-4b91-a395-658a0b5ffa24

Managed application in local directory
aad-token-test-dev



Add API access

1 Select an API
AzureDatabricks ✓

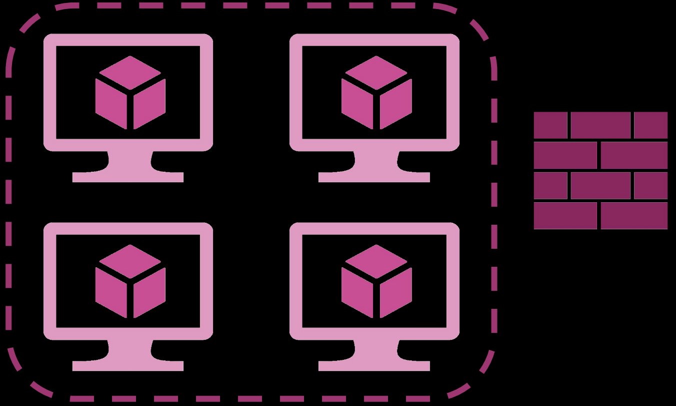
2 Select permissions
0 role, 1 scope

Enable Access

☑ DELEGATED PERMISSIONS	REQUIRES ADMIN
✓ user_impersonation	⛔ No

Azure Databricks Security | Network Security

Network Security



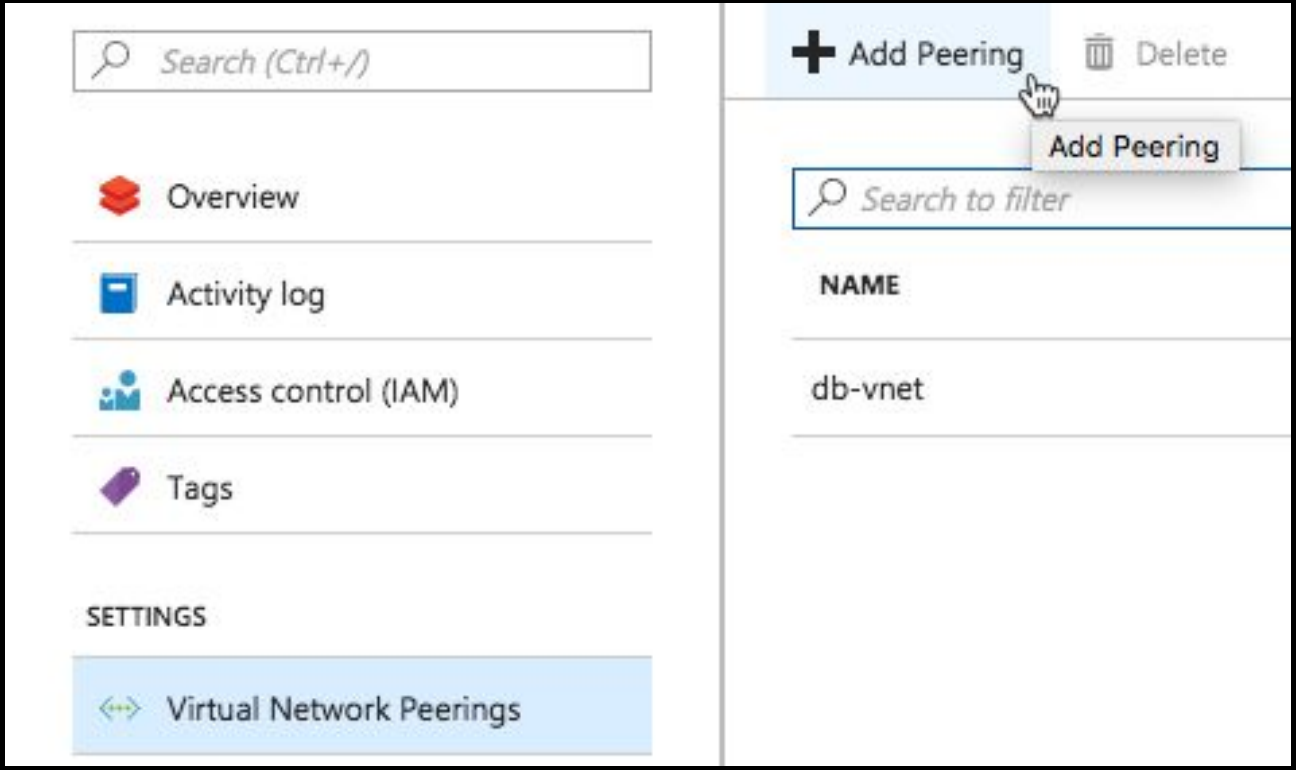
- Managed VNets
- VNet Peering
- VNET Injection/BYO VNET
  - On-Premises Data Access
  - Single-IP SNAT and Firewall-based filtering via custom routing
  - Service Endpoint

* Preview feature

databricks

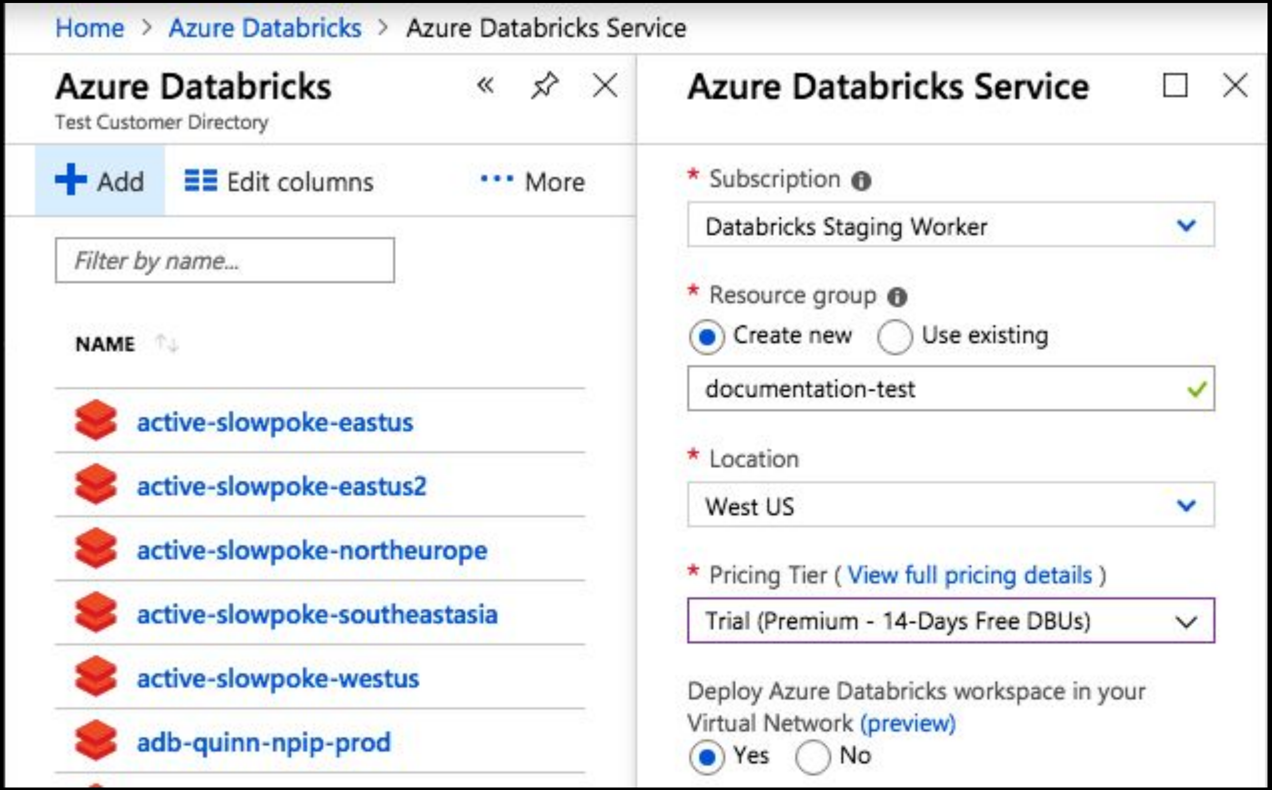
Network Security | VNET Peering

Virtual network (VNet) peering allows the virtual network in which your Azure Databricks resource is running to peer with another Azure virtual network. Traffic between virtual machines in the peered virtual networks is routed through the Microsoft backbone infrastructure, much like traffic is routed between virtual machines in the same virtual network, through private IP addresses only.



Network Security | VNET Injection / BYO VNET

If you’re looking to do specific network customizations, you could deploy Azure Databricks data plane resources in your own VNET



Azure Databricks
Test Customer Directory

NAME

- active-slowpoke-eastus
- active-slowpoke-eastus2
- active-slowpoke-northeurope
- active-slowpoke-southeastasia
- active-slowpoke-westus
- adb-quinn-npip-prod

Azure Databricks Service

* Subscription: Databricks Staging Worker

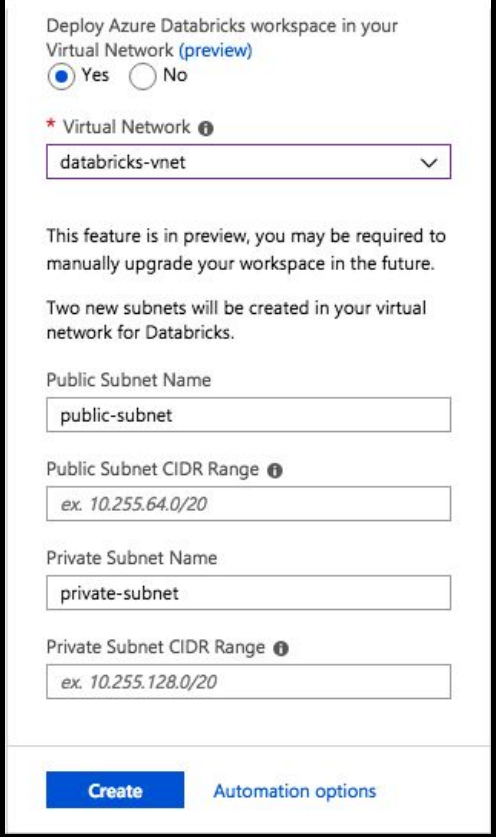
* Resource group: ● Create new ○ Use existing

documentation-test ✓

* Location: West US

* Pricing Tier (View full pricing details): Trial (Premium - 14-Days Free DBUs)

Deploy Azure Databricks workspace in your Virtual Network (preview)
● Yes ○ No



Deploy Azure Databricks workspace in your Virtual Network (preview)
● Yes ○ No

* Virtual Network: databricks-vnet

This feature is in preview, you may be required to manually upgrade your workspace in the future.

Two new subnets will be created in your virtual network for Databricks.

Public Subnet Name: public-subnet

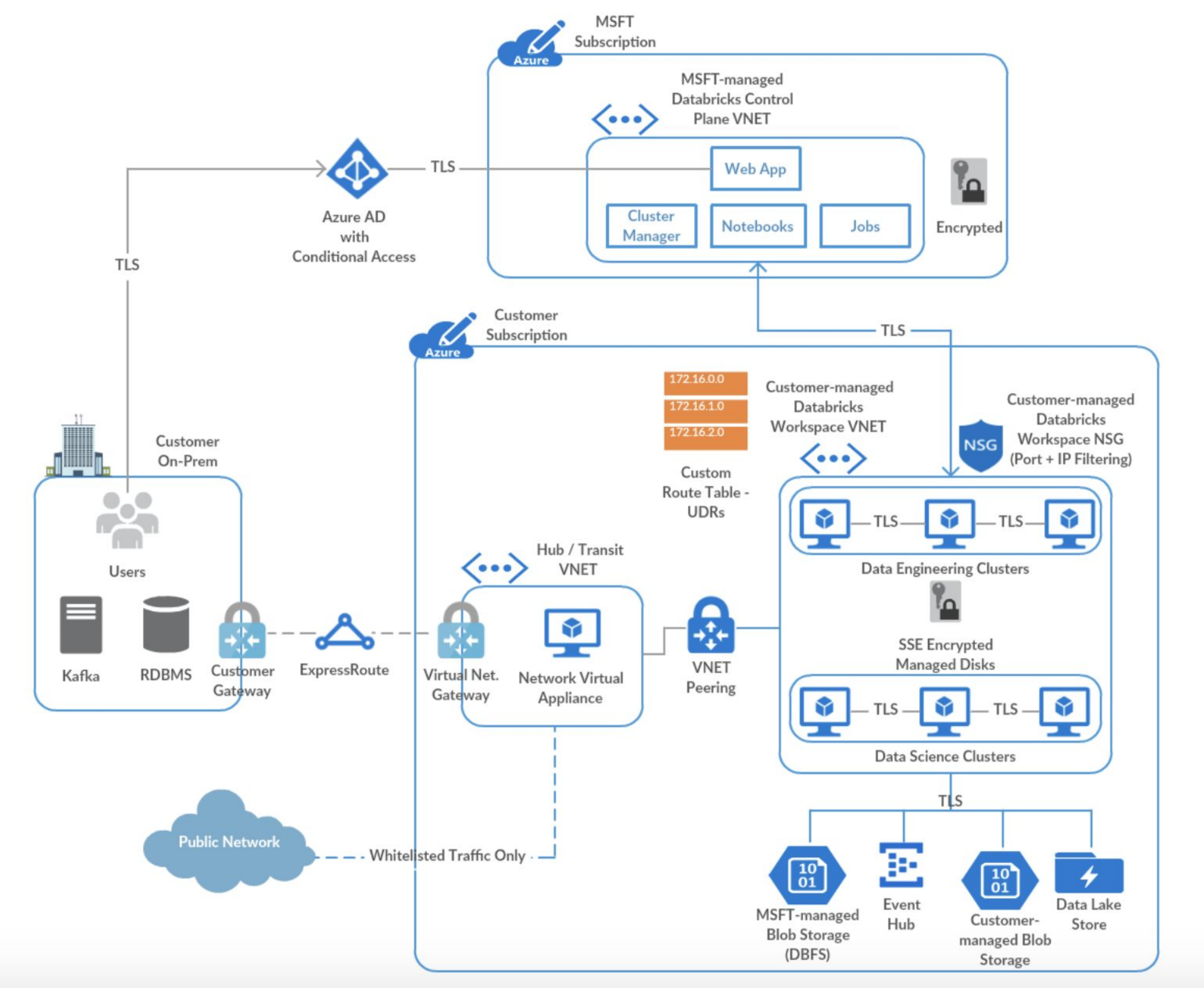
Public Subnet CIDR Range: ex. 10.255.64.0/20

Private Subnet Name: private-subnet

Private Subnet CIDR Range: ex. 10.255.128.0/20

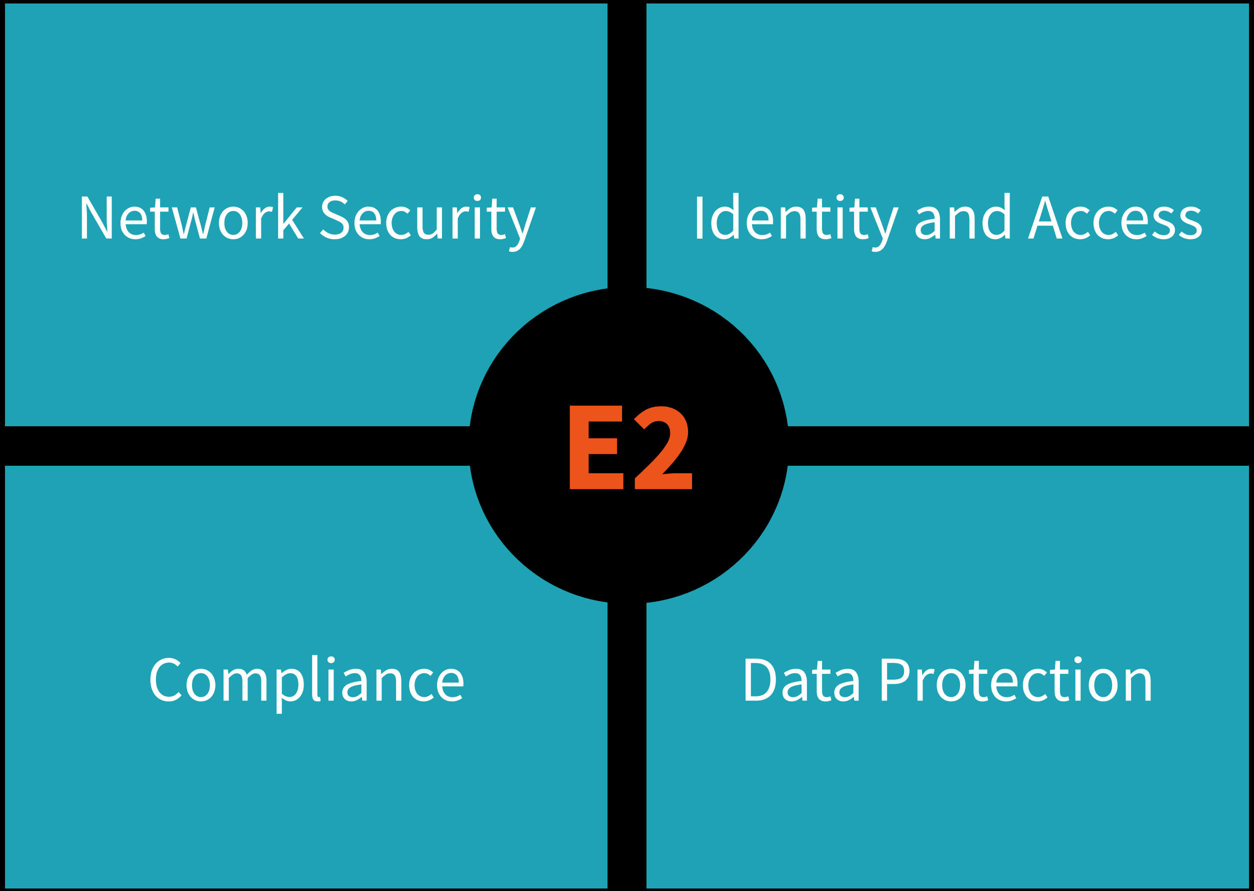
Azure Databricks Platform Architecture

Deployment with VNET Injection and inter-node TLS (one could be used without the other)


MSFT Subscription
Azure
MSFT-managed Databricks Control Plane VNET
Web App
Cluster Manager
Notebooks
Jobs
Encrypted
TLS
Azure AD with Conditional Access
TLS
Customer Subscription
Azure
TLS
172.16.0.0
172.16.1.0
172.16.2.0
Customer-managed Databricks Workspace VNET
Customer-managed Databricks Workspace NSG (Port + IP Filtering)
NSG
Custom Route Table - UDRs
Customer On-Prem
Users
Kafka
RDBMS
Customer Gateway
ExpressRoute
Hub / Transit VNET
Virtual Net. Gateway
Network Virtual Appliance
VNET Peering
TLS
TLS
Data Engineering Clusters
SSE Encrypted Managed Disks
TLS
TLS
Data Science Clusters
TLS
Public Network
Whitelisted Traffic Only
MSFT-managed Blob Storage (DBFS)
Event Hub
Customer-managed Blob Storage
Data Lake Store

Private, secure, encrypted with compute in your network

Plug into your identity system for seamless control



Network Security

Identity and Access

E2

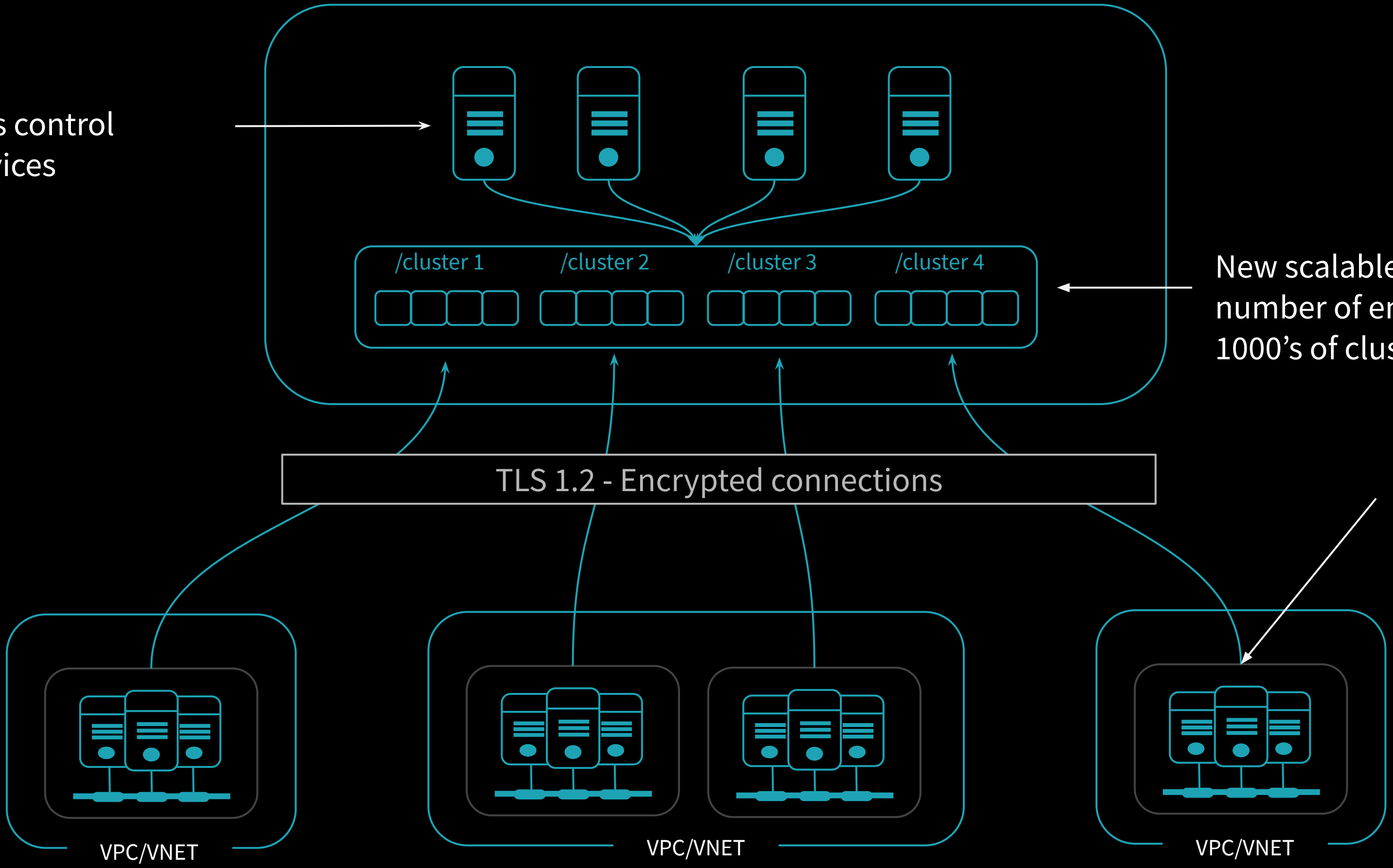
Compliance

Data Protection

Battle tested for compliance and other sensitive data policies

Extend identity all the way down to the data natively

Secure network connectivity



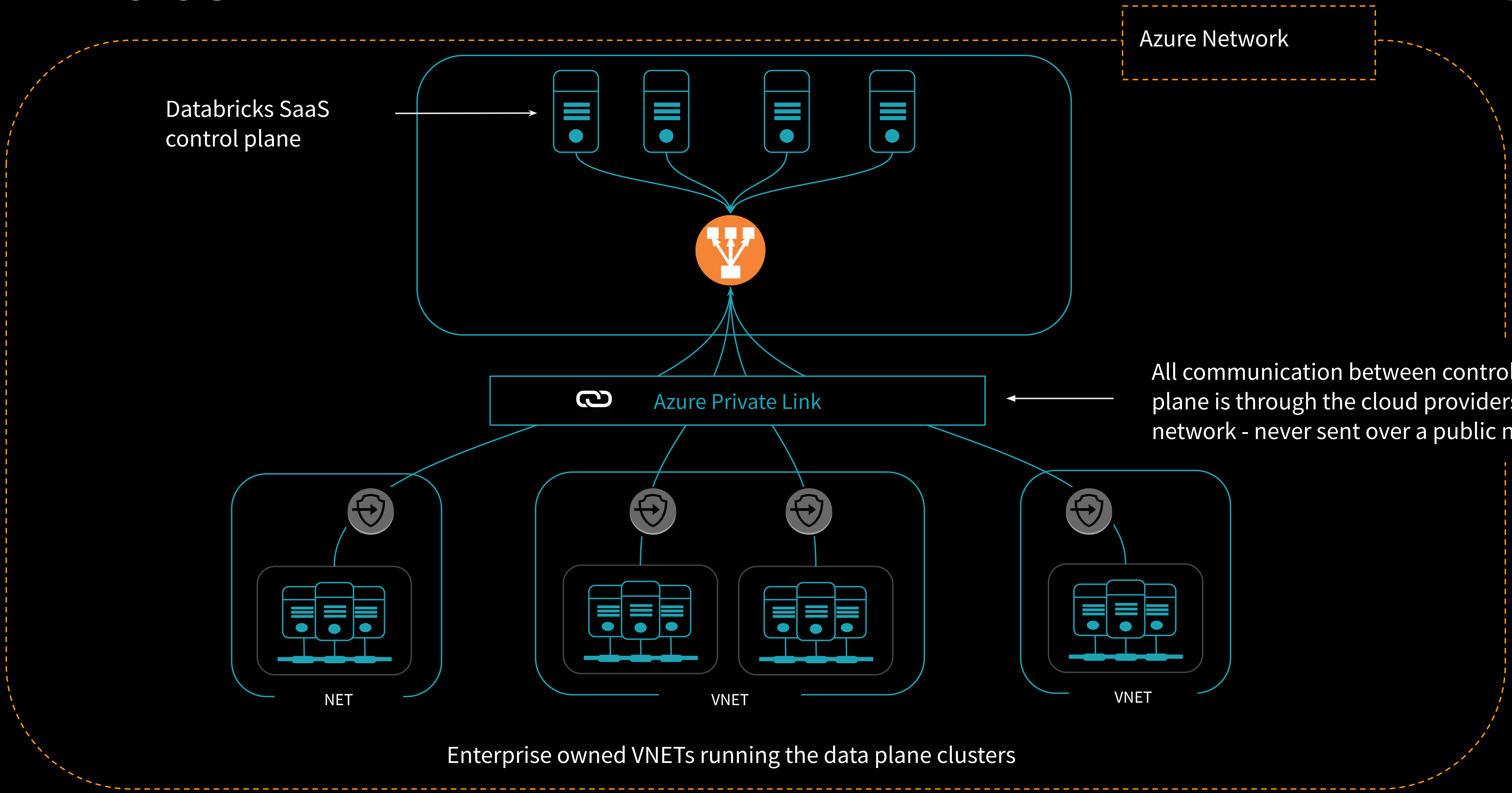
Databricks control plane services

New scalable relay enables large number of encrypted connections for 1000’s of clusters

Only outbound connections from enterprise environments.

Enterprise owned VPCs/VNETs

Private Link



Azure Network

Databricks SaaS control plane

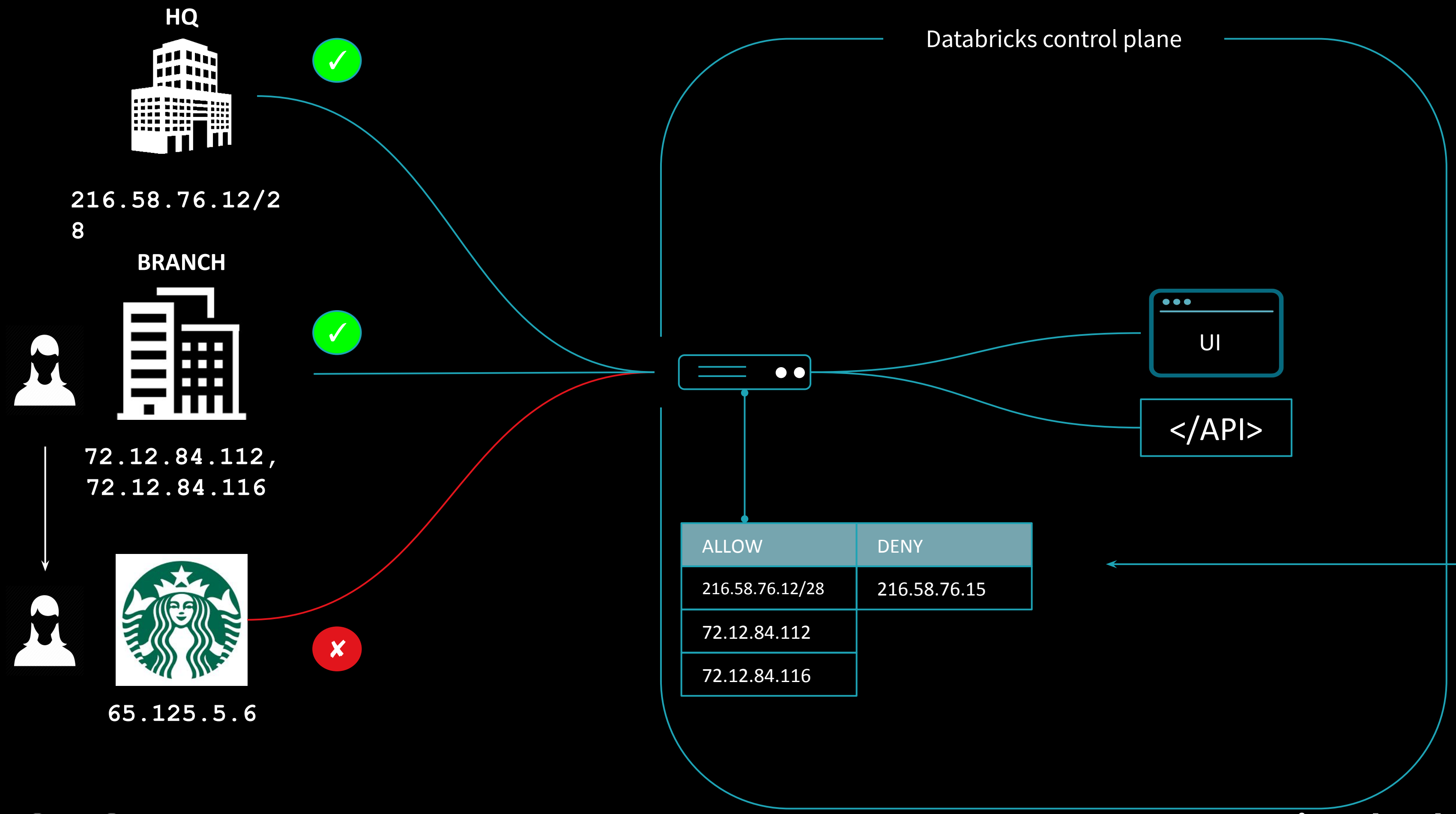
Azure Private Link

All communication between control and data plane is through the cloud providers private network - never sent over a public network

Enterprise owned VNETs running the data plane clusters

IP Access Lists

Control the networks that can access databricks



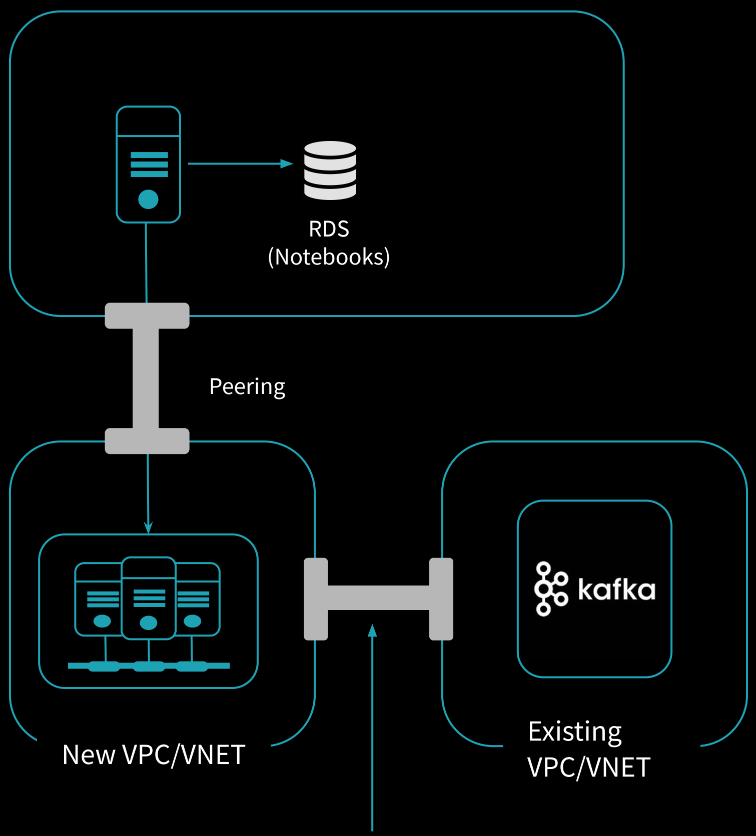
ALLOW	DENY
216.58.76.12/28	216.58.76.15
72.12.84.112	
72.12.84.116	

Dynamically update the list of networks

Deny IPs within a permitted subnet to shrink exposure

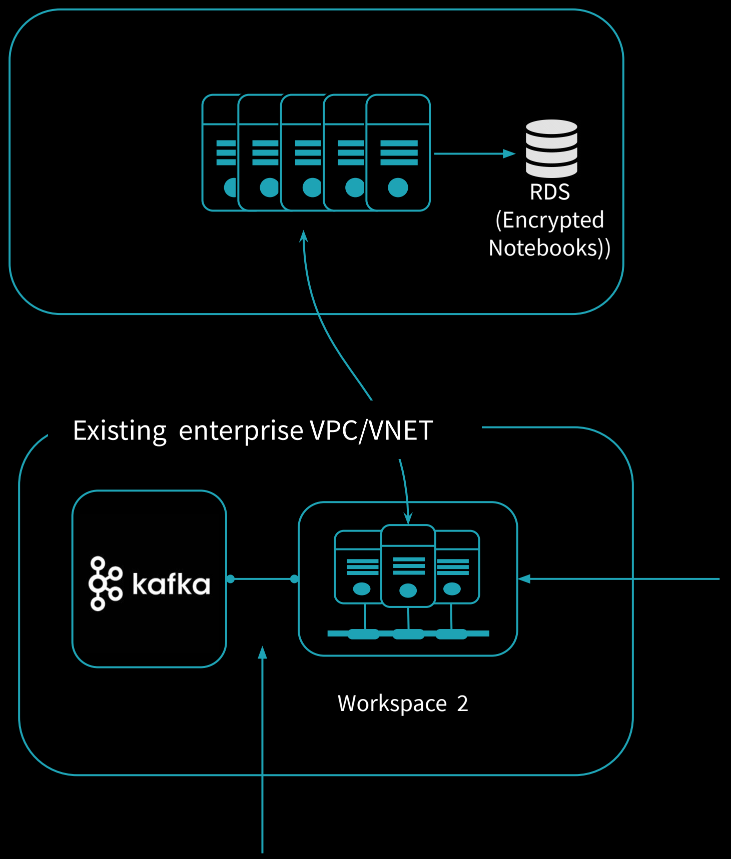
Bring your own VNET

Today



Connectivity to other applications through peering

Q4

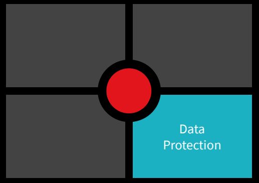


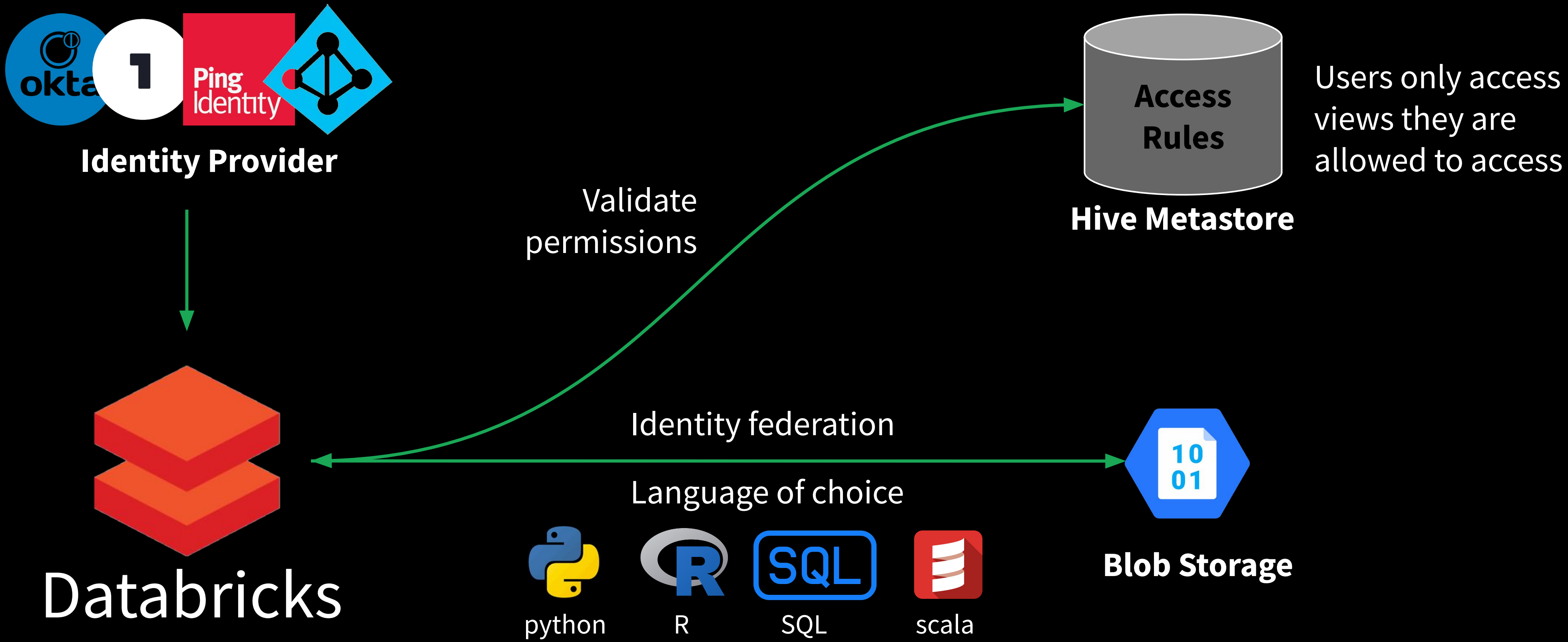
Databricks managed clusters in enterprise managed VPC/VNET

Local connectivity to other applications without peering

Data Centric Security

Example: End to end security for your data lake, defined in your metastore



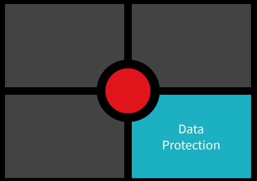


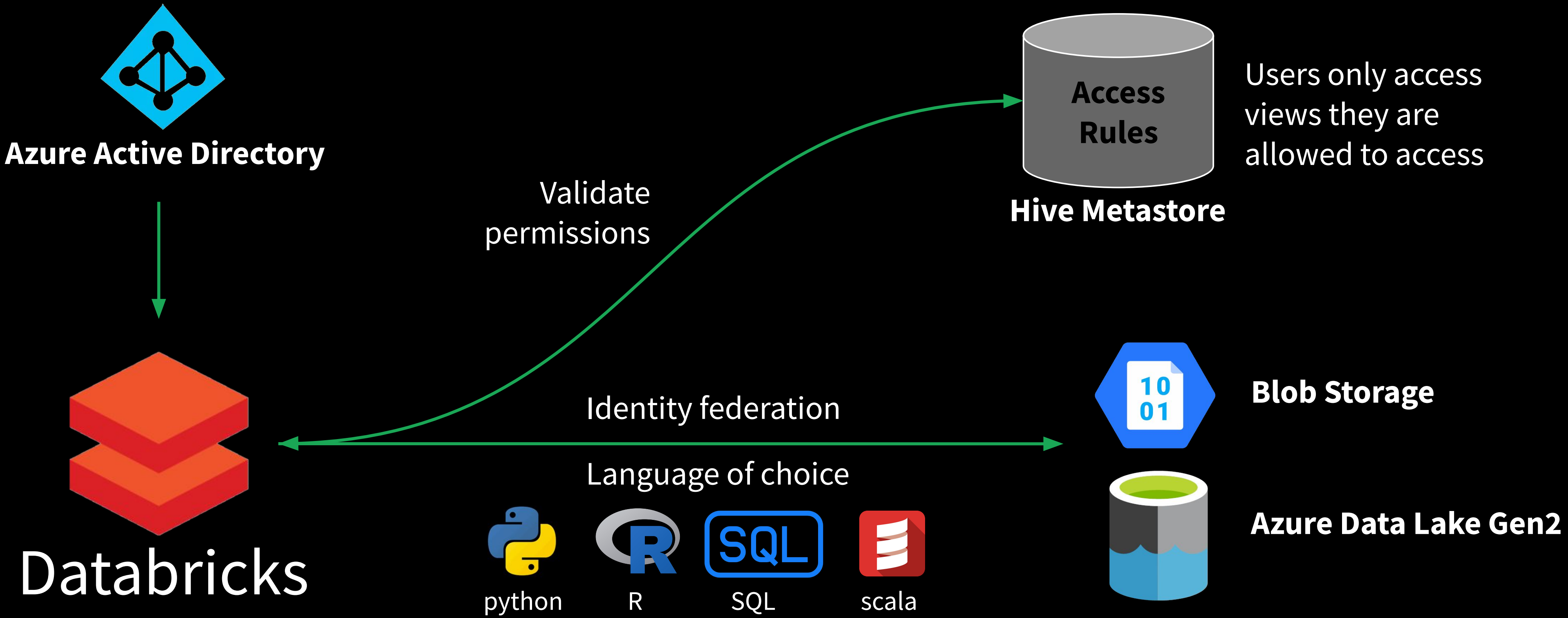
Users only access views they are allowed to access

Azure Databricks

Data Centric Security

Example: End to end security for your data lake, defined in your metastore



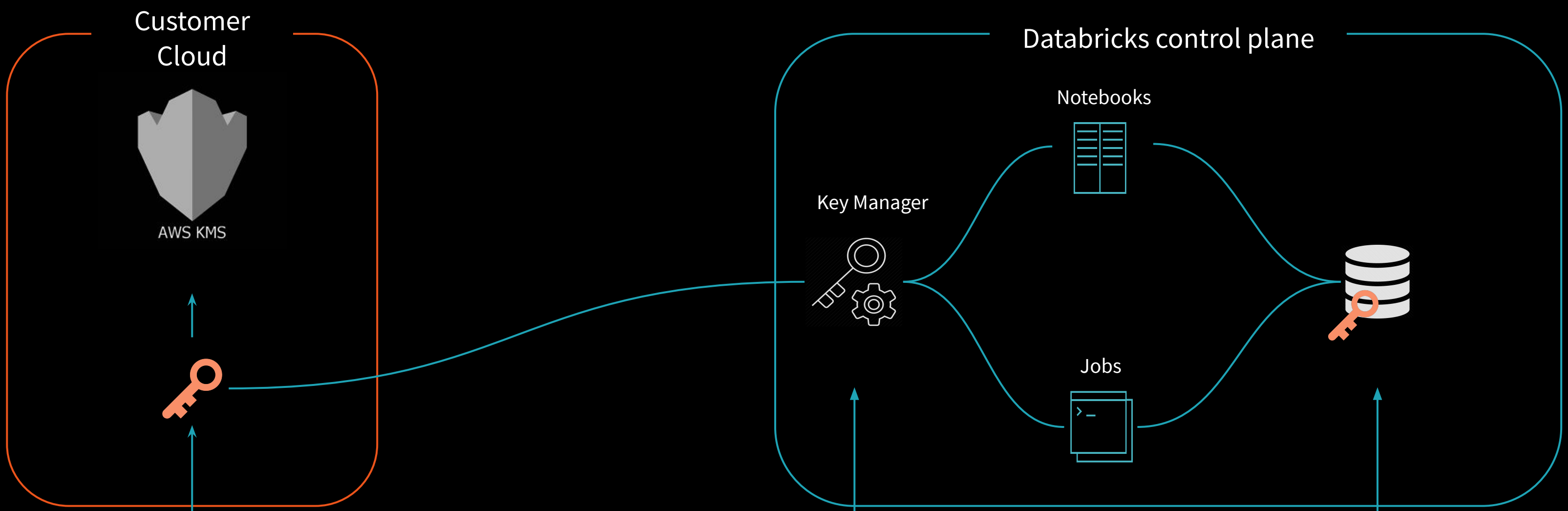


databricks

Enterprise Cloud Platform

Currently Preview

Encryption with enterprise root keys



Customer creates key in Key Vault for an account or a workspace

Databricks creates data encrypting keys rooted in customer key

Applications use customer key to encrypt all the data

Get full control over keys used to encrypt data in the control plane. Revoking key revokes data access

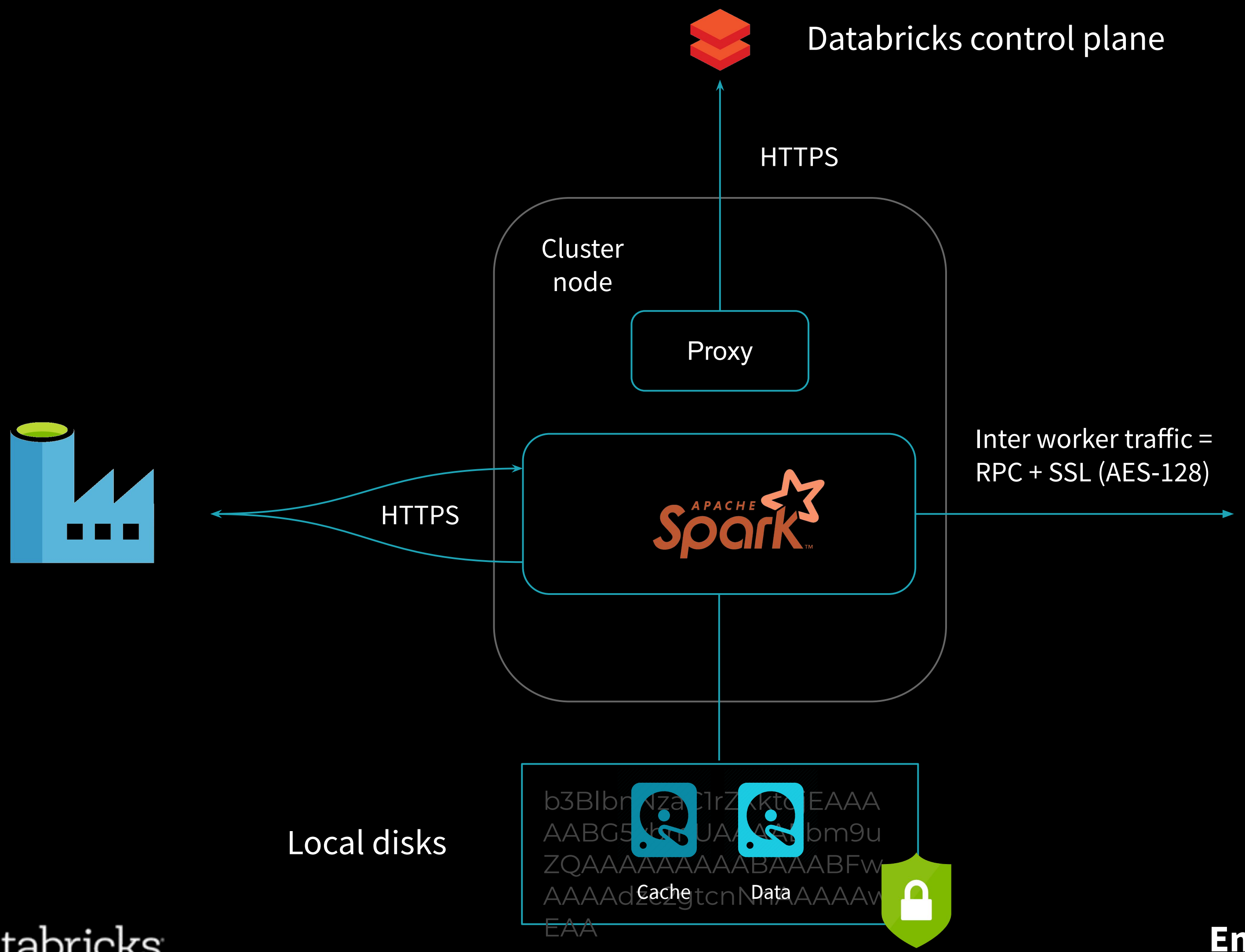
Key hierarchy enables use of different keys for different notebooks

An audit log of key operations makes for easy reporting and audit requests

Currently Preview

End-to-end encrypted clusters

Data Protection



Databricks control plane

HTTPS

Cluster node

Proxy

HTTPS

Inter worker traffic = RPC + SSL (AES-128)

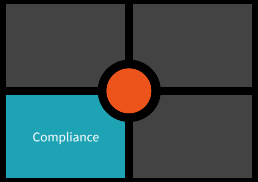
Local disks

Enable encryption for a cluster - no key/cert management necessary

Ensure that data shared between cluster nodes is always encrypted

Guarantee that data is always encrypted no matter where its stored on the cluster - root, ephemeral or network attached disks

Security and Privacy



Security

1. ISO 27001
2. SOC 2 Type 2
3. HITRUST (end of 2019 on Azure)
4. GovCloud & FedRAMP (2020 on Azure)

Privacy

1. Privacy Shield
2. ISO 27018
3. GDPR compliant

Azure Databricks Security

Compliance

- Audit Logs
- ISO 27001
- ISO 27018
- HIPAA (Covered by MSFT BAA)
- SOC2, Type 2

* Preview feature

Compliance | Audit Logs

Databricks provides comprehensive end-to-end audit logs of activities performed by Databricks users, allowing your enterprise to monitor detailed Databricks usage patterns.

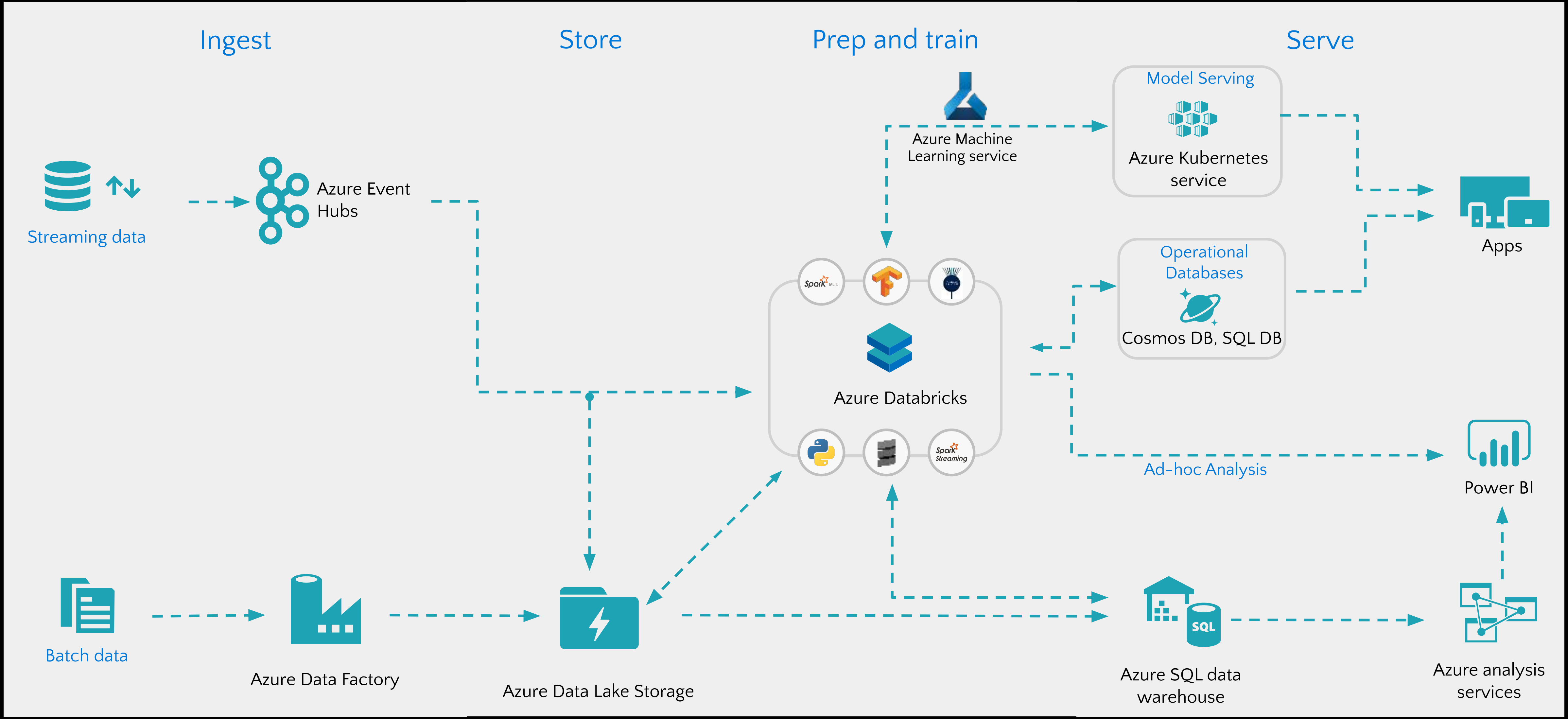
Integration with Azure Monitor

Services / Entities included are:

- Accounts
- Clusters
- DBFS
- Genie
- Jobs
- ACLs
- SSH
- Tables

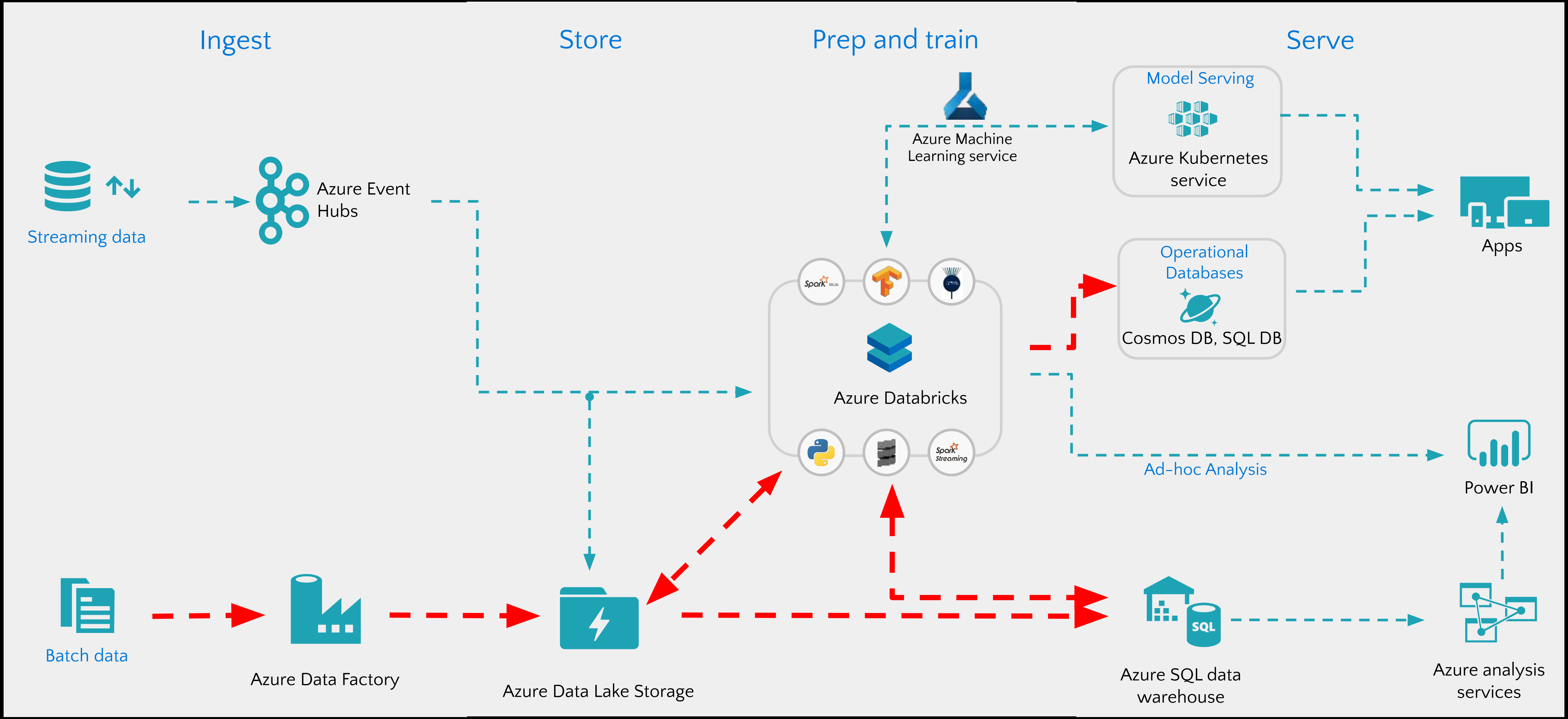
Reference Architectures

Recommended End-to-End Architecture



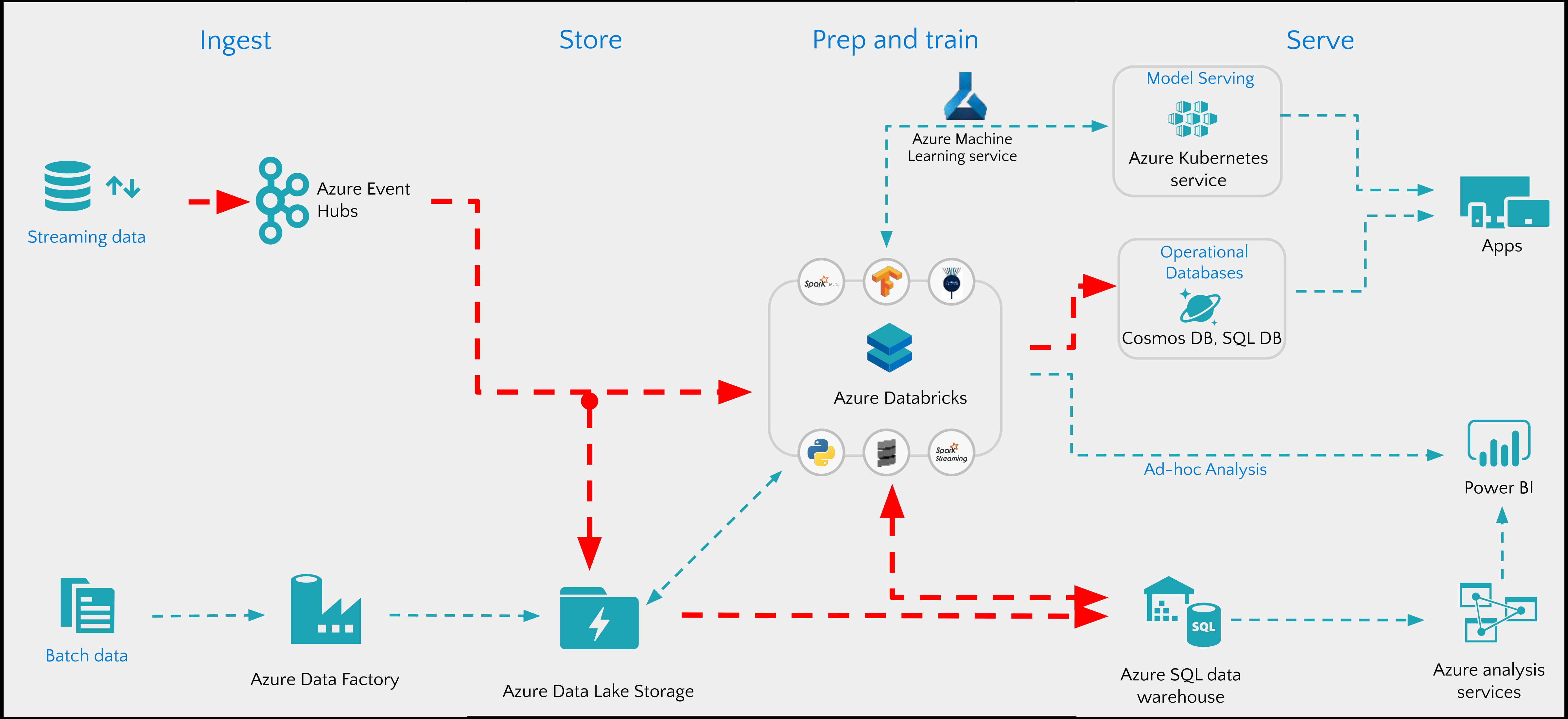
databricks

Recommended End-to-End Architecture - Batch ETL



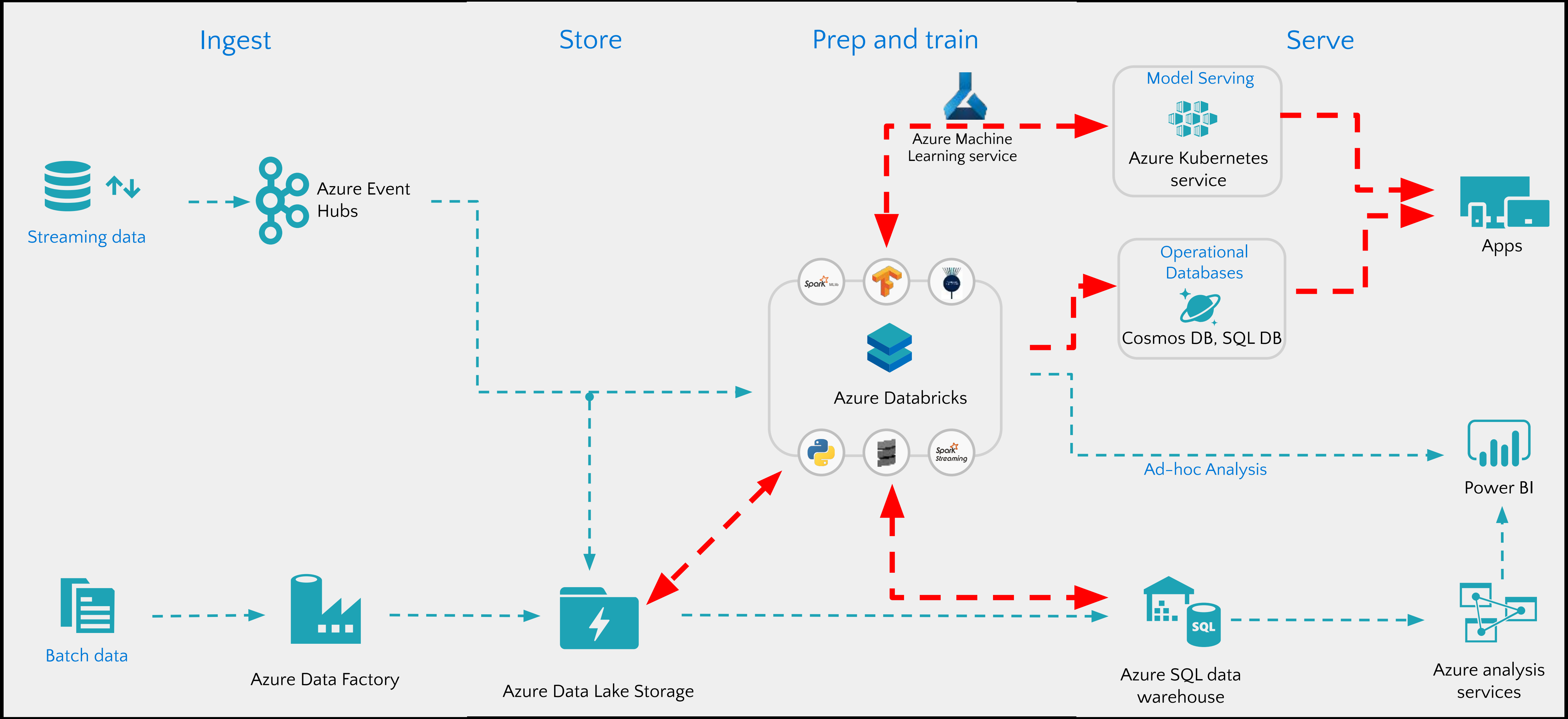
databricks

Recommended End-to-End Architecture - Stream ETL



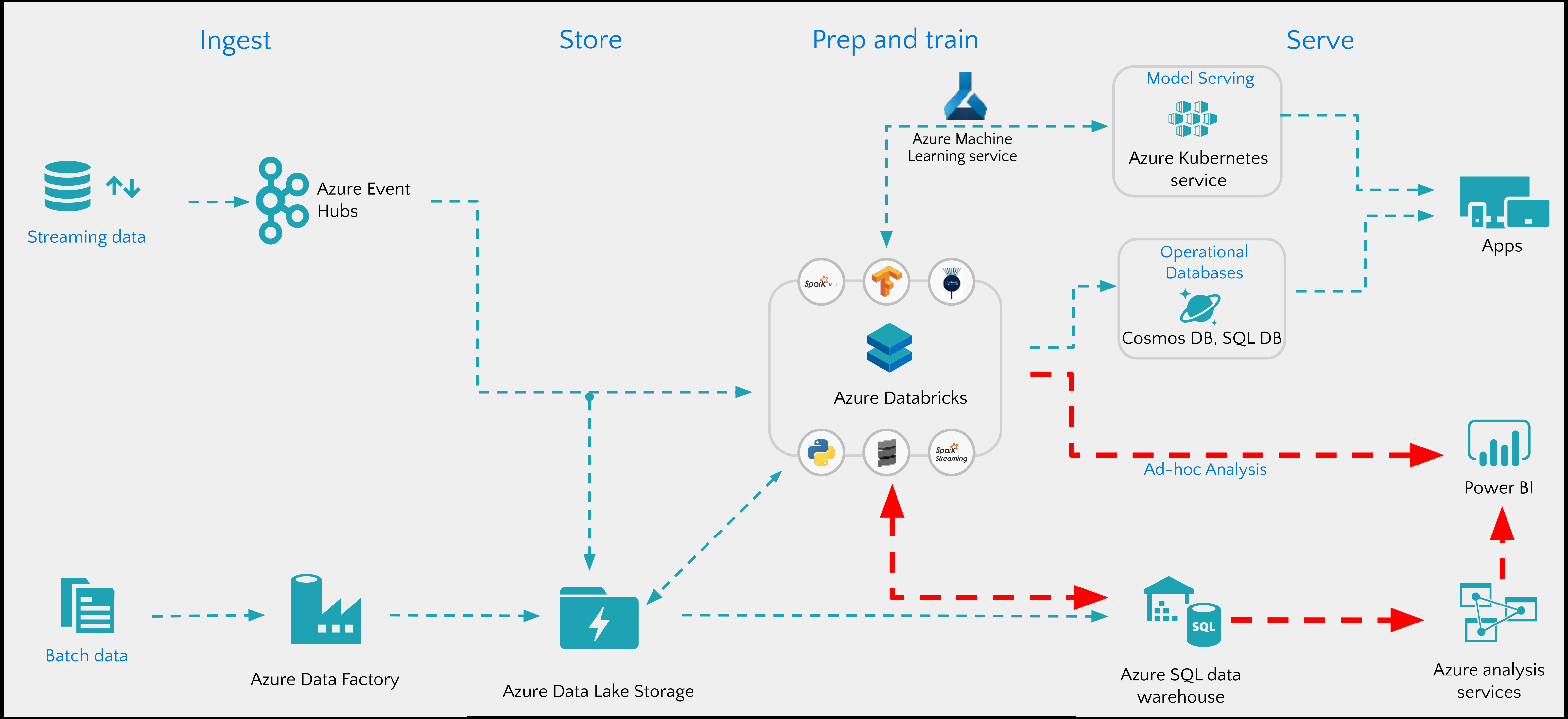
databricks

Recommended End-to-End Architecture - ML/Prediction



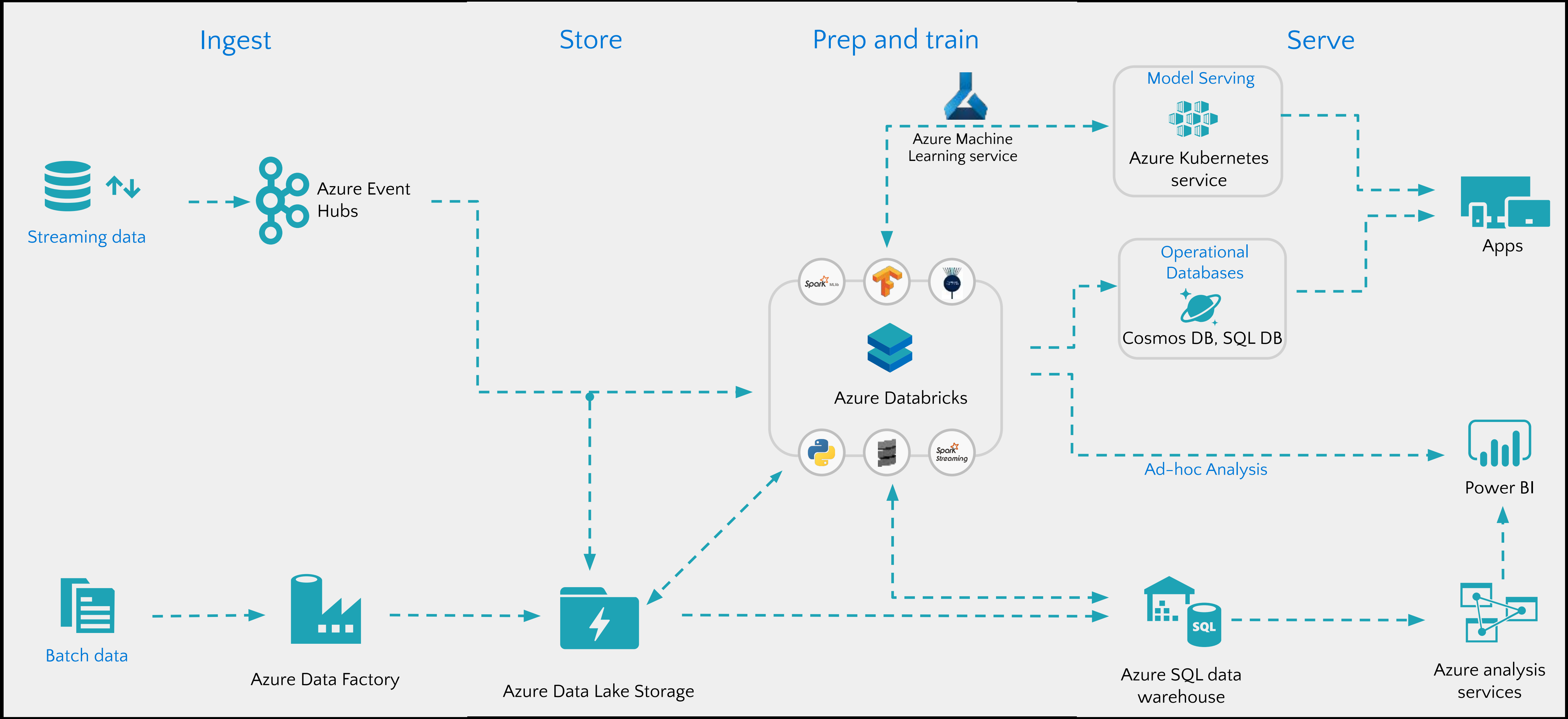
databricks

Recommended End-to-End Architecture - BI and Analysis



databricks

Recommended End-to-End Architecture



Ingest

Store

Prep and train

Serve

Streaming data

Azure Event Hubs

Azure Machine Learning service

Model Serving

Azure Kubernetes service

Apps

Operational Databases

Cosmos DB, SQL DB

Azure Databricks

Ad-hoc Analysis

Power BI

Batch data

Azure Data Factory

Azure Data Lake Storage

Azure SQL data warehouse

Azure analysis services

databricks

Azure Databricks Best Practices

Workspace Admin Best Practices

- Create different workspaces by different department / business team / data tier, and per environment (dev, qa, prod) - across relevant Azure subscriptions
- Define workspace level tags which propagate to initially provisioned resources in managed resource group (Tags could also propagate from parent resource group)
- Use ARM templates (search “databricks”) to have a more managed way of deploying the workspaces - whether via CLI, powershell or some SDK
- Create relevant groups of users - using Group REST API or by using AAD Group Sync with SCIM

Security Best Practices

- Do not store any production data on DBFS (use it only for toy / experimental datasets).
- Configure encryption-at-rest for Blob Storage and ADLS, preferably by using customer-managed keys in Azure Key Vault.
- Use Secrets with Azure Key Vault backend to obfuscate passwords and keys in notebooks.
- Prefer to use ADLS credential passthrough over Table ACLs (if possible).
- Configure access control for Databricks-native resources (clusters, notebooks, jobs etc.)
- Deploy workspace in your VNET to enable networking customizations.
- Configure Audit Logs to monitor the activity in a workspace.

Tools & Integration Best Practices

- Use Azure Data Factory to orchestrate pipelines / workflows (or something like Airflow).
- Connect your IDE or custom applications to Azure Databricks clusters using DB-Connect (Private Preview).
- Sync notebooks with Azure Devops for seamless version control.
- Use Databricks CLI for CI / CD from relevant enterprise tools/products, or to integrate with other systems like on-prem SCM or Library Repos etc.
- Use Library Utilities to install python libraries scoped at notebook level (cluster-scoped libraries may make more sense in certain cases).
- Use Init Scripts to do custom installs at cluster level.

Databricks Runtime Best Practices

- Use Delta wherever you can, to get the best performance and reliability for your big data workloads, and to create no-fuss multi-step data pipelines.
- Use Machine Learning Runtime for working with the latest ML/DL libraries (including HorovodRunner for distributed DL).
- Use DBIO Cache for accelerating reads from Blob Storage or ADLS.
- Use ABS-AQS connector for structured streaming when working with consistent rate of incoming files on Blob Storage.
- Turn on Databricks Advisor for automated tips on how to optimize workload processing.

HA and DR Best Practices

- Deploy Azure Databricks in two paired azure regions, ideally mapped to different control plane regions.
  - E.g. East US2 and West US2 will map to different control planes
  - Whereas West and North Europe will map to same control plane
- Use Azure Traffic Manager to load balance and distribute API requests between two deployments, when the platform is primarily being used in a backend non-interactive mode.
- Design to honor API and other limits of the platform.
  - Max API calls/ hr = 1500
  - Jobs per hour per workspace = 1000
  - Maximum concurrent Notebooks per cluster = 145

Cluster Best Practices

- Use autoscaling and auto-termination wherever applicable (e.g. auto-termination doesn't make sense if you need a cluster for data analysis by multiple users almost through the day, etc.).
- Use latest Databricks Runtime version to take advantage of latest performance & other optimizations (applicable in most cases, though not all).
- Use High-concurrency cluster mode for data analysis by a team of users via notebooks or a BI tool, or if you want to enforce data protection via Table ACLs or ADLS Passthrough.
- Use cluster tags for project / team based chargeback.

Cluster Best Practices Contd..

- Use Spark config tab if certain tuning would make sense for a specific workload (like config to use broadcast join).
- Use Event Log and Spark UI to see how different queries / workload executions perform, and what affect those have on a cluster's health.
- Configure Cluster Log Delivery
- Use Cluster ACLs to configure what each user or a group of users are allowed to do.
- Refer this blog by a customer, which more or less mentions what we've covered here. Rest is really workload dependent where it requires evidence-based tuning.

Appendix - Choosing the instance type

Different Azure Instance Types

Compute Optimized

- Fs
  - Haswell processor (Skylake not supported yet)
  - 1 core ~ 2GB RAM
  - SSD Storage: 1 core ~ 16GB
- H
  - High-performance
  - 1 core ~ 7GB RAM
  - SSD Storage: 1 core ~ 125GB

Memory Optimized

- DSv2
  - Haswell processor
  - 1 core ~ 7GB RAM
  - SSD Storage: 1 core ~ 14 GB
- ESv3
  - High-performance (Broadwell processor)
  - 1 core ~ 8GB RAM
  - SSD Storage: 1 core ~ 16GB

Storage Optimized

- L
  - 1 core ~ 8GB RAM
  - SSD Storage: 1 core ~ 170GB
  - Price : .156

General Purpose

- DSv2 and DSv3
  - DSv2 - 1 core ~ 3.5GB RAM
  - DSv3 - 1 core ~ 4GB RAM
  - SSD Storage:
    - DSv2 - 1 core ~ 7GB
    - DSv3 - 1 core ~ 8GB

Cluster Sizing Starting Points

Rules of Thumb

- Fewer big instances > more small instances
  - Reduce network shuffle; Databricks has 1 executor / machine
  - Applies to batch ETL mainly (for streaming, one could start with smaller instances depending on complexity of transformation)
  - Not set in stone, and reverse would make sense in many cases - so sizing exercise matters
- Size based on the number of tasks initially, tweak later
  - Run the job with a small cluster to get idea of # of tasks (use 2-3x tasks per core for base sizing)
- Choose based on workload (Probably start with F-series or DSv2):
  - ETL with full file scans and no data reuse - F / DSv2
  - ML workload with data caching - DSv2 / F
  - Data Analysis - L
  - Streaming - F

How do we tweak these?

Workload requires caching (like machine learning)

- Look at the Storage tab in Spark UI to see if the entirety of the training dataset is cached
  - Fully cached with room to spare -> less instances
  - Partially cached
    - Almost completely cached? -> Increase the cluster size
    - Not even close to cached -> Consider L series or DSv2 memory-optimized
      - Check to see if persist is MEMORY_ONLY, or MEMORY_AND_DISK
      - Spill to disk with SSD isn't so bad
- Still not good enough? Follow the steps in the next section

How do we tweak these?

ETL and Analytic Workloads

- Are we compute bound?
  - Check CPU Usage (Ganglia metrics to come to Azure Databricks soon)
  - Only way to make faster is more cores
- Are we network bound?
  - Check for high spikes before compute heavy steps
  - Use bigger/fewer machines to reduce the shuffle
  - Use an ssd backed instance for faster remote reads
- Are we spilling a ton?
  - Check Spark SQL tab for spill (pre-agg before shuffles are common to spill)
    - Use L-series
    - Or use more memory

Q&A