

17 aprile 2026
azuremeetup
VENETO



Microsoft

#GLOBALAZURE

Dal Networking alla Data Platform
Architetture Azure Databricks per Scalabilità e
Sicurezza

Salvatore Cavallaro

Senior Data Consultant Insight



/cavallarosalvatore

Carlo Pio Luigi Ciciriello

Chief Network Architect & Consultant

Kyndryl



/cplciciriello



DIAMOND PARTNER



PLATINUM PARTNER



GOLD PARTNER



SILVER PARTNER



Who We Are



Hi there. Here's **Carlo**



Chief Network Architect & Sr Managing Consultant @ Kyndryl
Certified ICT Trainer
Cisco CCIE EI | Tech Blogger & Public Speaker

Key Focus Areas:

Cloud Networking & Security | Network Automation & Observability | IPv6 | Segment Routing | BGP Security | DevOps | AI



Hi there. Here's **Salvatore**

Senior Data Consultant @ Insight
Data Solution Architect
Tech Blogger | Public Speaker

Key Focus Areas:

Cloud & Hybrid Data Platforms | Data Architecture | Data Engineering | Data-Driven Solutions | Cloud Transformation | Technical Advisory | AI





Agenda

- Deploy di Databricks in 2 minuti (Demo)
- Databricks Control Plane vs Compute Plane
- Unity Catalog: Overview & Update
- Architettura Enterprise
- VNet Injection
- Considerazioni sui servizi Serverless

17 aprile 2026
azuremeetup
VENETO



Demo: Deploy in 2 minuti

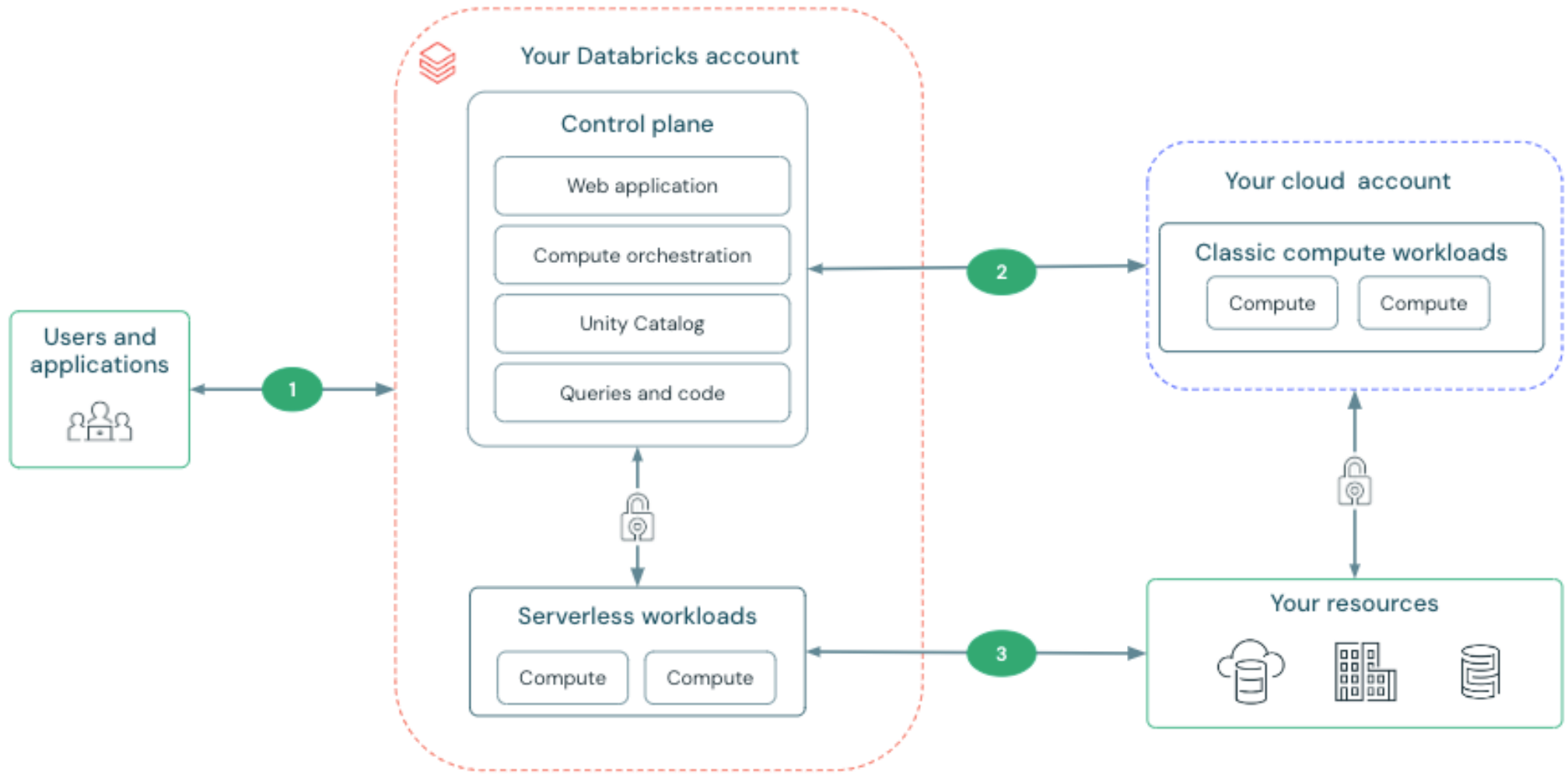
17 aprile 2026
azuremeetup
VENETO



Control Plane vs Compute Plane



Control Plane vs Compute Plane



17 aprile 2026
azuremeetup
VENETO



Unity Catalog



Unity Catalog: Governance Unificata



Cos'è Unity Catalog?

Soluzione di governance nativa di Databricks che centralizza la gestione di dati, modelli ML, notebook e funzioni in un unico metastore condiviso tra tutti i workspace.

- ✓ Metastore centralizzato multi-workspace
- ✓ Namespace gerarchico: Catalog → Schema → Object
- ✓ Fine-grained ACL (tabelle, colonne, righe)
- ✓ Data lineage automatico e auditabile
- ✓ Supporto per tabelle, view, volume, model, function

PRIMA (Hive Metastore)

- ✗ Un metastore per workspace
- ✗ Nessun controllo cross-workspace
- ✗ ACL limitate a tabella

DOPO (Unity Catalog)

- ✓ Un metastore per regione/account
- ✓ Governance centralizzata
- ✓ ACL fino a livello colonna/riga
- ✓ Lineage e audit integrati



Unity Catalog: Modello



Privilege Model

| Securable | Privileges | Ereditarietà |
|------------------|--------------------------------------|----------------------------|
| Catalog | USE CATALOG, CREATE SCHEMA | Sì → schema e oggetti |
| Schema | USE SCHEMA, CREATE TABLE/VIEW/VOLUME | Sì → oggetti contenuti |
| Table / View | SELECT, MODIFY, ALL PRIVILEGES | Column-level masking |
| Volume | READ VOLUME, WRITE VOLUME | Gestione file unstructured |
| Model / Function | EXECUTE, ALL PRIVILEGES | Governance su ML e UDF |



Unity Catalog: Tags e Policy di Governance



Governance Tags

I tag permettono di classificare e annotare qualsiasi securable nel metastore per applicare policy basate su metadati.



Tag su Catalog / Schema / Table / Column

Classificazione gerarchica flessibile



Tag di compliance

PII, GDPR, HIPAA, confidential, public



Tag personalizzati

cost_center, data_owner, team, domain



Tag-based access policies

Applica regole automatiche su dati taggati



Propagazione ereditaria

Tag su schema si propaga a tutte le tabelle



Data Access Policies

Le policy controllano chi può vedere, mascherare o filtrare i dati sensibili in modo dichiarativo.



Row-Level Security (RLS)

Filtra righe in base all'identità utente



Column Masking

Maschera valori sensibili (es. email, SSN)



Attribute-Based Access (ABAC)

Policy dinamiche basate sui tag dei dati



Audit Logging

Ogni accesso e modifica viene tracciato



Data Classification automatica

Rilevamento automatico di PII e dati sensibili

LATEST FEATURES

PUBLIC PREVIEW!

17 aprile 2026
azuremeetup
VENETO



Classic Compute Plane
VNet Injection



VNet Injection: Caratteristiche della VNet



VNet Configuration

- Stessa Region/Subscription del workspace
- 2 subnet dedicate: Container sbn & Host sbn
- IPv4 CIDR block minimo per subnet: /26
- Subnet di pari dimensione (consigliato)



Security Best Practices

- Regole NSG restrittive (principio del *least privilege*)
- NSG per ciascun workspace (consigliato)



Address Space Guidance

- Delegation a Microsoft.Databricks/workspaces
- Subnet ad uso esclusivo di Databricks
- Subnet non condivisibili tra workspace
- Per ciascuna subnet: 5 IP riservati da Azure + 1 IP per ogni Databricks cluster node



Serverless & Network Connectivity Config

Networking sicuro per Serverless SQL Warehouse, Jobs, Model Serving e Lakeflow

Serverless Compute

Infrastruttura completamente gestita da Databricks. No VNet Injection, no VM cluster nella subscription.

Il compute gira nel Control Plane di Databricks.

- ✓ Serverless SQL Warehouse
- ✓ Serverless Jobs & Notebooks
- ✓ Model Serving / Lakeflow Pipelines

NCC (Network Connectivity Config)

Oggetto account-level che definisce come il Serverless Compute raggiunge i tuoi data services in modo sicuro e privato.

- ✓ Associato al Workspace
- ✓ Private Endpoint Rules

Private Endpoint Rules

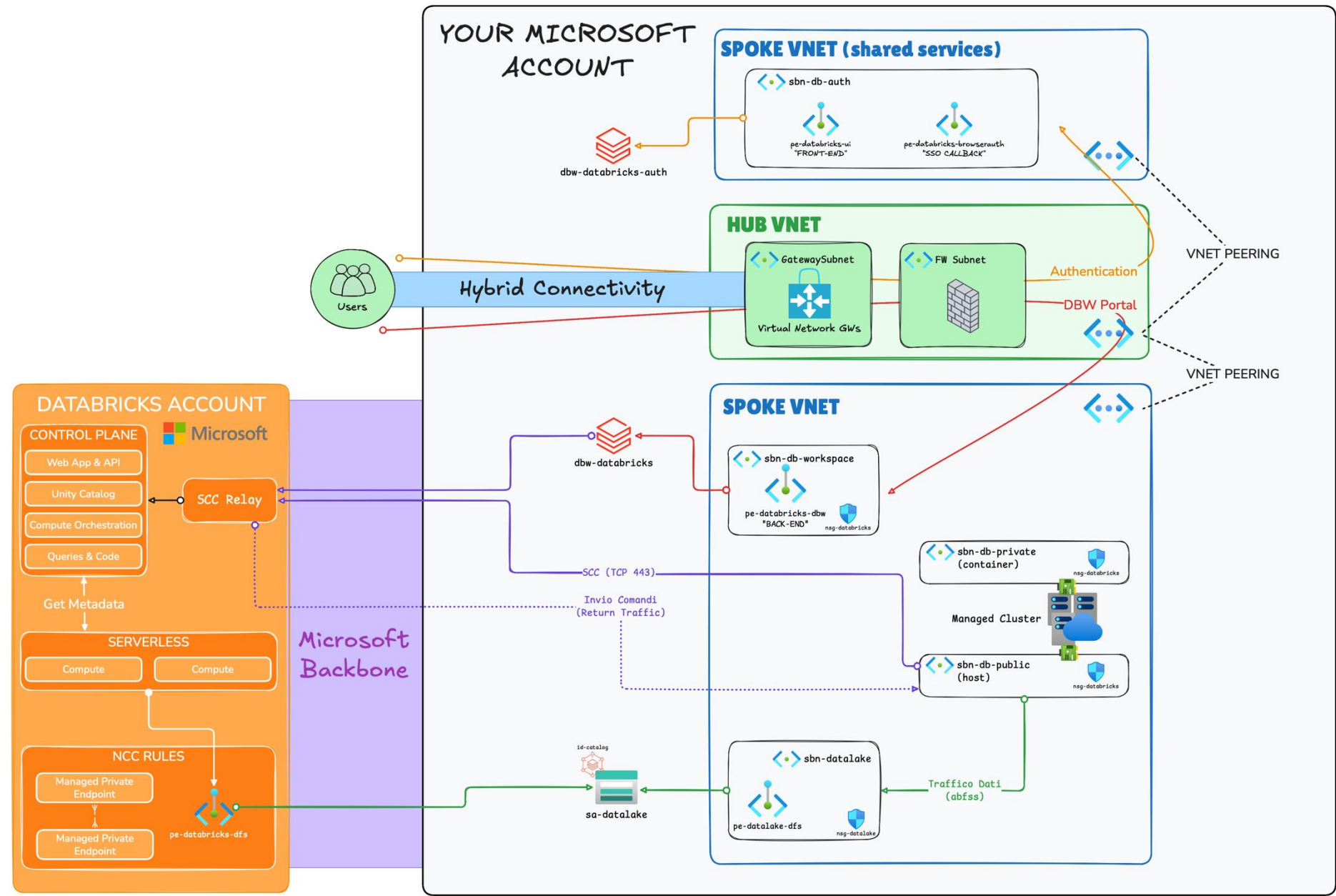
- PE verso Storage Account e servizi Azure.
- Richiesto customer approval.
- Traffico su rete Microsoft.

NCC vs VNet Injection

- VNet Injection: cluster classici, full control su routing e NSG.
- NCC: Serverless, PE gestiti da Databricks, meno Ops overhead.



Architettura Enterprise: Classic + Serverless Compute



17 aprile 2026
azuremeetup
VENETO



Microsoft

Grazie!



Ti aspettiamo a Global Azure
2027

Salvatore Cavallaro

Senior Data Consultant Insight



/cavallarosalvatore

Carlo Pio Luigi Ciciriello

*Chief Network Architect & Consultant
Kyndryl*



/cplciciriello