

# Veza for Databricks

Modern Identity Security Across Workspace-Level and Unity Catalog Access Models

Veza allows you to definitively answer the question of:

**Who** can take **what action** on **what resources**?

## Overview

Databricks powers modern data ecosystems—from AI/ML pipelines to enterprise-scale analytics. As organizations adopt Unity Catalog as the new standard for access control, legacy workspace-level permissions often persist, creating complexity and risk. Over-permissioned service principals, siloed workspace configurations, and opaque access paths introduce unnecessary exposure.

Veza supports both Unity Catalog and legacy workspace-level permission models to deliver fine-grained visibility into who has access to what, and why. By unifying access data across Catalog, workspace, and account layers, Veza enables identity and security teams to enforce least privilege, reduce audit overhead, and ensure compliance, regardless of deployment complexity or cloud provider.

## Access Challenges in Databricks Deployments



### Excessive Admin & Service Principal Access

Privileged access to clusters, notebooks, and data Catalogs often remains in place long after it's needed.



### Siloed Access Management Across Workspaces

In non-Unity Catalog configurations, each workspace enforces permissions independently, making organization-wide access reviews nearly impossible.



### Limited Oversight of Non-Human Identities

Service principals and automation accounts often go unmanaged, despite controlling sensitive pipelines and data lake access.



### Cloud-Specific, Manual Compliance Workflows

Databricks-native tools lack centralized visibility across cloud regions and tenants, slowing down audit prep and increasing risk.



### Layered, Hard-to-Audit Unity Catalog Permissions

Entitlements span users, groups, schemas, Catalogs, and metastores—creating tangled access paths that native tools struggle to surface.

## How Veza Helps

Veza integrates directly with both Unity Catalog-enabled and legacy workspace-level Databricks configurations to:

- ✓ Discover user → group → service principal → resource access relationships
- ✓ Visualize access across Catalogs, clusters, notebooks, schemas, and more with Veza's Access Graph
- ✓ Identify excessive group assignments, admin overreach, and service principal sprawl
- ✓ Detect stale, inactive, or unused access, both human and machine
- ✓ Track changes to permissions and configurations in near real-time
- ✓ Simplify access reviews, audit readiness, and compliance workflows

**Result:** Unified, identity-centric governance across your Databricks estate—whether you're fully migrated to Unity Catalog or still managing legacy access paths.

## Key Benefits of Veza for Databricks



### Unified Visibility

Gain single-pane-of-glass visibility into users, groups, service principals, and resource entitlements across all workspaces and federated Unity Catalog layers.



### Access Risk Detection

Surface dormant access, misconfigured privileges, and over-extended entitlements—whether for humans or automation identities.



### Fine-Grained Audit Trails

Trace true access paths and generate export-ready reports aligned to SOX, GDPR, PCI DSS, and internal controls.



### Multi-Cloud Compliance Readiness

Support consistent, automated access reviews across AWS, Azure, and GCP-hosted Databricks deployments.

# Why Veza for Databricks



## Challenge

## Veza Advantage

Siloed access controls across workspaces

Federated visibility across groups, users, and resources

Complex Unity Catalog access models

Access Graph visualizes entitlements across Catalogs, schemas, and metastores

Admin sprawl and unmanaged service principals

Identity insights into human and machine accounts

Reactive, manual compliance reporting

Near real-time monitoring and audit-ready documentation

Transitioning from the workspace to the Unity Catalog model

Full support for legacy and modern Databricks permission layers

The screenshot displays the 'Databricks Insights' section of the Veza interface. It includes a sidebar with navigation icons, a top navigation bar with links like Overview, Risks, Alerts, Analyze, Compare, Recommend, Role Mining, and Reports. The main content area shows a table titled 'Local Users (14)' with columns for NAME, RESULTS, % CHANGE, VISIBILITY, LABELS, INTEGRATIONS, LAST REFRESHED, and ACTIONS. The table lists various user groups and their associated permissions and access levels.

| NAME   | RESULTS | % CHANGE | VISIBILITY | LABELS             | INTEGRATIONS      | LAST REFRESHED | ACTIONS |
|--|---------|----------|------------|--------------------|-------------------|----------------|---------|
| Databricks Users with no mapped Azure AD Users             | 131     | → 0%     | Public     |                    | Azure, Databricks | 27 minutes ago |         |
| Databricks Local Users with write permissions              | 3       | → 0%     | Public     | Write Permissions  | Databricks        | 27 minutes ago |         |
| Databricks local users                                     | 132     | → 0%     | Public     |                    | Databricks        | 27 minutes ago |         |
| Databricks Users with no mapped Okta Users                 | 131     | → 0%     | Public     |                    | Databricks, Okta  | 27 minutes ago |         |
| Databricks Users with Workspace Admin permissions          | 0       | → 0%     | Public     | Privileged Access  | Databricks        | 27 minutes ago |         |
| Azure AD Users with Databricks access                      | 0       | → 0%     | Public     |                    | Azure, Databricks | 30 minutes ago |         |
| Databricks Users with no permissions                       | 0       | → 0%     | Public     | Best Practice      | Databricks        | 27 minutes ago |         |
| Azure AD Users with Databricks delete permissions          | 0       | → 0%     | Public     | Delete Permissions | Azure, Databricks | 30 minutes ago |         |
| Azure AD Users with Databricks write permissions           | 0       | → 0%     | Public     | Write Permissions  | Azure, Databricks | 30 minutes ago |         |
| Databricks Users with delete permissions                   | 1       | → 0%     | Public     | Delete Permissions | Databricks        | 27 minutes ago |         |
| Databricks Local Users that are deactivated                | 103     | → 0%     | Public     |                    | Databricks        | 27 minutes ago |         |
| Databricks Groups without Users                            | 0       | → 0%     | Public     | No Assigned Users  | Databricks        | 27 minutes ago |         |
| Azure AD Users with Databricks workspace owner permissions | 0       | → 0%     | Public     | Privileged Access  | Azure, Databricks | 30 minutes ago |         |
| Databricks Users with OWN privilege on an object           | 1       | → 0%     | Public     |                    | Databricks        | 27 minutes ago |         |

# Technical Overview

Veza ingests identity and access metadata across all Databricks access layers—whether your deployment uses Unity Catalog, workspace-level permissions, or a hybrid of both:



## Users & Groups

Source (e.g., SCIM, Identity Federation), membership, and access to Catalogs, schemas, and tables

## Service Principals

Usage scope, active status, and access privileges across data and compute

## Workspace Admins

Centralized vs. workspace-specific permissions across environments

## Metastores (Unity Catalog only)

Catalog grouping and cross-workspace visibility

## Tables & Views

Read/write privileges, group entitlements, and access lineage

## Catalogs & Schemas

Ownership, ACLs, and usage frequency

## Clusters

Ownership, admin access, and usage status

## Notebooks

Shared access, edit privileges, and visibility into collaboration patterns

Reviews

Configurations

Settings

← Back

Admin

Actions

Filters

Complete Review

Sign-off (0)

**Databricks Review**

Completed Items: 1/3 

1 Approved

0 Rejected

2 Need review

+ Group by

3 Total Items

View

Export

Columns

| USER                     |                    |                    | PERMISSIONS |               |  | DESTINATION           |                        |                        |         |          |         |
|--------------------------|--------------------|--------------------|-------------|---------------|--|-----------------------|------------------------|------------------------|---------|----------|---------|
| <input type="checkbox"/> | User Name          | User Unique Id     | Risk Score  | Permissions   |  | Name                  | Type                   | Reviewers              | Risk Li |          | Actions |
| <input type="checkbox"/> | admin@sigmacorp... | admin@sigmacorp... | 52          | C R W D I M N |  | Create,Write,Delet... | Databricks Effectiv... | gary.ward@sigmacorp... | None    | ✓        | ✗       |
| <input type="checkbox"/> | admin@sigmacorp... | admin@sigmacorp... | 52          | C R W D I M N |  | patient               | Databricks Table       | gary.ward@sigmacorp... | None    | ✓        | ✗       |
| <input type="checkbox"/> | admin@sigmacorp... | admin@sigmacorp... | 52          | C R W D I M N |  | people                | Databricks Table       | gary.ward@sigmacorp... | None    | Approved | ✗       |

50 per page

page 1 of 1

## Get Started Today

Secure access across your entire Databricks deployment—from legacy workspace-level permissions to modern Unity Catalog-based governance.

Visit [veza.com/integrations](https://veza.com/integrations) or contact your Veza representative to schedule a demo.