veza | Solution Brief

Veza for AWS

Easily understand and manage AWS IAM policies, how they interact with service level permissions and ACLs, and who in your identity system can use them

AWS Identity and Access Management (IAM) is the product of choice for many enterprise organizations to manage authentication and authorization; it allows customers to specify authorization policies to permit or deny actions for services and resources within and across accounts.

However, the vast scope of granular service-level permissions, VM and service account authorization to AWS resources, and user federation in AWS IAM make it inherently complex. The AWS IAM User Guide alone is up to 888 pages and continues to expand. As a result, managing AWS IAM and auditing access permissions is error-prone, time-consuming, and costly.

Veza discovers the relationships between human and non-human (e.g., service account) AWS IAM principals, policies, services, and data sources, and enables security teams to assess, query, and monitor authorization across your organization's AWS accounts. Veza surfaces insights into ACLs and local users that might have permissions invisible to AWS IAM. We can connect to your identity provider to give a complete end-to-end picture, beyond simply the role in AWS, of who can and should take what action on what data.

Meet Veza

The Data Security Platform that helps you answer ***who can*** and ***should take what action*** on what data in AWS

veza | aws

Challenges for AWS IAM Customers

AWS provides a modern, scalable, and cost-effective approach to running business-critical applications and managing data warehousing and analytics. However, lack of visibility within AWS can make it difficult for security teams to maintain access permissions, prioritize security risks, and manage complex, large, and interconnected environments.

Given the potential blast radius of AWS security incidents, it is imperative to understand what actions your users, groups, and service principals can take on sensitive data sets, production dev environments, and other critical resources.

Primary challenges faced by organizations managing AWS include:

- Visualizing which users, roles, and apps can reach AWS resources and understanding the layers of IAM controls enabling access.
- Understanding how federated users (e.g., Okta, Azure AD) get limited security credentials to access AWS services and resources they usually don't have access to, typically via the AssumeRole action.
- Identifying effective permissions on data (e.g., read PII data sets, modify S3 configurations, drop database schema/table, etc.)
- Merging information from service-level ACL permissions and local users in AWS to get a truly comprehensive view of permissions

Choose Veza to demystify AWS IAM

Veza demystifies the complexities of AWS by helping you understand and manage access permissions for any account, human and non-human, through the power of authorization. Veza's support for AWS resources spans across -

AWS users, roles and groups

S3 buckets

EC2 instances and security groups

KMS policies

EMR services

RDS Postgres

RedShift

DynamoDB

Aurora

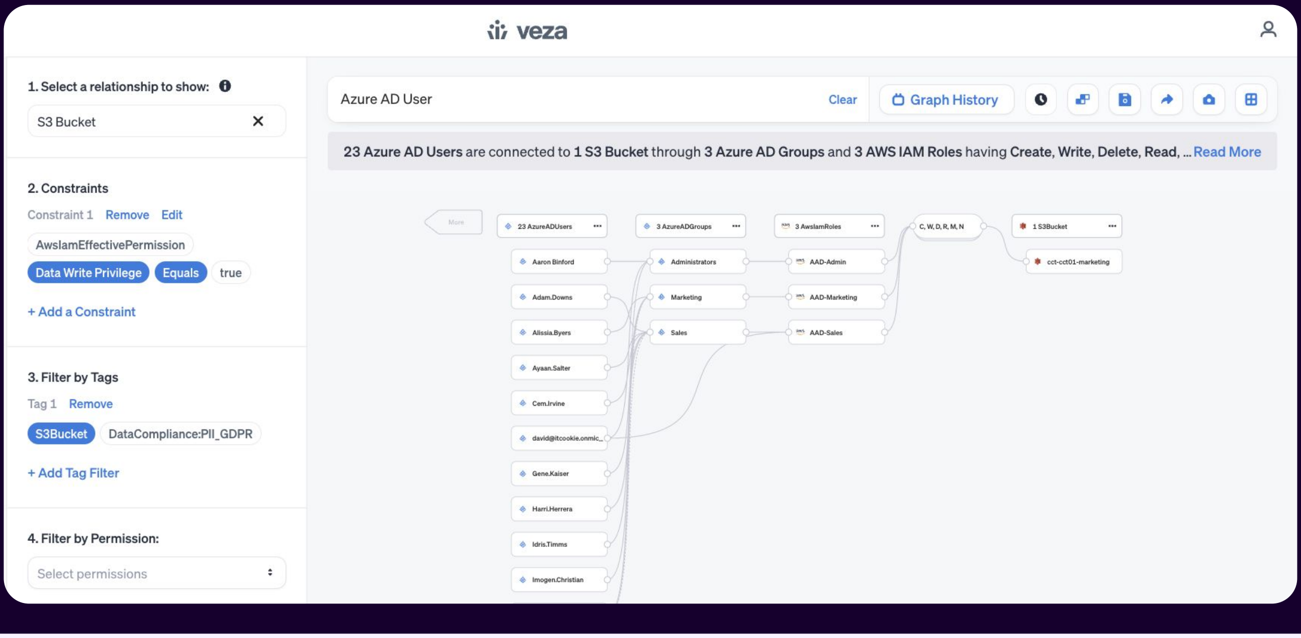
Through a rich, consumer-like search for effective permissions on AWS resources, Veza offers the following benefits to security teams and data owners -

- A comprehensive map of access permissions for federated users and service-level AWS IAM users, roles, policies, and services, presented in an easy-to-understand language of CRUD
- Increased time savings by streamlining audit and compliance reviews
- Enhanced confidence in maintaining zero trust controls for AWS resources

Read on to understand how Veza helps to manage and secure your AWS environment.

Search & Discover

- ✓ A single control plane for multi-cloud authorization, illuminating cross-service connections between AWS accounts and to/from IdP/data providers: Snowflake, Google Cloud BigQuery, Azure AD, Okta, etc.
- ✓ Integrate with AWS Control Tower, allowing easy automated integration of new AWS accounts into Veza.
- ✓ Find all identities (people and service accounts) with access to AWS critical resources using the **Authorization Graph**, leveraging metadata from your identity provider, AWS IAM, and service-level access controls (when applicable). For example, address use cases like "which Okta users have access to delete sensitive data in AWS S3 buckets?"
- ✓ Manage permissions for popular AWS data services like DynamoDB, EMR, Aurora, RDS, Redshift, KMS, and more.
- ✓ Parse and explain "effective permissions" in human-understandable language, including the resulting permissions from cross-account assume role actions, Service Control Policies, permissions boundaries, and conflicting policy statements.
- ✓ Leverage searchable properties like AWS tags alongside custom **Tags** in Veza to categorize principals, authorization controls, and data - helping you manage resource-centric entitlements for objects like S3 buckets containing sensitive data.



1. Select a relationship to show:

S3 Bucket ✕

2. Constraints

Constraint 1 Remove Edit

AwsIamEffectivePermission

Data Write Privilege Equals true

+ Add a Constraint

3. Filter by Tags

Tag 1 Remove

S3Bucket DataCompliance:PII_GDPR

+ Add Tag Filter

4. Filter by Permission:

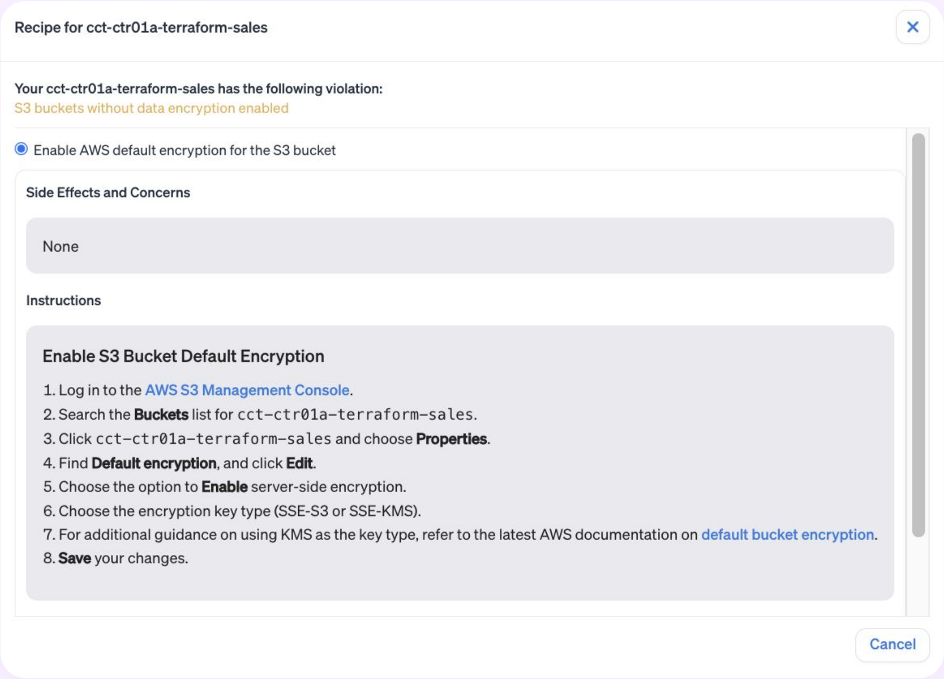
Select permissions

Azure AD User Clear Graph History

23 Azure AD Users are connected to 1 S3 Bucket through 3 Azure AD Groups and 3 AWS IAM Roles having Create, Write, Delete, Read, ... Read More

Compare & Correct

- Monitor changes, track trends, and get rapid insight into anomalies and risks specific to your organization's AWS IAM environments using **Privilege Insights** and **Search**. For example, find federated users directly assigned to an IAM role, or locate users and roles that allow for privilege escalation due to managed and inline policy permissions.
- Use **Recipes** to quickly resolve misconfigurations and excessive permissions, including a preview of potential side effects. For example, visualize the impact of an authorization change when a user is removed from an IDP group.
- Define organization-specific security **Violations** and **Alerts**, connecting with SOAR and ITSM tools to establish actionable and automatable monitoring. For example, create a rule to trigger alerts when an IAM policy providing full administrative privileges is given to a role attached to your EC2 instances.
- Leverage actionable intelligence with pre-built assessments for AWS services, IAM configurations, and data risk vulnerabilities. For example, document all IAM policies with full admin privileges or find AW3 S3 buckets with no access logging.



Recipe for cct-ctr01a-terraform-sales ✕

Your cct-ctr01a-terraform-sales has the following violation:
S3 buckets without data encryption enabled

● Enable AWS default encryption for the S3 bucket

Side Effects and Concerns

None

Instructions

Enable S3 Bucket Default Encryption

1. Log in to the AWS S3 Management Console.
2. Search the **Buckets** list for `cct-ctr01a-terraform-sales`.
3. Click `cct-ctr01a-terraform-sales` and choose **Properties**.
4. Find **Default encryption**, and click **Edit**.
5. Choose the option to **Enable** server-side encryption.
6. Choose the encryption key type (SSE-S3 or SSE-KMS).
7. For additional guidance on using KMS as the key type, refer to the latest AWS documentation on default bucket encryption.
8. **Save** your changes.

Cancel

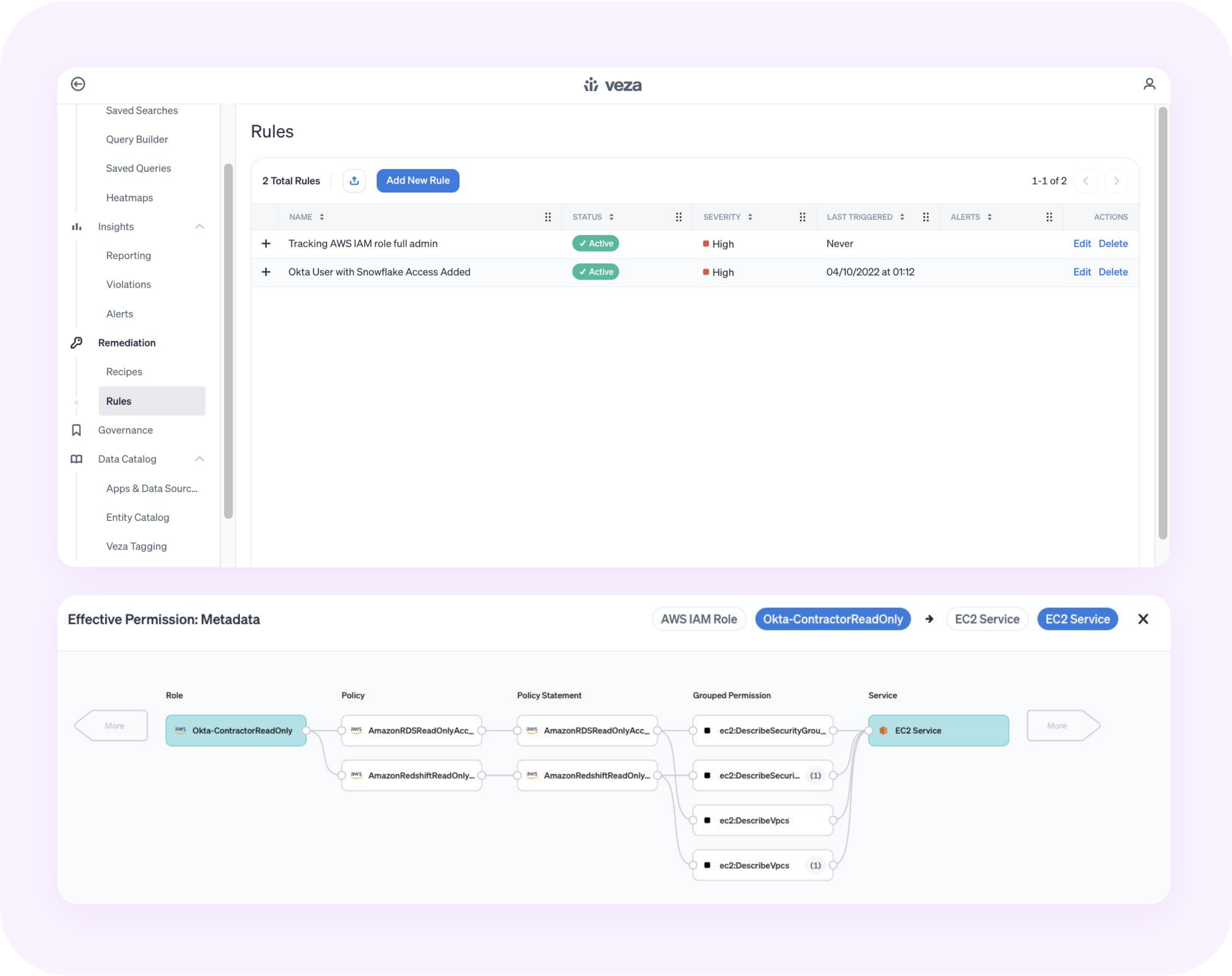
Define & Control

- Configure **Rules** across your entire cloud ecosystem and monitor for recent changes and violations of best practices. For example, find IDP (e.g., Okta & Azure AD) users that are disabled but have AWS IAM access, or detect an increase in the number of AWS IAM roles allowing delete actions on production RDS instances.

- Set AWS IAM permissions for new deployments based on your organization's policies and current implementation.

- Complete faster compliance reviews using **Access Review Workflows** – a product to collaboratively and periodically certify that the proper authorization controls are working as intended within AWS. For example, ensure permissions on AWS S3 buckets remain appropriate for every account, including service accounts.

- Monitor your AWS environment for policy misconfigurations using **Entity Monitoring** to detect when new IAM roles are created, and determine if remediation actions might be needed, like limiting permissions to reduce the attack surface and potential data breach risks.



Rules

2 Total Rules | Add New Rule | 1-1 of 2

	NAME	STATUS	SEVERITY	LAST TRIGGERED	ALERTS	ACTIONS
+	Tracking AWS IAM role full admin	✓ Active	High	Never		Edit Delete
+	Okta User with Snowflake Access Added	✓ Active	High	04/10/2022 at 01:12		Edit Delete

Effective Permission: Metadata

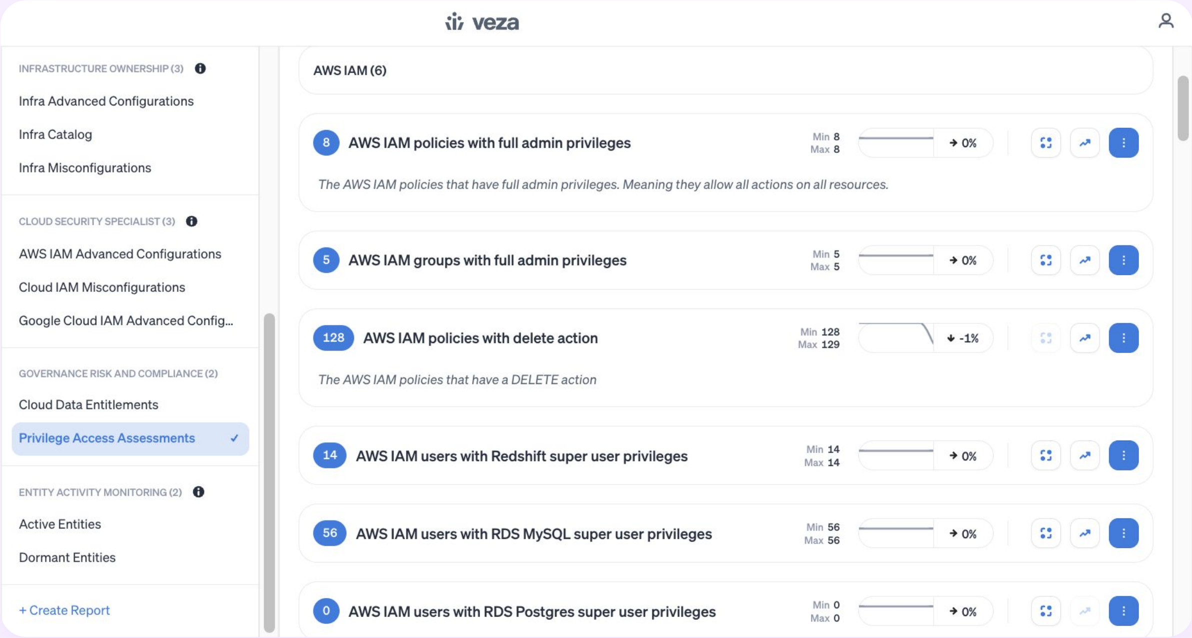
Three quick steps to get started

Veza typically connects to AWS by assuming a role granted with limited, read-only permissions to extract authorization metadata. No additional agents, proxies, or sidecars are required to connect to your AWS environment, adding no risk of downtime and data availability.

1. Create a read-only role in AWS to connect to Veza.

2. Configure a new AWS connection in Veza and optionally select individual services to exclude.

3. Discovery will begin automatically - check Veza logs to monitor progress, and start reviewing the **Entity Catalog**, freshly-populated **Dashboards**, and **Reports**.



veza

INFRASTRUCTURE OWNERSHIP (3)

Infra Advanced Configurations

Infra Catalog

Infra Misconfigurations

CLOUD SECURITY SPECIALIST (3)

AWS IAM Advanced Configurations

Cloud IAM Misconfigurations

Google Cloud IAM Advanced Config...

GOVERNANCE RISK AND COMPLIANCE (2)

Cloud Data Entitlements

Privilege Access Assessments ✓

ENTITY ACTIVITY MONITORING (2)

Active Entities

Dormant Entities

+ Create Report

AWS IAM (6)

8 AWS IAM policies with full admin privileges — Min 8 Max 8 → 0%

The AWS IAM policies that have full admin privileges. Meaning they allow all actions on all resources.

5 AWS IAM groups with full admin privileges — Min 5 Max 5 → 0%

128 AWS IAM policies with delete action — Min 128 Max 129 ↓ -1%

The AWS IAM policies that have a DELETE action

14 AWS IAM users with Redshift super user privileges — Min 14 Max 14 → 0%

56 AWS IAM users with RDS MySQL super user privileges — Min 56 Max 56 → 0%

0 AWS IAM users with RDS Postgres super user privileges — Min 0 Max 0 → 0%

It's as simple as that! If you're interested in learning more about how Veza can work alongside your AWS environment and other solutions to simplify data access permissions, check out www.veza.com/platform.

● Sign up for a free trial

About Veza

Veza is the data security platform powered by authorization. Our platform is purpose-built for multi-cloud environments to help you use and share your data more safely. Veza makes it easy to dynamically visualize, understand and control who can and should take what action on what data. We organize authorization metadata across identity providers, data systems, cloud service providers, and applications — all to address the toughest data security challenges of the modern era. Founded in 2020, the company is remote-first and funded by top-tier venture capital firms including Accel Partners, Google Ventures, Norwest Venture Partners, and True Ventures. To learn more, please visit us at veza.com.