CockroachDB

Identity Access Management (IAM)

Identity access management (IAM) is the process of authenticating and authorizing users (or services) to securely access systems and data.

IAM systems are mission critical because they allow users or services to gain access to the right systems and data at the right time. This use case is often connected to user metadata since they both deal with the management of user activity.

Usually IAM comes in two forms: authentication or authorization. Authentication verifies the identity of a user/service, whereas authorization allows the user/service to gain access to parts of a system and data. This use case requires a database that can deliver fast, consistent access to users regardless of their location.

Challenges

IAM systems cannot go offline because the business impact is too substantial. Every minute that authentication or authorization systems are down, the company loses money and their customers' trust. Even planned downtime for maintenance or software upgrades is unacceptable, since many businesses serve a global audience spanning different time zones.

Catering to global users also creates challenges when it comes to maintaining high availability. You want your database to be physically located close to users for fast access, yet you also need to make sure that you replicate your authentication data to a backup region. In the event of a node, zone, or region failure, chaos can ensue.

Additionally, data inconsistencies can cause major security issues when authorizing users (i.e. the right permissions aren't attached to their profile). As you continue to scale the volume of users, more inconsistencies can be introduced if you aren't using a resilient database system that guarantees data correctness through synchronous data replication.

Database requirements

Because most IAM systems cater to users or systems that are distributed in different locations, they require a database that can span multiple regions and/or data centers and have the ability to domicile data in a particular location to aid with compliance. A multi-region database also allows you to maintain high availability in the event of a total region failure.

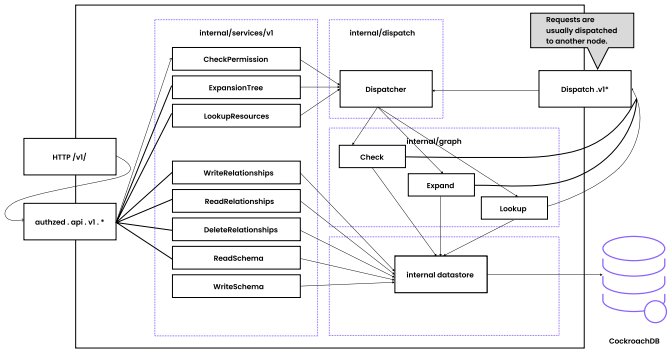
Additionally, IAM systems must be able to handle an increase in users and/or services added to the system. They require a distributed database that can seamlessly adapt to an uptick in workloads without causing outages or the need for complex manual sharding configurations. Even as you scale, your data must always be consistent, which requires a database with ACID guarantees to ensure data integrity is maintained.

Why CockroachDB for identity access management?

IAM systems require CockroachDB's built-in replication, geo-distribution, and ACID guarantees to quickly authenticate and authorize secure access to systems and data anywhere, every time.

Reference architecture

This diagram is a high-level overview of a SpiceDB deployment (an open-source system for managing security-critical app permissions with CockroachDB as the distributed backend store). The request is handled by the dispatch interface and persisted into the datastore.



SALTO

Customer Story: Salto's IAM system powered by CockroachDB

SALTO is a leader in cloud-based access management technology and needed a highly available database to back their user access management system.

They previously built systems on SQL Server where they often experienced downtime for schema changes/database upgrades, and knew they were at risk for outages on an active-passive system. They built a new product from scratch on CockroachDB which runs across 3 regions and delivers 24/7 availability on an multi-active system. They no longer need to take the database offline for maintenance and were able to simplify their architecture by leveraging CDC.

> *"We wanted to decouple the developer from the infrastructure team. We didn't want to make the developer responsible for knowing that there's a difference between primary, failover, or read replicas. We just wanted them to use the database; that's all... we were impressed with how CockroachDB just worked."*

Gorka Lerchundi
Engineering Manager & Tech Lead

To learn more about Salto's use case and read other customer stories, visit cockroachlabs.com/customers ↗