WEST

Summit & Awards

20 YEARS

Safely in Command: Engineering Access in AWS

Ryan Breidenbach

Senior Director of Architecture

Invitation Homes

Nominee Showcase Presentation

Company Overview

- Invitation Homes is the nation's premier single-family home leasing company, meeting changing lifestyle demands by providing access to high-quality, updated homes with valued features such as close proximity to jobs and access to good schools.
- Inventory – Over 85,000 homes
- Employees – Approx. 1600
- Annual Revenue - $2.2B
- Operations - National
  - Washington, California, Nevada, Arizona, Texas, Georgia, Florida, Carolinas, Illinois & Minnesota
- The company's mission, "Together with you, we make a house a home," reflects its commitment to providing homes where individuals and families can thrive and high-touch service that continuously enhances residents' living experiences.

Presentation Overview

How can we allow our Engineering teams to ***safely*** run and support their Cloud applications?

- Role-based access groups + Attribute-Based Access Controls
- Add custom permissions to roles as necessary
- Application-specific support policies + permission boundaries + security policies

Presentation Slide

Context: Invitation Homes was "born in the cloud," but at the start of 2022 we were still not "cloud native." In January of 2022:

- Most applications in our cloud had tradition architecture
- We did not have any serverless applications
- Most deployments required assistance from our Cloud team

But all of this was about to change...

Presentation Slide

Phase 1 – Leverage AWS resource tagging and Attribute-Based Access Controls (ABAC) paired with Azure AD federated access to AWS.

- Create AWS Identify Profiles whose membership was mapped to Azure AD groups.
- Standardized **Owner** tag for all AWS resources.
- Use ABAC to control which teams could access which resources.

Challenge Encountered: *This scaled well, but not all AWS resources supported ABAC..... Interesting twist that could impact the plan.*

Presentation Slide

Phase 2 – Supplement out-of-the-box policies with custom permissions as needed.

- Since ABAC support was inconsistent across AWS resource types, we also added custom permissions to roles associated with the Identity profiles as needed.

This filled the gaps when permissions could not be granted using ABAC. However, this process was manual and required support from Cloud team for each change.

Challenge Encountered: *Still not at the low friction process envisioned..... Another interesting twist that could impact the plan.*

Presentation Slide

Phase 3 – To make it easier for teams to define permissions necessary for application support:

- Introduced custom IAM policies that are attached to the roles associated with the Identity profiles.
- Added permission boundaries to prevent privilege escalation
  - Enforced on new users and roles as well. No Permission > Creator
- Defined Sentinel policies that require approval from Cloud team before attaching a support policy to a role.

Pivotal Solutioning: *The simple yet effective process to bring stability and provide the key controls needed for success.*

Presentation Slide

Where Are We Today?

- Close to 350 serverless functions running production, supporting dozens of individual services.
- Cloud team in the role of "Innovator and Advisor" instead of gate keeper.
- Continuing to evolve our strategies of how to let teams safely support their applications (e.g., break-glass emergency support role).

Lessons Learned/Best Practices

How to go from no cloud-native capabilities to dozens of serverless applications running in production in less than two years?

- Security can't review every change. To scale, you must provide a framework for engineers to follow and guardrails to keep the enterprise safe.
- Partnerships between engineers and security team members is critical.
- Infrastructure-as-code (IaC) is necessary for consistent and safe delivery of cloud applications.
  - Offers patterns to replicate best practices & provides an audit trail.