



Implementing Identity Management on GCP

Learn to Solve Customer and
Workforce IAM Challenges on GCP

Advait Patel
Saai Krishnan Udayakumar
Hariharan Ragothaman

Apress®

Implementing Identity Management on GCP

**Learn to Solve Customer
and Workforce IAM Challenges
on GCP**

**Advait Patel
Saai Krishnan Udayakumar
Hariharan Ragothaman**

Apress®

Implementing Identity Management on GCP: Learn to Solve Customer and Workforce IAM Challenges on GCP

Advait Patel
Software Engineering, Broadcom,
Glenview, IL, USA

Saai Krishnan Udayakumar
Washington, WA, USA

Hariharan Ragothaman
Massachusetts, MA, USA

ISBN-13 (pbk): 979-8-8688-1696-3
<https://doi.org/10.1007/979-8-8688-1697-0>

ISBN-13 (electronic): 979-8-8688-1697-0

Copyright © 2025 by Advait Patel, Saai Krishnan Udayakumar and
Hariharan Ragothaman

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Aditee Mirashi
Coordinating Editor: Jacob Shmulewitz

Distributed to the book trade worldwide by Springer Science+Business Media New York, 1 New York Plaza, New York, NY 10004. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a Delaware LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at <http://www.apress.com/bulk-sales>.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub (<https://github.com/Apress>). For more detailed information, please visit <https://www.apress.com/gp/services/source-code>.

If disposing of this product, please recycle the paper

*To my parents, **Nikunj and Rajesh Patel**, for your unwavering love and belief that shaped the person I am today; to my wife, **Charmi Patel**, for your constant strength, support, and faith in every step of my journey; to my uncle, **Prashant Patel**, whose guidance and steadfast presence have been a quiet pillar of strength throughout my life; and to my son, **Avyakt Patel**, may this work be a part of the legacy I build for you, with all the love and hope a father holds for the future.*

—Advait Patel

*To my son **Darsh Krishnan** whose smile keeps me going; and to my wife **Ramya Sudarsan** for being my pillar through every high and low.*

—Saai Krishnan Udayakumar

*To my mother, **Jayalakshmi Ragothaman**, whose love continues to guide me; to my wife, **Aishwarya Murali**, my steadfast anchor; and to **Beacon**, whose joy brightens even the darkest days.*

—Hariharan Ragothaman

Table of Contents

About the Authors.....	xi
About the Technical Reviewer	xiii
Acknowledgments	xv
Introduction	xvii
Chapter 1: Introduction to Identity and Access Management on Google Cloud Platform.....	1
Overview of Identity and Access Management.....	1
Benefits of IAM	3
IAM in Modern Organizational Environments	4
Future Directions of IAM.....	4
Overview of IAM on GCP	5
Identities.....	5
Resources.....	6
Roles.....	7
Policies	7
Real-World Significance of IAM	8
IAM Use in Fintech: Fostering Security and Compliance	8
Use of IAM in Healthcare to Protect Patient Data and Enable Continued Access	9
IAM in Gaming to Enhance User Experience and Address Cheating.....	10
Tools Required	11
Emerging Trends	12
References.....	14

TABLE OF CONTENTS

Chapter 2: Managing Roles, Policies, and Permissions 17

Types of Roles 17

 Predefined Roles 17

 Custom Roles..... 19

 Basic Roles 20

 Best Practices in Role Management in GCP IAM 21

IAM Policies and Inheritance in the GCP Resource Hierarchy 21

 IAM Policies in GCP..... 22

 GCP Resource Hierarchy..... 22

 IAM policy inheritance 24

 Policy Evaluation in the Resource Hierarchy 24

 Overriding IAM Policies..... 25

 Best Practices for Inheritance and IAM Policies..... 25

Real-World Use Case: Managing Permissions in a Multiproject Organization 26

 Spotify Challenge..... 26

 Solution 27

 Spotify's Outcome 28

Real-World Insights: Lessons Learned from IAM Misconfigurations in Large Enterprises..... 28

References 30

Chapter 3: Advanced IAM Features 33

Using IAM Conditions for Context-Aware Access 33

 IAM Conditions..... 33

 IAM Conditions and Context-Aware Access 34

 Benefits of Using IAM Conditions 36

 Best Practices in IAM Conditions..... 37

Cross-Project and Cross-Organization Access with IAM Policies 38

 Cross-Project and Cross-Organization Access 38

 Enabling Cross-Project and Cross-Organization Access 40

 Benefits of Enabling Cross-Project and Cross-Organization Access 41

 Best Practices for Cross-Project and Cross-Organization Access 42

Implementing Temporary and Time-Bound Access Securely	43
Demand for Temporary and Time-Bound Access.....	44
Strategies for Secure Time-Bound Access	44
Industry-Specific Examples of Context-Aware Access Policies in Healthcare and Education	46
Context-Aware Access in Healthcare	46
Context-Aware Access in Education	47
References.....	48
Chapter 4: Service Accounts and Workload Identity	51
I. Service Accounts: Types and Best Practices	51
Types of Service Accounts.....	51
Best Practices in Service Accounts	55
II. Workload Identity Federation for Secure Service Access.....	57
Benefits of Workload Identity Federation.....	59
Enabling WIF.....	59
Real-World Use.....	60
Implementing Workload Identity Federation.....	61
III. Managing and Rotating Service Account Keys.....	62
Service Account Key Rotation.....	63
Strategies for Key Management.....	65
References.....	67
Chapter 5: Securing API and Workloads.....	69
I. IAM Permissions for API Gateway, Cloud Functions, and Cloud Run	69
IAM Use in Google Cloud.....	69
IAM Permissions in Using API Gateway	70
IAM Permissions for Cloud Functions.....	71
IAM Permissions for Cloud Run	72
Managing Service Accounts	73
Troubleshooting IAM Issues.....	74
II. Service-to-service Authentication Using OAuth2.0 and API Keys.....	74
Service-to-Service Authentication.....	75

TABLE OF CONTENTS

Using OAuth 2.0 for Service-to-Service Authentication..... 75

API Keys for Service-to-Service Authentication 77

III. Real-World Example: Securing an API-Based SaaS Product..... 80

References..... 81

Chapter 6: Automating IAM Policies..... 83

I. Using Terraform to Manage IAM at Scale..... 83

 Setting Up Terraform for GCP IAM Management 84

II. Automating Workflows with Scripts and the IAM API..... 89

III. Real-World Governance Strategies for Large Enterprises..... 93

IV. Pro Tips for Automating Policy Updates Efficiently..... 96

References..... 96

Chapter 7: Auditing and Monitoring IAM Policies..... 99

I. Using Cloud Audit Logs to Track IAM Policy Changes..... 99

 Understanding Cloud Audit Logs 99

 Enabling Cloud Audit Logs..... 100

 Tracking IAM Policy Changes with Cloud Audit Logs..... 100

 Best Practices in Using Cloud Audit Logs to Track IAM Policy Changes 102

II. Setting Up IAM Alerts with Cloud Monitoring 103

 Cloud Monitoring for IAM..... 105

 Requirements for Setting Up IAM Alerts..... 105

 Process of Setting Up IAM Alerts in Cloud Monitoring..... 105

 Advanced Alerting Strategies 106

 Best Practices to Be Used in IAM Alerting Activities..... 107

III. Leveraging Cloud Asset Inventory for Compliance..... 108

 Best Practices to Assert Compliance with CAI..... 111

IV. Case Study: How a Healthcare Organization Uses IAM Monitoring to Meet HIPAA
Compliance 112

References..... 113

Chapter 8: Managing Multicloud and Hybrid IAM.....	115
I. Integrating GCP IAM with AWS and Azure for Hybrid Environments	115
Integration Strategies	116
Best Practices in Securing Multicloud IAM Integration	118
II. Best Practices for Cross-Cloud IAM Governance	120
Implementation of Centralized Identity Provider (IdP)	120
Principle of Least Privilege	120
Standardization of IAM Policies on Different Cloud Platforms.....	120
Monitoring and Auditing Cloud Access Practices	121
Secure Service Accounts and Workload Identities	121
Emergency Access Planning Activities	121
Automating IAM Compliance Checks.....	122
III. Challenges and Solutions in Managing Multicloud Access	122
Identity Fragmentation and Siloed Access	123
Inconsistent Permission Models.....	123
Lack of Centralized Auditing and Compliance	125
Managing Service Accounts and Machine Identities.....	125
Compliance on Various Jurisdictions.....	126
IV. Emerging Trend: The Role of Zero-Trust Architecture (ZTA) in Hybrid Cloud Environments	127
Key Strategies to Use	128
References	129
Chapter 9: Securing Sensitive Data with IAM.....	131
I. Managing Access to BigQuery, Cloud Storage, and Spanner	131
Fundamentals in IAM for BigQuery, Cloud Storage, and Spanner	131
Handling Access to BigQuery	132
Handling Access to Cloud Storage.....	134
Handling Access to Cloud Spanner.....	136
Auditing and Monitoring Access	138
II. Using Customer-Managed Encryption Keys (CMEK) for Data Security in Google Cloud.....	138
Implementing CMEK Across Key GCP Services	139
Best Practices for Managing CMEK.....	140

TABLE OF CONTENTS

III. Fine-Grained Access Control for Sensitive Resources 141

 Best Practices for the Implementation of Fine-Grained Access 142

IV. Industry-Specific Use Case: Protecting Healthcare Records with CMEK and IAM..... 143

References..... 144

Chapter 10: AI-Driven Identity and Access Management..... 147

 I. Introduction to AI in IAM..... 147

 AI in Cloud Security 147

 Benefits of Using AI in IAM 148

 AI-Driven IAM Tools in GCP 149

 II. Anomaly Detection with AI 149

 Using Policy Troubleshooter and Cloud Audit Logs with AI 150

 III. Automating Policy Management with AI..... 151

 AI-Based Policy Recommendations in GCP 152

 Predicting Least Privilege Access Using Historical Data 153

 Real-World Example: Automating Role Assignments in a Multi Project Organization 153

 Implementing AI-Driven Policy Management 154

 IV. AI-Powered Identity Verification 155

 Leveraging AI Tools for Biometric Verification 155

 Automating Identity Verification Workflows..... 156

 Use Case: Implementation of AI-Enhanced Multifactor Authentication 156

 V. Ethical Considerations in AI-Driven IAM 157

 Addressing Bias in AI Models for Identity Management..... 157

 Ensuring Transparency and Fairness in AI-Driven Access Control 157

 Aligning AI with Compliance Standards..... 158

 VI. Emerging Trends and Future Directions 158

 Predictive IAM: Proactive Access Basing on Behavioral Patterns..... 158

 AI-Enhanced Zero-trust Frameworks 159

 Real-World Case Study: Using AI-Driven IAM at a Global Enterprise 161

References..... 161

Index..... 163

About the Authors



Advait Patel is a skilled senior site reliability engineer based in Chicago, with a passion for leveraging technology to drive impactful solutions. With extensive experience in cloud computing, cloud security, and cybersecurity, he currently works at Broadcom, where he plays a key role in managing, building, and securing multimillion-dollar revenue-generating products. Advait is also an advocate for professional growth and is eager to share his expertise with the next generation of tech talent through community involvement and mentorship. In his free time, he enjoys connecting with like-minded professionals and exploring innovative developments in the tech industry.



Saai Krishnan Udayakumar is a seasoned software engineer and cybersecurity practitioner based in Seattle, with more than a decade of experience building secure, scalable identity and access management systems. At a Fortune 500 enterprise, he leads critical initiatives in access governance, compliance automation, and platform security—safeguarding large-scale, high-impact infrastructure. Saai actively contributes to the broader tech community through his involvement in professional societies, technical peer reviews, and global speaking engagements. Passionate about bridging security, engineering, and operations, he enjoys mentoring emerging talent and exploring advancements in identity and cloud security.

ABOUT THE AUTHORS



Hariharan Ragothaman is a seasoned senior software engineer with more than a decade of experience architecting scalable systems across embedded platforms, cloud-native environments, and AI-powered infrastructure. At Advanced Micro Devices (AMD), he leads mission-critical initiatives in data center validation and server-side systems. Previously, he contributed to DevSecOps transformations at Athenahealth and played a key role in launching flagship consumer audio products at Bose Corporation.

He earned his MS in electrical and computer engineering at Northeastern University and his BE at Anna University. Hariharan thrives at the intersection of embedded software, distributed systems, robotics, and DevSecOps—solving high-impact technical challenges through principled system design and execution.

In parallel with his industry work, Hariharan actively contributes to academic and research communities. He has authored peer-reviewed publications in leading IEEE conferences and journals, with interests spanning edge computing, secure AI systems, and resilient infrastructure. He reviews for top-tier venues including AAAI, NeurIPS, ICLR, ICML, IJCAI, IJCNN, iLRN, SoftwareX, and the Journal of Open-Source Software. A recognized thought leader, Hariharan has delivered talks at ACM, OWASP, Conf42, SwampUP, and IEEE events. He frequently serves as a mentor and judge at global hackathons hosted by MIT, UC Berkeley, and Boston University.

His work has earned several accolades, including the Global InfoSec Award for Cybersecurity Identity Governance at RSA Conference 2025, multiple Awards of Excellence at Bose, and induction into the Athenahealth Hall of Fame.

About the Technical Reviewer



Aparna Achanta is a security architect and leader at IBM Consulting with extensive experience driving mission-critical cybersecurity initiatives, particularly in federal agencies. She has successfully implemented cybersecurity frameworks like zero trust and security by design for federal clients, strengthening the security posture and enhancing data protection and security standards across cloud applications. Her leadership has resulted in the establishment of security review boards, secure development practices, vendor evaluations, threat modeling, vulnerability management, code scanning, observability,

and performance monitoring to ensure that enterprise comply with stringent federal guidelines.

Aparna specializes in securing emerging technologies in federal agencies, including low-code, no-code applications, and generative AI applications.

Aparna is a member of the Forbes Technology Council. She shares valuable insights on generative AI security challenges, contributing to industry discourse. A passionate advocate for women in tech, Aparna is a founding member and speaker at the WomenTech Network, where she inspires and empowers more than 140,000 women with talks on cybersecurity career growth. She is also an executive board member at the Austin chapter of Women in Cybersecurity (WiCyS) and an advisory board member at George Mason University's Center for Excellence in Government Cybersecurity Risk Management and Resilience.

Aparna was named to the list of 40 Under 40 in Cybersecurity by TopCyber News Magazine for her contributions to the cybersecurity community.

Acknowledgments

We would like to express our sincere gratitude to **Aditee** and **Nirmal** from the Springer Nature publication team for their invaluable support, patience, and guidance throughout the publishing process. Their attention to detail, responsiveness, and encouragement made this journey both smooth and rewarding.

A heartfelt thank-you to **Julie Ann Davis** for her unwavering support and encouragement, which played a key role in bringing this book to life.

We are especially grateful to **Aparna Achanta** for her thoughtful and constructive review of the manuscript. Her insights helped refine our ideas and elevate the clarity and impact of this book.

To our families, friends, and mentors—thank you for the love, inspiration, and belief in us throughout this journey. Your presence has made all the difference.

And to **Beacon**, for reminding us to pause, play, and be present.

Introduction

Security is no longer a background process; it's a strategic priority in a world where digital transformation is what sets businesses apart. Companies in every field are moving to the cloud to grow quickly, but this raises an important question: who should be able to see what, and how do we make sure it's safe?

Identity and Access Management (IAM) on Google Cloud Platform is where this book starts to tackle this problem. IAM is more than just a technical standard; it's the plan for building trust online. If you work in IT, security, or cloud architecture, you need to know about IAM to protect your infrastructure, make sure you're following the rules, and let innovation happen without compromising security.

We explain the basic ideas behind IAM, look at its most important parts, and talk about how it is becoming more important in a wide range of real-world fields, from healthcare to fintech. You'll learn about how IAM affects cloud strategies today and why GCP is a strong, flexible platform for putting them into action.

Let's look at the "why" behind the "how" before we get into policy settings and command-line tools. In the world of cloud security, knowing the lay of the land is just as important as getting around it.

CHAPTER 1

Introduction to Identity and Access Management on Google Cloud Platform

Overview of Identity and Access Management

Identity and Access Management (IAM) contains policies, technologies, and processes that enable organizations to decide who has the right to access resources at different points in the organization. This ensures that the resources in the organization are protected from unauthorized access. Notably, IAM plays an instrumental function in handling user identities, ensuring access controls, and complying with security regulations in contemporary organizations. IAM has key components that help in administering the organization, as summarized in Figure 1-1.

Key components of IAM include the following:

- **Access management:** IAM ensures that every user can access only the resources that they are authorized to have. The access control policies like role-based access control (RBAC) and attribute access control (ABAC) help to siphon whoever has access to whatever resource on the system, enabling an increased capacity to manage whatever needs are on the system. Additionally, mechanisms that can be used on access management include multifactor authentication (MFA), single sign-on (SSO), and session management.

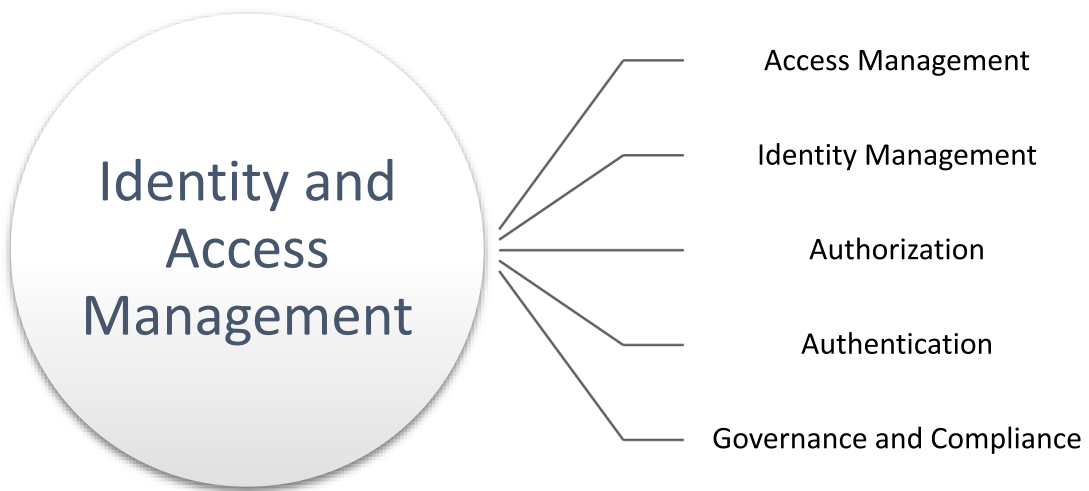


Figure 1-1. *Components of IAM*

- **Identity management:** This is a critical component that helps create user identities. The platform helps with profile management, user registration, and the authentication process to advance the needs of the system (Ghaffari et al., [2022](#)). Thus, identity management ensures that every user has a unique identifier that can help in addressing whatever devices, users, and services can be handled in the organization.
- **Authorization:** This is a key component that determines the actions a user can carry out on the organizational resources. This specifies the access control list policies for the users. Therefore, users have to work based on identities that design and administer critical frameworks of desired components.
- **Authentication:** This component helps in verifying user identities and making sure that users can access a resource. Authentication can be in the form of passwords, tokens, biometrics, and certificates. These methods assist in appropriately managing the platforms (Carnley & Kettani, [2019](#)).
- **Governance and compliance:** This component helps enforce organizational policies. The component helps to affirm access reviews and audit trails mechanisms of reporting. The framework ensures successful modeling of the IAM within the company.