Saviynt

What Is Identity & Access Management (IAM) For The Cloud?

The permanent and official location for Identity and Access Management Working Group is **https://cloudsecurityalliance.org/research/working-groups/identity-and-access-management**

Acknowledgements

Lead Authors

Ravi Erukulla

Ramesh Gupta

Shruti Kulkarni

Alon Nachmany

Contributors

Faye Dixon

Jonathan Flack

Paul Mezzera

Ansuman Mishra

Venkat Raghavan

Heinrich Smit

David Strommer

Reviewers

Samuel Addington

Radhika Bajpai

Shannon Chisenga

Ivan Djordjevic

Shamik Kacker

Claude Mandy

Adnan Rafique

Michael Roza

Nishanth Singarapu

CSA Global Staff

Ryan Gifford

Stephen Lumpe

Contents

Abstract

Identity and Access Management (IAM) is not a novel solution. IAM tools and practices are used to secure digital (and, at times, physical) resources and meet regulatory/ compliance requirements.

IAM was originally intended as a general-purpose mechanism to restrict and control access to organizational resources by granting permissions to authorized identities or groups of identities. The initial goal was to validate entitlement, and access was based entirely on assertions of username and password, coupled with group membership or permissions directly assigned at the resource. This model later evolved to centralize IAM, and access decisions were concentrated centrally at an authority such as a service, server, or identity infrastructure. The threat landscape has materially changed over the years, and today, IAM has become a pivotal component of any digital access model. It has evolved to employ ever-increasing visibility, granularity, and control as the nature of users, resources, and systems change. For instance, roles (RBAC), attributes (ABAC), or other adaptive (or heuristic) access controls, have had distributed or transaction-based access added. The authentication tools and techniques have evolved with the addition of multifactor authentication, passkeys, and digital certificates that considerably strengthens IAM.

IAM today is much more than securing resources or meeting compliance. Due to the recent trends with cloud proliferation, digitalization, and COVID-induced remote and hybrid work, IAM has become a business enabler and often the first line of defense for cybersecurity. IAM is the first phase in an organization's Zero Trust journey, which is often a board-level initiative. As organizations undergo cloud transformation and follow cloud-first approaches, IAM needs and practices must evolve to catch up with the new dynamics of the cloud environment.

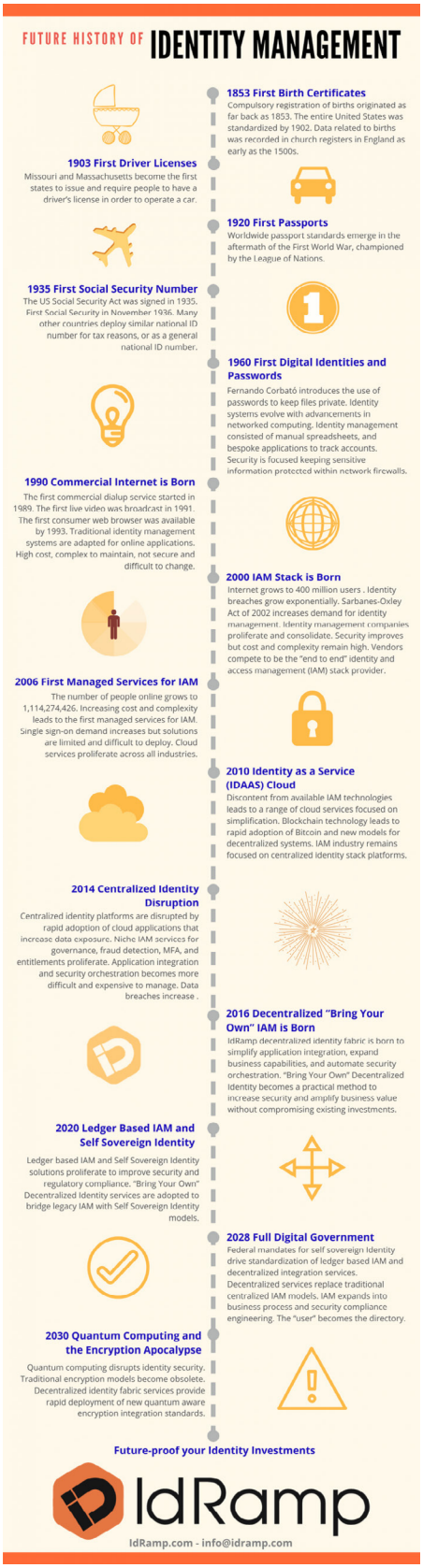

Figure 1 - Credit: IDRamp

Traditional IAM practices for on-premises environments do not suit cloud environments, which can be much more ephemeral, agile, and accessible beyond corporate boundaries. However, not all IAM teams/practitioners understand and follow the best practices with IAM for the cloud environment, leading to suboptimal value, increased costs, and reduced satisfaction.

In this article, we aim to provide an overview of:

- The differences between cloud environments vs. on-prem that affect IAM
- The factors that affect IAM, how IAM has evolved to solve them, and how it is going to further evolve in the future
- The ever-increasing significance of IAM in a cloud environment
- Challenges faced by organizations when adopting IAM effectively for the cloud
- Considerations and best practices for an effective IAM program for cloud environment
- Tips for Security/IAM leaders and practitioners on communicating the value of IAM

Introduction

Identity and Access Management (IAM) is a critical component of any organization's technology stack and security infrastructure, particularly in the cloud. The primary audience for this document is IAM program leads and security operations teams, with a secondary audience of Chief Information Security Officers (CISO) and senior leadership. The purpose of this document is to provide an understanding of the challenges and considerations involved in managing IAM in the cloud, as well as the importance of IAM to an organization's overall security strategy.

The Differences Between Cloud Environments vs. On-Premises Affecting IAM

Ownership is one fundamental difference between an enterprise using a cloud-delivered IAM solution versus managing IAM in an on-premises environment. When an organization deploys an IAM solution on-prem, the deploying organization owns everything, including software licenses and user administration; the responsibility for the ongoing capital expenses associated with an IAM solution, such as hardware (e.g., server purchases), power consumption, and physical space; and all the other expenditures required to sustain the infrastructure required to support an internally managed IAM solution. Customers build applications leveraging the CSP IAM using a shared responsibility model with a subscription model.

Another basic distinction between using a cloud-based IAM solution versus deploying an on-prem IAM solution is control. In an on-premises deployment, organizations manage all aspects of IAM including vulnerability management, patching, penetration testing, and so on. When a service like Infrastructure-as-a-Service is procured from a cloud service provider (CSP) by an organization the procuring organization does not need to factor vulnerability management, patching, and so on, as these aspects of “cloud security” are taken care of by the CSP.

The bigger challenge and complication of using cloud IAM is the proliferation of cloud environments procured by an organization. When an organization runs several Infrastructure-as-a-Service environments, Platform-as-a-Service procurements, and Software-as-a-Service, IAM gets complex and challenging. Provisioning of identities in each environment may be simple but access control reviews and deprovisioning of identities may not be, potentially leading to leavers retaining access to the environments.

Retrospective analysis of IAM

As noted earlier, IAM is not a novel solution. It has been around since the mainframe era but became a more prominent discipline during the client/server era, where applications became more distributed and contained their identity silos. Every user and entitlement had to be managed with the application, which greatly contributed to the proliferation of many user identities and passwords required to access these applications.

Directory services were designed to address this problem by providing centralized user repositories, along with an access protocol called Lightweight Directory Access Protocol (LDAP). Directory services enabled same sign-on across multiple platforms, including operating systems, databases, and web servers. During this time, Microsoft's Active Directory became the corporate standard for managing computers, as well as providing an architecture to manage users, groups, and access policies. During the early days of the Internet, the problem with multiple credentials and sign-on was exacerbated, so Single Sign-On (SSO) was developed to facilitate authentication and authorization of users across an organization's applications, leveraging an LDAP directory in most cases as the identity store.

In addition, the problem of managing user lifecycle management and access policies was mostly automated through custom-built applications, which eventually became productized as user provisioning and administration solutions. Governance features were also required to address regulatory requirements and eventually converged with identity administration and provisioning solutions to become what is now known as Identity Governance and Administration (IGA). Over the last decade, these solutions have been offered as cloud solutions that leverage all the benefits of the cloud, including maintaining IAM platforms, which in many cases required specialized resources to maintain. To further streamline IAM use cases and deployments, and reduce the costs and burden associated with implementing a multitude of solutions, solutions are converging to provide a combination of IAM solutions, such as Identity Governance and Administration (IGA), Privileged Access Management (PAM), and Customer Identity and Access Management (CIAM).

Where IAM Is Headed

Given today's data economy, the proliferation of cloud-based solutions, and digital transformation by organizations that is further accelerated by the shift to hybrid and remote work scenarios, many organizations are taking a more aggressive cloud-first strategy when adopting applications and security solutions. Moreover, cloud platforms implement IAM solutions to manage users and entitlements, which are unique to each platform. IAM in the cloud introduces a whole set of identity actors that are endemic and native to the cloud, such as machine identities, service accounts, workload identities, and human identities. Key trends include:

- Adoption of Decentralized Identity Models: Blockchain and self-sovereign identity models, where users control their own identity data, could become more mainstream, providing an alternative to traditional centralized identity providers.
- Just-In-Time and Risk-Based Access Controls: Instead of granting broad and long-lasting permissions, organizations may increasingly adopt methods that provide access only when it's needed and for as long as it's needed. Additionally, access decisions may be made based on the risk level of the user and the requested resource.

Many organizations struggle to have the right visibility and management of their users and entitlements. These are more commonly spread across several cloud platforms, in addition to the management of the cloud services that implement a more ephemeral set of workloads that are typically instantiated by DevOps tools. IAM solutions must include managing access across cloud services such as containers, serverless infrastructure, and DevOps and CI/CD tools that all require access policies to function.

IAM for the Cloud Environment

Managing IAM in the cloud presents unique challenges compared to on-prem environments, including volatility and faster growth, the need for agility, and different risks related to compliance and other issues. One key difference is the increased use of APIs in cloud environments, as opposed to the group policy-based approach often used in on-prem environments. These differences in technology and approach require a shift in mindset and the adaptation of on-prem practices to the cloud.

The Ever-Increasing Significance of IAM in a Multi-cloud/Hybrid Environment

Cloud technology provides numerous benefits to an enterprise, such as pay-as-you-go, quick implementation, Opex vs. Capex, and scaling resources up and down in minutes, just to name a few. Due to this, we have seen enormous growth in cloud implementation during the last several years. It is both at the enterprise level as well as the consumer level. In the journey to the cloud, enterprises are still using resources in a hybrid model (some resources on-prem, some in cloud) and even adopting multi-cloud strategies to take advantage of the best-in-breed solution.

Having resources moving to the cloud, both human and non-human entities need to be authenticated and authorized to use these resources from anywhere, anytime, and with the right set of privileges. At the same time, these resources become more vulnerable to adversaries as resources are no longer in your network perimeter. You need to ensure that entities have the right access to the right resources.

Users need to access various scattered resources in a multi-cloud environment. How do you ensure that the user has appropriate access to the right resources? How do you manage their entitlement? Service accounts and machine identities need to run separate automated processes connecting to different workloads in a multi-cloud environment. How do you manage such identities and their entitlements? A good IAM strategy for a cloud environment is the answer to these questions.

Importance of IAM to Senior Leadership

IAM plays a critical role in protecting an organization's assets and data. Senior leadership should be aware of the value of IAM in reducing risk, enabling compliance, and supporting the organization's overall security strategy. IAM teams can help present this value by highlighting the benefits of cloud migration, such as improved multi-cloud visibility and the ability to maintain visibility into the state of role assignments and alerts on changes.

Challenges Organizations Face When Adopting IAM Effectively for the Cloud

Top 10 Challenges in Identity

1. Managing identities across multiple cloud environments
2. Threat materialization in cloud-based Identity Providers
3. Ensuring compliance with regulations and standards
4. Managing identities for non-human entities
5. Integration with emerging trends
6. Keeping pace with the ever-evolving threat landscape
7. Managing identities for external users and partners
8. Addressing the unique challenges of BYOD and Identity
9. Managing identities for IT/OT, that are located on-premises, but interface with cloud-based solutions
10. Maintaining visibility and control over role bindings and access controls

For a closer look at the top Identity challenges, check out our blog titled **"Navigating the Top 10 Challenges in Cloud Identity and Access Management."**

Cloud IAM Opportunities

IAM is the glue that binds Cloud services. A responsible and well-thought-out cloud IAM strategy opens up tremendous business opportunities and facilitates more agile responsiveness to new business requirements.

a. Accelerate digital transformation initiatives

b. Drive new business model innovation

c. Accelerate the transition to a data economy

d. The automation potential of cloud IAM delivers tremendous productivity for developers and builders

e. Reduce operational cost

f. Streamline compliance and governance

Considerations and Best Practices for an Effective IAM Program for Cloud Environments

In cloud environments, the considerations and best practices for an effective IAM program may differ from traditional on-prem environments. Some of the important considerations are:

- Centralized management of identities, access and authorization across multi-cloud and hybrid environments
- Automation and integration with existing systems
- Robust and secure authentication methods
- Authorization and access control policies based on user roles and attributes
- Regular monitoring and auditing of access and activities
- Compliance with data protection regulations
- Integration with other security measures such as encryption and threat protection
- Apply least privileges as much as possible and need-to-know basis rules
- Leverage advanced features such as Just-in-Time (JIT), PAM, and Privileged Identity Management (PIM)
- Automate IAM processes
- Comprehensive monitoring and auditing

To effectively implement an IAM program in a cloud environment, it is important to follow best practices such as:

- Implementing multifactor authentication to secure access
- Creating and enforcing strong password policies
- Wherever possible shifting from strong passwords to passwordless
- Implementing role-based access control (RBAC) for users and applications
- Encrypting sensitive data (including credentials) in transit and at rest
- Regularly monitoring access and activity logs for anomalies and security incidents
- Continuously assessing and updating security policies to stay up-to-date with the latest threats
- Understanding that IAM in a cloud environment directly impacts cloud data security

Tips for Security/IAM Leaders and Practitioners on Communicating the Value of IAM

- Clearly articulate the business benefits of IAM, such as improved end-user experience, seamless Single Sign-On, improved security, compliance, and efficiency.
- Provide tangible examples of how IAM has helped other organizations achieve their security goals.
- Use data and metrics to demonstrate the ROI of your IAM program.
- Communicate the importance of IAM as a critical component of the organization's overall security strategy.
- Provide training and education to all employees to ensure that they understand the importance of IAM and their role in keeping the organization secure.
- Foster a security culture within the organization and encourage employees to report any security concerns.
- Regularly communicate updates and progress on the IAM program to all stakeholders.

Conclusion

In conclusion, managing IAM in the cloud presents unique challenges and considerations compared to on-premises environments. Organizations need to have a clear strategy in place to address these challenges and ensure the security of their assets and data. IAM teams should work closely with senior leadership to communicate the value of IAM and its role in the organization's overall security strategy. Additionally, organizations should have processes in place for monitoring and verifying identities, and be aware of the unique challenges that come with managing identities for both human and non-human entities.