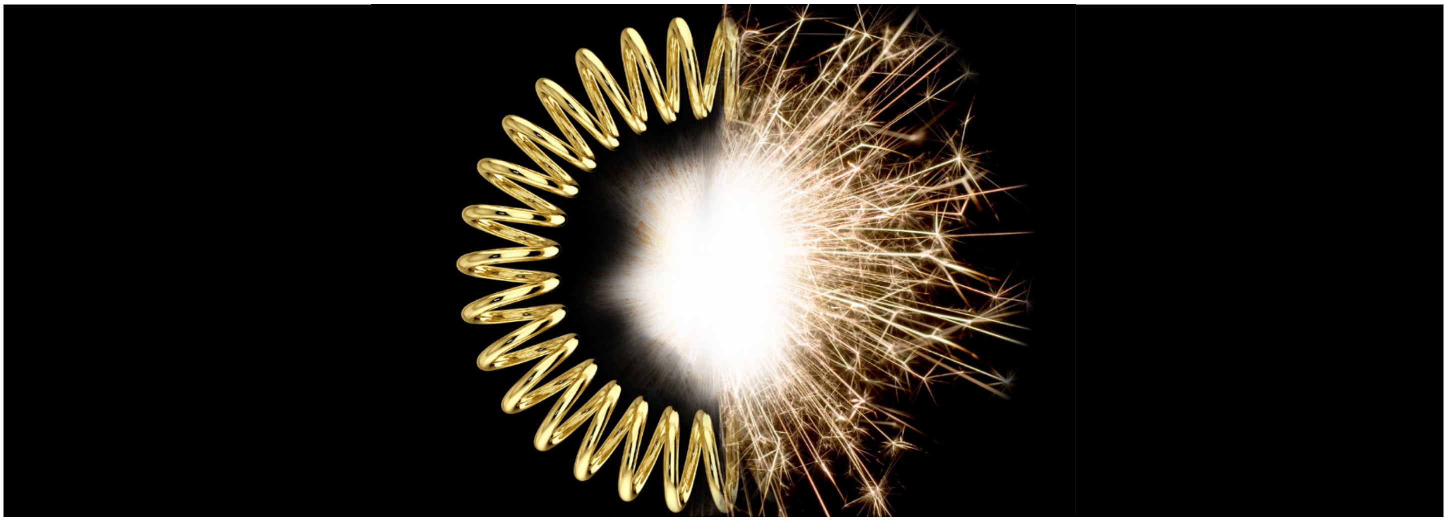


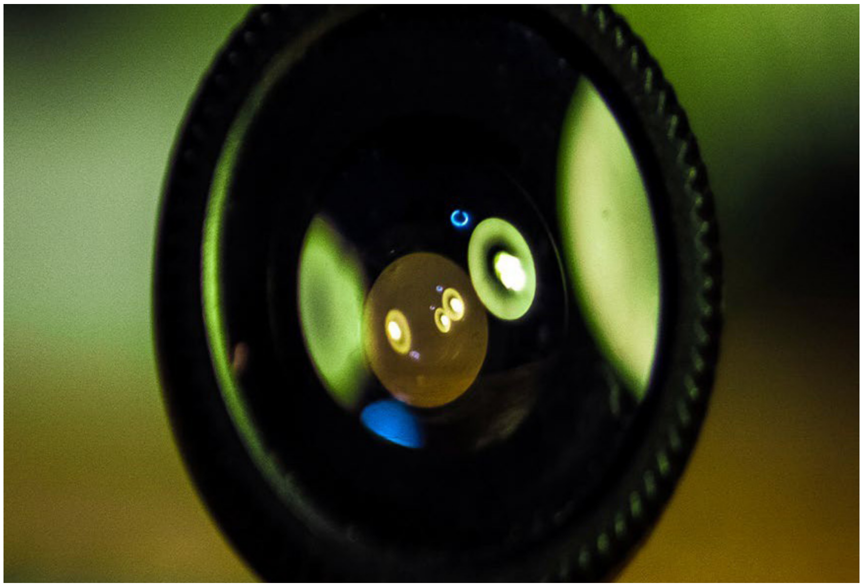
Cloud and Identity and Access Management

How to do Identity and Access Management in Amazon Web Services

Identity and Access Management (IAM)—A challenge

Access is the gateway to the crown jewels of an organization. Access controls form an important line of defense to protect these assets against inappropriate access. It is essential to address the principle of least privilege and separation of duties while granting the minimum required access only when it is needed.

A sound IAM strategy is also fundamental for an effective migration to the cloud as it provides for an integrated access solution that is cost-effective, agile, and highly flexible to rapidly enable new authentication methods.



Since the inception of cloud adoption, the requirements of digital businesses have grown significantly and so has the Amazon Web Services (AWS) service catalog to address those requirements. New services such as the Internet of Things (IoT) have driven expansion in identity and device proliferation. With regard to IAM, this expansion has resulted in additional user types, along with new authentication and access methods that can help AWS meet a wide range of clients' requirements and get new services to the market promptly.

The wide variety of people requiring access, complex access control policy management, and lack of standards-driven authentication solutions often leads to technical challenges for IAM administrators. For example, not being able to create access policies that do not also lock out authorized users or grant excessive permissions.

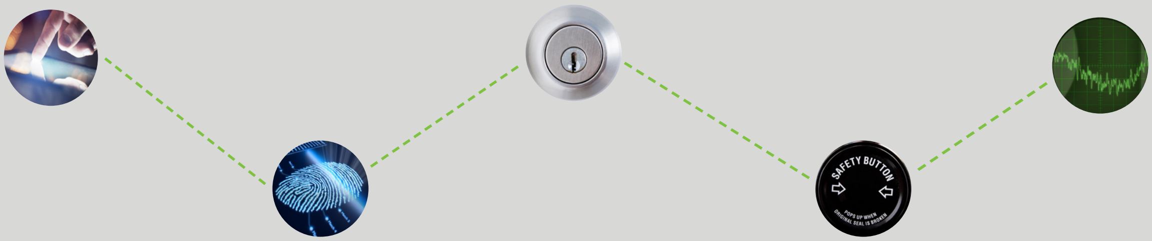
Even though AWS has added many features and services to bolster its IAM capabilities, IAM administrators still face a steep learning curve to work with this powerful yet complex array of functionalities, which can lead to gaps in security fabric due to weak planning, higher overhead, manual processes, and lower agility due to the complex IAM system.

Deloitte’s approach to IAM

In order to help organizations better address the complexity of current identity requirements as well as to empower them to effectively plan the implementation of identity products, our Cyber Risk team has developed a broad IAM security framework. This framework consists of the five distinctive yet complementary domains of identification, authentication, authorization, access governance, and accountability.

The IAM security approach is tied to Deloitte's Cyber framework, which supports traditional on- premise implementations as well as public, private or hybrid cloud deployments. AWS Organizations is a service that can be used to apply IAM policies, roles and permissions across multiple AWS accounts to multi-account customers.

IAM Domains



Describes a process by which a user, program, or device claims to have identity

Identification

Authentication

To gain entry into a system an user or program is required to present a set of credentials like a password or authentication token

After authentication, system determines via comparison to a stored access control matrix if the user has privileges to perform the requested action

Authorization

Access Governance

Process and procedures that are required to request, approve, grant, manage and audit access.

The user or program accessing the system should be held accountable for the actions taken within the system

Accountability

Identification

Identities form the basis for identification. They are a digital map of a user and are comparable to fingerprints. Like fingerprints are unique to each person, similarly an identity is unique to each individual. These identities have to be created and managed properly by organizations as Authentication, Authorization, Access Governance and Accountability are enforced using them.

In the AWS environment, the first required identity is the root user account. This user is created during the account creation process, and gains access by signing in with the username and password that was used to create the account. Special care should be taken when defining the registered email as a distribution list so that messages from AWS will not be missed. The root user has complete control over the environment and there is no way to restrict permissions for this account. Malicious access to this user account could result in the complete compromise of all information and resources. Consequently, it is critical to secure the root user account properly. Use of the root user account must be strictly controlled and limited to activities that can only be performed by someone that requires root access.

To determine that root accounts are properly secured, a centralized AWS account creation and root account management strategy should be developed. This centralized team should create all AWS accounts, retain control of the root access, and monitor for the creation of unauthorized AWS accounts. The first thing that the centralized team should consider to protect the root account is to apply multi-factor authentication (MFA). The root account should never be used for administering the AWS environment. There are only a few functions that should be performed as root.

Organizations with multiple AWS accounts will need strategies and procedures to manage multiple accounts properly. The AWS Organizations service can help to apply polices across multiple accounts.

Authentication

Authentication is the act of a user, process, or device proving who they are.
After the root account is secured, IAM user accounts must be created for all personnel who will be responsible for implementing and operating the AWS infrastructure. The leading practice is to integrate AWS with an internal directory service using Security Assertion Markup Language (SAML)-based single sign-on (SSO). AWS offers services such as Cognito and AD Connector, which could be leveraged to accomplish this integration with an existing user directory. Users are then granted access to AWS using role-based access control methods. Users with privileged or elevated access also need to have MFA enabled for their account access. This practice allows the AWS customer to retain full control over users and permissions in AWS. Existing governance practices like onboarding, off boarding, and access reviews can be used to grant and revoke access to the AWS resources.

MFA provides a higher level of assurance that a user is who they claim to be. For public cloud services, strong authentication using MFA is an important component for identity proofing.

Many organizations should be able to leverage their existing infrastructures and processes for account onboarding, off boarding and access governance for the cloud. This process involves setting up a trust between your IT environment and the cloud services provider, referred to as Federation.

AWS Application Programming Interface (API) access is authenticated using an access key and secret key. A method to periodically rotate these keys is required to reduce the risks of keys being used by an unauthorized actor.

For operating system (OS) access management, a leading practice is to leverage an existing directory service, join all virtual instances to this domain, and grant users access rights and permissions based on directory attributes, such as group membership. Customers can use a directory that is completely on-premise and connect using SAML and Identity Provider (IdP). However, if desired, there are numerous ways in which customers can run a directory service on AWS. This could be accomplished using AWS Simple Active Directory (AD), AWS Managed AD, AWS AD Connector, or a self-deployed directory service on Amazon Elastic Compute Cloud (Amazon EC2) instances. If Secure Shell (SSH) is used for OS access, a method of managing SSH private keys is required.

Without this key management, OS access could be lost without the private key. The SSH private keys should be rotated on a periodic basis.

Application layer access management can leverage directory services or could integrate with the IdP to provide the required capabilities. This typically includes authenticating users, assigning them to a role that dictates application permissions, and enabling single-sign-on (SSO) to improve the user experience.

Authorization

Authorization refers to the strategy and methods that are used to authorize actions that specific users are allowed to perform.

Authenticating users and authorizing the actions that they can perform is a critical component of any defense-in- depth strategy. Within an AWS environment, access management strategies are needed at the AWS Infrastructure layer, at the operating system layer, and at the application layer.

Each must be addressed.

Authorization in AWS is accomplished by permissions that are contained within policies and then applying these to users via role mapping or group membership. A strategy for creating policies and assigning them to users is required to grant administrators the rights they need to perform their job functions while not granting excessive or risky permissions. When an IdP is used with AWS, the method of applying policies to users is achieved with roles. Users are mapped to roles within the IdP, and then they assume the role in AWS. Roles and the permissions granted per role should adhere to the principles of least privilege and segregation of duties.

This integration of identity between AWS and an enterprise directory is accomplished using an identity provider that supports either SAML or OpenID Connect. Developing a strategy for granting access to users and assigning them roles that grant the permissions needed without granting excessive permissions is essential for secure AWS operations.

Additional consideration and strategies are needed for access conditions that can be applied to AWS IAM policies. For example, an organization may have a requirement to restrict access to a specific region, resource, or source IP address, or may want to enforce security policies like data encryption and MFA. Conditional access policy can further restrict access based on constraints such as source IP address.

Programmatic (direct application program interface (API) calls) access is accomplished using an authorization key and a private key which allows the AWS user to assume a role which authorizes actions they can perform. Processes to secure these keys are required, in addition to policy conditions, to ensure that unauthorized users cannot assume the role. In summary, AWS policy conditions can be used to restrict access to the minimal resources and actions that are required to allow users to perform their job functions. Due to the extremely rapid pace of deployment that is enabled by Identity-as-a-Service, many organizations fail to develop effective strategies and methodologies for access management. The easiest and riskiest method is to grant excessive administrative access to the AWS account and trust that users will not perform any malicious actions or make mistakes.

While fast and easy, this is highly risky for AWS environments that contain sensitive information and may also violate regulatory compliance standards. Developing and implementing mature access management procedures can help meet compliance requirements and can significantly reduce risks.

Access Governance

Cloud services accelerate the deployment of services and increases interaction with the enterprise IT environment by vendors, partners, and customers. This increases the importance of using federated identities, strong authentication, and mature processes and procedures. Access governance refers to the processes and procedures that are used to request, approve, grant, manage and audit access. For compliance purposes, it is necessary to develop procedures that establish formal requests and approvals for granting access.

The request and approval should be captured and retained to serve as audit artifacts. Access privileges tend to grow over time. Rights that are needed for deployments and troubleshooting do not normally get revoked. Rights that are no longer needed or authorized need to be periodically reviewed and reapproved. This process is referred to as access certification. The intention is to review all access that has been granted and verify that it still appropriate. The certification should be performed at regular periodic intervals.

Automation is essential for a comprehensive access certification approach.

A comprehensive certification also should review the AWS entitlements that are granted to each role. The IdP can be queried to identify which users are able to assume each role. AWS can be queried to determine entitlements for each role. A report can be created showing users, roles, and entitlements. This report can then be reviewed by resource owners to reauthorize that each user should still have the granted permissions. Organizations with complex and mature access management procedures may find it useful to automate and frequently collect the entitlements and identities together and store them in a database where they can query for either entitlements granted to any specific user or users granted a specific entitlement. This can be very useful during compliance audits and during incident investigations. Access governance in an AWS environment should cover the AWS infrastructure, operating systems, and applications. Risk-acceptable access governance at each layer is essential for operating a secure environment and realizing the many benefits of cloud services.

Accountability

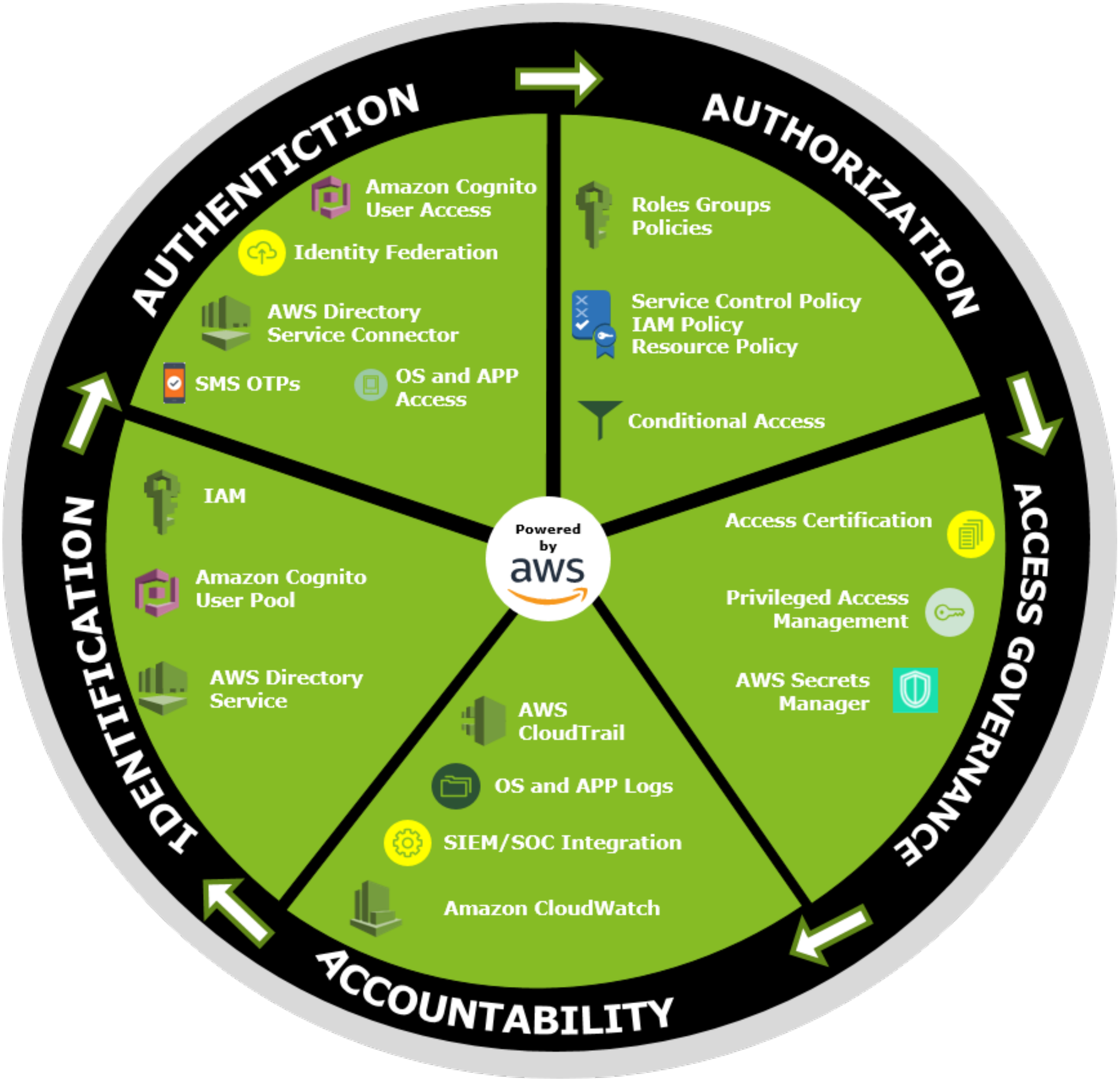
Users or programs accessing a system must be held accountable for their actions within the system. This requires all authenticated identities to be uniquely identifiable and all activities pertaining to their identities centrally stored to track and monitor cases of improper access, unenforced policies or to investigate malicious intent. Deloitte recommends that organizations consider leveraging the rich audit and data access logging telemetry provided by AWS CloudTrail, AWS Config, Amazon Virtual Private Cloud (VPC) flow logs, Amazon Simple Storage Service (Amazon S3) access logs, Elastic Load Balancer (ELB) access logs, Amazon CloudFront access logs, etc. to centrally store all AWS infrastructure, guest operating systems, and application- level logs in a single Amazon S3 bucket or Amazon CloudWatch log group.

It is essential to maintain the integrity of stored logs. The access control policy on this centralized logging resource should be updated to explicitly deny any edit/delete action from any subject.

Data archival and retention policies should also be setup as per organizational policy to automatically archive logs to cold storage to save on data storage costs.

These logs should be ingested by either third-party security information and event monitoring (SIEM) products or AWS-native threat intelligence service (Amazon GuardDuty) for log correlation across the service stack and security alerting. Security alerts can signify a range of events from misconfiguration of corporate security controls to potentially malicious behavior. It is important to note here that to enable Amazon GuardDuty, customers do not need to enable log sources as it gets access to the AWS CloudTrail, VPC Flow Logs and Domain Name Service (DNS) logs from the backend. Either way, alarms and notifications should be sent out to the Security Operations Center (SOC) team to follow run-book instructions to properly triage and neutralize the threat. Root cause analysis should also be carried out to identify areas of improvement so that tools and procedures can be fine-tuned to mitigate future instances of similar threat.

IAM Domains and Supporting Services



Secure the privilege access credentials

There are some additional areas to be considered for a broad coverage of identity and IAM in cloud. Privilege access management (PAM) covers methods that are used to grant privileged access to information resources. This may cover system administrator access to the underlying operating systems installed on virtual instances in the cloud. It could also cover how emergency break-glass access to the cloud infrastructure can be obtained only when required. An organization's existing PAM procedures should be considered and extended into the cloud infrastructure. In addition to PAM, emphasis should also be given to service accounts that grant administrative access to allow users or processes to perform actions in the cloud environment.

While interactive logon may be restricted for these accounts, there should be more scrutiny on who has access to these service accounts (governance) and more monitoring / alerting (SIEM) for anomalous behavior of these accounts.

The strength of the Deloitte /AWS relationship

aws Partner network

Premier

Consulting Partner

Security Competency

GovernmentCompetency

Financial Services Competency

Public Sector Partner

MSP Partner

Our relationship brings together Deloitte's extensive industry experience in cyber and enterprise risk management **with the security-enabled cloud infrastructure of AWS.** In 2006, AWS began offering IT infrastructure services to businesses in the form of web services—now commonly known as cloud computing. Today AWS provides a highly **reliable, secure, scalable, low-cost** infrastructure that powers hundreds of thousands of businesses in 190 countries around the world, with over a million active customers spread across many industries and geographies.

Deloitte can help organizations adopt AWS securely and establish a security-first cloud strategy. Deloitte is a leading information technology and advisory company. Deloitte is an **APN Premier Consulting Partner** and an **AWS Security Competency Partner (Launch Partner)** and was one of the first eight organizations globally to achieve the **Security Competency** as a launch partner. Deloitte's vast experience in Cyber Risk, combined with its extensive experience with AWS and Cloud technologies, enable us to provide **end-to-end** security solutions.

Authors

Aaron Brown
Partner, Cyber Risk Services
AWS Alliance Leader Deloitte & Touche LLP
aaronbrown@deloitte.com

Les Addison
Specialist Master, Cyber Risk Services
Cloud IAM Architect
Deloitte & Touche LLP
laddison@deloitte.com

Ravi Dhaval
Manager, Cyber Risk Services
Cloud & IoT Security Architect
Deloitte & Touche LLP
rdhaval@deloitte.com

Anunay Bhatt
Senior Consultant, Cyber Risk Services
Deloitte & Touche LLP
anunbhatt@deloitte.com

Amazon Web Services

Piyum Zonooz
Global Partner Solution Architect
pzonooz@amazon.com

About Deloitte
This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.
As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.