Chapter 3

Identity and Access Management (IAM) in Cloud

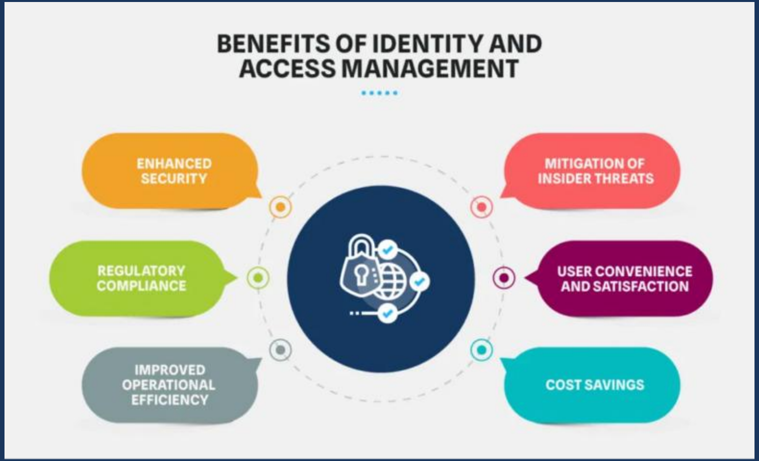
Dr. Mohammed Tawfik

Cloud Computing Security

Introduction to IAM

Identity and Access Management (IAM) is a framework of policies, processes, and technologies that enables organizations to manage digital identities and control their access to resources in cloud environments.

- **Security Foundation:** IAM serves as a critical security layer, ensuring only authorized users can access specific resources.
- **Key Components:** Identity management, authentication mechanisms, authorization policies, and access governance.
- **Cloud IAM Challenges:** Multi-tenancy, distributed resources, dynamic scaling, and cross-platform integration.
- **Benefits:** Enhanced security, regulatory compliance, operational efficiency, and improved user experience.


BENEFITS OF IDENTITY AND ACCESS MANAGEMENT
ENHANCED SECURITY
MITIGATION OF INSIDER THREATS
REGULATORY COMPLIANCE
USER CONVENIENCE AND SATISFACTION
IMPROVED OPERATIONAL EFFICIENCY
COST SAVINGS

Core IAM Concepts: Authentication, Authorization, Accounting (AAA)

Authentication

Verifies the identity of users or systems attempting to access resources. Answers the question: *"Who are you?"*

Methods include passwords, biometrics, certificates, tokens, and multi-factor authentication.

Authorization

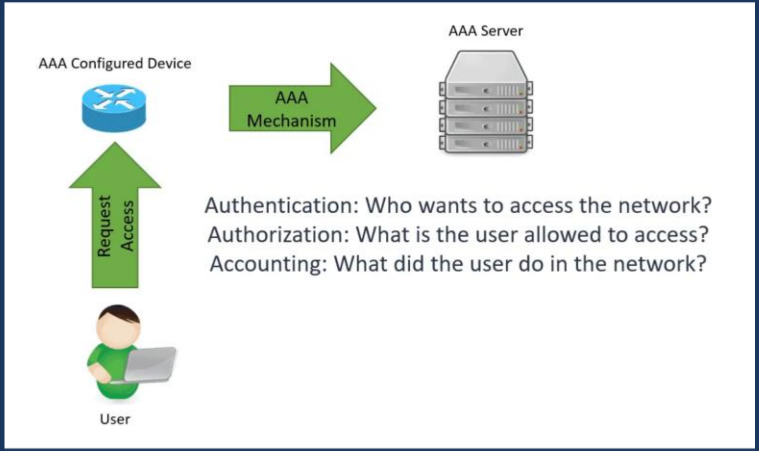
Determines what authenticated users or systems are permitted to do. Answers the question: *"What are you allowed to access?"*

Implemented through roles, policies, permissions, and access control lists.

Accounting

Tracks user activities and resource usage. Answers the question: *"What did you do?"*

Includes logging, monitoring, auditing, and reporting of access



Authentication: Who wants to access the network?
Authorization: What is the user allowed to access?
Accounting: What did the user do in the network?

Identity Providers (IdP)

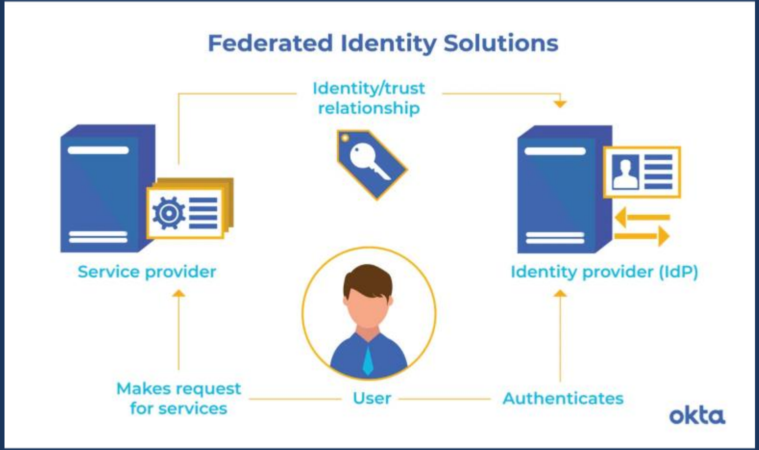
Identity Providers (IdP) are systems that create, maintain, and manage identity information while providing authentication services to applications.

Key Concepts

- **Federation:** Allows users to access multiple applications using a single identity across security domains.
- **Single Sign-On (SSO):** Enables users to authenticate once and access multiple applications without re-authentication.

Common Protocols

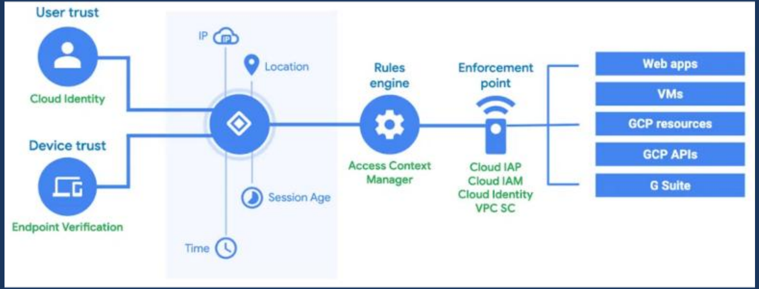
- **SAML** Security Assertion Markup Language XML-based protocol for exchanging authentication and authorization data.
- **OAuth 2.0** Open Authorization Framework that enables third-party applications to obtain limited access to a service.
- **OpenID Connect** OIDC Identity layer built on top of OAuth 2.0, adding authentication capabilities.


Federated Identity Solutions
Identity/trust relationship
Service provider
Identity provider (IdP)
Makes request for services
User
Authenticates
okta

User Management

Key User Management Functions

- **User Provisioning:** Creating and configuring user accounts with appropriate access rights based on job roles or business needs.
- **User Modification:** Updating user profiles, credentials, permissions, and group memberships as roles change.
- **User Deprovisioning:** Disabling or deleting accounts when users leave or change roles to prevent unauthorized access.
- **Password Management:** Enforcing password policies, handling resets, and managing credential lifecycles.



User Lifecycle Management

A structured approach to managing identities from creation to retirement, ensuring appropriate access throughout employment changes and preventing orphaned accounts.

Group Management

What are Groups?

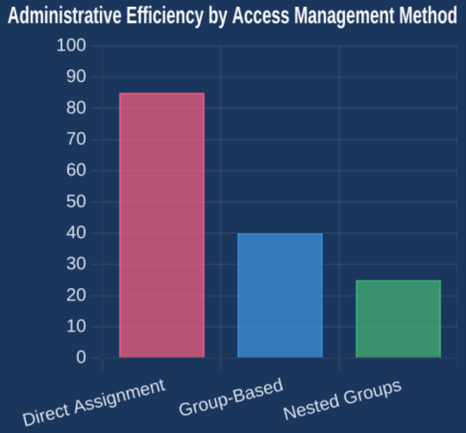
- Collections of users that share common access requirements and permissions

Benefits of Group-Based Access Control

- **Simplified Administration:** Manage permissions for multiple users at once
- **Consistency:** Ensures uniform access rights for users with similar roles
- **Scalability:** Efficiently manage access as organization grows

Group Management Best Practices

- Use hierarchical group structures with inheritance for complex organizations
- Implement regular group membership reviews and cleanup processes



Role-Based Access Control (RBAC)

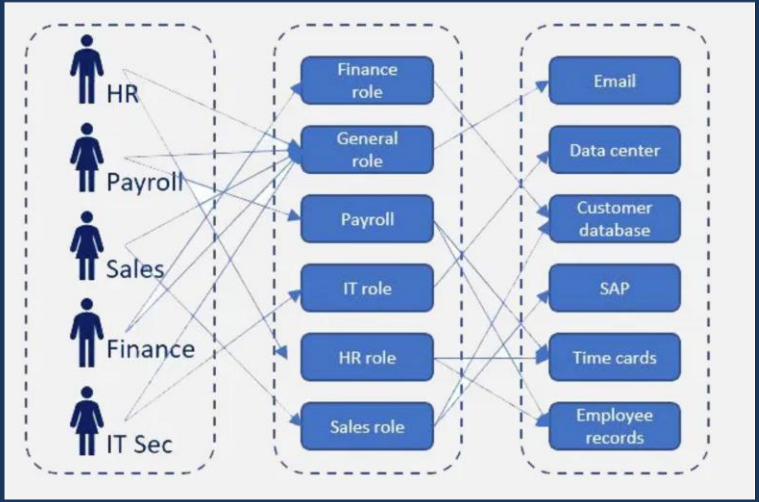
Role-Based Access Control (RBAC) is an approach to restricting system access to authorized users based on roles rather than individual identities.

Key Components

- **Roles:** Collections of permissions that represent job functions or responsibilities within an organization.
- **Role Assignment:** Users are assigned to appropriate roles based on their responsibilities and qualifications.
- **Permissions:** Define the operations that can be performed on specific resources.

Benefits in Cloud

- **Simplified Administration:** Reduces complexity by managing permissions at role level rather than individual user level.
- **Scalability:** Easily accommodates organizational growth and changes in user responsibilities.



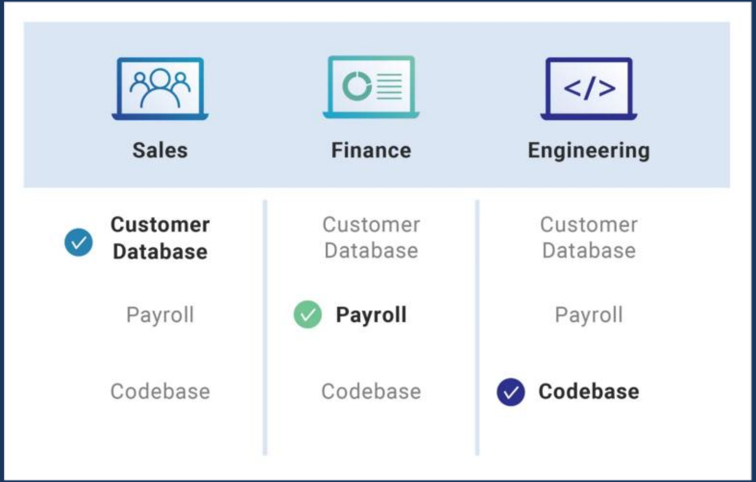
Policy-Based Access Control (PBAC)

Policy-Based Access Control (PBAC) uses centrally managed policies to define granular permissions based on attributes, conditions, and context.

Key Characteristics

- **Attribute-Based:** Decisions based on user attributes, resource properties, and environmental conditions.
- **Fine-Grained Control:** Enables highly specific permissions with conditional logic (if-then statements).
- **Cloud Implementation:** Used in AWS IAM policies, Azure Policy, GCP IAM conditions.
- **Advantages:** Centralized management, dynamic adaptation to changing conditions, reduced policy sprawl.

```
{
"Effect": "Allow",
"Action": ["s3:GetObject"],
"Resource": "arn:aws:s3:::example-bucket/*",
"Condition": {
```



Sales	Finance	Engineering
✓ **Customer Database**	Customer Database	Customer Database
Payroll	✓ **Payroll**	Payroll
Codebase	Codebase	✓ **Codebase**

Multi-Factor Authentication (MFA)

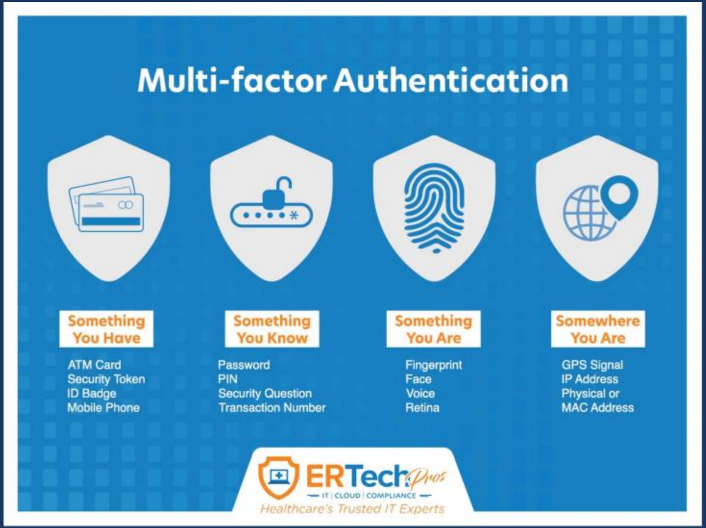
Multi-Factor Authentication (MFA) is a security mechanism that requires users to provide two or more verification factors to gain access to a resource, enhancing security beyond just passwords.

Authentication Factors

- **Something You Know** - Passwords, PINs, security questions

- **Something You Have** - Mobile devices, hardware tokens, smart cards

- **Something You Are** - Biometrics (fingerprints, facial recognition, voice)



Cloud MFA Implementation

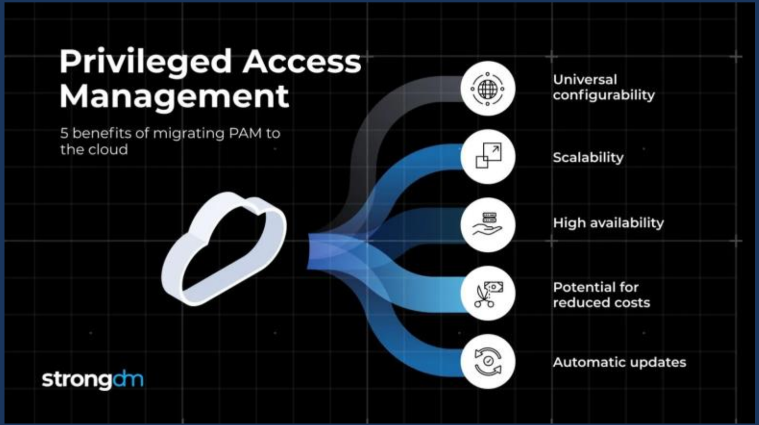
- ✓ **Critical for Cloud Security:** Protects against credential

Privileged Access Management (PAM)

Privileged Access Management (PAM) is a security strategy focused on controlling, monitoring, and securing elevated access to critical systems and sensitive data.

Key Components

- **Privileged Account Discovery:** Identifying and inventorying all privileged accounts across cloud environments.
- **Credential Vaulting:** Secure storage and automated rotation of privileged credentials.
- **Just-in-Time Access:** Providing temporary, time-limited privileged access only when needed.
- **Session Monitoring:** Recording and auditing privileged sessions for security and compliance.



Privileged Access Management

5 benefits of migrating PAM to the cloud

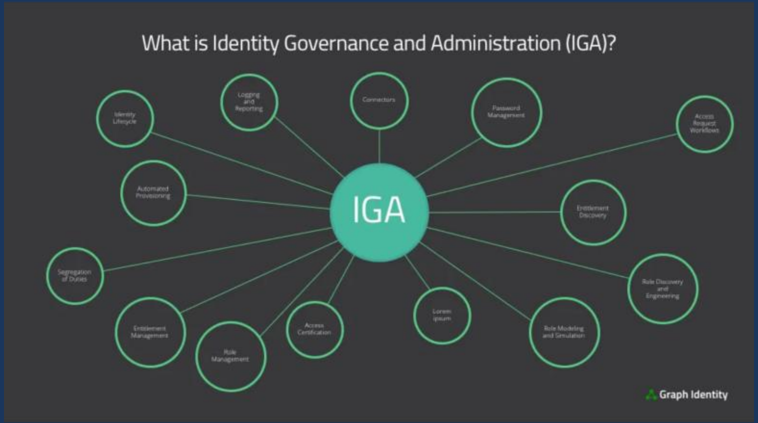
⚠ Cloud PAM Challenges

Identity Governance and Administration (IGA)

Identity Governance and Administration (IGA) combines identity administration with identity governance to ensure appropriate access to resources while maintaining compliance and reducing risk.

Key Components

- **Identity Lifecycle Management:** Automated provisioning, modification, and deprovisioning of user accounts across systems.
- **Access Certification:** Regular reviews of user access rights to ensure they remain appropriate and compliant.
- **Segregation of Duties (SoD):** Preventing conflicts of interest by ensuring critical functions are divided among different individuals.
- **Reporting and Analytics:** Visibility into identity data, access patterns, and compliance metrics for auditing and decision-making.
- **Policy Management:** Centralized definition and



Common IAM Challenges in Cloud

Scale and Complexity

Managing thousands of identities across multiple cloud platforms with different IAM models and interfaces.

Privilege Creep

Accumulation of excessive permissions over time as users change roles or responsibilities.

Compliance Requirements

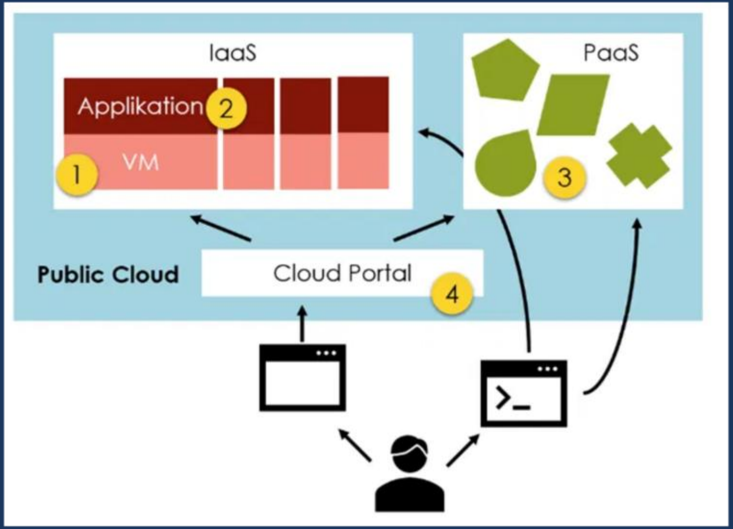
Meeting regulatory standards (GDPR, HIPAA, PCI DSS) across distributed cloud environments.

Multi-Cloud Strategy

Implementing consistent IAM policies across different cloud service providers with varying capabilities.

Shadow IT

Unauthorized cloud resources provisioned outside of governance processes, creating security blind spots.



Advanced Authentication Methods

Passwordless Authentication

Eliminates passwords in favor of more secure alternatives like biometrics, security keys, or mobile authenticator apps.

FIDO2/WebAuthn

Open standard for strong, phishing-resistant authentication using hardware security keys, biometrics, or mobile devices.

Adaptive Authentication

Dynamically adjusts authentication requirements based on risk factors like location, device, behavior patterns, and time of access.

Behavioral Biometrics

Analyzes unique patterns in user behavior (typing rhythm, mouse movements) for continuous authentication without disrupting workflow.

Passwordless Authentication Techniques
ENTER YOUR OTP
DONE
Biometrics
OTPs
REMINDER
1
Push Notifications
Magic Links

Authorization Models in Cloud

Role-Based Access Control (RBAC)

Assigns permissions to roles, which are then assigned to users. Simplifies management but can lead to role explosion in complex environments.

Attribute-Based Access Control (ABAC)

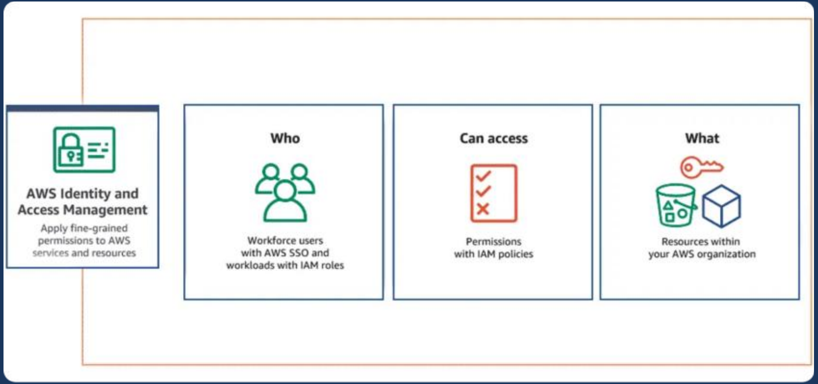
Uses attributes (user, resource, environment) to determine access. More flexible than RBAC but more complex to implement and manage.

Policy-Based Access Control (PBAC)

Centralizes access decisions through policies that can incorporate both roles and attributes. Common in cloud platforms like AWS IAM.

Graph-Based Access Control

Models relationships between entities as a graph, enabling complex


AWS Identity and Access Management
Apply fine-grained permissions to AWS services and resources
Who
Workforce users with AWS SSO and workloads with IAM roles
Can access
Permissions with IAM policies
What
Resources within your AWS organization

Identity Federation and Trust

SAML 2.0

XML-based protocol for exchanging authentication and authorization data. Primarily used for enterprise web applications and SSO.

OAuth 2.0

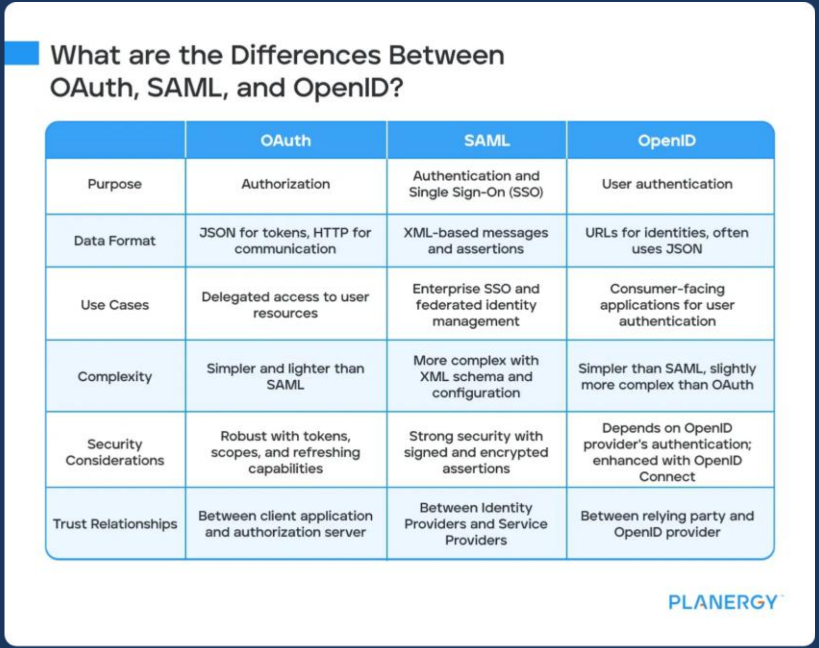
Authorization framework that enables third-party applications to obtain limited access to a user's account. Focuses on authorization, not authentication.

OpenID Connect (OIDC)

Identity layer built on top of OAuth 2.0, adding authentication capabilities. Uses JSON Web Tokens (JWTs) for identity information.

Cross-Domain Identity Management

Enables identity information exchange between cloud service



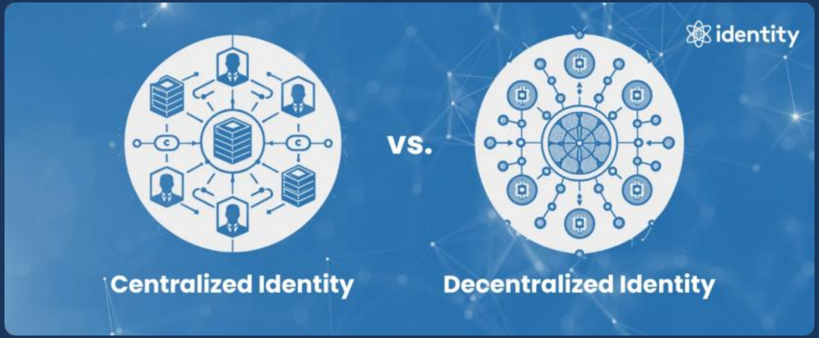
What are the Differences Between OAuth, SAML, and OpenID?

	OAuth	SAML	OpenID
Purpose	Authorization	Authentication and Single Sign-On (SSO)	User authentication
Data Format	JSON for tokens, HTTP for communication	XML-based messages and assertions	URLs for identities, often uses JSON
Use Cases	Delegated access to user resources	Enterprise SSO and federated identity management	Consumer-facing applications for user authentication
Complexity	Simpler and lighter than SAML	More complex with XML schema and configuration	Simpler than SAML, slightly more complex than OAuth
Security Considerations	Robust with tokens, scopes, and refreshing capabilities	Strong security with signed and encrypted assertions	Depends on OpenID provider's authentication; enhanced with OpenID Connect
Trust Relationships	Between client application and authorization server	Between Identity Providers and Service Providers	Between relying party and OpenID provider

PLANERGY

Centralized vs. Decentralized IAM

Aspect	Centralized IAM	Decentralized IAM
Control	Single authority manages all identities and access	Distributed across multiple systems or domains
Scalability	Limited by central system capacity	Highly scalable across distributed systems
Consistency	Strong policy consistency and enforcement	Potential inconsistencies across domains
Resilience	Single point of failure risk	Higher fault tolerance and availability
Complexity	Simpler to manage and audit	More complex integration and synchronization



IAM for Cloud-Native Applications

Service Accounts

Non-human identities used by applications and services to authenticate and access resources. Critical for microservices architecture.

Workload Identity

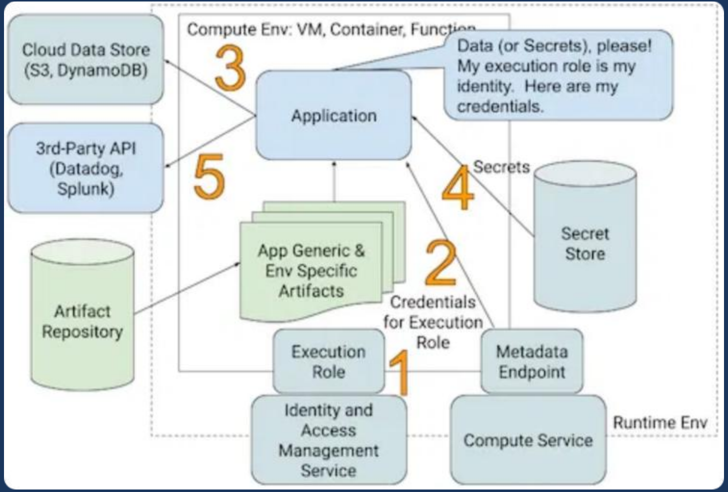
Enables Kubernetes pods to authenticate to cloud services using service account credentials, eliminating the need for static credentials.

Dynamic Secrets

Short-lived, automatically rotated credentials that reduce the risk of credential exposure in containerized environments.

Zero-Trust Architecture

Assumes no implicit trust based on network location. Every access request is fully authenticated, authorized, and encrypted.



Cloud Data Store (S3, DynamoDB)
Compute Env: VM, Container, Function
3
Data (or Secrets), please! My execution role is my identity. Here are my credentials.
Application
3rd-Party API (Datadog, Splunk)
5
Secrets
4
Secret Store
App Generic & Env Specific Artifacts
2
Artifact Repository
Credentials for Execution Role
Execution Role
1
Metadata Endpoint
Identity and Access Management Service
Compute Service
Runtime Env

Managing Secrets and Credentials

Secrets Management Services

Dedicated services like HashiCorp Vault, AWS Secrets Manager, or Azure Key Vault that securely store, manage, and control access to tokens, passwords, certificates, and encryption keys.

Dynamic Secrets Generation

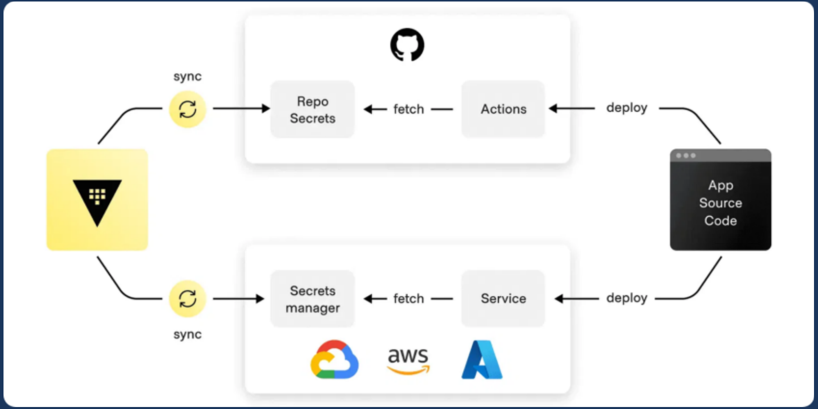
On-demand creation of short-lived credentials with automatic rotation, reducing the risk window of credential exposure and eliminating the need for manual rotation.

Encryption and Access Controls

Encryption at rest and in transit for all secrets, with fine-grained access controls to limit who can retrieve or manage specific secrets.

Secrets Lifecycle Management

Automated processes for creation, distribution, rotation, and



IAM Policy Best Practices

Principle of Least Privilege

Grant only the permissions necessary to perform required tasks. Start with minimal permissions and add as needed rather than starting with broad access.

Use Groups and Roles

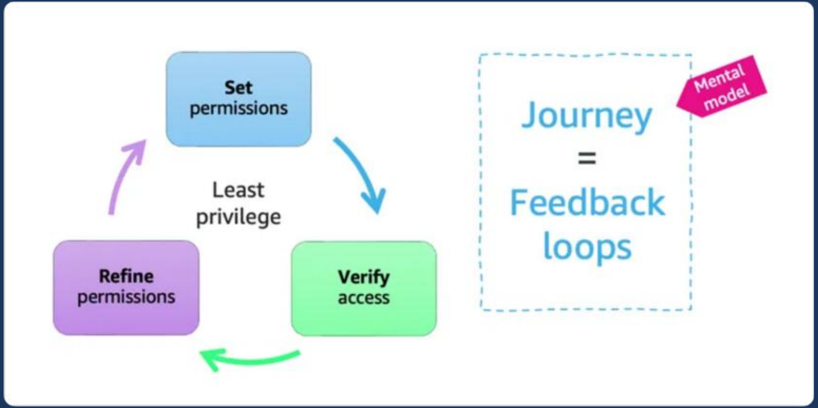
Assign permissions to groups and roles rather than individual users to simplify management and ensure consistency across similar users.

Regular Access Reviews

Conduct periodic reviews of access rights to identify and remove unnecessary permissions, inactive accounts, and policy drift.

Conditional Access Policies

Implement context-aware policies that consider factors like location, device, risk level, and time when granting access to sensitive



Identity Governance and Administration (IGA) Deep Dive

Identity Lifecycle Management

Automated processes for creating, modifying, and deactivating identities across systems, ensuring proper access throughout the identity lifecycle.

Access Certification and Reviews

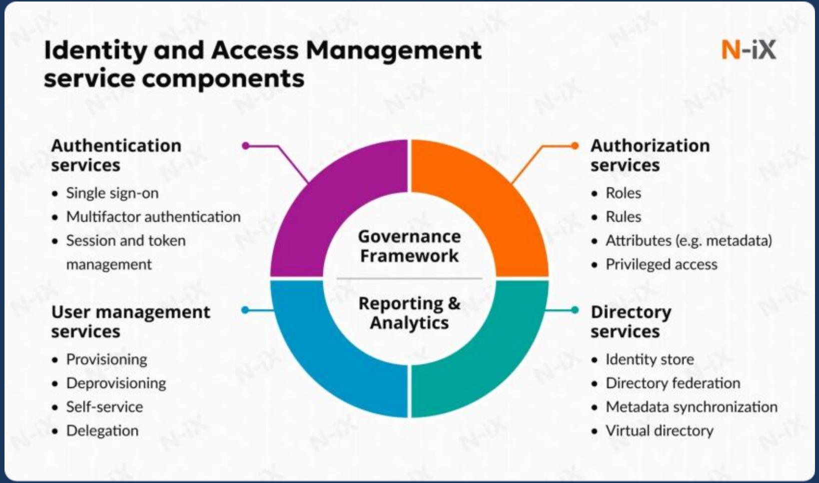
Periodic validation of user access rights by managers or resource owners to ensure appropriate access and compliance with policies.

Segregation of Duties (SoD)

Prevents conflicts of interest by ensuring no single individual has excessive control over critical processes, reducing fraud and error risks.

Policy Administration and Enforcement

Centralized management of access policies with automated



Incident Response for IAM

Preparation

Establish IAM-specific incident response plans, define roles and responsibilities, and implement monitoring for identity-related security events.

Detection and Analysis

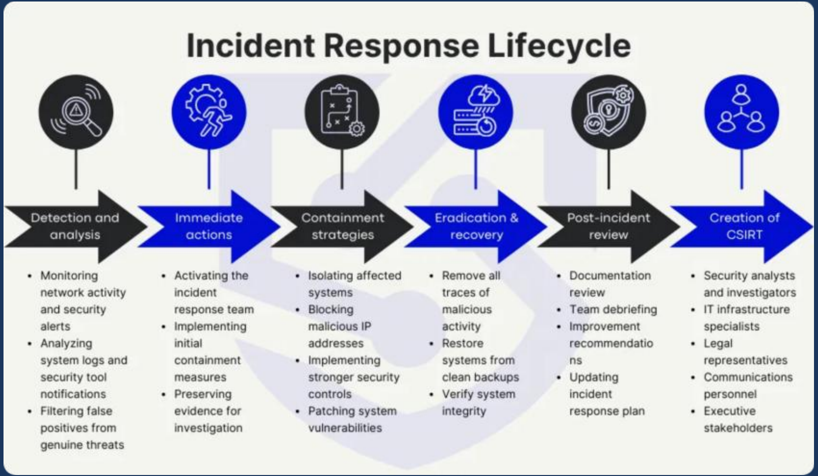
Monitor for suspicious authentication patterns, privilege escalation, unauthorized access attempts, and anomalous identity behavior.

Containment and Eradication

Isolate compromised accounts, revoke active sessions, rotate compromised credentials, and remove unauthorized access rights.

Recovery and Post-Incident

Restore proper access controls, implement additional security



Incident Response Lifecycle

Detection and analysis
- Monitoring network activity and security alerts
- Analyzing system logs and security tool notifications
- Filtering false positives from genuine threats

Immediate actions
- Activating the incident response team
- Implementing initial containment measures
- Preserving evidence for investigation

Containment strategies
- Isolating affected systems
- Blocking malicious IP addresses
- Implementing stronger security controls
- Patching system vulnerabilities

Eradication & recovery
- Remove all traces of malicious activity
- Restore systems from clean backups
- Verify system integrity

Post-incident review
- Documentation review
- Team debriefing
- Improvement recommendatio ns
- Updating incident response plan

Creation of CSIRT
- Security analysts and investigators
- IT infrastructure specialists
- Legal representatives
- Communications personnel
- Executive stakeholders

Compliance and Audit in Cloud IAM

Regulatory Requirements

Key regulations affecting IAM include GDPR, HIPAA, PCI DSS, SOX, and industry-specific standards that mandate access controls, authentication, and identity protection.

Audit Logging and Monitoring

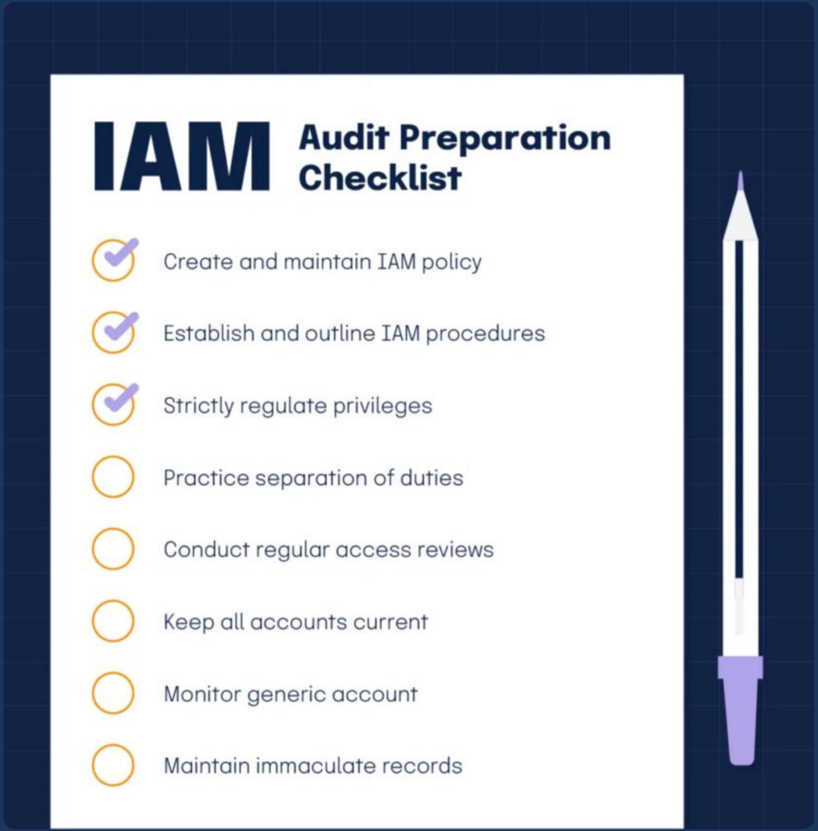
Comprehensive logging of all identity and access events with tamper-proof storage, real-time monitoring, and alerting for suspicious activities.

Compliance Reporting

Automated generation of compliance reports showing user access rights, policy enforcement, segregation of duties, and access certification status.

Continuous Compliance

Automated controls that continuously validate IAM configurations



IAM Audit Preparation Checklist

- ✓ Create and maintain IAM policy
- ✓ Establish and outline IAM procedures
- ✓ Strictly regulate privileges
- ○ Practice separation of duties
- ○ Conduct regular access reviews
- ○ Keep all accounts current
- ○ Monitor generic account
- ○ Maintain immaculate records

Future Trends in IAM

AI and Machine Learning

Intelligent systems that detect anomalous access patterns, predict potential threats, and automate access decisions based on behavioral analytics and risk scoring.

Decentralized Identity

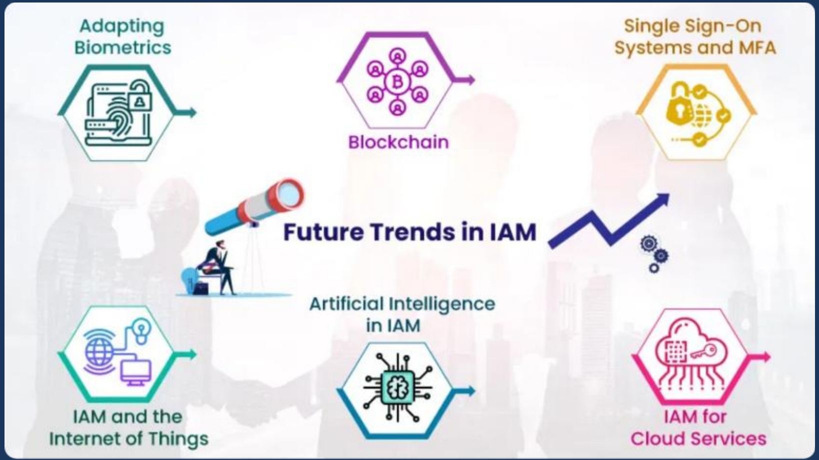
Blockchain-based identity solutions that give users control over their digital identities while providing verifiable credentials that don't depend on central authorities.

Passwordless Authentication

Elimination of passwords in favor of biometrics, hardware tokens, and contextual authentication methods that improve security and user experience.

Zero Trust Architecture

Evolution of "never trust, always verify" approach with continuous


Adapting Biometrics
Blockchain
Single Sign-On Systems and MFA
Future Trends in IAM
Artificial Intelligence in IAM
IAM and the Internet of Things
IAM for Cloud Services

Summary of Chapter 3: Identity and Access Management (Part 1)

Core IAM Concepts

Authentication, authorization, and accounting form the foundation of IAM systems, with various models like RBAC, ABAC, and PBAC providing flexible access control.

Identity Federation

Standards like SAML, OAuth, and OpenID Connect enable secure identity sharing across domains, supporting single sign-on and third-party authentication.

Advanced Authentication

Multi-factor, passwordless, and adaptive authentication methods enhance security while improving user experience in cloud environments.

Cloud-Native IAM

Service accounts, workload identity, and dynamic secrets address the unique identity challenges of containerized and microservices architectures.

Governance and Compliance

Identity governance, access certification, and comprehensive audit logging ensure regulatory compliance and reduce security risks.

Incident Response

Specialized IAM incident response procedures focus on detecting, containing, and remediating identity-related security breaches.

Coming in Part 2

Implementation strategies, cloud provider IAM services comparison, IAM architecture patterns, and hands-on labs for practical experience

IAM in Multi-Cloud and Hybrid Cloud Environments

Multi-Cloud Reality: Organizations use 2-6 different cloud providers on average

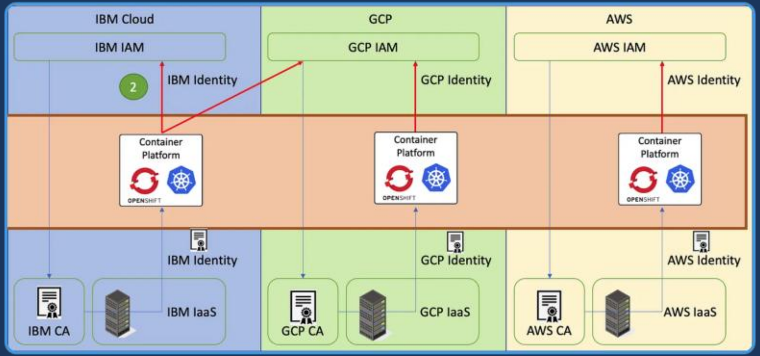
Identity Fragmentation: Separate identity stores across providers create security gaps

Centralized Identity Hub: Single source of truth for identities across environments

Federated Authentication: Extend on-premises identity to multiple clouds

Consistent Access Policies: Unified policy enforcement across environments

Consolidated Visibility: Unified monitoring and reporting across clouds



Decentralized Identity and Self-Sovereign Identity (SSI)

Self-Sovereign Identity: Users own and control their digital identities

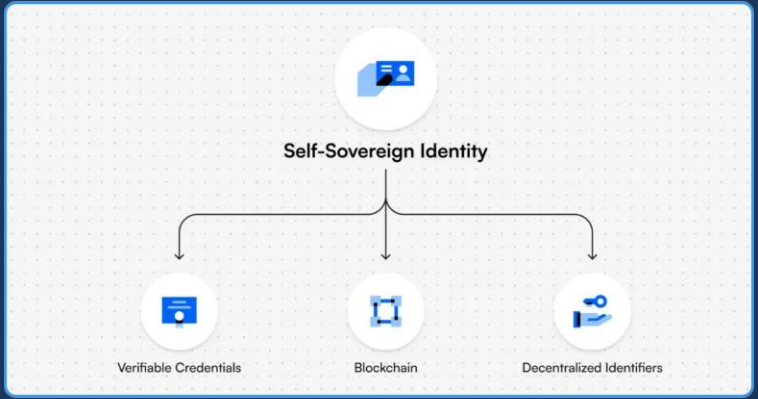
Blockchain Foundation: Immutable, distributed ledger for identity verification

Verifiable Credentials: Cryptographically signed attestations by trusted issuers

Zero-Knowledge Proofs: Prove identity claims without revealing underlying data

Decentralized Identifiers (DIDs): Globally unique identifiers not dependent on centralized registries

Cloud Integration: Emerging standards for SSI in cloud environments



Behavioral Analytics in IAM

User and Entity Behavior Analytics (UEBA): Detecting anomalies in user behavior patterns

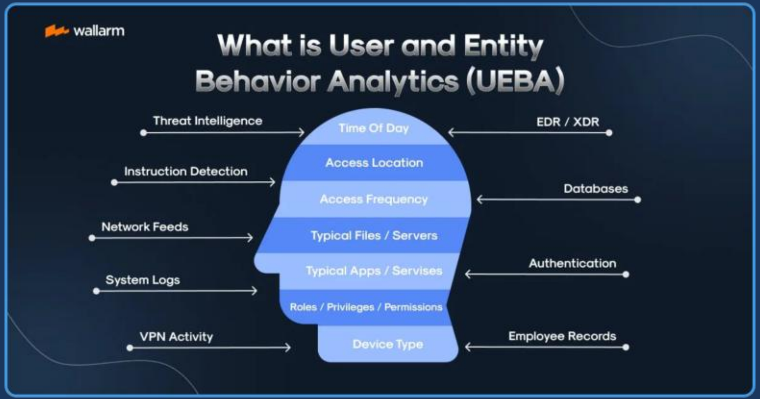
Machine Learning Models: Establish baselines of normal behavior for each user

Risk-Based Authentication: Dynamically adjust authentication requirements based on risk score

Contextual Factors: Time, location, device, network, and resource sensitivity

Continuous Authentication: Ongoing verification throughout user sessions

Automated Response: Trigger additional verification or block access based on risk



Zero Trust and IAM Integration

Zero Trust Principle: "Never trust, always verify" - no implicit trust based on network location

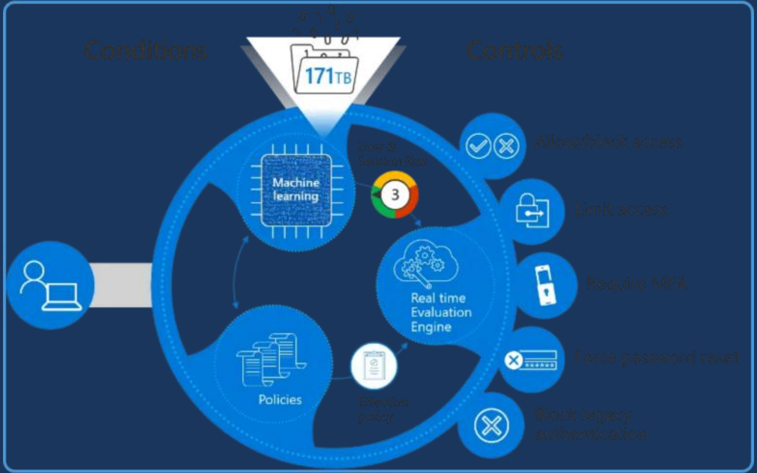
Identity as the New Perimeter: IAM becomes the foundation of Zero Trust security

Continuous Verification: Authentication at every access request, not just at login

Least Privilege Access: Granular permissions based on just-in-time, just-enough access

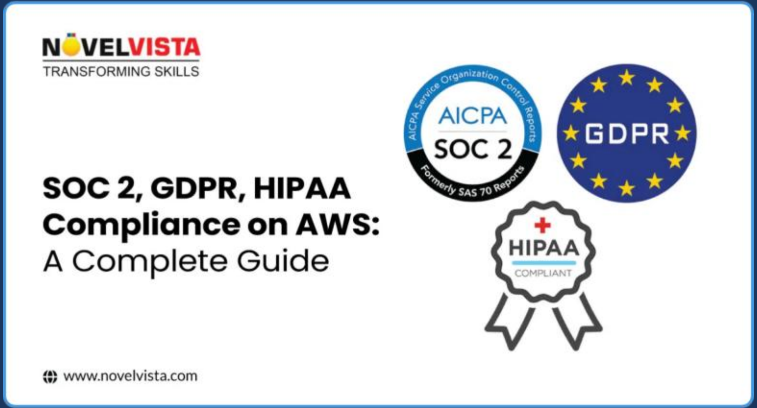
Micro-Segmentation: Identity-based network segmentation for cloud resources

End-to-End Visibility: Comprehensive monitoring of all identity activities



Compliance Frameworks and IAM (Deep Dive)

- **GDPR:** Requires strong identity controls, data subject access rights, and consent management
- **HIPAA:** Demands strict access controls, audit trails, and authentication for PHI
- **PCI DSS:** Mandates role-based access, MFA, and least privilege for cardholder data
- **SOC 2:** Focuses on access control, user provisioning, and authentication processes
- **ISO 27001:** Requires comprehensive identity management and access control policies
- **Compliance Automation:** IAM tools for continuous compliance monitoring and reporting

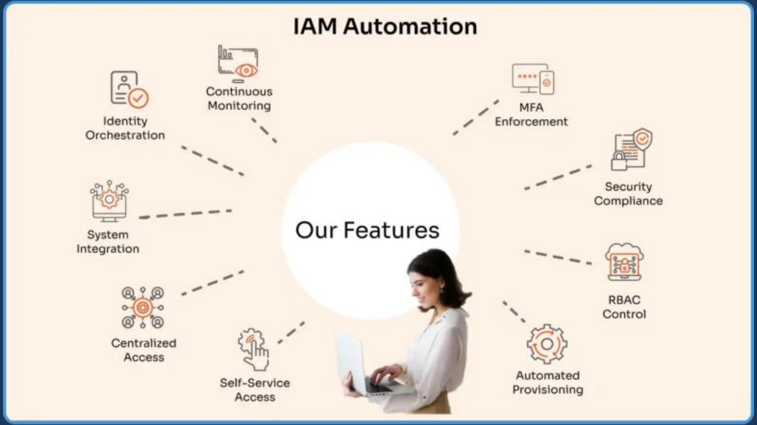

NOVELVISTA
TRANSFORMING SKILLS

SOC 2, GDPR, HIPAA Compliance on AWS:
A Complete Guide

www.novelvista.com

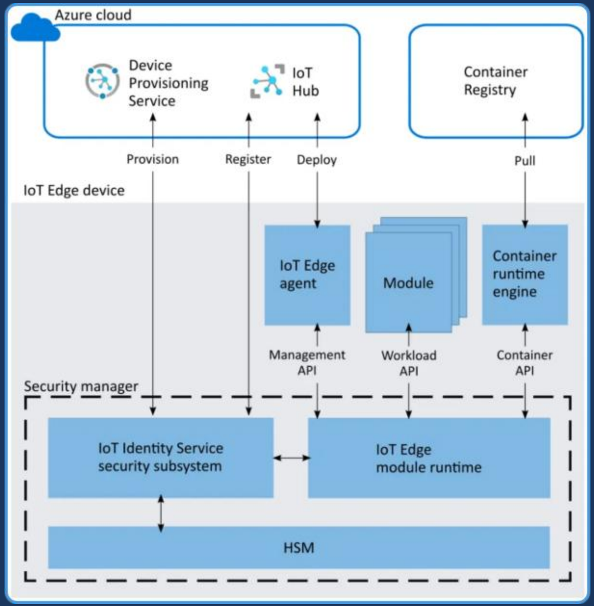
IAM Automation and Orchestration

- **Automated Provisioning:** Just-in-time creation of accounts and access rights
- **Automated Deprovisioning:** Immediate removal of access when no longer needed
- **Orchestration vs. Automation:** Coordinating multiple automated processes across systems
- **Infrastructure as Code (IaC):** Managing IAM configurations through code
- **Workflow Automation:** Streamlining approvals, certifications, and access requests
- **Benefits:** Reduced errors, improved security posture, and operational efficiency



IAM for IoT and Edge Devices

- **Device Identity:** Unique identifiers and credentials for each IoT device
- **Certificate-Based Authentication:** X.509 certificates for secure device authentication
- **Secure Key Management:** Hardware security modules (HSMs) for credential protection
- **Device Lifecycle Management:** Provisioning, monitoring, and decommissioning
- **Edge Computing Security:** IAM controls for distributed processing environments
- **Scalability Challenges:** Managing millions of device identities in cloud environments

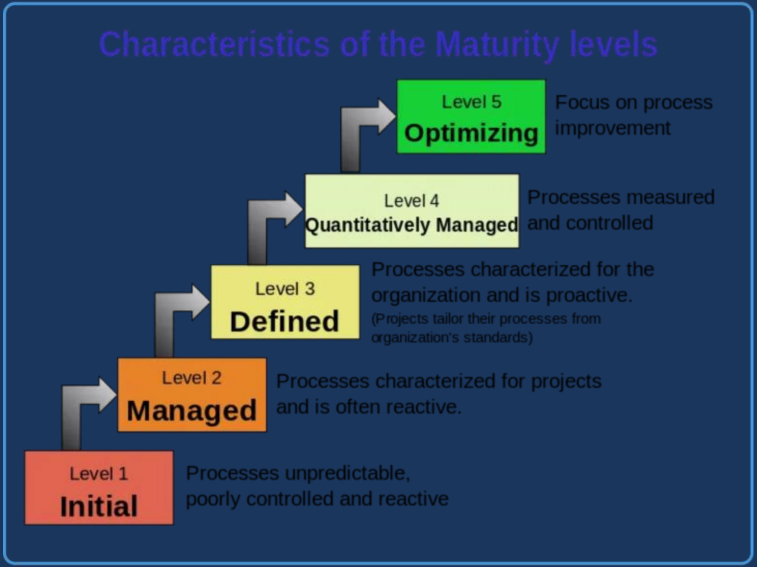


Quantum-Resistant Cryptography and IAM

- **Quantum Computing Threat:** Ability to break current cryptographic algorithms (RSA, ECC)
- **Post-Quantum Cryptography (PQC):** Algorithms resistant to quantum computing attacks
- **Lattice-Based Cryptography:** Leading PQC approach for authentication and key exchange
- **Crypto-Agility:** Designing IAM systems to easily transition between cryptographic algorithms
- **Transition Timeline:** Preparing now for the "harvest now, decrypt later" threat
- **Cloud IAM Implications:** Updating authentication, federation, and key management systems

IAM Maturity Model

- **Level 1 - Initial:** Ad-hoc, reactive IAM processes with minimal controls
- **Level 2 - Managed:** Basic IAM policies and procedures established
- **Level 3 - Defined:** Standardized IAM processes across the organization
- **Level 4 - Quantitatively Managed:** Metrics-driven IAM with continuous monitoring
- **Level 5 - Optimizing:** Proactive IAM with continuous improvement
- **Assessment Framework:** Evaluating current state and planning improvement roadmap



Characteristics of the Maturity levels
Level 5
Optimizing
Focus on process improvement
Level 4
Quantitatively Managed
Processes measured and controlled
Level 3
Defined
Processes characterized for the organization and is proactive.
(Projects tailor their processes from organization's standards)
Level 2
Managed
Processes characterized for projects and is often reactive.
Level 1
Initial
Processes unpredictable, poorly controlled and reactive

Case Study: IAM Breach Analysis

- **Incident Overview:** Major cloud service provider breach via compromised admin credentials

- **Root Cause Analysis:** Privileged account without MFA, excessive permissions

- **Attack Path:** Initial phishing → credential theft → privilege escalation → lateral movement

- **IAM Control Failures:** Inadequate MFA, excessive privileges, poor monitoring

- **Remediation Actions:** Enforced MFA, implemented JIT access, enhanced monitoring

- **Key Lessons:** Defense in depth, continuous monitoring, and least privilege are essential

IAM Breach Analysis

Best Practices for Cloud IAM Implementation

- **Enforce MFA Everywhere:** Require multi-factor authentication for all users, especially privileged accounts
- **Implement Least Privilege:** Grant only the minimum permissions needed for each role or function
- **Use Just-in-Time Access:** Provide temporary, time-limited access for administrative tasks
- **Automate Lifecycle Management:** Ensure timely provisioning and deprovisioning of accounts
- **Continuous Monitoring:** Implement real-time monitoring and alerting for suspicious activities
- **Regular Access Reviews:** Conduct periodic certification of all access rights

Cloud IAM Best Practices

Future of IAM: AI, Blockchain, and Beyond

AI-Powered IAM: Machine learning for anomaly detection and adaptive authentication

Blockchain for Identity: Immutable, distributed identity verification without central authorities

Biometric Evolution: Advanced biometrics with liveness detection and continuous authentication

Zero-Knowledge Identity: Proving identity attributes without revealing underlying data

Global Identity Standards: Cross-border, interoperable identity frameworks

Autonomous IAM: Self-healing, self-optimizing identity systems with minimal human intervention

Future IAM Technologies

Chapter 3 Summary (Part 2) & Conclusion

- **Advanced IAM Topics:** Multi-cloud, decentralized identity, behavioral analytics, zero trust
- **Emerging Technologies:** Quantum-resistant cryptography, AI-powered IAM, blockchain identity
- **Implementation Best Practices:** Least privilege, MFA, automation, continuous monitoring
- **Key Takeaways:** IAM is the foundation of cloud security and requires a comprehensive approach
- **Next Chapter Preview:** Chapter 4 will cover Data Security in Cloud Environments
- **Recommended Reading:** CSA Security Guidance, NIST SP 800-204, Cloud Identity Summit papers

Cloud IAM Summary