WHITE PAPER

AUTOMATED CLOUD IAM FACTORY MODELING

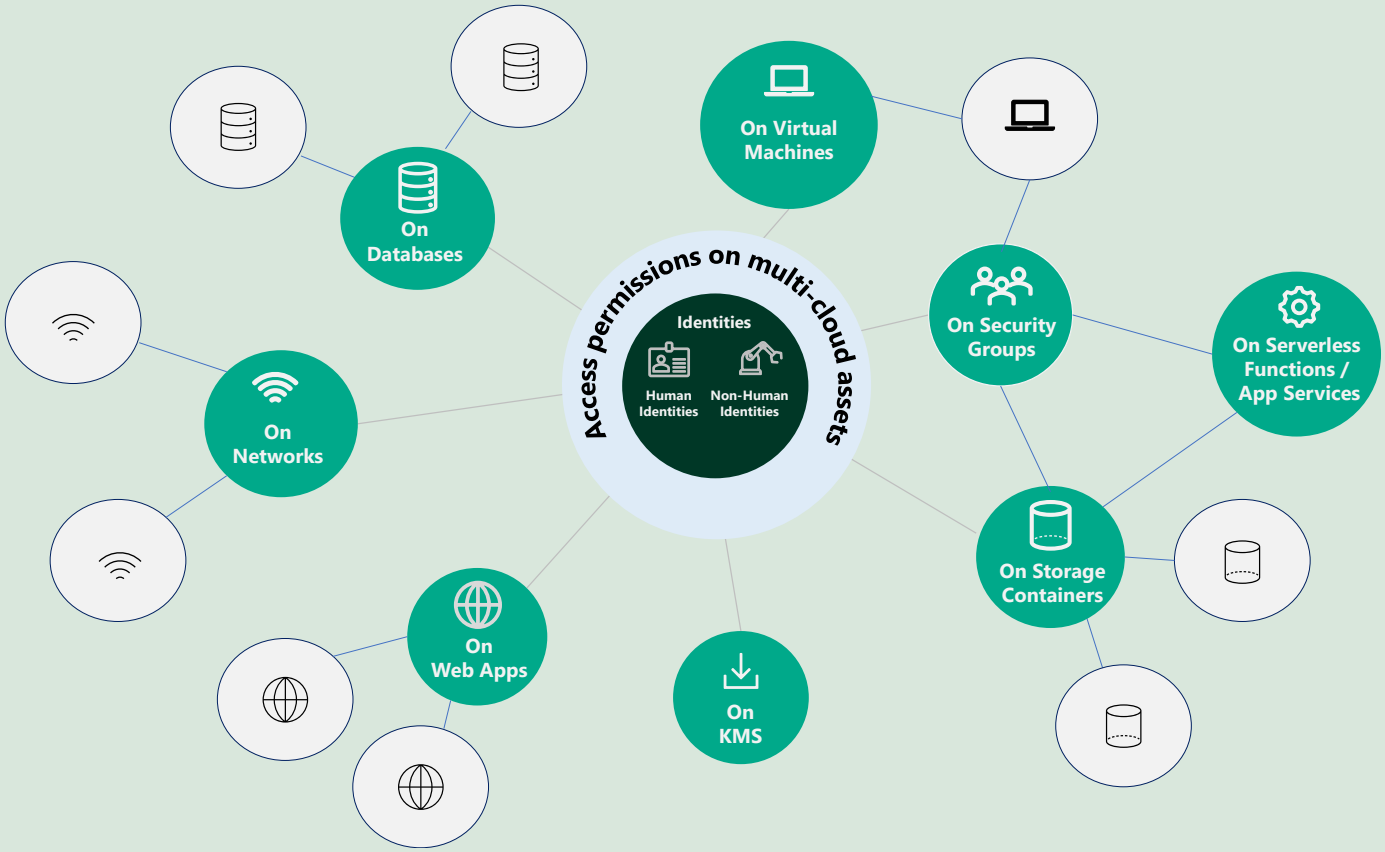
Abstract

With the dynamic and ever evolving nature of cloud security tenets, it is important to have a risk aware approach and built in risk resiliency to achieve sustained growth. Various analysts and our experience suggest that identity is the primary threat vector, as organizations embark on digitalization journey into cloud. Due to vast differential of the identity fabric between on-premises and cloud ecosystems it is imperative that correct processes are strapped in for better and accurate pivot for alignment with Cloud Identity and Access Management. The document talks about a maturity journey for cloud identity management with increased focus on automation at each step. We also look at human and non-human identity management separately and having distinct process for the same. The document culminates into an end goal architectural design for th factory setup. This document would be ideal for enterprises or engineers with focus on refining identity fabric and providing code-based automated identity management structure.

Infosys®
Navigate your next

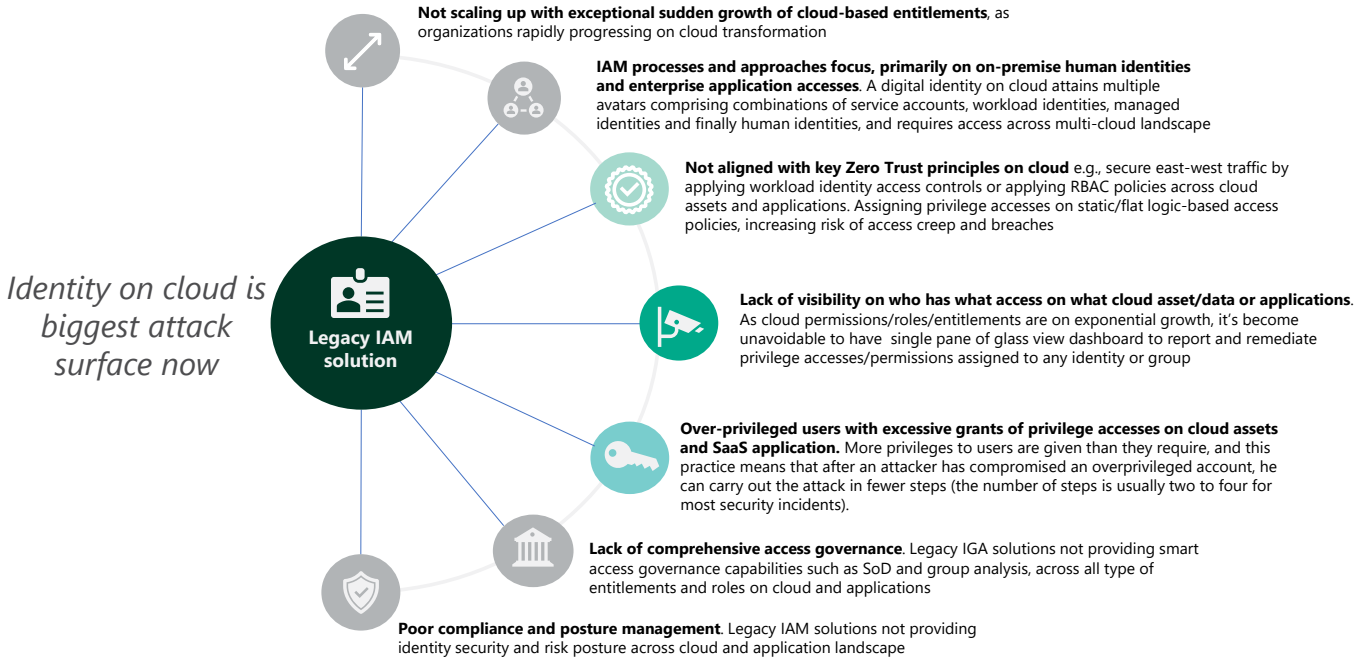
Introduction

"Identity is the biggest threat vector" is a sentence we hear very often while helping customers in their digitalization & cloud transformation journey. Trying to make sense of the threat and the magnanimity of it is very difficult and help is required no matter the size of the organization to ensure a level of diligence in the process of identity and access management. The process also needs to be consistent and under constant scrutiny for change and improvement. Document further envisions a concept that would not only automate the entire process but also delegate non-human cloud identity creation and management responsibilities to the application or platform owner teams. The Security Ops will then be required to follow only a governance model and approve exceptional non-human identity creations.



Need for IAM Factory

- **Legacy IAM processes and approaches focus,** primarily on on-premises human identities and enterprise application accesses.
- **Potential risk of human error** due to manual identity requests execution
- **Alignment with key zero trust principles** on cloud
- **Huge scale** of cloud and burst of cloud identities.
- **Pushing** the creation **responsibility** onto the **application owners** while **retaining** the **governance overlay**
- Singular **discipline** and **posture** in creation of both Human and non-Human identities



Tenets of Cloud IAM factory

Before we get into the granular discussion of the concept. Below are the foundational pillars around which the entire solution is designed.

Fig. 1. Cloud IAM Factory foundational pillars

Cloud IAM Factory Building Blocks			
Cloud guardrails	Role Definition	Access Provisioning	Risk mitigation & governance
• Guardrail definition & baseline (Azure Policy) • Administrator definition & exception policies • Guardrail implementation strategy & hierarchy • Guardrail enforcement	• Base role model for access to cloud resources (birthright vs requestable, human vs non-human) • Entitlement mapping with roles • Reviewer group definition & empowerment • Role governance	• Identity workflows • Playbook definition for identity-entitlement mapping • 6-eye review process for critical resource provisioning	• Cloud Infrastructure Entitlement Management (CIEM) based continuous identity hygiene • Identity recertification & risk definition • Identity behavior baselining (anomaly detection) • ITSM integration
Cloud IAM Factory Key Outcomes			
Cloud services baseline & governance framework	Role Based Access Control model for cloud services	Automated Cloud Identity lifecycle management	Anomaly detection, entitlement correlation & identity posture

The diagram when followed from left to right, paints a high level picture of the concept.

Reduce Attack Surface : Design & deploy cloud gaurdrail Setup The journey of the factory model starts by helping to design accurate and business specific guardrails. There is a lot of importance to this step not only from the perspective of creating solid security foundation but also to reduce the attack surface right at the outset. These guardrails are available out of box from hyperscalers i.e., AWS, Azure, GCP and can also be customized specially focusing on cloud identity & entitlements.

Managing the Entitlement with setup of RBAC policies: Next the role definitions are looked upon, both for human and non-human identities. The enterprise users will float into the cloud with the AD group structure definition and then promoting those groups and associated roles onto the cloud. Based on

cloud services chosen at the guardrail definition stage, birthright entitlement list will be derived and the same will be associated to the AD group. For the non-human identities there will also be definition of permissions that can be associated by default and others which will require exceptions.

Cloud Identity Provisioning with hyperautomation: In the next stage, it is required to create a catalogue of mapping cloud services with associated permissions. This catalogue will further work as source of truth for the decision whether an identity is BAU (needs no explicit approval), identity is risky (needs approval) or identity is out of scope for requesting (admin permissions for critical services). A quick example of the type of data in catalogue is below.

At the same stage, definition of the identity creation with code with associated security controls will be completed. Important control here is the 6-eye approval process. 6-eye review process entails 3 separate config checkpoints, first is the IAC developer himself, flowed by engineer in his peer review group, final and most critical approval is from the identity review board which is equipped with enterprise level risk definitions for identity role entitlements. So, identity creation on the cloud will be classified as sensitive deployment and will require approvals in addition to the peer review within the application development group. This additional approval will come from the identity creation approval board. The basis of the approval will be the catalogue logic created earlier in this step. Also in this step, design plan will be drafted for including the catalogue into the identity request process in Snow or any other ITSM tool.

Real Time Automated Identity Governance: Finally, after the entire automation engine is setup, the governance of the entire model and identities must be looked upon, which would be created by the IAM factory. Enabling Ops, Process Adoption drives, Technology awareness sessions and Knowledge transfer to Engineer teams will be traditional steps that will be carried out at this stage. In addition, CIEM (Cloud Infrastructure Entitlement Management) technology is proposed. This technology will do continuously posture assessment and discovery of identities in Cloud. Recertification of identities, potential privilege escalation and alignment with principle of least privilege will be ensured by this tool.

Cloud IAM UseCases	Category	Applicability
Read-only access for EC2	BAU	AWS-EC2
View EC2 service dashboard	BAU	AWS-EC2
EBS volumes attach/Detach on EC2	Approve with exception	AWS-EC2
EC2 security groups administration	Admin Only Task	AWS-EC2
Elastic Ips creation/deletion	Admin Only Task	AWS-EC2
Reserved Instances provision/deprovision	Admin Only Task	AWS-EC2

How to adopt Cloud IAM Factory?

Cloud IAM factory foundational steps have been defined. But this can't be adopted right of the bat. Adoption of cloud IAM factory will require to follow a formal maturity process.

Below is definition of maturity as we take small steps to create a fully functional Cloud IAM factory.

Stage 1:

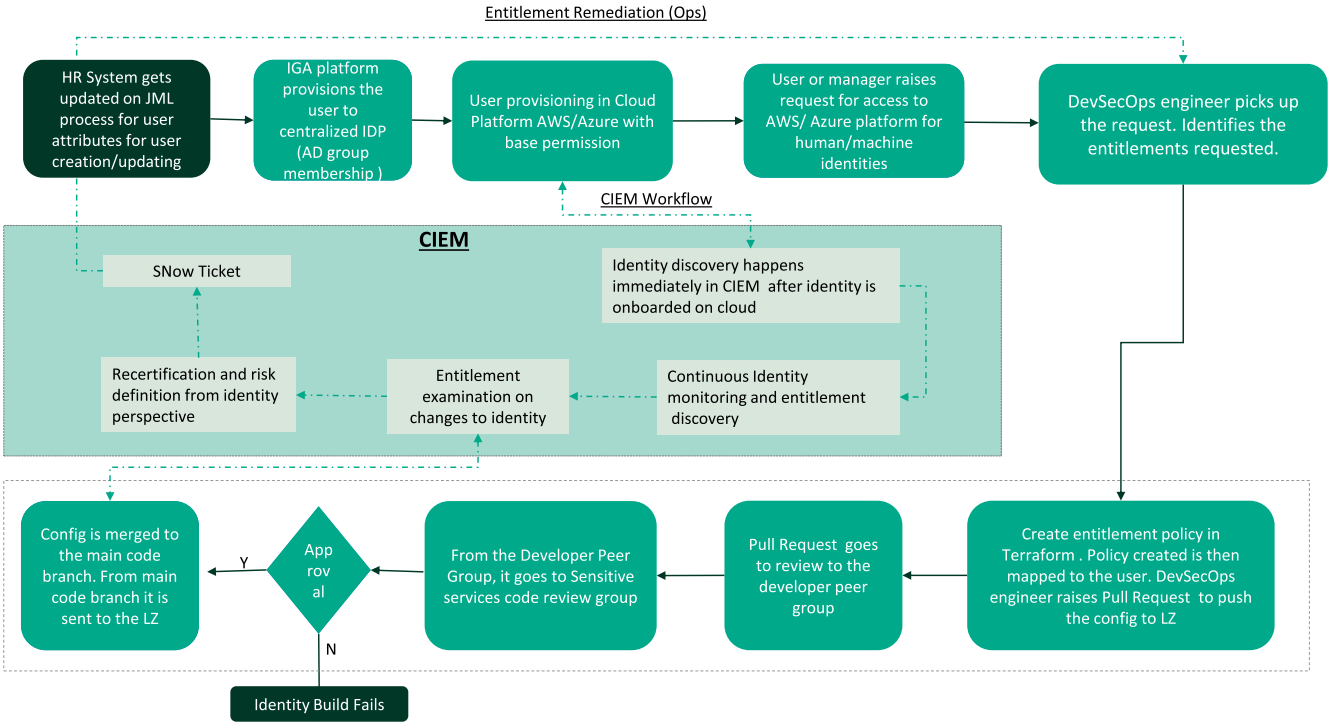
Enterprise Readiness Requirements :

- There is an established Enterprise user lifecycle process with well architected AD and IGA tooling
- DevOps Team structure
- CIEM tool has been procured.

Functional Flow:

1. It starts with the initial flow of user getting created in enterprise AD and then with IGA identity gets modeled into appropriate groups and birthright permissions. User along with group floats into the cloud with the birthright permissions. This will be done as part of the account baselining process.
2. There are 2 types of Identity and Access Management requests that might come:
   a. Modification to enterprise user entitlements
   b. Creation/Modification/Deletion of Non-Human User identity

Fig. 2. Creation of new cloud identity- human or non-human



3. The request goes to the enterprise ITSM tool which would be picked up by DevSecOps group engineer. This stage takes into account the existing technology stack for the enterprise. For example, if they don't have a ITSM backed process for Identity request we can directly move to stage II.
4. The DevSecOps Engineer then creates Infrastructure as code (IAC) code blocks i.e., Terraform code to create/modify/delete identity. Further, the engineer creates Pull Request (PR) which is requested to indicate developer intention to mv config to cloud landing zone.
5. The Pull Request (PR) goes to through 2 levels of Peer Review:

a. Peer from the developer group

b. Identity Change Review Board

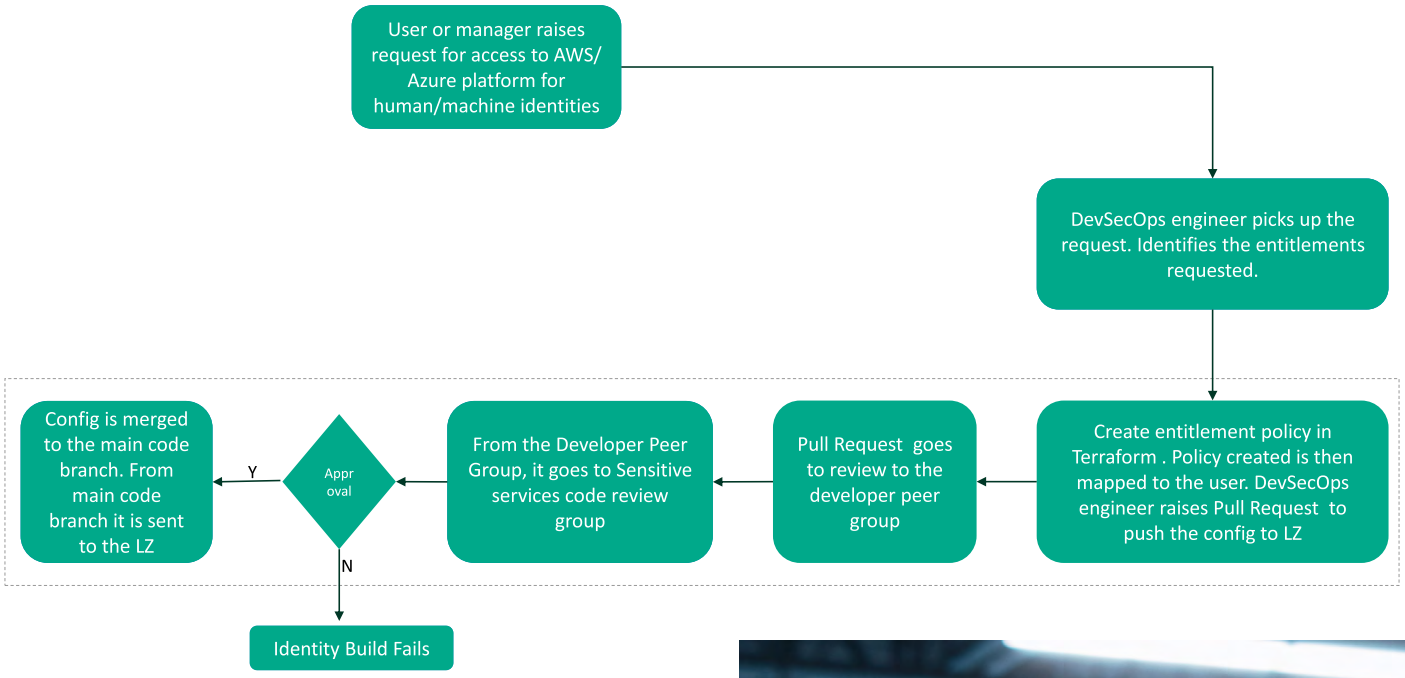
The Change Review Board is equipped with the catalogue of Cloud Service to Entitlement risk matrix.

They are required to approve based on the risk score of the identity chosen to be created. So, if there is an identity that only mandates BAU permission set, it can be immediately approved. If the permissions requested are riskier, explanation will be sought from the requestor. If there are admin level permissions, then PR will be declined.

6. Finally on receiving all the approvals, the PR is merged with the environment branch. The config then gets pushed into the cloud environment.
7. Important step is the introduction of CIEM tool. The CIEM tool will be responsible for continuous inventorying and analyzing

identities as they get created/modified/deleted in the cloud landscape. CIEM uses API based approach for continuous discovery and monitoring of the cloud landscape

Fig. 3. Modification of existing identity



Stage 2:

Enterprise Readiness Requirments:

- Identity process maturity has happened in adoption of cloud factory. As part of maturity catalogues have been introduced into the ITSM workflows to make risk decisions for the identity requested
- Application teams have been educated about the consequences of bad identity hygiene and the role they can play in correcting process.
- DevOps structure is further strengthened to ensure security controls in the pipelines delivering identity to cloud.
- CIEM observations are actioned for at least 40% improvement so that inherited identity deficiencies are corrected.
- Workbooks are created so that they can be manually triggered for specific category of identities.

Functional Flow:

There are 2 functional approaches that will have to be adopted:

Approach 1: ServiceNow backed approach for Human Users

In this approach, ServiceNow workflows will be created and enabled with decision making data for entitlements requested. Associated with workflows will be downstream playbooks which will be required to be triggered by SecOps engineer basis on the entitlement selected. The playbooks will have templated structures which will be auto populated for a request with the entitlements requested. The below diagram is a logical progression of the Fig. 2 above but it adds little more automation. It also now requires a SecOps engineer only to deliver the identity.

Functional Flow:

There are 2 functional approaches that will have to be adopted:

Approach 1: ServiceNow backed approach for Human Users

In this approach, ServiceNow workflows will be created and enabled with decision making data for entitlements requested. Associated with workflows will be downstream playbooks which will be required to be triggered by SecOps engineer basis on the entitlement selected. The playbooks will have templated structures which will be auto populated for a request with the entitlements requested. The below diagram is a logical progression of the Fig. 2 above but it adds little more automation. It also now requires a SecOps engineer only to deliver the identity.

Approach 2: Delegating the complete non-human cloud Identity creation to Application/Project Owners.

In this approach (assume Terraform for IAC), Terraform modules will be created and approved for security and enterprise requirements. Next the application will be instructed to consume these templates for creation of all non-human cloud identities. For the identity creation, secure IAC code pipeline will be structured, and this pipeline will have 6-eye review for each Pull request. Additionally, code pipelines controls will be controlled with plugins such as Sentinel plugin in Terraform enterprise. These plugins will help to create gating controls to ensure that identity created aligns with security best practices and enterprise hygiene. As part of the 6-eye approval process will be approval from the identity review board. This review board will be responsible will be empowered with all the catalogue data for cloud services and

associated entitlements mapping. Additionally, this mapping study will be continuous exercise and will be responsibility of the IAM governance team to continuous add to the catalogue to match the dynamic changing nature of the cloud.

Fig. 4. Phase2 Approach for Human Users

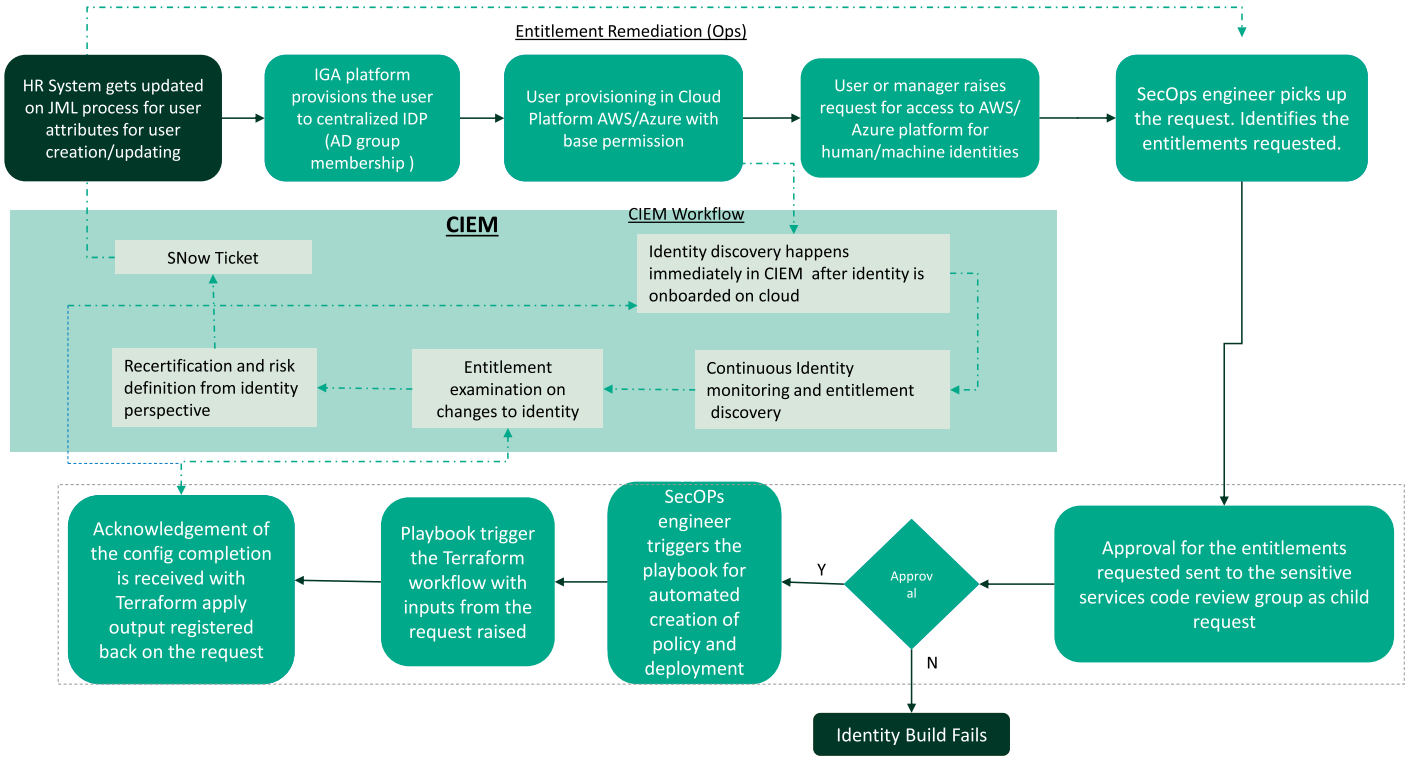
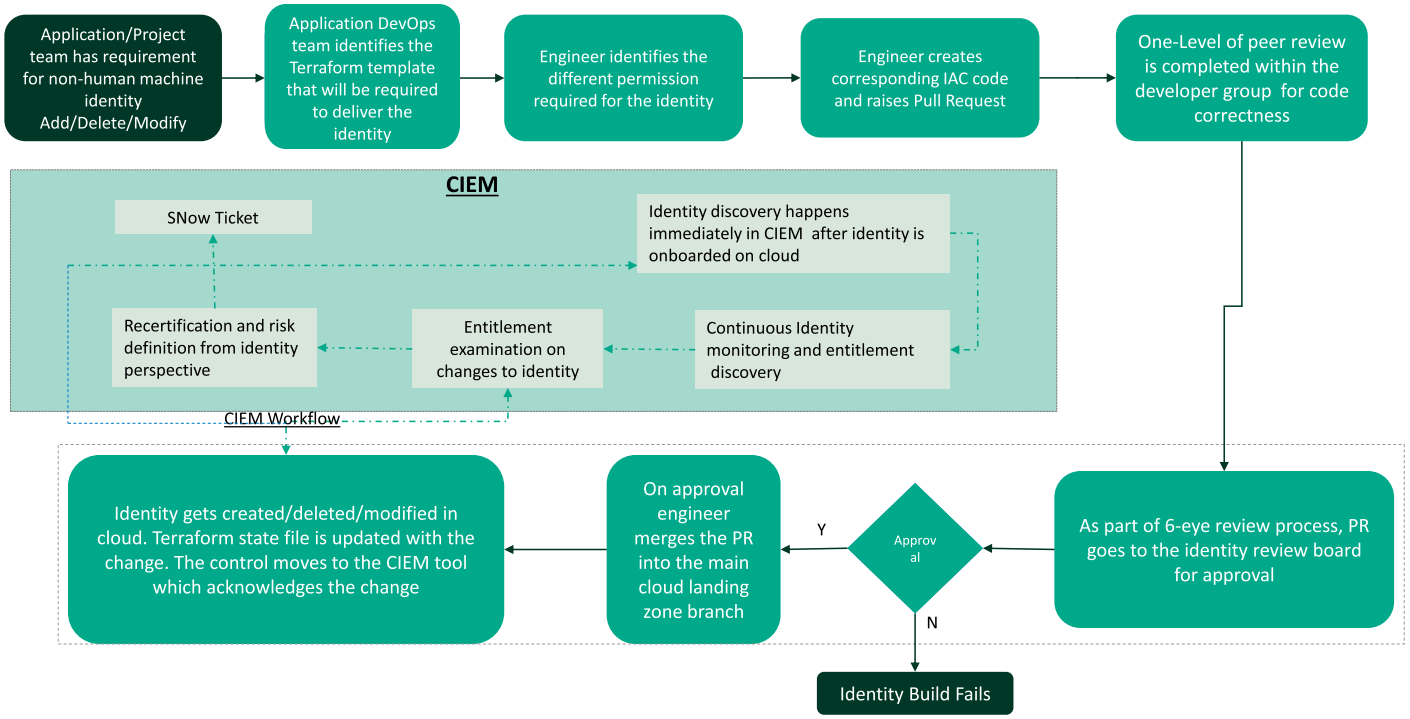


Fig. 5. Phase2 approach for non-human users



Phase 3: Further refinement of the human user change with Service now with full automation

Enterprise Readiness Requirement:

- Complete identity catalogue workflows integration into ServiceNow has been completed
- Downstream action triggers and automated scripts at the backend of the workflows have been configured and tested
- CIEM tool maturity has improved and we are at close to 95% on mitigation of critical and high identity risks

Functional flow:

At the final stage of implementation, there is a semi automated factory model for human identities which has been derived from Phase 2. The non-human identity structure and lifecycle is pretty much set at phase 2, however continuous improvement with Sentinel type plugin optimization and Terraform modules restructuring is security mandate.

At this stage, ServiceNow structure will be completely automated and end to delivery of Human-User Lifecycle on cloud will further be completely automated.

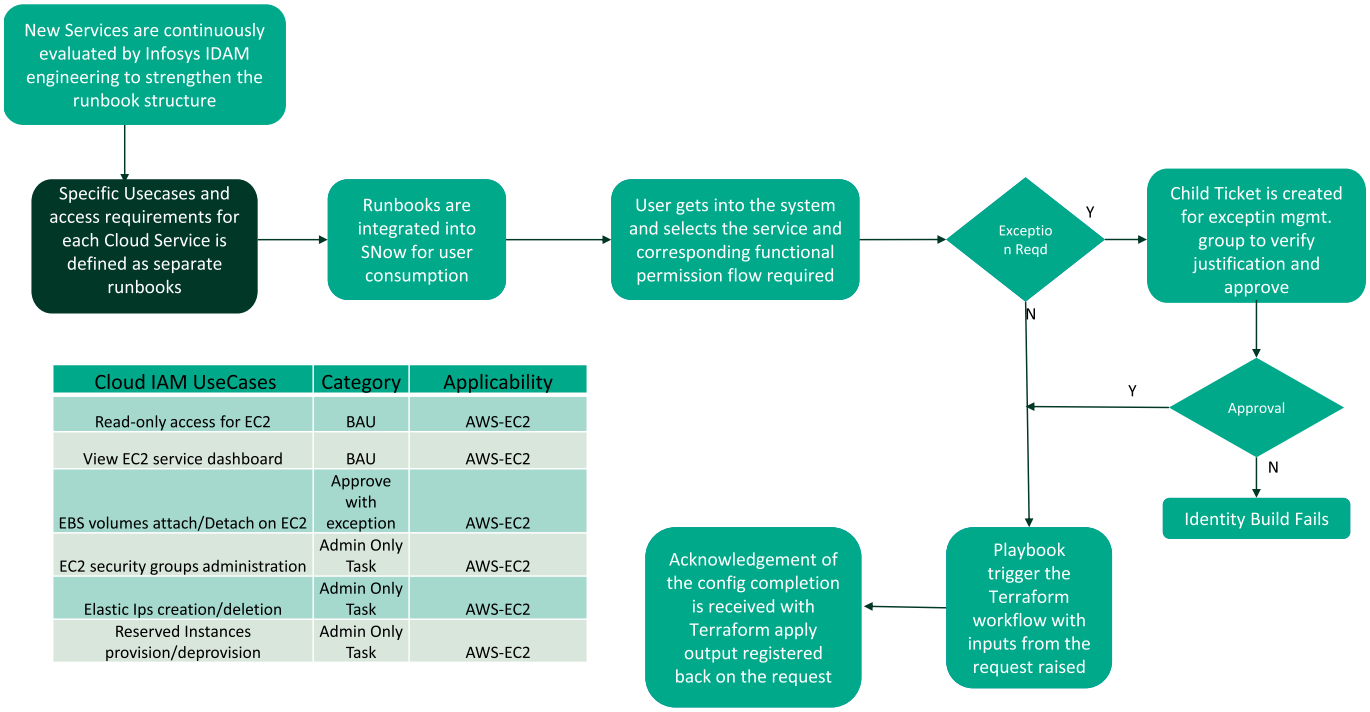
As part of the end-to-end process, identity catalogue which has been in development from Phase 1 will be completely integrated into the Service Now. As an identity change gets requested, based on the entitlements requested they will be quantified as "BAU", "approve with exception" or "Admin Only Task". Further, after risk type association with request, appropriate runbook will be chosen according to the risk. The runbook will have a back ending

template which will be auto populated with the entitlements requested. If it is a BAU identity, then as part of the runbook the identity change will directly be configured on cloud platform with no human touch. However, if exception-based entitlements are requested child ticket for approval will be created. Based on approval identity change will go further. Finally, if admin-only change is requested, request will be directly rejected and same will be communicated back to requestor.

The Fig. 6 above shows an outline of the process from AWS entitlement point of view for risk calibration. It further talks about the end-to-end approach with no human touch.

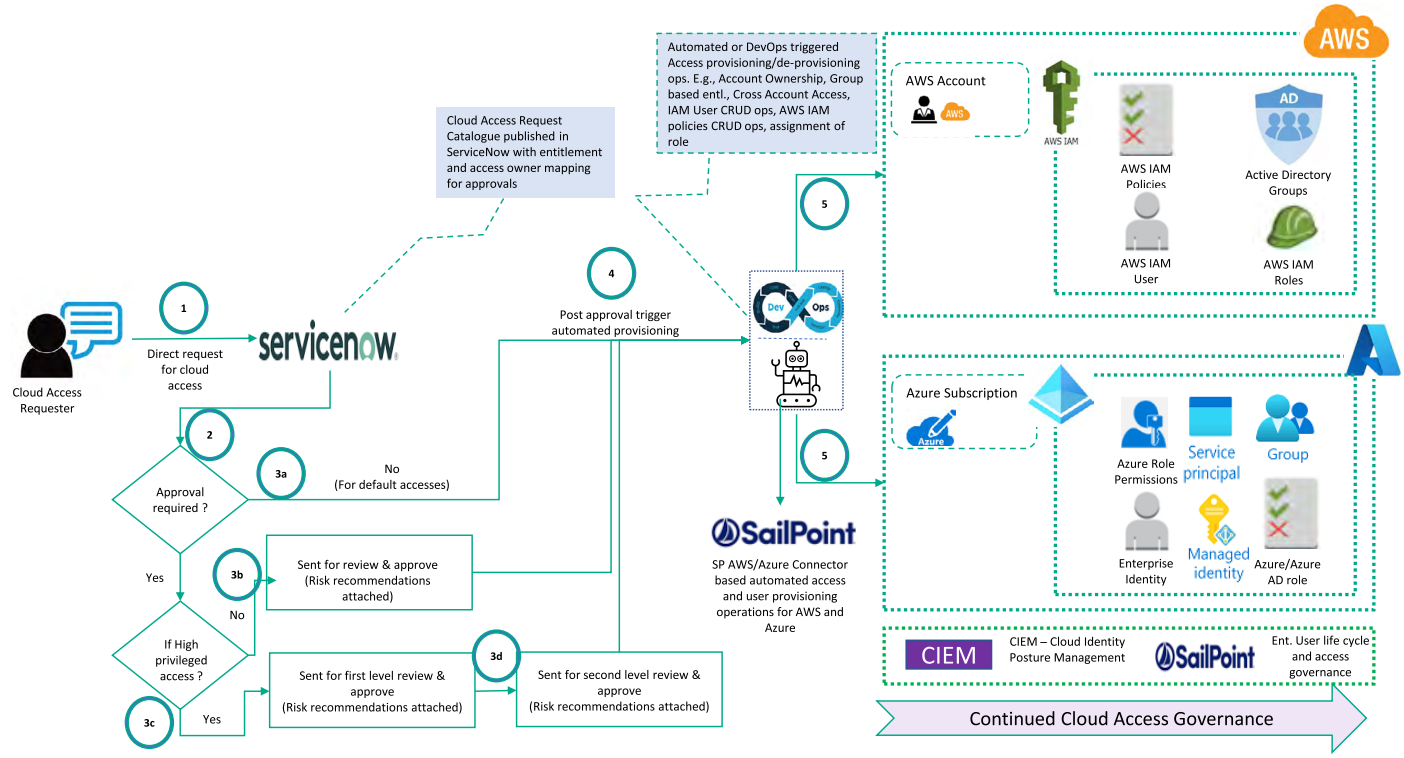
Below is the culmination of the design (fig 7) that has been envisioned as part of this whitepaper.

Fig. 6. Phase 3 Cloud IAM Factory



Cloud IAM UseCases	Category	Applicability
Read-only access for EC2	BAU	AWS-EC2
View EC2 service dashboard	BAU	AWS-EC2
EBS volumes attach/Detach on EC2	Approve with exception	AWS-EC2
EC2 security groups administration	Admin Only Task	AWS-EC2
Elastic Ips creation/deletion	Admin Only Task	AWS-EC2
Reserved Instances provision/deprovision	Admin Only Task	AWS-EC2

Final High Level Design (Human User)



Deviation Options/Opportunities:

1. **Handling both human and non-Human identities with code:** This process will eliminate the entire involvement of ServiceNow in the identity management process. After the initial landing zone and user group creation with birthright permissions, all other human and non-human user entitlement changes will be managed with code.

- **Pros:**

  1. Eliminates the development overhead for ServiceNow.

  2. Pushes the entire cloud identity lifecycle to the Application Team

  3. Identity Ops will be restricted to governance after the initial landing zone creation.

- **Cons:**

  1. For Human users, no cloud entitlement view in your traditional IGA systems. This breaks the visibility principle for human identity.

2. **Lightweight ServiceNow and Scripting Approach:** In this approach, the existing ServiceNow setup will be pushed to the customer with a well architected request form. Post which SecOps engineer will pick up the request and directly run scripts to configure/modify the cloud identity. This is in line with Phase 1 suggested above, but it will be faster with very few moving parts. Approval system will be retained to provide governance.

- **Pros:**

  1. Minimal DevOps requirements

  2. Centralized Cloud Identity creation, management, and governance

  3. Less time to delivery of the model

- **Cons:**

  1. As the cloud landscape grows, model becomes unscalable.

  2. Approach doesn't eliminate issues with traditional IAM management.

  3. Human error is very much in play which could lead to major cloud disasters.

Potential challenges:

1. Adoption of the factory model and general culture change requirement
2. Competency across various technologies and processes such as Service Now, cloud IAM and DevOps
3. Continuous improvement on the catalogue document corelating cloud services with associated entitlements
4. Native IGA tools scaling and adding value to cloud IAM process.
5. Increased Automation requires increased governance, so it is very important in process of application deployments that the governance shouldn't take a backseat.

6. Operations Team Support, for regular maintenance and update of the factory model and structure.

Conclusion:

As organization embark or mature in their digitalization, solving the identity management problem will be a major objective. Through this whitepaper, vision is to assist teams or enterprises in their endeavor to conquer that objective. Document discussed the different phases of maturity and doesn't indicate a big bang move which helps enterprises to gradually adopt and settle into the solution. While identity delivery is the main objective, equal emphasis is placed on the peripherals around the same. Hence, there is mention of getting good organization guardrail definition and continuous governance with a tool like CIEM (Cloud Infrastructure Entitlement Management). If the document is followed through the phases defined, operational efficiency up to 80% can be achieved. Also, free up cycles for Identity Ops team to focus on governance and continually optimize policies inline with the dynamic structure of cloud.

About the Author

Vinit Ajgaonkar

Principal Consultant

Vinit is a Cloud Security Architect with an excellent ability to help the customer in their digital transformation journey. He holds a rich experience of more than 14 years in Cybersecurity domain and has the right mix of technology thought leadership, backed by hands-on tool/technology-focused curiosity. Vinit is currently a part of the Infosys Cyber Innovation, Strategy & Excellence team which dwells into next generation cybersecurity solutions and strategies.

For more information, contact askus@infosys.com

Infosys®
Navigate your next