WCIR | Wipro Council for Industry Research

WIPRO
Applying Thought

IDENTITY & ACCESS MANAGEMENT IN THE CLOUD

www.wipro.com

Niraj Kumar Shukla

Table of Contents

Cloud is changing the way a business operates, driven by cost efficiencies and economies of scale. However, failure to implement effective security can undermine the benefits of cloud computing. Identities, trust, authentication and access controls have obtained additional significance in the cloud world. Hence, the planning and implementation of Identity and Access management (IAM) for the cloud has become a key control in cloud adoption. Ensuring IAM is appropriately considered and implemented would not only help an organization meet compliance obligations but would also ensure optimum cost benefits of the cloud transition.

1. Introduction

This paper intends to provide a Point of View (POV) on the various considerations for IAM for the cloud and guidance to organizations on the approach to take for IAM deployment.

2. IAM Approach

Phased approach to deploy IAM for the cloud helps minimize the risks and leverage benefits of the cloud faster.

1. Plan – This phase includes understanding the environment and risk analysis for IAM when moving to the cloud.
2. Design – The IAM framework and architecture for target state, and the test plan should be created in this phase. Additionally, metrics for measuring IAM effectiveness should also be defined.
3. Pilot – In this phase, the IAM solution should be rolled out for a subset of users, and tests related to workflows, connectivity, performance etc. should be carried out.
4. Deploy – On success of the pilot phase, full scale deployment for all users should be rolled out.

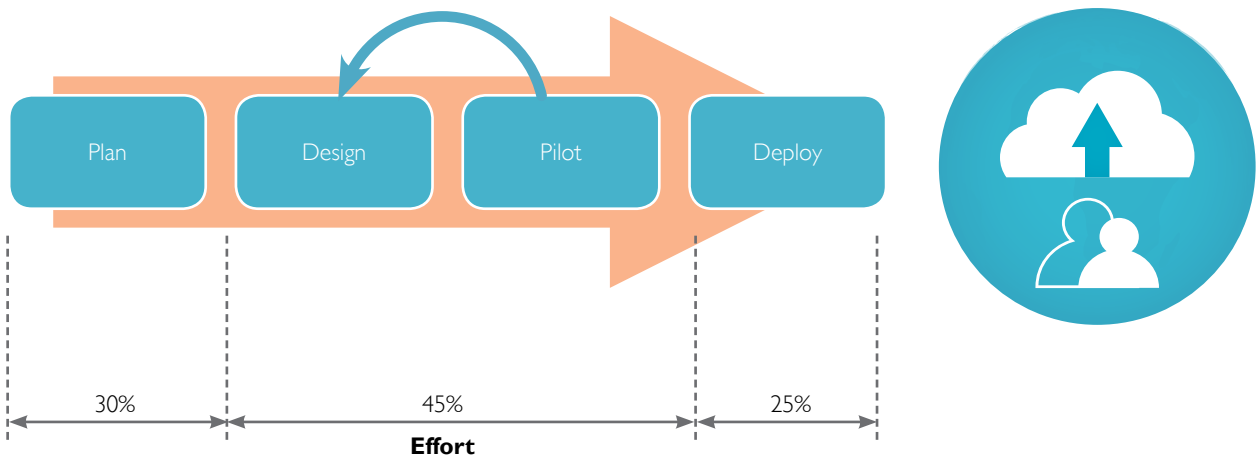

Figure 1: Phased Approach for IAM deployment

Effort breakup between phases would depend on the cloud service/ deployment model, organization risk appetite, solution complexity and the user base (volume and type of users). However, as a general guidance, we recommend about 30% effort for Plan, 45% for Design and Pilot, with the remaining effort for Deploy.

It is recommended that significant effort be dedicated to planning for IAM, since proper planning leads to successful deployment. Due to the evolving nature of the cloud, the Design and Pilot phases typically tend to be iterative with feedback from the Pilot leading to further design updates. Effort for the Deploy phase can be comparatively lower, as it is assumed that design issues are addressed before full scale deployment. However, one should factor in some additional effort in Deploy to address risk of any full scale deployment issue.

2.1 Phase I - Plan

Planning is a very important part of IAM deployment on the cloud. An organization needs to think through the cloud use cases, understand the risks and evaluate the technical options to build a reliable and sustainable process and technical architecture/framework. Additionally, all aspects related to compliance requirements must also be assessed and addressed.

Wipro recommends the following activities in this phase:

1. Understanding the Environment
2. Identification of users and required Access Controls
3. Risk Assessment and Gap Analysis

2.1.1 Understanding the Environment

It is essential to understand details about the:

» Target Cloud

» Existing IAM Solutions / Directory Services

Target Cloud

The cloud being considered could be of any one of the different service models (IaaS, PaaS, SaaS) or any one of the deployment type (Public, Private). In more complex scenarios, it could be even a combination of different cloud types. Eg: an organization could be considering deploying an application on AWS (IaaS) and may also be using Salesforce or Workday (SaaS) for the same user set.

The type of cloud chosen impacts the risk and how the identities and access would be handled. For eg: for public IaaS one may need to consider identities and access for administrators managing the server instances; however, for private IaaS one would need to additionally consider access controls for underlying hardware, virtualization platform and network components (switches, firewalls etc.) as well.

Organizations also need to assess cloud provider capabilities with respect to identity and access management and its support for various industry standards such as SPML, SAML, OAuth etc.

Existing IAM Solutions / Directory Services

Organizations may want to leverage the existing IAM environments for cloud for various reasons, such as but not limited to –

» Existing investments

» Tight coupling with application migration candidates

» Well defined and matured workflow

It becomes important to ensure that documentation regarding existing solution capabilities and deployment is available, so that integration feasibility can be ascertained and the appropriate design can be built.

2.1.2 Identification of Users and required Access Controls

Next, the organization must look at and categorize the type of users for the cloud. If we consider IaaS as an example, the users could broadly be categorized into the following types of users, as per the table below.

Users	Responsibilities
Cloud Administrators	This set of users would be responsible for managing the cloud environment. For example, on AWS these would be users responsible for creating new EC2 instances, managing VPN connectivity to AWS, Security groups management, S3 access management etc.
OS and application administrators	These users would need access to specific cloud instances for configuring the OS or application parameters, installing software, monitoring and remediating OS/app performance etc.
Application Users	End users requiring access to the application deployed on the cloud

Table 1: IaaS User Types

For each type of user, it is important to map the access controls required. One can do a high-level access control mapping at this stage. Fine-grained access for users and groups can be defined during the design stage.

2.1.3 Risk Assessment and Gap Analysis

A better understanding of the cloud environment and user access requirements would help in carrying out Risk Assessment and Gap Analysis for IAM. It is important to understand the risks so that the organization can suitably address them. The organization may then decide to treat the risks in any of the following ways:

- Avoid – by deciding to forego features leading to the risk
- Mitigate – by addressing it in the IAM design, or
- Transfer –to the cloud service provider (by suitably including in contracts), or
- Accept – the risk and suitably budget for it.

2.2 Phase II - Design

This phase includes the following activities:

1. Technical Design, Process Framework and Policy Creation
2. Test Plan Creation
3. Defining the Metrics

2.2.1 Technical Design, Process Framework and Policy Creation

The final design would emerge from this step. The design should not only include the technical architecture but also define the process framework. All process workflows (eg: provisioning/de-provisioning, access requests etc.) for the cloud should be clearly documented.

There are different architecture models for IAM and careful consideration should be given to each when designing the solution. IAM for the cloud can leverage either IAM deployment in the datacenter or IAM in the cloud. The IAM in the datacenter could either use an existing solution (discussed in earlier sections) or a new solution. There are pros and cons to each approach and the table below provides a general guidance for consideration of the factors of comparison, when evaluating the alternative approaches.

One can also consider a hybrid approach where the identity store resides within the corporate datacenter and the cloud based IAM solution integrates with it. This approach addresses the key concern of loss of control over the identity store and at the same time enables the organization to leverage other benefits of IAM on the cloud.

	IAM in the datacenter	IAM in the cloud
Cost	**High Capex.** Cost of hardware, software licenses, setup etc. Need to factor for growth.	**Cost effective.** Dependent on usage
Security of Identity store	Dependent on providers security controls. Organizations are generally more wary of **loss of control** of identity store.	Since the Identity store is in the **organization control,** it generally feels more comfortable.
Integration with on-premise applications	**Easier** integration.	More **difficult.**
Technology updates	**Slower.**	Generally providers rollout **faster** updates to keep up with market demands and for competitive advantage
Vendor Lock-in	**Depends** on the deployment architecture	Could be **High**

Table 2: Evaluation factors for IAM deployment models

The Cloud Security Alliance (CSA) identifies the following major IAM functions essential for successful and effective management of identities in the cloud:

- Identity Provisioning/de-provisioning – secure and timely management of on-boarding and off-boarding users in the cloud
- Authentication – includes considerations for authentication-related challenges such as credential management, strong authentication (multi-factor authentication), delegated authentication, and managing trust across all types of cloud services
- Federation – secure exchange of identity attributes between the service provider (SP) and Identity Provider (IdP) and solutions to address challenges with respect to identity lifecycle management, available authentication methods to protect confidentiality, and integrity while supporting non-repudiation.
- Authorization and user profile management – includes establishing trusted user profile and policy information, using it to control access within the cloud service and doing this in an auditable way.

The design should factor in the above and ensure that compliance is a key consideration throughout.

User and group policies should be defined at this stage. Careful consideration should be given to policy formation and should be done in discussions with stakeholders to keep optimum balance between security and ease of access.

2.2.2 Test Plan Creation

Test Plan should be created and test cases designed such that all possible use cases are covered. The testing should not only verify the functionality but performance, reliability and security as well. Suitable test planning would help to ascertain the success or failure of deployment.

2.2.3 Defining the Metrics

The final activity in the Design phase should be to define the metrics to measure process effectiveness. Data sources should be identified and basic measurements should be established. Many organizations do not put focus on metrics; however this activity should not be neglected as it helps an organization get improved visibility on its security operations. As a practical approach, one could start with a smaller set of metrics and gradually build the metrics program.

2.3 Phase III - Pilot

The third phase of IAM deployment should be to implement the design for a subset of users. This is an important phase because the success of the IAM deployment depends on this phase. If testing is not appropriately done or if the coverage is not complete, the deployment may fail, leading to cost escalations for the organization.

Issues observed during testing should serve as a feedback to the design. Once issues are rectified and design updated, the corrected configuration should be re-tested. This iterative process should continue until all issues are resolved. The final design, after inclusion of all corrections, should then be made available for the Deploy phase.

2.4 Phase IV - Deploy

This is the final phase where the IAM design, suitably tested and verified, is deployed for the entire user base. The metrics program and measurements should be put in place. The operations team should be involved from the inception of the IAM program to facilitate smooth handover. Relevant documents should be created and published so that these can be available to operations and other teams, as needed.

3. Conclusion

Identity & Access Management is a security consideration that cannot be overlooked. It requires careful planning and strong understanding of the technologies involved. IAM is a large domain and consideration of every IAM function and technical details/options is beyond the scope of this paper. The approach outlined here however, is intended to provide a high-level guidance to organizations on deployment considerations and steps to follow for IAM, ensuring a process approach that can provide the cost benefit an organization seeks from its cloud migration.

4. References

1. Security Guidance for Critical Areas of Focus in Cloud Computing - https://cloudsecurityalliance.org/research/security-guidance/
2. Cloud Security Alliance: Security as a Service (SecaaS) - https://cloudsecurityalliance.org/research/secaas/

About the Author

Niraj Kumar Shukla is a Security Architect with the Cloud Enablement Services at Advanced Technologies. In his experience of over 14 years, he has led information security consulting engagements and solution architecting for customers across domains and has been instrumental in setting up security CoEs. His interests and experiences span diverse areas including Security strategy and governance, network, application and data security. As part of his current role, he is responsible for practice and solution development for Cloud security.

About Wipro Integrated Cloud Services

Wipro's Integrated Cloud Services focuses on creating differentiation for customers across Cloud Infrastructure, Platforms, Applications, and Business Processes. Driven by a strong set of Cloud IPs and partnerships with the world's leading Cloud vendors, Wipro has established itself as a leading integrated Cloud services provider, and has already proven its expertise in large transformational Cloud engagements with leading global enterprises across industry verticals.

About Wipro Council for Industry Research

The Wipro Council for Industry Research, comprised of domain and technology experts from the organization, aims to address the needs of customers by specifically looking at innovative strategies that will help them gain competitive advantage in the market. The Council, in collaboration with leading academic institutions and industry bodies, studies market trends to equip organizations with insights that facilitate their IT and business strategies. For more information please visit www.wipro.com/insights/business-research

About Wipro Technologies

Wipro Technologies, the global IT business of Wipro Limited (NYSE:WIT) is a leading Information Technology, Consulting and Outsourcing company, that delivers solutions to enable its clients do business better. Wipro Technologies delivers winning business outcomes through its deep industry experience and a 360 degree view of "Business through Technology"– helping clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, a practitioner's approach to delivering innovation and an organization wide commitment to sustainability, Wipro Technologies has over 140,000 employees and clients across 54 countries.

For more information, please visit www.wipro.com or contact us at info@wipro.com

DO BUSINESS BETTER

WWW.WIPRO.COM

NYSE:WIT | OVER 140,000 EMPLOYEES | 54 COUNTRIES | CONSULTING | SYSTEM INTEGRATION | OUTSOURCING

WIPRO TECHNOLOGIES, DODDAKANNELLI, SARJAPUR ROAD, BANGALORE - 560 035, INDIA

TEL: +91 (80) 2844 0011, FAX: +91 (80) 2844 0256

North America South America Canada United Kingdom Germany France Switzerland Poland Austria Sweden Finland Benelux Portugal Romania Japan Philippines Singapore Malaysia Australia