CMSGu2013-05

NCB

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Implementing Cloud Identity and Access Management

CERT-MU

National Computer Board
Mauritius

Version 1.0

November 2013

Issue No. 5

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this document is to give organisations an indication on the secure implementation of a cloud Identity and Access Management.

1.2 Audience

The target audience for this document includes cloud administrators, operating system and application administrators, cloud application users and all other relevant parties involved in the deployment of identity and access management for a cloud environment.

1.3 Document Structure

This document is organised into the following sections:

Section 1 provides an overview on the document's content, the targeted audience and the document's structure.

Section 2 gives a background on Identity and Access Management in the cloud.

Section 3 presents the main Identity and Access Management functions.

Section 4 explains how to deploy a secure cloud Identity and Access Management.

Section 5 concludes the document.

Section 6 consists of a list of references that have been used in this document.

Appendix A provides a list of acronyms that have been used in the document.

2.0 Background

Cloud computing has gained much prominence these days because of its ability to provide very scalable services at low costs. However, the concern for security is perceived as a blocking point towards its adoption. Managing identities and access control for enterprise applications remains one of the greatest challenges facing the IT industry today.

In Cloud computing the entire users' data is kept on the service provider's side, therefore requiring the need for proper security measures and frameworks. Proper identity management may be seen as the first step towards securely accessing any kind of service from the cloud. Organisations need to control who has access to which systems and technology within the enterprise. Establishing and maintaining that control efficiently and effectively can be a challenge, and incorporating cloud technologies to an existing IT infrastructure adds further complexity and risk.

The constant need for security and compliance is pushing some organisations to find better ways to link enterprise Identity and Access Management (IAM) and cloud provider applications.

3.0 Identity and Access Management (IAM) Functions

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

3.1 Identity Provisioning

One of the main challenges for organisations utilising cloud computing services is the secure and judicious management of on-boarding (provisioning) and off-boarding (deprovisioning) of users in the cloud. In addition, enterprises which have invested in user management processes within an enterprise will seek to extend those processes to cloud services.

3.2 Authentication

When organisations make use of cloud services, authenticating users in a reliable and convenient manner is a fundamental requirement. Organisations have to address authentication-related challenges such as credential management, strong authentication, delegated authentication, and managing trust across all types of cloud services.

3.3 Federation (Partnership)

In the cloud computing environment, Federated Identity Management plays a crucial role in enabling organisations to authenticate their users of cloud services using the organisation's chosen identity provider (IdP). In this context, exchanging identity attributes between the service provider (SP) and the IdP securely is also required. Organisations considering federated identity management in the cloud should understand the different challenges and possible solutions to address those challenges with respect to identity management, available authentication methods to protect confidentiality, and integrity, while at the same time, supporting non-repudiation.

3.4 Authorisation and User Profile Management

The requirements for user profiles and access control policy vary, depending on whether the user is acting on their own behalf (such as a consumer) or as a member of an organisation (such as an employer, university, hospital, or other enterprise). The access control requirements in cloud environments include establishing trusted user profile and policy information to control access within the cloud service.

3.5 Compliance

For customers who rely on cloud services, it is important to understand IAM can enable compliance with internal or regulatory requirements. Well designed identity management can ensure that information about accounts, access grants, and segregation of duty enforcement at cloud providers, can all be combined to satisfy an enterprise's audit and compliance reporting requirements.

4.0 Deploying a secure Cloud IAM

According to Wipro, a phased approach can be used to deploy IAM for the cloud as this helps minimise the risks and leverage benefits of the cloud faster.

1. **Plan:** This phase includes understanding the environment and risk analysis for IAM when shifting to the cloud.

2. **Design:** The IAM framework and architecture for target state, and the test plan should be created in this phase. Metrics for measuring IAM effectiveness should also be defined here.

3. **Pilot:** In this phase, the IAM solution should be rolled out for a selected group of users, and workflows, connectivity and performance should be tested.

4. **Deploy:** Upon the successful migration during the pilot phase, full scale deployment for all users should be rolled out.

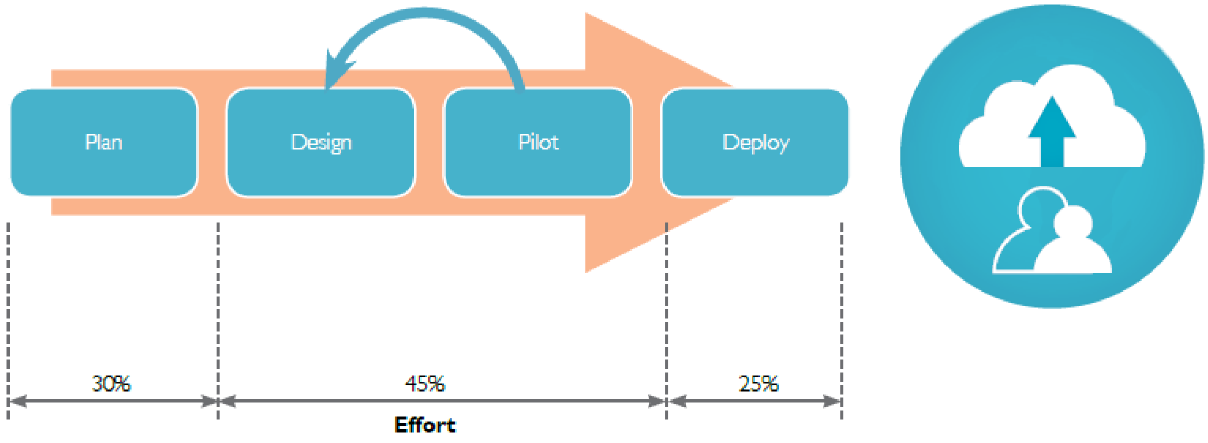

Figure 1 Phased Approach for IAM Deployment

The distribution of effort between phases would depend on the following:

- The cloud deployment model
- The organisation’s risk appetite
- The solution complexity
- The number and type of users

However, as a general rule, about 30% effort for “Plan”, 45% for “Design and Pilot” and 25% for “Deploy” may be allocated.

It is also recommended that considerable effort be given to planning for IAM, since proper planning leads to successful deployment. Due to the growing nature of the cloud, the Design and Pilot phases usually tend to be iterative with feedback from the Pilot leading to further design updates. Effort for the Deploy phase can be fairly lower because all design issues should already be addressed before full scale deployment.

However, some additional effort should be put in Deploy to address any arising risks during full scale deployment.

4.1 Phase I – Plan

Planning is a very important part of IAM deployment in the cloud. An organisation needs to grasp the cloud use cases, understand the risks and evaluate the technical requirements to build a reliable and sustainable process and technical framework. Furthermore, all compliance requirements must be assessed and addressed at this stage. In general, the following activities should be carried out:

4.1.1 Understanding the Environment

It is essential to know about the:

- **Type of Cloud under consideration**

  The cloud being considered could be of any one of the different service models (Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS)) or any one of the deployment type (Public or Private). It could be even a blend of different types of cloud. The type of cloud chosen impacts the risk and how the identities and access would be handled. For instance, for public IaaS, identities and access for administrators managing the server instances should be considered; however, for private IaaS, access controls for underlying hardware, virtualization platform and network components (switches, firewalls etc.) should be considered as well.

  Organisations also need to assess cloud provider capabilities with respect to IAM and its support for various industry standards such as Service Provisioning Markup Language (SPML), Security Assertion Markup Language (SAML) and Open Standard for Authorisation (OAuth).

- **Existing IAM Solutions / Directory Services**

  Organisations may want to leverage the existing IAM environments for cloud for various reasons. These include, but are not limited to:

  - Existing investments
  - Tight coupling with application migration candidates
  - Well defined and matured workflow

It is essential to ensure that documentation with regards to existing solution capabilities and deployment is accessible, so that proper integration can be established and the correct design built.

4.1.2 Identifying the Users and required Access Controls

Users	Responsibilities
Cloud Administrators	This set of users would be responsible for managing the cloud environment. For example on Amazon Web Services these would be users responsible for creating new EC2 instances, managing VPN connectivity to Amazon Web Services, Security groups management, and S3 access management.
Operating System and Application Administrators	There users would need access to specific cloud instances for configuring the OS or application parameters, installing software, monitoring and remediating Operating System/Application performance.
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. Granular access for users and groups can be defined during the design stage.

4.1.3 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 organisation can effectively address them. The organisation may then decide to treat the risks in any of the following ways:

1. **Avoid –** by deciding to forego features leading to the risk
2. **Mitigate –** by addressing the risk in the IAM design
3. **Transfer –** to the cloud service provider (by duly including it in contracts), or
4. **Accept –** the risk and allocate the appropriate budget for it.

4.2 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

4.2.1 Technical Design, Process Framework and Policy Development

The final design would materialise from this step. The design should not only include the technical architecture, but also define the process framework. All process workflows (for example, 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 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 organisation to leverage other benefits of IAM in the cloud.

	IAM in the Data Centre	**IAM in the cloud**
Cost	High. (Cost of hardware, software licenses, setup etc. Need to cater for growth).	Low. (Cost effective, dependent on usage).

Security of Identity store	Dependent on the provision of security controls. Organisations are generally more wary of loss of control of Identity store.	Since the Identity store is in the orgnisation control, it generally feels more comfortable.
Integration with existing applications	Easier.	More complex.
Technology updates	Slower.	Faster. (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

As mentioned earlier, the following major IAM functions essential for successful and effective management of identities in the cloud:

- Identity Provisioning/de-provisioning
- Authentication
- Federation
- Authorisation and user profile management

The design phase should include the above and ensure that compliance is a key concern all the way through. User and group policies should be defined at this stage. Careful consideration should be given to policy development and should be done in discussions with stakeholders to keep the best possible balance between security and ease of access.

4.2.2 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 determine the success or failure of deployment.

4.2.3 Defining the Metrics

The final activity in the Design phase should be to define the metrics to evaluate process efficiency. Data sources should be identified and basic measurements should be established.

Many organisations do not focus on metrics; however this activity should not be ignored as it helps an organisation achieve better visibility on its security operations. As a practical approach, one could start with a smaller set of metrics and gradually build the metrics program.

4.3 Phase III - Pilot

The third phase of IAM deployment should be to implement the design for a small group of users. This is an important phase because the success of the IAM deployment depends on this phase. If testing is not properly done or if the coverage is not complete, the deployment may fail, adding cost to the organisation.

Issues found during testing should be used as feedback for the design phase. Once the issues are addressed and design updated, the updated configuration should be re-tested. This iterative process should continue until all issues are resolved. The final design, after all updates have been done, should then be made available for the deploy phase.

4.4 Phase IV - Deploy

This is the final phase where the IAM design, correctly tested and verified, is deployed for all users in the organisation. The metrics program and measurements should be established. The operations team should be involved from the start of the IAM program to ensure a proper and smooth handing over. Relevant documents such as policies, procedures and guidelines should be created and published so that these can be available to operations and other teams, as and when required.

5.0 Conclusion

Cloud is changing the way organisations operate, driven by its low cost and large scale. However, failure to implement effective security can weaken its benefits. Identities and access controls have gained much significance in the cloud arena. Hence, the proper planning and implementation of IAM has become a key control in the cloud adoption. Ensuring an appropriate IAM implementation would not only help an organisation meet compliance requirements, but would also ensure the best cost benefits of the cloud migration.

6.0 References

- Cloud Security Alliance, **https://cloudsecurityalliance.org/**
- Wipro Council for Industry Research, **http://www.wipro.com**
- DELL, **www.dell.com**
- Dark Reading, **www.darkreading.com**

Appendix A

List of Acronyms

CSA	Cloud Security Alliance
IAM	Identity and Access Management
IaaS	Infrastructure-as-a-Service
IdP	Identity Provider
OAuth	Open Standard for Authorisation
PaaS	Platform-as-a-Service
SaaS	Software-as-a-Service
SAML	Security Assertion Markup Language
SP	Service Provider
SPML	Service Provisioning Markup Language