Integrated IdM System in Hybrid IT Environment

Real-time inter-operability between IAM Platform based On-Premise and On-Cloud

Identity Bridge: Vol. 2.01.2017

Table of Contents

Section 1 Introduction to Challenges in Hybrid IdM

IT Systems are transforming at a great speed. In a business setup, hybrid setup is fueling the digitization agenda – the technical capabilities are dependent on cloud and premise. Some applications are linked on premise, and some to cloud – it is crucial to ensure that the identity and access dynamism falls in line with required enterprise's considerations and compliant with regulations. In keeping with strategic requirements of IT function, Hybrid setup is aligning to future needs by transforming IT architectures and the role supported by IT.

What was set with a novel intent – needs perpetual support of IT geeks and relevant tools! Amidst workflows and identity considerations, IT teams are deputed to ensure operational efficiency and reduced complexity. They are busy consolidating workloads, juggling with concerns regarding user life cycle management, IT Security, Corporate Governance, System performance, migration, upgrades and integrations.

The struggle is further accentuated as one navigates between disparate systems, bring identity consistency and manage admin dashboards of multiple applications. All this is to be done while ensuring that any of the systems or tools is not going out of operation.

While enterprises are grappling with the challenge of ensuring that systems are running smooth - the problem can be broadly categorized into following sections:

- Lack of synchronization between data fed into the platforms, IT department has to be on its toes to ensure that the information is entered in manually on all IdM systems to ensure consistency
- Unifying identities from multiple target sources such as Active Directories becomes a challenge and results into creation of duplicate identities in Identity Management System
- Struggling with multiple integrations, thereby seeking support from a complex, cluttered and burdened IT System? Establishing integrations amongst Applications and tools with IAM platform can be a challenging and costly task

As businesses are increasingly seen to be moving towards cloud-based platforms, not much thought is taken into consideration for ease of integrate with existing on-premise applications and/or IAM Setup. Hybrid integration solutions are becoming an essential tool for organizations that are considering to combine on-premises applications with cloud-applications, there are complexities in the overall scheme of IT Systems.

In the successive sections we will run through various cases and situations where key challenges of Hybrid IT can be subverted via IAM technology. We will discuss about Identity Bridge, a solution to fix the integration problems in hybrid setup.

Section 2 Creating Integrated IdM Systems

Seamless interaction between numerous IT Systems can power synchronous interaction between two distinct systems, enabling them to undertake IAM tasks in real-time. It is crucial to ensure any interaction between different infrastructures falls in-line with company's access governance policy, enforces controls and reduced complexity.

Many cloud-based applications are being used to support enterprise operations. It leads to creation of identities directly on applications or on cloud based IdM System. This creates a problem of overlapping identity information, which in turn requires massive identity management efforts and maintaining multiple IAM Ecosystems. The IT Department have to achieve consistency in managing identity, together with maintaining multiple IdM platforms on a perpetual basis. That's where the need to integrate IAM platforms On-Cloud and On-Premises arises as asynchronous IdM platforms are error prone systems that lack scalability potential.

Furthermore, unification of identities is an important aspect of any IdM System. Identities unification from multiple target sources such as Active Directories becomes a challenge and results into creation of duplicate identities in IdM System. For IT integrations, target sources are burdened to supply identity related information to ensure correct access to applications, tools and/or IT Systems. This integration approach necessitates the target sources to link identities with diverse and unrelated information, impacting system efficiency and IT workflows. In many cases target sources are not the true identity sources, therefore pulling identity from an untrue identity source results into additional maintenance challenges.

Identity information on multiple target sources may be overlapping or outdated. This pushes redundant information in cloud IdM system, leading to optimization issues and a cluttered system. In such scenario, the recommended concept of One Identity - One Login for managing identities becomes nearly impossible to achieve. The ideal approach to fix the identity unification is to take away the burden from target source such as active directories, allow transition of identities from on-premise IdM to on-cloud IdM and vice versa.

Section 2.01 Benefits of Integrated Hybrid IdM

An integrated IdM system helps in bringing real-time interaction between identities, IdM platforms and connected applications. It facilitates information and data flow to enables multiple distributed IdM Systems to function in synchrony, while handling and transferring information/data. Such a system de-tangles identity flow in a hybrid setup on a real-time basis, ensuring that one-identity one-login concept among IdM Systems is achieved.

Listed below are quantifiable benefits of Integrated Hybrid IdM:

- Saving the cost of dual tasks and frequent manual intervention. Integration between premises and cloud platforms help in addressing the question on dealing with an environment of duplicity as well as managing On-Premise IAM together with Cloud based IAM platforms without any manual intervention.
- Do not miss out on the benefits of Cloud. Given the competitive space in which businesses operate in the present times, it is impossible to operate with no presence on cloud. As most organizations are not able to fix the problem of managing dual platforms, moving beyond primary/legacy IdM setup is problem. With seamless integration between the two platforms, conventional organizations may finally move beyond on-premise solutions.
- Subverting huge cost of numerous application integrators and establishing relevant connections. There is also a huge cost for integrating various applications as well as establishing relevant connections. These most likely run into hundreds depending on the scale of applications integrating with the primary IT System.
- Doing away with incompatible platform integration glitches. There could be integration glitches which may discourage cloud IdM and on-premise IdM to co-exist seamlessly. Identities can interact alongside various applications that are based on endpoints on application connectors. Many of these connectors are to be customized as per IAM product's requirements and organization's needs.
- Bringing consistency in security and compliance. When integrating IAM solution and connecting it with a set of application integrators, it is mostly to do with maintaining fine balance – between compliance, security and operations. While looking at IT integration, slipping out on capabilities can lead to security and data breach. It becomes imperative for implementing a technical formula which can look at agility for IT Systems as well as eases users when they are operating. This perhaps leads to a legacy IT system that can work vertically and horizontally aligning towards the global IT infrastructure, professional and cloud software services.
- Focusing on features while investing in IT. Investing in a customized product may lead to additional cost, being thorough in plans will help minimize the cost. Products integrated into the systems should not complicate IT infrastructure, thus it is important to bring in solutions that streamline the workflows systems.

Section 3 Integration Essentials for Hybrid IdM

Enterprises are seen to rely both on the cloud and on premise legacy systems for different capabilities, and it is unlikely that they would shift completely to the cloud anytime soon. The coexistence of on-premise and on cloud infrastructure has resulted into complexity in application integration between these two platforms. Listed below are some of the integration challenges that organizations in hybrid environment usually face:

Firstly, let's factor in the challenge of lack of synchronization. IAM focuses on creating synchrony between identities, access criteria and varied applications/tools/databases. However, in most cases, cloud-based IdM is being seen to be purchased without considering its integration with on-premise platform, resulting into challenges in synchronization between the two systems. In the current situation, hybrid enterprises are seen to intervene manually to create synchrony, which results into errors and security vulnerabilities.

Secondly, inability of unifying Identities is a challenge that is becoming system requirement. Protocol driven conversion and routing to detect that the messages are in line with current access criteria is the user/identity game. Identities are often pulled from multiple trusted sources and directed to the IAM platform. It further converts identity information to the format required by the end user. Routing is also undertaken wherein the IT System to determine the correct end users based on both pre-configured rules. The system, therefore, fails to perform to the optimal levels when conflicting or confusing information is pulled from a target source and fed in to the system.

Thirdly the struggle of integrating, maintaining and managing multiple Integrations. The complexity involved in management of integration of application hosted in a different platform than the host IAM platform must be managed. In case of IdM technology, various applications are to interoperate within the purview of Identity and Access governance guidelines. An Application integrator is therefore required that would together components of the infrastructure that may use different operating systems, data formats, and languages, preventing connection to a standardized interface.

In order to overcome these challenges, a robust integration solution that offers the following essential elements should be considered:

Essential 1# Synchronized IdM as a systematic flow. Typically, multiple IAM systems do not interact with each other - the tasks and commands are required to be fed in parallel to each platform. Synchronous interaction between cloud and on-premises IdM Platforms can enable IAM tasks in real-time. The interaction between different infrastructures gets in line with the company's access governance policy. Synchronizing IAM platforms can bring greater controls and can be beneficial in achieving following:

- Discourage any delay in access/notification/prompts with real time interaction routed via installed IAM solution
- Ensure that the IT department is notified of any IAM / IT security theft that might need urgent attention
- Get business applications to collaborate instantly whether they are hosted in-house or remotely

- Collate Information and data flow to enables multiple (generally two) distributed IdM Systems to function while handling and transferring information/data
- Synchrony between user endpoint, applications and IAM systems enforces consistency across the database

Essential 2# Unification of identities from disparate sources. Identity unification could be achieved by doing away with Active Directory Bridges to achieve real-time bi-directional transition of identities. Visualizing how identities from multiple setup interact with each indigenous IAM setup (therefore with identities, users and their access criteria in a hybrid setting points at a complexity. A secure system is that kills the complexity and act as a transient path for identities to interact with each other. Any conflicting, overlapping identities are flagged to the system admin, furthermore identity information is unified (merged) – taking down manhours spent on the task.

Essential 3# Integrated Apps for coherent and simplified IdM Systems. Create robust systems for quicker integration and access roll-out.Bring together enterprise IT platforms, databases, directories, business applications and SaaS applications to run the IAM infrastructure smoothly. Further, the need is to create intelligent identity integration with the following features:

- Scalable integration and effective automation of IAM capabilities in IT Hybrid environment that attune IT infrastructure to create structure, provision scalability and provide simplification.
- Interacts with the IAM Setup in a hybrid environment, creating intelligent Hybrid IdM Model - Structure, Scalability and Simplification.

Section 3.01 Elements of Robust Hybrid IdM System

- ✓ **Consistent Provisioning and Federation of Users:** Create, update, disable, enable and delete identities in a synchronized way to form an indigenous IAM infrastructure. It uses standardized SSO to bring consistency with partner application.

- ✓ **Enforce Protocol based Access Governance:** Replicate correct and required access to IT Assets on a defined fashion to ensure that multiple IdM platforms work in tandem and they are not out-of-sync.

- ✓ **Role Specific Standardized Access Management:** Manage access to IT Assets by granting authorized roles to users to maintain least privilege access. The system ensures that a business role created in On-Premise is also available in cloud platform and is assigned relevant access.

- ✓ **Synchronized Interaction between IAM platforms:** Exchange information related to users, identity and access details from On-Premise IAM to On-Cloud IAM and vice versa. It is crucial for a strong interoperability amongst IAM Systems.

- ✓ **System Administration capabilities for IT department:** Stay on top to pass commands easily by making use of a robust admin portal to conduct tasks such as detecting duplicity, merge identities, adding multiple identity systems, bulk uploading users to multiple systems and more.

- ✓ **Monitoring & Reporting Tasks for better Controls:** Get IAM specifics quantifiable reports related to the traffic metrics that flows between On-Premises and On-Cloud Identity Management Systems.

- ✓ **Supports Compliance with Comprehensive Audit Feature:** Complete audit feature for logs and any commands passed on through the system, for login and access related details. Enables transparent connections between Identity Management Systems.

Section 4 Optimized System through Identity Bridge

As the business models being used these days are highly digitalized, the need of the hour is to create interoperable hybrid identity. Avancer's Identity Bridge is helping in creating an optimized identity management system, solving integration challenges and ensuring effective automation of IAM capabilities in hybrid environments. The solution sets a mechanism in place to bring together Hybrid IAM Systems. There are other crucial issues that are resolved through the Avancer's Identity Bridge, including taking down the complexity in terms of on-boarding identities, user roles and application in enterprise IT Systems, achieving secure and smart integration of identities, getting new identities to on-boarded seamlessly, reducing the hidden cost of IT inefficiency, etc.

Some of the benefits Avancer's Identity Bridge include:

- **Bi-directional unification of identities:** Identity Bridge synchronizes all identity related user data to achieve consistency. This enables identity information to flow between IAM Platforms and allowing bi-directional synchronization of user profile data.
- **Single-Point IAM System Interaction: With** Identity Bridge do away with multiple IAM connections and establish just single robust connection between cloud and On-Premise IAM Systems.
- **Impactful End-Point Integration:** Uniform propagation of identity changes and management of related data can be challenging. With IdM Bridge, one can achieve consistent and collective technical end-point integration.
- **Set-Up Security Compliant Protocol:** IdM Bridge attends to regulations and standards compliance-based requirements through protocol-based access governance.
- **Established Processes with Strong IT System:** Identity Bridge enhances capabilities for IT department towards automating systems by taking down manual tasks for managing identities.
- **Ameliorated Hybrid IT Infrastructure:** IdM Bridge helps in bringing together information from multiple Active Directories through transactional Identity Bridge.
- **Strategic IT for optimized IAM Capabilities:** Role-specific access management is provided through IdM Bridge which helps in standardization of role based requirements to ensure consistency across all platforms.
- **Globally Aligned Enterprise IT Systems:** The IT departments can gain agility through centralized management of cloud and On-premise setups as Identity Bridge creates rationalized and scalable IdM systems.

Section 5 Way Forward in IdM Integration

Securing identities and governing accesses in a hybrid environment requires intelligent and cost-effective integration solution, which could address complexity of system / application integration. As on cloud solutions are yet to gain a complete foothold, and on-premise IT system would still be around for some time, the major requirement for any business is to bridge the gap between these two platforms with the help of integrators.

Such integrators would help in addressing the big question of hybrid enterprises, i.e. How to do away with duplicity of simultaneous management of On-Permise IAM and Cloud based IAM platforms. Further, these integrators could run into tens or hundreds depending upon the scale of applications integrated with the primary IT System (could be the Cloud platform or Premise-based setup).

Also, such an integration model would provide a secure data gateway for protected interaction between data kept on cloud and on-premises, allowing a seamless development of a hybrid environment. This would ensure that enterprises are able to rely on and optimally use the technology investments made on existing on-premises applications, while drawing the best out of on-cloud platforms. As moving to cloud-based applications often leads to the risk of creating information silos, data duplication and other issues, IdM integration could eliminate these, helping enterprises get maximum benefit from their investments in cloud technology.

Further, integrators should provide the ease of transiting identity information from Premise based IdM to Cloud-based IdM and vice versa on a real-time basis. Also, trusted information and applications stored on Cloud after often needed to be transited to Cloud-based or On-Premise IAM. Thus, such integrators would be required to provide not only real-time Identity transition from On-Premise Trusted System(s) such as PeopleSoft HRMS, Active Directory, Oracle E-Business Suite and others to Cloud based IAM, but also real-time Identity transition from Cloud-Based Trusted System(s) to either On-Premise or Cloud based IAM.

With a right integration solution, such as Identity Bridge, organizations will be able to meet these challenges with flexibility and ease.

Identity Bridge

Identity Bridge sets in place a mechanism to brings together Hybrid IAM Systems. It solves integration challenges, enables effective IT workflows and ensures automated interaction between multiple IAM systems spread across Hybrid IT environments. Identity bridge deals in standard Identity Management concepts such as Organization's Group, roles (entitlements) users, password policies, Active Directory integration, etc. It enables transition of unlimited number of identities between On-Premise and Cloud IAM Setup on a real-time basis. Identity Bridge is hosted as a single tenant model hosted on AWS Cloud and is meant for a client. All communication starting and ending in Identity Bridge are secured communication over https. Identity Bridge UI Portal is multitenant model to manage client configuration of Identity Bridge. All data at rest is encrypted and located in the same geography as client's location. In cases where the client geography is spread-out, client gets to decide the location of Identity Bridge Server.
For more on Identity Bridge, visit https://www.identitybridge.us

Avancer Corporation

Avancer Corporation is a multi-system integrator focusing on Identity and Access Management (IAM) Technology. Founded in 2004, it has over a decade's expertise in the field of Identity and Access Governance, IT Security and Big Data Management. With a depth of experience in end-to-end IT Security Solutions, Avancer has evolved as a specialist in integrating enterprise IT security through a range of solutions, products and services focused in IAM Technology. Our services ranges from full term project life-cycle implementation to tailor made short-haul projects including software procurement, architectural advisement, design and development through deployment, administration and training.

For more on Avancer Corporation, visit https://www.avancercorp.com