Leverage the Identity Fabric Approach to Modernize IAM

Contents

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 1

Assessing Whether to Migrate your IAM

Why Migrate Your IAM

Many scenarios call for a migration from one identity and access management (IAM) system to another.

Some Common Reasons for Migration :

COMPLIANCE

The IAM system no longer meets legal requirements. Cybersecurity and privacy regulation have become progressively tighter across all industries, with new laws coming into effect every year. SOX, HIPAA, regional data protections, financial services directives—the list goes on, and often the new rules mean that existing IAM solutions are no longer adequate or compliant.

SECURITY

Stricter standards for compliance require even tighter management of data. Just a few examples include: encryption throughout data lifecycles, audit trails, specific identity proofing and authentication requirements. There are also requirements for accessibility, and personal data laws mandating that personal data must be stored only in (or replicated to) the user's home jurisdiction.

USABILITY

A growing organization brings new challenges. User accounts, roles and attributes may expand until the once-adequate IAM system reaches or exceeds its limits. If the IAM system cannot perform at scale, problems with management, slow logins or system limits can kick in, forcing a company to find a replacement.

ARCHITECTURE

An aging IAM system cannot always maintain pace with changing integration methods and authentication capabilities. Integration with modern applications or cloud services can become awkward, costly—sometimes even impossible. Newer environment deployment methods may not work, causing frustration at the team level as management techniques evolve beyond system capabilities.

COST

What once looked like a terrific cost model may suddenly become less attractive, even unsustainable, as policy changes or marketing pivots cause contract renegotiation. Organization evolution that affects the bottom line, like expansion in to new regions or an increase/decrease in user or transaction volume, can seriously impact the system cost structure, forcing a change. Legacy systems can become costly and inefficient to maintain, as technicians move on to newer technologies or the pool of available talent shrinks. If a company is unable to find and keep staff that can develop and maintain the older systems, the likelihood of failure of a critical business system can be all too real.

IAM SYSTEM END-OF-LIFE

Any number of reasons can contribute to a vendor decision to cease support for the software powering your IAM system. When the end-of-life message hits home, decisions must be made. Will you continue to run unsupported software? What are the business risks involved? Most likely, those risks are unacceptable, and it becomes clear that a replacement system is necessary – and the less disruptive the solution and process of replacement, the better it will be for your business.

CHAPTER 2

Migrating

1. Migration Approaches

There are multiple ways to handle a migration project. The best option for your organization depends on your business requirements, but there are two main strategies: Big Bang migration and phased migration. Let's examine both.

• Big Bang migration

With Big Bang migration, a.k.a. 'rip & replace', the basic idea is to extract data from the legacy system, import it into a new one and reconfigure all related applications for all users in one go.

All of the system's identities must be switched to a new system during a certain maintenance window, usually overnight, when there is a minimal traffic flow to your applications. Most times, users won't even notice the difference after the change has been done. If the new IAM system is API-based then the user interfaces will not need to change—functionality is simply integrated to the existing application. If the new system is not API-based, users might have to deal with new front-end screens and operating procedures, etc.

Scheduling-wise, Big Bang migration is simpler, since you can accomplish the actual data import execution of the project inside a relatively small, predefined time window.

• Phased migration

During a phased migration, you keep the two systems (old and new) running in parallel, while migrating target applications one at a time and gradually decommissioning the old system, until everything is running in the new IAM system.

This method's incremental approach gives you time to monitor the migration process step by step, ensuring the successful execution of each phase, while the services are still partly relying on the old system and running simultaneously with the new one.

2. Taxonomies of Cloud Architectures

Moving your IAM to the cloud is an attractive option, reducing operational costs and infrastructure overhead, and shifting IT expenditure to a pay-as-you-go model. There are several options.

2.1. Single Cloud

Relying on a single service provider for rolling out your new IAM will typically shorten your time-to-market, because a whole suite of services (MFA, SSO, etc.) can be implemented pretty much “out of the box”. Since those services are all maintained by the same vendor, the integration will be relatively seamless, as long as you don’t introduce a non-standard third-party component that is not part of the suite.

On the down side, vendor lock-in is a very likely risk with this approach; so it is highly recommended that you choose a service provider that relies on IAM standards. (Commonly used IAM standards are OpenID Connect (OIDC), SAML, SCIM and FIDO.) That way, if you need to migrate to a different service provider in the future, as long as the new one builds on the same set of standards as the previous one, your transition should be pretty smooth.

⬆ 3

THREE OR MORE CLOUDS

Enterprises are running an average of three clouds, including Microsoft Azure Active Directory, Amazon Web Services (AWS), Google Cloud Platform

2.2. Multi-Cloud

Single Cloud is only feasible in a ‘green field’ scenario, where migrating to the cloud is still in the works. There might be pilots running, but the options are still open. The more common scenario is that there’s a cloud migration initiative already taking place as part of your ‘Shadow IT’, targeting all sorts of SaaS, PaaS and IaaS providers. Going multi-cloud translates to a ‘best of breed’ approach, where you can mix and match pure play solutions that are more in alignment with the IT ecosystem as well as any budgetary constraints.

OUR RECOMMENDATION

If your organization is medium to large, assume that your IAM will be multi-cloud. Given the complexity of the cloud ecosystem, it’s unlikely that all requirements can be covered by a single vendor.

CHAPTER 3

Accelerating Multi-Cloud Migrations

1. Multi-Cloud Challenges

Business applications cause the most friction during migration to the cloud, since their retrofitting can take months and, in the end, might not even be technically feasible.

In the past decade, IDaaS solutions have emerged as an integral part of any digital transformation initiative where moving to the cloud is seen as a route to agility and cost effectiveness.

The problem is that most existing enterprise IAM infrastructure is essentially a mashup of point products with little interoperability, significantly intertwined with business applications and the underlying IT infrastructure. What's more, most of those products cannot deliver an updated experience for today's mobile users.

Migrating identity services and stores is fairly straightforward with the tooling provided by most IDaaS and PaaS providers. For instance, Microsoft Azure provides a solution for synchronizing identities (Azure AD Connect Sync) with on-premises Active Directory. Okta, with their Okta Access Gateway, allows bridging the legacy ecosystem with their cloud. These can be an option if your IAM ecosystem is rather small and your organization is willing to increase the risk of vendor lock-in by employing a Big Bang migration approach to migration. But these types of middleware solutions do not cover legacy IAM and non-standards-based applications.

OUR RECOMMENDATION

Embrace an Identity Fabric approach. It's a key enabler for supporting Digital Transformation initiatives without disrupting legacy applications or IAM services. Instead, the Identity Fabric promotes an agile approach, rolling out new capabilities in an incremental and iterative fashion, allowing the organization to gain support from stakeholders as the project is executed, as well as improving the user experience.

2. The Atricore Identity Fabric (AIF)

> **“Identity Fabrics are focused on delivering a scalable, comprehensive set of identity services to developers and to the users of digital services, and form the core of modern IAM.” – Kuppinger Cole**

The Identity Fabric approach builds around the concept of an abstraction layer meant to break any coupling between your IT and the specifics of the underlying IAM stack, independently of where it resides and any associated implementation details. Your IAM is no longer a friction point - it is fully aligned with your IT strategy. The Atricore Identity Fabric platform is based on the following capabilities:

2.1. Features

2.1.1. Embraces no-code approach

Making the move to multi-cloud identity is definitely a game changer. But the complexity remains, since any multi-cloud identity architecture is complex by definition—whether or not implementation details are in plain sight.

Your IT ecosystem is constantly evolving as new applications, services, and infrastructure components are on-boarded while keeping up to date with regulatory requirements. This introduces new challenges, raising the bar for the expertise that’s required for cybersecurity engineers and CxOs to understand and make the changes required to keep up with the pace of digital transformation.

Additionally, as the process of moving to multi-cloud IAM progresses, the footprint of any required middleware must be kept to the minimum to avoid introducing a major new vendor lock-in. Licensing issues might arise, as well.

Wouldn’t it be preferable to avoid these issues altogether, by building on commercial-friendly open source stacks?

Model-driven multi-cloud identity encourages the participation of both technical and business stakeholders. Analysis and decisions happen based on a visual model that begins with a bird's eye view of the current IAM ecosystem. Any new IAM-relevant component is automatically discovered and captured within this view. The new IAM system can also be represented, along with how to deliver it from the current one. Once the migration path is clearly identified and defined, it will allow for repeatable and consistent provisioning, building on Infrastructure-as-Code (IaC) standard tooling like Terraform so that it can harmonize with your DevSecOps processes. Deploying any middleware is optional, and if it is needed it will be visible at the architecture level.

2.1.2. IAM Cloud-agnostic

Taking a single-provider approach toward migrating IAM to the cloud creates risk by introducing a potential vendor lock-in that could reduce your agility in the mid and long-term.

The Atricore Identity Fabric uses the concept of an abstraction layer, de-coupling your IT and the specifics of the underlying IAM stack. Your IAM is no longer a friction point - it is fully aligned with your IT strategy.

2.1.3. Pre-integrated with End-of-Life IAM products

With AIF, you can bring modern SSO and MFA to on-premises applications without changing code.

This allows you to reduce identity infrastructure up to 90% by replacing deprecated on-prem web access management (WAM) systems like CA Siteminder, IBM Tivoli Access, and Oracle Access Manager. As a result, you'll diminish the operational burden surrounding identity, while adding SSO, MFA, and intelligent security from the cloud for legacy apps that you want to retain indefinitely.

2.1.4. Just-in-time identity synchronization

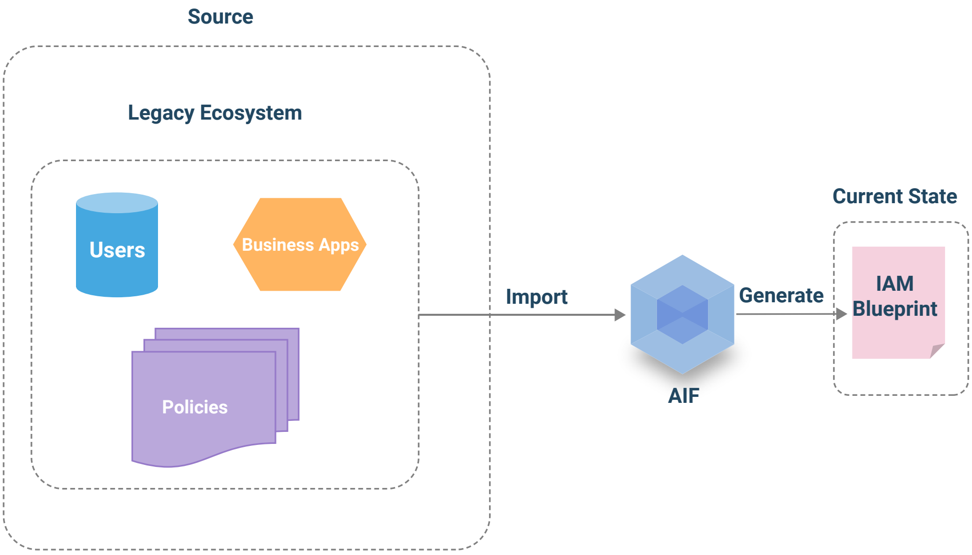
You can import all the accounts to the new system and, when a user signs into it for the first time, their password validity will be checked against the user directory of the old back-end service. If it is correct, the new IAM system rehashes and saves the password. Just-in-time migration allows a smooth registration during the login process that is transparent to the end user.

2.2. How it works

Discovery

Defining your current state of your IAM

Given the complexity of typical IAM infrastructure, a bird's eye view is critical in order to understand what the current state is. This can be shown in an IAM blueprint where all unnecessary implementation details remain hidden, to help with analysis and decision making. Discovery is a mostly automated and continuous process, requiring continuous manual augmentation and review.

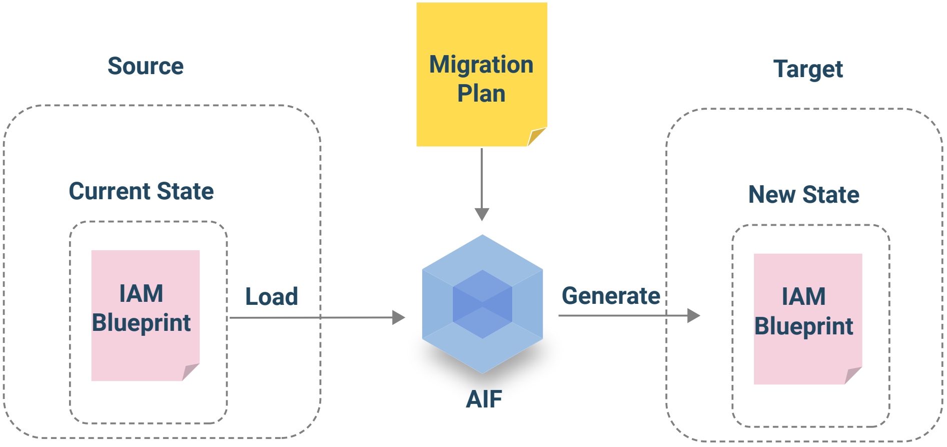


Design

Defining the future state of your IAM

Once the discovery stage is complete, it's time to define a migration plan. You'll identify the target state in terms of IAM; namely which building blocks (such as IDaaS and IT components) will need to be introduced, and how those will be interacting, in order to run your modernized ecosystem.

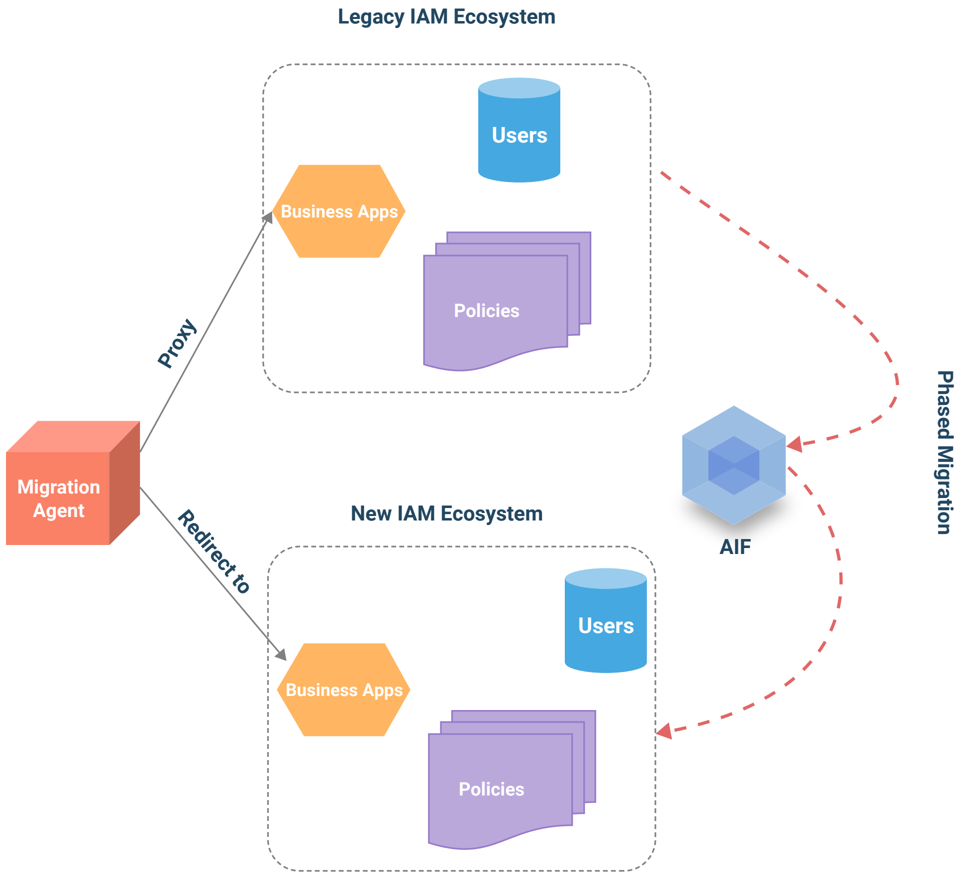
In order to deliver the IAM system the migration plan will have to be executed through the AIF, in accordance with the migration plan.



Migration

Shift incrementally to the future state

Having defined your intent through the migration plan, you can now move on to deploying and running your system accordingly. This includes enabling all the required middleware (the IAM Migration Agent) acting as a bridge between the legacy and modern IAM infrastructure, thus allowing for the seamless operation of connected applications and the incremental migration of data. At this stage both legacy and modern IAM infrastructure are functioning in parallel, so that the user experience and application remain unchanged.



Evolution

Decommission and Iterate

Once the migration is complete, the legacy IAM solution can be decommissioned. Legacy applications that are tightly coupled with the legacy IAM solution, and that have not been retrofitted, will still need to rely on the Atricore Identity Fabric to "play nice" with the modern IAM infrastructure.

Management of the IAM infrastructure can now be performed visually through the universal IAM model, instead of having to deal with each provider's administrative interface. Additionally, it can be used as input for achieving IAM-as-code, as well as for the implementation of future migration initiatives.

Since applications are going through the Atricore Identity Fabric via standard technologies, there is no coupling between them. This translates to allowing future IAM initiatives, such as migrating to a different service provider, to happen with little disruption.

Learn more

For more information about how Atricore can support your IAM modernization initiative for both workforce and customer applications, visit https://www.atricore.com/.