Brought to you by:

IBM

Cloud Identity

for dummies®

A Wiley Brand

Understand Identity as a Service (IDaaS)

Plan your IDaaS strategy

Use IDaaS in the real world

Mike Wessler

Sean Brown

IBM Limited Edition

Cloud Identity

IBM Limited Edition

by Mike Wessler and Sean Brown

for dummies®
A Wiley Brand

Cloud Identity For Dummies®, IBM Limited Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-47264-3 (pbk); ISBN: 978-1-119-47271-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Carrie A. Burchfield
Editorial Manager: Rev Mengle
Acquisitions Editor: Steve Hayes
Business Development Representative: Sue Blessing
Production Editor: G. Vasanth Koilraj

Table of Contents

Introduction

Organizations are faced with providing secure authentication, authorization, and Single Sign On (SSO) access to thousands of users accessing hundreds of disparate applications. Ensuring that each user has only the necessary and authorized permissions, managing the user's identity throughout its life cycle, and maintaining regulatory compliance and auditing further adds to the complexity. These daunting challenges are solved by Identity and Access Management (IAM) software.

Traditional IAM supports on-premises applications, but its ability to support Software-as-a-Service (SaaS)-based applications, mobile computing, and new technologies such as Big Data, analytics, and the Internet of Things (IoT) is limited. Supporting on-premises IAM is expensive, complex, and time-consuming, and frequently incurs security gaps.

Identity as a Service (IDaaS) is an SaaS-based IAM solution deployed from the cloud. By providing seamless SSO integration to legacy on-premises applications and modern cloud-based SaaS applications, Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) resources, mobile, Big Data, and the IoT, IDaaS provides end-to-end enterprise IAM services. Via the cloud, organizations gain simplified IT architecture, faster deployments, lower total cost of ownership (TCO), and enhanced capabilities enabling digital transformation.

About This Book

Secure access into applications and identity management is a complex and important topic. Many organizations struggle to keep up with IAM and seek a better solution. Deploying IAM as a cloud-based IDaaS solution solves the challenges of organizations facing increasing complexity, costs, and security compliance requirements. IDaaS lowers TCO, simplifies architecture, improves security and compliance, and provides seamless SSO integration for on-premises, SaaS, and mobile applications.

The focus of this book is learning what IDaaS provides, why it benefits organizations, and how to implement it for your applications. A great deal of attention is given to explain IAM and cloud computing so you understand the context and benefits of a cloud-based IAM solution, which is IDaaS. ***Note:*** Cloud Identity is IBM's IDaaS offering, and this book uses IDaaS and Cloud Identity interchangeably. Via Cloud Identity, organizations gain robust governance, risk, and compliance (GRC), identity governance and administration (IGA), and security, while users enjoy self-service registration and seamless SSO access into the applications they need.

Icons Used in This Book

Throughout this book, you occasionally see special icons to bring your attention to a point we want to emphasize. We keep them brief, and sometimes a little funny, but if you see one take note because it's something you should know.

REMEMBER

Take a look at the information here because it's something you should keep in mind as an important takeaway.

TIP

Tips indicate information that you may find useful. Often, they relate to an experience we had (or we wish we had at the time), or they add additional context and perspective to a topic.

WARNING

Warnings mean just that: Be careful! We use warnings to alert you to common mistakes and serious issues for you to avoid.

TECHNICAL STUFF

We can be technical people at heart, and we love to understand how and why things work (or don't). Yes, this is a *For Dummies* book, but sometimes we delve deeper into a subject so you understand the "why" and "how" for a key topic.

Beyond the Book

This book can't teach you everything about IAM and IDaaS, but we do cover the fundamentals. Unfortunately, we can't dive into the detail we'd normally like for a security architecture book, so here are a few additional resources:

- www.securityintelligence.com
- www.ibm.com/security/identity-access-management/cloud-identity
- www.ibm.com/us-en/marketplace/cloud-identity-connect

IN THIS CHAPTER

- Following the evolution of Identity Management from past to present
- Understanding core components of Identity and Access Management (IAM)
- Recognizing IAM business drivers
- Building the foundation of cloud computing and why it is important

Chapter 1
Surveying the Identity Management Landscape

Identity and Access Management (IAM) is a continually evolving technology with inherent complexities and challenges to be overcome. Coupled with increasing business drivers of agility, simplicity, and lower cost, a new approach to solving IAM challenges is needed.

Cloud computing solutions for delivering IAM to customers are attractive because they meet the complex technical challenges for IT systems (on-premises, cloud-based, mobile), and they align with business drivers delivering consistent solutions faster and with lower total cost of ownership (TCO).

In this chapter, we describe how IAM has evolved into its present state and explain the value of cloud computing.

Evolution of IAM over the Years

IAM has evolved over the years in response to IT and business needs. During the first generation of computer systems, IAM was conceptually simple:

- Limited in scope with a focus on users, with only usernames and passwords for traditional employees
- Relatively few users and even fewer applications; each account was unique to a specific application
- Users and applications were located on-premises with little remote computing
- Fewer regulatory controls, auditing requirements, and security concerns

Those early days didn't last long as the demand for technology increased, security and compliance became drivers, and the concept of employee life cycle management evolved. As IT grew out of its infancy into a second generation of computer systems, so did the need for more effective security and access controls. IAM evolved as a discipline and technology with these present fundamentals:

- User life cycle management with provisioning and deprovisioning
- Role-based and fine-grained access control
- Centralized Directory Services (DS) such as Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory (AD)
- Movement toward centralized identities and federated access with Single Sign On (SSO) access into applications
- Strengthened password protections for length, passphrases, One-Time Passwords (OTP)
- Strong authentication mechanisms including Multifactor Authentication (MFA) and biometrics
- Enhanced governance, auditing, monitoring, and security controls

Clearly, IAM was moving forward and showing value. Unfortunately, most organizations didn't have a well-defined IAM road map showing the bumpy terrain of IT and business requirements, and IAM

solutions at the time didn't meet the full spectrum of capabilities or support all technologies. The ecosystem is further complicated by vendor mergers and acquisitions and frequently changing IAM solutions, causing reworking and integration challenges for IT staff.

As a result, the third generation of IT brought IAM its own set of challenges:

- Multiple siloed on-premises IAM solutions adding cost and complexity; no single IAM solution for the enterprise
- Reactive, iterative improvements resulting in piecemeal patchwork architecture; difficult to secure and manage
- Frequently supporting different applications for provisioning, authorization, access control, governance, auditing, and security monitoring; too often building applications with governance and auditing as an after-thought
- Overemphasis on legacy and on-premises applications with limited capability for distributed mobile users, cloud-based applications, or business-to-business applications

Increasingly, traditional on-premises IAM solutions are now coupled with cloud-based IAM to more effectively support the rapidly evolving nature of digital transformation and computing requirements.

Diving into IAM

Modern IAM solutions build on previous generations of software, but they're more expansive in their scope (process and technology). One can expect these features from today's IAM solutions:

- Strong access management controls for authentication and authorization, ensuring only the right people get access into applications with the correct permissions and within defined usage parameters (time, location, source address, and so on)
- Single Sign On (SSO) technology and federated access, allowing a user's identity to be used across a wide spectrum of applications without the need to login multiple times with different accounts and passwords (a security risk)

  Cloud Identity enables SSO support for all applications, including on-premises and cloud.

UNDERSTANDING LIFE CYCLE MANAGEMENT

At the heart of IAM is the life cycle management process — specifically the creation, modification, and removal of a person's identity and access. Provisioning and deprovisioning activities are the mechanisms within this process. Consider the use case of an employee within an organization:

- A new employee is hired into an organization. The IAM creates (provisions) the employee's account into one or more applications with only the access and privileges authorized to that employee.
- The employee is promoted and moves to a different role in the organization. The IAM modifies the employee's access and privileges in the corresponding applications to match the new position. During this process, old privileges and access are removed and new privileges and access are granted. It is important to ensure that *permission creep* (also known as *entitlement creep*) doesn't occur where the user collects excessive permission or retains unnecessary access.
- The employee leaves the organization. The IAM removes access (deprovisions) the employee in the corresponding applications. Rather than deleting accounts, simply removing access is beneficial from an audit perspective or in the event the employee returns.

All actions and approvals in the life cycle should be documented and auditable. Failure to remove necessary permissions when an employee changes roles and removing access when an employee leaves creates easily exploitable security vulnerabilities. Mature IAM systems perform these tasks in an automated manner in response to authorized workflow requests.


TIP

» Adaptive Authentication, eliminating passwords (and costly password management) while enhancing security

Using authentication mechanisms that adapt to the application and user can increase security to your applications while easing the burden of passwords.

- Self-service employee launch pads and portals, enabling registration into applications and password management/resets rather than contacting a staffed helpdesk
- Identity Governance and Administration (IGA) to support access requests and certification, account provisioning workflows, role life cycle management, delegation, reconciliation, recertification, and auditing and reporting
- Business risk management for users of cloud-based Software as a Service (SaaS) applications

  Ensure only secure and trusted SaaS applications are used with appropriate controls and automatically monitor for deviations and suspicious activity.

REMEMBER

Solutions claiming to support IAM should be measured against modern criteria. Not all solutions are at the same level of maturity, nor do they have the same depth or breadth. When evaluating vendor offerings, use this list as a baseline for modern solutions.

Supporting IAM Business Needs

Business requirements drive technology, and IAM solutions are no different. In some cases, industry regulations or policies necessitate auditing and compliance aspects of user access and permissions. In other situations, operational requirements forcing usage of multiple applications will drive access technologies such as SSO. Common business drivers in IAM are centered on security and compliance and ways to do business better for customers.

Security

No business wants to make the news for leaked customer data; failure to take proper precautions frequently results in very public disasters (examples are too vast to list). Unauthorized access, elevated privileges, and stolen usernames and passwords are all examples of security issues addressed by strong IAM solutions. In the event of a security breach, if an organization is *not* performing strong IAM functions, IT staff and application owners will face a high degree of scrutiny.

Digital transformation

Businesses are being forced to change *how* they do business. Beyond traditional methods, being proactive and actively engaged in new technology, reaching and forming relationships with customers faster, and lowering costs and barriers to innovation are core aspects of digital transformation. Mature IAM solutions enable this change in business. IAM must eliminate antiquated, siloed system access processes, delays, inefficiencies, and errors that impede digital transformation and move the organization *forward* (not against) this paradigm shift in business.

Customer Identity Access Management (CIAM)

Ensuring that customers' information is protected and that they have the access they need within your organization is critical. Customers expect an efficient and secure self-registration process to do business with your organization; if they don't receive that they will go elsewhere. Much focus exists on the employee aspect of IAM, but Customer Identity Access Management (CIAM) and how organizations manage their customers are equally important.

Compliance

Providing proof of compliance with relevant laws and regulations is both essential and expensive. Frequently driven by events where laws or security were *not* followed, compliance is now a requirement for everyone. IAM solutions are inherently well-positioned to provide the monitoring, auditing, and proof to satisfy compliance and governance requirements as part of IGA. Furthermore, IAM solutions perform this function more effectively and with less overhead, complexity, and cost than piecemeal or homegrown solutions do.

Forward-thinking organizations view IAM as an enabler for greater business value. Evaluate IAM solutions against core business drivers to ensure that IT solutions are working *with* (and not counter to) the business.

REMEMBER

A key component of compliance is *recertification;* that is the documented review and validation of accounts and privileges to ensure that they match what is properly authorized. Governance, risk, and compliance (GRC) tools should streamline and document the recertification process. Remember, it is just not enough that you

recertify accounts on the agreed-on schedule; you must be able to prove that you have met your recertification requirements.

Defining the Cloud Paradigm

By any standard, cloud computing is a disruptive, transformative force on how organizations deploy and manage their IT applications and data centers. To some, cloud is little more than "just hosting in someone else's data center." To others and the majority of industry vendors, cloud computing represents a completely new and revolutionary way of doing business.

Before making your own judgement (and that judgement may fall in between both extremes), it is necessary to have an objective understanding of cloud absent from marketing influences.

National Institute of Standards and Technology (NIST) Special Publication 800-145 states that "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, application, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud computing providers offer computing resources as *services*. Cloud computing *providers* make their services available to customers who are *subscribers* or *consumers*. By leveraging a metered pay-as-you-go model, consumers identify the service(s) they require and then select the provider(s) offering desired capabilities and price.

Available cloud computing resources are categorized "as a Service" with three general *service models* as defined by NIST with these generally accepted definitions:

- **Software as a Service (SaaS):** Consumers are provided their software applications from the cloud service provider. The consumer gains access to application software while the provider manages the underlying software and infrastructure used to provide that application software.

- **Platform as a Service (PaaS):** Consumers use programming languages, libraries, and tools from the provider as an application development and deployment platform.
- **Infrastructure as a Service (IaaS):** Cloud service provider manages the underlying physical infrastructure (servers, networking, storage, operating systems) while the consumer deploys and runs their own application software.

The cloud is expanding to the benefit of organizations, but the benefit isn't just limited to those entities. Increasingly, individual consumers are leveraging the cloud for personal use such as backing up their mobile devices and personal productivity applications.

Despite the continual evolution, several common use cases have emerged:

- SaaS is fast-growing, with consumers at the private individual and organizational level seeking new software packages.
- PaaS is especially popular for software developers prototyping new capabilities and "crash and burn" environments.
- IaaS is growing as legacy data centers shrink and organizations shift their infrastructure to the cloud for savings and agility.

As cloud computing matures, specialized cloud service models have evolved and will continue to expand (for example, Database as a Service [DBaaS], Data Warehouse as a Service [DWaaS], Backup as a Service ([BaaS], and so on).

Cloud Deployment Models

The relationship of where computing resources reside and who else is using those resources is a key defining factor in cloud computing architecture. Keeping computer resources in a customer's traditional data center is *on-premises* hosting. Moving computing resources out of the data center into the cloud is considered *off-premises* hosting.

NIST recognizes four different cloud deployment models:

- **Private clouds:** Used exclusively for a single, private organization but may support multiple internal consumers; widely considered the most secure deployment model
- **Public clouds:** Used by multiple, unrelated organizations on a shared basis; very common deployment model, particularly for SaaS applications
- **Community clouds:** Used by organizations with a common purpose, mission, or audience
- **Hybrid clouds:** A combination of two or more cloud models (private, public, and community)


TECHNICAL STUFF

The industry frequently uses this term to define a combination of traditional on-premises and off-premises hosting options; essentially on-premises combined with any cloud model.

Hybrid computing is a common architecture today and will be for the foreseeable future because many organizations can't or won't move all their computing resources (applications, data, and infrastructure) to an off-premises cloud. Valid technical, operational, or regulatory and policy reasons exist why some applications and data must remain on-premises, thus ensuring the hybrid cloud deployment model will endure.

Why Cloud Makes Business Sense

Organizations move to the cloud because the computing architecture makes good business sense on multiple levels. Several factors increasingly make traditional, on-premises hosting difficult to sustain and justify:

- Increasing costs and complexity of IT infrastructure is difficult to support; never ending upgrades and technology refreshes magnify the impact.
- High cost of and limited availability of skilled labor makes recruitment, training, and retention a continual challenge.
- Understaffed and overbooked resources delay implementations for new projects, impeding business agility.
- New technologies and specialized capabilities (for example, Big Data, analytics, mobile, Internet of Things [IoT]) aren't supportable with current infrastructure, staff, and skillsets.

- Scaling capacity upward to meet increased processing demands is expensive and time-consuming, frequently leads to unused (wasted) capacity, and too often is reactive to business needs.
- Patchworks of outdated applications and disparate technologies lead to security and compliance issues.

Conversely, embracing cloud computing turns many of the weaknesses of on-premises hosting into strengths for the cloud-savvy organization:

- Subscription-based computing, based on usage, is a lower, more accurate cost and doesn't require large capital expenditures.
- Standardized cloud computing environments simplify the IT landscape and reduce complexity.
- Time-consuming upgrades and costly technology refreshes are the responsibility of the cloud service provider.
- Highly specialized IT infrastructure support duties are performed by full-time cloud service provider staff.
- Business agility is increased because in-house IT staff is freed from operational support to deliver new business-centric opportunities.
- New technology capabilities and opportunities are enabled using existing cloud-based Big Data, analytics, mobile, and IoT services.
- Unlimited scalability and capacity-on-demand rapidly meets business processing needs without procurement and on-going support of on-premises infrastructure that isn't fully utilized.
- Modern, fully patched, and supported cloud computing assets with automated monitoring and auditing enhances security and supports compliance.

Cloud computing solves many of the infrastructure support problems with cost and complexity, but more importantly it gives organizations greater agility and access to new capabilities via SaaS applications and unlimited scalability.

IN THIS CHAPTER

- Understanding why IAM capability from the cloud is a better solution
- Exploring IDaaS architecture and components
- Describing technical and business advantages of IDaaS

Chapter 2
Understanding IDaaS

As Identity and Access Management (IAM) has evolved as a powerful on-premises solution for identity management and governance, cloud computing is reshaping how IT and businesses operate. The natural evolution of cloud-based IAM solutions in the form of Identity as a Service (IDaaS) was inevitable. At its core, IDaaS deploys as a cloud-based IAM Software-as-a-Service (SaaS) offering. Leveraging the capabilities of a mature IAM solution with cloud services features, IDaaS uses proven architecture to provide technical advantages and meet business objectives, and opens the door to advanced integration capabilities.

In this chapter, we explain how IAM as SaaS in the form of IDaaS is executed and why it's so powerful.

Finding a Better Way

Change in IT is constant and driven by business: Digital transformation, global markets, Big Data, analytics, the Internet of Things (IoT), mobile devices, cloud hosting, cloud-based applications, and so on. In the wake of security breaches and global privacy concerns, the demand for governance, risk, and compliance (GRC), security, and accountability is rapidly expanding.

What hasn't changed is the need for IAM functions. In this environment, the need for IAM to expand into the new ways of doing business has never been greater.

WARNING

Are stand-alone, on-premises IAM solutions up to the challenges of new business and computing paradigms? Are all IDaaS solutions the answer to all IAM challenges, including fine-grained controls for legacy on-premises applications? The answer to both questions is no. Most enterprises have a hybrid environment today whereby they have a mix of on-premises and cloud apps that need to be incorporated into the IAM solution. Cloud Identity provides the best of both worlds — an IDaaS component to embrace the fast-growing world of cloud apps married to an integrated on-premises component for support of complex legacy environments.

IAM solutions that haven't evolved to the cloud have numerous downsides:

- Expensive to build and support
- Inconsistent patchwork of components to secure
- Frequently siloed custom solutions and legacy systems

Traditional IAM solutions fail to meet future needs:

- Inefficient at securing cloud-hosted environments
- Unable to keep up availability of new SaaS applications
- Slow to respond to rapidly changing requirements and opportunities
- Difficulty managing global users without complex infrastructure

The root problem lies in that traditional IAM solutions were designed to manage on-premises applications; they weren't designed for managing *upward* into the cloud. This inherent architectural deficiency necessitates a shift where IAM is deployed and managed *downward* from the cloud into on-premises applications. This SaaS delivery model of cloud-based IAM is IDaaS.

The power and capabilities of SaaS cloud computing provide a natural platform to support IDaaS. The benefits of standardization

and secure, modern technology, unlimited capacity, the ability to reach customers both on-premises and in any cloud deployment model, and a subscription-based cost model are powerful drivers for why cloud-based IAM as IDaaS is being adopted by so many organizations.


TIP

SaaS is one of the fastest-growing, easiest-to-adopt cloud service models. SaaS offerings excel at providing software at a fraction of the cost and complexity required to purchase and deploy in-house.

Countless vendor applications exist spanning the spectrum from small personal applications, medium-sized office productivity applications, and large and complex workflows, to Human Resource (HR), Customer Relationship Management (CRM), and Enterprise Resource Planning (ERP) applications. SaaS offerings are powerful and a compelling cloud entry point for many consumers.

Introducing IDaaS

IDaaS is a cloud-based implementation of IAM. As a cloud-based offering, several core characteristics are required and should be expected regardless of vendor:

- **SaaS offering providing all the benefits of cloud computing architecture:** Although the cloud service provider is maintaining IAM on its infrastructure, this deployment model is SaaS (not IaaS or PaaS) as the consumer only accesses the IAM software via approved interfaces (web browsers, APIs, and so on) and is not responsible for management or maintenance of cloud-based assets.
- **Multitenant architecture with multiple customers sharing the same cloud IAM infrastructure in a secure manner:** This distinction ensures that customers are indeed receiving cloud-deployed solutions rather than on-premises IAM deployed from another hosting provider (masquerading as cloud).
- **Hybrid support of on-premises and cloud-based applications:** Organizations have on-premises applications but also

distributed, mobile, and cloud-hosted applications; IDaaS solutions support an increasing number of on-premises applications.

The ability of cloud-based applications to reach down into consumers' data centers, outward to their mobile users, and across to other cloud-based applications (hosted via SaaS, PaaS, or IaaS) is a powerful capability inherent to mature IDaaS solutions.

In Figure 2-1, you see a representative IDaaS implementation supporting applications in different environments.

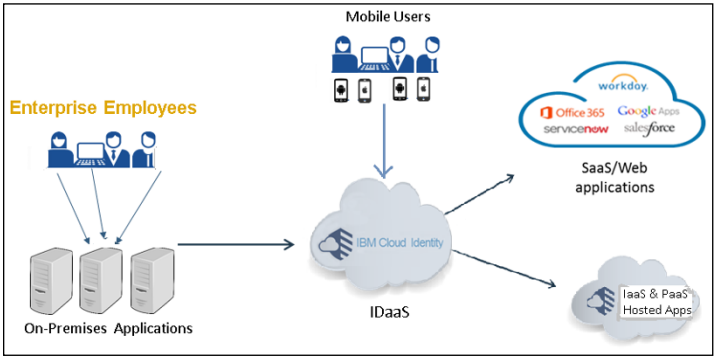

FIGURE 2-1: Deploying IDaaS across applications with Cloud Identity.

Because IDaaS is hosted from the cloud, it supports applications regardless of their location or topology:

- On-premises enterprise users
- Mobile users located anywhere on the globe
- Web-based or SaaS applications such as MS Office 365, Salesforce, Google Apps, Workday, or ServiceNow
- Applications hosted in IaaS or PaaS cloud environments

IDaaS is powerful because as a SaaS application, it has the ability to reach anywhere there is a network (even wireless) connection without the need for hardware at the customer site.

Understanding IDaaS Advantages

IDaaS provides relief to those managing data centers and frustrated with many challenges of on-premises applications. Many of the challenges encountered by those managing IAM solutions in their own environments are negated with IDaaS.

IDaaS solutions provide customers relief from the overhead of infrastructure support, specialized staffing, providing consistent deployments, and maintenance and upgrades. As you evaluate IDaaS, be sure to factor the benefits in this section into your decision matrix with their associated savings.

Infrastructure

IDaaS solutions don't require servers, storage, or other infrastructure installed and maintained at the consumer's location; everything is hosted from the cloud. For IDaaS, the only client side equipment required is smart card readers or biometric devices on workstations if MFA is utilized, but those devices are necessary regardless of IDaaS or IAM. The benefit to the consumer is that there are no capital expenditures (CAPEX) on hardware or infrastructure.

Staffing

IDaaS transfers administrative support from the consumer to the cloud service provider. The infrastructure administrative duties such as installation and configuration are already performed by the cloud service provider at the multitenant level for all consumers; the cloud provider staff performs these tasks for everyone. Application level configuration specific to the customer's application environment may still be performed by the consumer, but wizards and templates ensure that the "heavy lifting" is no longer required. The consumer reaps the benefit of highly skilled, on-premises staff being freed up to support other business-centric initiatives.

Deployment

IDaaS solutions are automatically deployed via the cloud by using a standardized multitenant architecture. When a new consumer starts its service, a new IDaaS environment is provisioned in the cloud by using virtualization and cloning technologies. A standardized baseline IDaaS image at the latest version and security patch level is then customized via the consumer using self-service portal access, wizards, and templates.

TIP

The benefit of a standardized deployment process ensures that the consumer is provided a secured, standardized, and baselined environment so he can start his application specific customizations sooner and at less risk.

Maintenance and upgrades

IDaaS solutions shift the overhead and complexity of mundane maintenance and upgrade tasks to the cloud service provider. As a SaaS application, these duties are transferred from the consumer to the cloud service staff. Centralizing these operations outside the responsibility of the consumer ensures that the IDaaS software and consumers' data and configurations are regularly patched and upgraded to the latest version and security release, properly backed-up and replicated to the Disaster Recovery (DR) environment, and tuned for optimal performance and efficiency. These technically complex tasks are shifted from the overworked consumer's staff to the full-time, specialized cloud service staff. The benefits are that the maintenance and upgrade workload is shifted to cloud staff specializing in these duties, which removes the burden from the consumer's IT staff.

Cloud Identity Benefits

Beyond the attributes inherent to any SaaS offering, cloud-based identity solutions offer specialized benefits for decision makers to consider. This is possible because IDaaS providers support IAM functions and product development on a daily basis — this is all they do. They are in tune with industry direction and customer requirements within the IAM space. While consumers perform IAM as part of their job, IDaaS providers perform IAM *as their job*. As a result, the specialized expertise brought by cloud identity experts exceeds what individual customers can provide. The enhanced capabilities delivered by cloud identity service providers translate to lower costs, but more importantly increased business agility, compliance and security assurance, and new opportunity in the age of digital transformation.

TIP

Lower infrastructure and staffing costs are nice, but they aren't the biggest driver for adopting specialized cloud service such as IDaaS. Innovation, new capabilities, and speed to implementation are where the greatest benefits exist. Lowering costs won't open new markets or create new customers, but innovation with new technologies will.

Simplified solutions


TIP

Delivering the right IDaaS functions the consumer needs is critical. Not overwhelming customers with things they don't want or need is important. The details behind IAM can be overwhelming, but IDaaS simplifies the offerings, and mature cloud service providers have the expertise to assist customers in determining what they need. Cloud identity solutions provide standardized solutions as a baseline to fully cover customers' core functions (avoiding any gaps), but are then customized to meet their specialized requirements.

Reduced integration challenges

Application integration (for example, making all pieces and parts work together) is some of the most complex, expensive, and time-consuming work facing an IT organization. The very nature of IAM solutions is to interface and integrate with a wide range of applications at multiple levels (user provisioning, access control, auditing, monitoring, and so on). Fortunately, cloud identity streamlines and simplifies application integration. Best-practices, wizards, and pre-configured APIs reduce the complexity and provide consumers streamlined application integration faster and at lower cost — and with fewer headaches.

Wide support of legacy, cloud, mobile, and IoT

The access and support requirements for IAM functionality has never been greater and is only expanding. Support of existing, legacy on-premises applications is necessary, but it can be challenging given the age and varied nature of legacy applications ranging from end-of-life desktop/workgroup systems to mainframe systems. Moving forward into the digital transformation, access to cloud applications (particularly the myriad of SaaS applications) is essential. As both employees and consumers shift to a mobile "anytime, anywhere" computing model, and with the advent of IoT devices everywhere, IAM capabilities must be immediately available and seamless to users.

A key value-add of IDaaS is simplified support of diverse applications, regardless of their location or technical maturity. Cloud Identity provides libraries of APIs and easy-to-use portal-based wizards, simplifying access to these different applications. In the

fast-growing world of SaaS applications, providers to the newest offerings, enabling digital transformation.

Faster delivery of solutions

Traditional, on-premises IAM solutions are procured, built, and implemented over many months and frequently extend over a year before any benefits are realized. This is due to the custom build, configuration, and integration work performed by over-worked IT staffs not well versed in IAM technology.

As a contrast to months and years, cloud-based identity solutions are provisioned in hours and operationally deployed in weeks to a few months. Leveraging pre-built and standardized IDaaS solutions with easy-to-use configuration tools, the time-to-value of cloud identity solutions is faster by orders of magnitude.

Scale as needed

Cloud-based solutions scale to provide additional processing capacity to meet surges in workload. Instead of procuring and supporting additional expensive on-premises infrastructure for workload spikes, IDaaS solutions simply expand to provide more capacity without the CAPEX and labor expenditure. And unlike on-premises hosting that must continue to support the infrastructure after the workload spike has subsided, IDaaS solutions shrink their capacity back to normal processing levels. Best of all, the IDaaS consumer only pays for what they used; no need to pay for unused capacity sitting idle in a datacenter.

Lower total cost of ownership

Eliminating the need to purchase on-premises infrastructure (hardware, software, networking, and so on), administrative support labor, and the mandated patch, upgrade, and technology refresh cycle significantly lowers TCO in comparison to cloud-based identity solutions. Standardization, economies-of-scale, and multitenancy on behalf of IDaaS service providers bring the cost to consumers down to lower levels than what individual organizations supporting on-premises IAM can do themselves.

IN THIS CHAPTER

- Learning the details of how IDaaS works
- Exploring common IDaaS deployment use cases
- Identifying key factors for IDaaS success

Chapter 3
Planning Your IDaaS Strategy

Identity as a Service (IDaaS) performs complex tasks and performs critical functions, but much of this is masked from consumers and users. Without going into deep detail, it is beneficial to have a working understanding of the "magic behind the curtain." Organizations come to IDaaS with different support requirements ranging from on-premises legacy applications, hybrid mixed workloads, and cloud-only implementations. Regardless of customer requirements, all can benefit from a refined checklist of critical capabilities and best practices.

In this chapter, we describe the technology behind IDaaS and the most common customer use cases, and provide a checklist of factors to consider as you develop your strategy.

Understanding How IDaaS Works

Although the IDaaS provider performs the detailed technology management, a basic working knowledge of the technical components supporting IDaaS is beneficial. A technical perspective enables smarter decision making and value judgements. Not all

environments will use all components for every application, and details of implementation will vary between vendors, but most IDaaS implementations have these components:

- **Directory Services (DS)** are the authoritative source (data store) of user identities. Typically these contain a username, full name, organization, potentially one or more roles, and account status. The IDaaS checks the user identity against the DS to see if a user exists, and if so, what level of access is granted within the application. Lightweight Directory Access Protocol (LDAP) is the oldest popular type of DS, and Microsoft Active Directory (AD) is the most common implementation of LDAP. Directory Services can be deployed on-premises or in the cloud, and organizations may have multiple DS deployed for different applications.
- **Single Sign On (SSO)** is the technology and implementation that allows one application identity and login event, enabling access to other applications without re-executing the login process. SSO is a convenience to users because they do *not* have to remember multiple usernames/passwords (enhancing security) and must login only once to access all their applications. After a user logs in, a token authorizing access is created. The IDaaS software uses that token to log in to other applications on behalf of the user whenever the user accesses a new application.
- **Federation** is the concept and technology that a user's identity is valid within her own enterprise, but it is also published and integrated outside the enterprise to other applications providing access. The IDaaS software performs the integration of users' identities across multiple enterprises to enable authorized access (user convenience) and to reduce the number of username/passwords to manage (enhancing security).
- **Security Assertion Markup Language (SAML), OAuth, and OpenID Connect (OIDC)** are protocols and standards for the exchange of authentication and authorization between services. These enable SSO and federation and are implemented by the IDaaS software. With continual version updates and releases, it is the IDaaS vendor's responsibility to manage updates, integration, and testing.

- **Multifactor Authentication (MFA)** is an authentication mechanism that requires users to provide two or more of the following:
  - Something they *know* (such as a pin number)
  - Something they *have* (such as an electronic token or smart card)
  - Something they *are* (a biometric attribute)

  MFA is far more secure than traditional username/passwords with many organizations mandating MFA.
- **Self-service** via web-based portals enables users to register themselves for application access, create accounts and passwords, and recover lost usernames and passwords. Additionally, profile management, delegated user management, workflow processing for requests and approvals, and recertification approvals are possible. Still secure and fully auditable, self-service portals are a real-time convenience for users and eliminate the overhead cost and complexity (and security risk) with a staffed helpdesk managing user account support and maintenance.
- **Launch pads** are centralized portal pages for employees to access applications from. Listing the Software as a Service (SaaS) and mobile applications available, employee launch pads provide centralized control and convenience for the applications employees may access.
- **Connectors** serve as integration points into applications from the IDaaS cloud. Leveraging connectors, users access disparate applications quickly with the same underlying credentials and with a similar process even though the applications themselves are from different vendors with varying technologies. IDaaS vendors create and maintain an ever-expanding library of connectors facilitating access.

Every IDaaS solution differs and the implementation details are as varied as the customers' applications. However, Figure 3-1 depicts the core components of an IDaaS implementation in a hybrid environment.

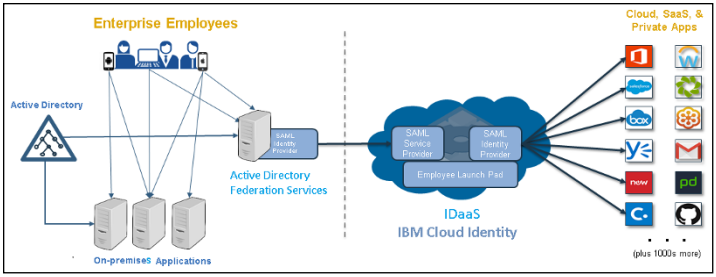

FIGURE 3-1: Accessing on-premises and SaaS applications with IDaaS.

In the example, a hybrid environment of on-premises enterprise users are using LDAP to access their on-premises applications with SAML to connect to the IDaaS in the cloud. From within their IDaaS, they're using their employee launch pad and pre-built connectors to access myriad cloud-based SaaS and private applications. Additionally, integration with mobile applications is strong with IDaaS.

ADAPTIVE AUTHENTICATION

As authentication technology advanced over the past decade, a more sophisticated form of authentication, or *adaptive authentication,* emerged as the standard. Adaptive authentication is a way that multi-factor authentication or two-factor authentication can be deployed. With adaptive authentication, the IAM solution is configured to ingest contextual information about the user and use that information to *adapt* the appropriate access decision. Based on the contextual information, the authentication mechanism can allow access immediately, trigger a second-factor challenge (such as an email one-time password or SMS verification code), or deny access altogether.

To achieve adaptive authentication, organizations have traditionally had to manually determine and encode risk-scoring scripts that process attributes such as device fingerprint and IP reputation — and execute the same access decision each time. In today's era of advanced machine learning, organizations want to integrate more intelligent detection technology that can process sophisticated behavioral signals — how a user holds her phone (for instance, in the left hand instead of the right) or device location data — and then use analytics to assess and "learn" signals of risky user behavior over time.

Exploring Key Use Cases for IDaaS

Specific needs for organizations are unique, but based on the organization's age, background and lineage, and cloud adoption maturity, three common use cases emerge.

On-premises only applications

Organizations that have not moved to the cloud and are 100 percent supporting on-premises are candidates for IDaaS. Frequently with long-established histories and/or those with strong security and risk aversion polices, these organizations adopt cloud and enterprise Identity and Access Management (IAM) solutions in a slower methodical, measured approach.


TIP

The benefits of IDaaS for on-premises consumers include

- Enhanced end-to-end capability, eliminating siloed IAM solutions, ensuring a secure governance, risk, and compliance (GRC) solution, and simplifying the landscape
- Elimination of infrastructure and support requirements for on-premise IAM solutions resulting in lower cost
- Laying the foundation for expansion into future cloud services by creating an IDaaS capability

Many organizations have a cloud footprint, but for those without, a SaaS solution such as IDaaS is a good way to start.


TIP

Not ready to jump into an enterprise IDaaS solution as your first cloud experience? You can use IDaaS for a subset of your applications and pull back anytime; you have easy entry and exit points.

Full cloud stack

At the other end of the spectrum are organizations that are 100 percent cloud deployed. Frequently, these are new entrants who leveraged cloud from Day 1 without ever building out an on-premises footprint.


TIP

The benefits of IDaaS for these consumers are

- End-to-end capability and no support of on-premises infrastructure and staffing for traditional IAM solution

- Simplified implementation and deployment for private web, mobile, and SaaS applications
- Accelerated delivery of new applications for customers in the B2C, B2B, B2E, and B2IoT spaces
- Robust GRC and IGA for the enterprise that's secure and auditable
- Self-service portals and employee launch pads for speed and convenience

Full stack IDaaS environments aren't for everyone, but for organizations in that category, they enjoy lower cost, faster and easier deployments, and enhanced security and compliance.

Hybrid environments

Organizations with a combination of on-premises and cloud-based applications are hybrid implementations. A majority of companies haven't or can't move all their on-premises applications to the cloud (for a variety of reasons), but they're leveraging cloud for commodity-based or new technology applications. Hybrid environments represent the majority of customers and IDaaS implementations. Hybrid environments are also the most complex environments to support, but they benefit greatly from IDaaS:

- Simplified end-to-end cloud-based IAM for the enterprise across on-premises and cloud-hosted applications
- Elimination of siloed piecemeal IAM solutions that are costly, complex, and have gaps in coverage
- Standardized and consistent IAM services for all types of customers regardless of applications utilized
- Self-service portals and employee launch pads to consolidate and simplify application access
- Accelerated access to new capabilities via SaaS and mobile applications while maintaining access to legacy applications

Providing an end-to-end enterprise-level solution for IAM is the strength of IDaaS solutions. Hybrid environments are particularly well suited for IDaaS to reduce complexity and costs for on-premises applications and extend functionality into the cloud for modern SaaS applications.

BEING A GOOD CLOUD TENANT

Remember, cloud computing leverages a *shared services* computing model; customers are sharing computing resources and capacity with other consumers (called *tenants*). *Multitenancy* is the sharing of cloud architecture by multiple tenants. Standardized, commodity-based resources leveraging economies of scale with multitenancy is key to how cloud service providers can charge attractive subscription prices and still make a profit.

Some consumers demand dedicated (not shared) resources and run highly custom applications; these are both barriers to cloud adoption. The best candidates for cloud applications are those that can run well in shared environments and use modern, standardized software tools and processes.

Security is often cited as a reason for not adopting a shared computing model, but cloud security is continually improving and has evolved to a level that many customers are willing to accept.

Consuming resources (CPU, memory, storage, network) in a controlled and predictable manner (for example, not being an uncontrolled "resource hog") is another characteristic of good cloud tenants. Cloud environments can support utilization spikes, but the consumer will pay for the increased workload and capacity.

Modernizing applications to run on standard, commodity software and infrastructure supported by cloud service providers is another key to being a good cloud tenant. Modern applications tend to "play well with others."

TIP

Customers with very specialized security requirements (for example, governmental organizations) are building private and community clouds on-premises within their data centers. Managed by the cloud service provider staff, but hosted on-premises, these environments provide the benefits of cloud while enabling additional security and GRC.

Planning Your Success with IDaaS

Prior to implementing IDaaS, developing a plan is essential for success. With a foundational knowledge of cloud and IAM

functions and technologies, the steps of planning for IDaaS are straightforward. Your checklist should include

- **Scope and capabilities:** How deep into your application stack do you want to extend IDaaS, and what do you want to achieve? IDaaS is designed to protect on-premises applications, but you must consider organizational constraints for how far you can implement cloud-based IAM.
- **Governance and management responsibilities:** What are the current rules and responsibilities, and how will those change with IDaaS? Positive organizational change and shifts are part of IDaaS and must be part of the planning process.
- **Web access requirements:** Who will access IDaaS supported systems, and where are the users located? Perform your due diligence and homework to know what ports, protocols, network access restrictions, and security requirements exist for the full population of your users (not just those in the office). Pre-made connectors, templates, and wizards enable IDaaS integration with most applications and technologies, but you still must identify the who, what, where, and how for your connections.
- **Mobile and cloud users:** What mobile and cloud applications and users do you have today and will have in the near future? Large legacy applications with thousands of users get all the attention; however, you must account for the mobile and cloud applications that you don't necessarily host but are critical to your users.
- **Auditing, reporting, and compliance requirements:** What organizational and industry specific compliance regulations must be accounted for? IDaaS brings powerful GRC and IGA capabilities, but your organization has specific requirements that must be supported. Ensure that your compliance experts are part of the planning sessions early on to ensure the IDaaS solution meets their needs.
- **Policies, standards, and strategies:** What are the current recommended and regulatory requirements for access control, account and password management, and monitoring and auditing? This is an excellent time to ensure that your practices and policies are meeting the standards and if not, to bring them up to the latest requirements.

Brainstorm with your team, collaborate with stakeholders, and research industry and vendor guidance to create the IDaaS planning checklist that meets the needs of *your* organization.

IN THIS CHAPTER

- Preparing to deploy IDaaS for your organization
- Envisioning full cloud deployment architectures
- Describing real impacts in the age of Digital Transformation

Chapter 4
Using IDaaS in the Real World

Implementing Identity as a Service (IDaaS) in operational environments requires planning and due diligence but the software and SaaS architecture reduces complexity lowering barriers to adoption. Organizations commonly deploy IDaaS in hybrid environments and increasingly into fully cloud-enabled organizations providing maximum access to new technologies and capabilities. Case studies consistently show the benefits of IDaaS are realized by organizations as they're empowered in the age of digital transformation. A new way of doing business smarter and better becomes a reality with organizations responding positively to this shift in thinking.

In this chapter, we identify the key evaluation and deployment steps for an IDaaS implementation, highlight the most capable full cloud architectures, and show how organizations take advantage of cloud-based Identity and Access Management (IAM) services.

Evaluating IDaaS Features

The IDaaS provider you select is a critical partner in the journey to cloud-based IAM; the support and features they provide have a significant impact on your success. There are three main categories to review:

- Technical features such as Single Sign On (SSO), Enterprise Directory Services storing user identities, pre-built connectors simplifying access to mobile, Software-as-a-Service (SaaS) applications, Big Data, and the Internet of Things (IoT), seamless integration across technologies and architectures, and Disaster Recovery (DR). Mature IDaaS solutions will have these features providing end-to-end coverage for all deployment architectures.
- Compliance, monitoring, and reporting capabilities that meet regulatory standards are automated and easy to understand, generate auditable reports and dashboards, and trigger alerts and corrective actions when suspicious activities occur. Robust governance, risk, and compliance (GRC) and Identity Governance and Administration (IGA) capabilities should be infused throughout the solution and not bolted-on as an afterthought.
- Support levels and self-service capabilities must match the operational needs of the organization and expectations of the user community. IDaaS is a critical component so system availability and vendor support must be robust; cloud architecture is frequently High Availability (HA) and vendor support should be 24/7. SaaS solutions should embrace self-service portals to empower users, and application launch pads are a feature of strong solutions.

In a nutshell, mature IDaaS solutions are technically strong and end-to-end, GRC and IGA capabilities are robust and appropriate to the customer, and support and service must meet operational needs and users' expectations.

REMEMBER

One last item to consider and it is important: Is the IDaaS vendor someone you *trust* to provide real solutions and to be with you for the long haul? Be sure to evaluate the vendor's past history, longevity, and commitment to the IDaaS space.

Taking Steps in IDaaS Deployment

Infusing IDaaS into an organization can be a relatively fast process (typically measured in months, not years) with the planning and communications often taking longer than the technical implementation itself. Remember that in addition to the technical aspects of implementation, you can expect that some GRC processes and IT roles and responsibilities will change, particularly for organizations new to cloud computing.

Success and ease-of-deployment is directly tied to the amount of planning, communication, and coordination you perform; we recommend assignment of an experienced Project Manager (PM) to streamline this process.

Milestone events during the IDaaS deployment project include

1. **Gather requirements to determine the scope and desired outcomes of the project.**

   In Chapter 3, we provide a checklist to tailor to your organization's requirements.

2. **Evaluate, select, and procure an IDaaS solution.**

   Do your market research and select your provider carefully; picking the right solution fit to your requirements and a partner that will assist you is crucial to success.

3. **Build an implementation plan that includes technical and non-technical process and staffing updates with all stakeholders.**

   PMs provide great value and ensure that all aspects of the deployment are addressed.

4. **Test the IDaaS implementation with target applications, get feedback, and update the implementation plan as needed.**

5. **Implement the IDaaS solution into production.**

6. **Review and evaluate results at the technical, operational, GRC, stakeholder and user satisfaction, and TCO levels.**

The journey to IDaaS is a trip, but it isn't a long odyssey. Selecting the right vendor and solution coupled with a well-planned implementation strategy brings the benefits of cloud-based IAM to your organization sooner rather than later.

Deployment into Full Cloud Environments

Organizations leverage IDaaS to securely integrate into these resources:

- Mobile applications
- IoT devices
- Big Data and analytics
- SaaS applications such as Microsoft Office 365, Google Apps, Salesforce, ServiceNow, Concur, and Workday
- Cloud-based PaaS and IaaS offerings
- Any resource accessible via a connector (the sky is the limit!)

Coupled with self-service portals to register access and address lost usernames/passwords, and with application launch pads, access to these resources is simplified, which empowers the users 24/7. Figure 4-1 depicts access into SaaS applications.

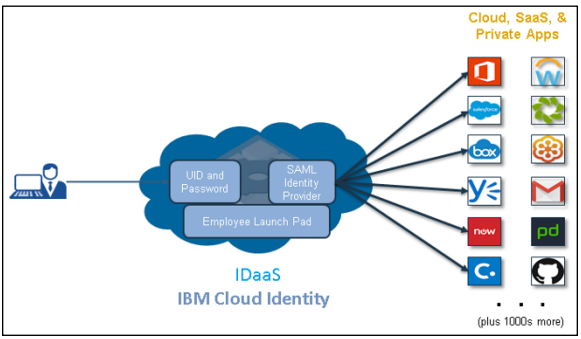

FIGURE 4-1: Leveraging SaaS applications via Cloud Identity.

THE EMERGING CHIEF DIGITAL OFFICER

Digital transformation is changing the way businesses operate. With the infusion of digital technology into the daily lives of human society in a world market, businesses must reshape how they view customers and business opportunities. Business practices and technologies that seamlessly extend into the lives of potential customers, reaching beyond traditional buyer-seller models, are central to digital transformation. The intent is to develop innovative business models, products, and services generating new revenue streams based on the deep, continual infusion of technology. The importance of digital transformation is so great that a new C-level executive is appearing: the Chief Digital Officer (CDO).

The CDO's role is to drive digital business transformation within the workforce and with external customers and business partners. The CDO works closely with the CIO and Line of Business (LoB) leaders to ensure that technologies and business opportunities driving digital transformation are promoted at all levels; this is a challenging new way of thinking for many. Creativity, innovation, "failing fast," and agility are all keys to successful digital transformation and are championed by the Chief Digital Officer.

Technologies such as IDaaS, which brings mobile and SaaS applications closer to the customer, provides self-service portals, and transparent integration and security, are strongly supported by CDOs.

Security is critical and often cited as a reason to deny or restrict access to mobile applications. Figure 4-2 shows how access into mobile applications is secured by IDaaS.

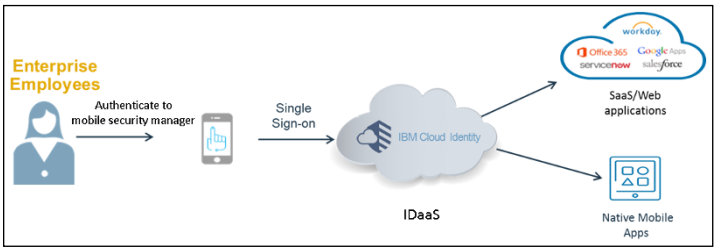

FIGURE 4-2: Securing mobile application access with Cloud Identity.

Deploying IDaaS into full cloud environments isn't as common as into hybrid environments where on-premises applications are present; this is because many organizations still have an on-premises footprint and will for years to come. However, the principles of full cloud environments translate to hybrid environments, with the largest challenge being integration with older legacy applications.

Achieving Results with IDaaS

Organizations deploy to IDaaS with a multitude of specific operational requirements, but the core drivers center around common themes:

- Lower operational and support costs driving down TCO
- Greater GRC and IGA compliance and security
- Quicker deployments and simplified environments
- Enhanced capabilities enabling digital transformation

The case studies in this section describe real-world organizations implementing IDaaS and how it transformed their businesses.

Supporting IoT applications

A large telco implemented Cloud Identity, enabling access to its new IoT platform. Its environment was production-ready within two months and provided over 10,000 users secure access to IoT applications. Some challenges the company faced included

- Required API-based access management into its IoT management platform
- IT staff faced a critical skills shortage and couldn't implement fast enough for the aggressive schedule
- Existing IAM infrastructure could not scale to meet new workload

Implementing IDaaS had many impacts:

- The environment was production-ready within 60 days.
- The organization is generating revenue in a new market.
- The telco was able to create, view, manage, and delete external users requiring access.
- It had new centralized authentication and SSO for external users.

Enabling a customer portal

A large distributor leveraged Cloud Identity to power its customer-facing enterprise portal. Its environment supports over 40,000 internal and external users with access to seven different applications requiring provisioning services. This distributor faced the following challenges:

- Excessive cost and complexity of deploying and managing on-premises IAM solutions
- Larger external user base suffered from minimal control over their identity management life cycles
- Unable to manage external identities separately from internal identities

Leveraging Cloud Identity had the following impact:

- Faster and easier deployments than with on-premises IAM
- Simplified administrative environment and less effort to manage the solution
- Easy integration with target applications and platforms

IBM CLOUD IDENTITY

IBM has an established and respected IDaaS offering portfolio: Cloud Identity. Cloud Identity supports a variety of deployment models, from lightweight SSO and advanced authentication, to a full stack of IAM services all delivered from the cloud as SaaS.

Cloud Identity is offered as a multitenant public cloud service designed to help organizations simplify and accelerate identity protection in a multi-perimeter environment. The full stack solution provides an end-to-end SaaS-based IAM capability:

- Hybrid and full cloud stack support
- End-user mobility management
- Enterprise grade IGA
- Advanced, adaptive authentication
- Lightweight SSO
- Self-service portals for account management and application launch pads into SaaS and mobile applications
- Hundreds of out-of-the-box connectors facilitating easy access and integration with external SaaS and internal on-premises applications

The benefits of IBM Cloud Identity include the following:

- Leverages a broad spectrum of on-demand IAM features from the cloud, including federation, Web Access Management (WAM), and IGA
- Reduces costs up to 60 percent and achieves predictability when planning for fixed and operating IAM costs
- Eliminates the need to build and manage infrastructure by leveraging an all-cloud IAM strategy

Visit `www.ibm.com/security/identity-access-management/cloud-identity` for more information.

IN THIS CHAPTER

- Learning tips and techniques to succeed with IDaaS
- Identifying the benefits you want from IDaaS
- Figuring out how IDaaS will be deployed and managed
- Evaluating and validating your cloud vendors

Chapter 5
Ten IDaaS Planning Items

Planning, implementing, and managing Identity as a Service (IDaaS) effectively is the key to a secure and integrated Identity and Access Management (IAM) solution for your organization. However, many of the best tips and tricks are non-technical and not in any vendor documentation; they come from hard-earned experience and lessons learned. In this chapter, we discuss some ideas, preparation steps, and cautions to help you have a successful IDaaS deployment.

Understand How Security and Compliance Is Managed Today

Computers perform tasks very fast; the challenge is that performing a bad process faster isn't helpful. Automating inefficient processes or performing steps that do add to security, governance, risk, and compliance (GRC), or business value isn't what we wish to achieve.

Prior to purchasing any IDaaS solution, make the time to do the internal research for how security and GRC is (or isn't) being managed today. Review the processes and documentation trails from several viewpoints: an auditor, security manager, technologist, business analyst, and end-user.

Plan for a Change in Culture

Change is initially uncomfortable, both on the personal and institutional level. Moving to a cloud environment is challenging for many; uncertainty and concern is natural. Workloads shift, job responsibilities change, and the comfort of knowing your environment (no matter how challenging it might be) is often reassuring.

Changes to security processes incurred by enhanced GRC via IDaaS software and processes are institutionally challenging too. Organizational processes and procedures take on a life of their own and they don't want to change; the phrases "it will never work" or "but our process is X,Y,Z" are common (and often why organizations are inefficient).

REMEMBER

Planning, communication, and transparency driven by strong leadership with a degree of patience and empathy is the way to overcome the paradigm shifts of cloud computing and IDaaS. Factor in communication, potential re-training, and organizational process changes into your IDaaS plan.

Identify the Benefits You Want Most from IDaaS

If you don't know what you want, it is very difficult to obtain or measure your success. Don't purchase IDaaS (or any tool) without a set of goals and metrics to chart your progress.

"Mission drives the gear" — what do you want your IDaaS solution to provide? Do you need end-to-end IAM functions, and do the vendors you are evaluating support that? To what degree must you support on-premises legacy applications versus mobile and Software-as-a-Service (SaaS) applications key to digital transformation?

After you have a list of your "must haves" and "nice to haves," you can then evaluate IDaaS offerings objectively and without purchasing features you don't need.

Define Explicitly How IDaaS Will Be Deployed and Managed

It is a cliché but accurate that "failing to plan is planning to fail." IDaaS has far-reaching (positive) impacts at the technical, support, and organization process levels; these are core to your implementation plan.


TIP

Build a road map showing the transition of your "as-is" environment into the "to-be" target architecture. Clearly define the ownership, roles, and responsibilities for each process and integration point against the target applications and user populations. Identify milestone events, sequence chains, and resulting timelines for each major action.

If implementing IDaaS sounds like a project, it's because it is. Appoint an empowered Project Manager (PM) to lead the effort and ensure strong executive sponsorship and support. IDaaS represents a powerful capability and vehicle for positive change, but it takes careful planning and leadership to drive it to successful implementation.

Accept That There Is No Limit to What Can Be Secured

IDaaS has far reaching tentacles into old and new applications alike; leverage that capability. Modern, mid-range technologies from major vendors pose little difficulty; the vendors of those applications want to integrate with IDaaS as a selling point. Applications and technologies at the new and old ends of the spectrum that pose the greatest challenges.


WARNING

On-premises legacy applications, often running on old, unsupported technologies, pose a significate concern. If an application isn't well documented or maintained, lacks modern security controls, and doesn't have strong visibility into its operations,

then it's a prime target for fraud, abuse, and hacking. "Security through obscurity" is a poor practice and only benefits the bad guys. Either decommission/upgrade these old applications or leverage the existing and custom application programming interfaces (APIs) of IDaaS to integrate them with the GRC capabilities.

New applications, SaaS applications in particular, present a risk at the other end of the spectrum. Forward-leaning vendors create new SaaS applications every day, and hungry users eagerly consume these before organizational IT is aware of their presence. Shadow IT is alive and well in the age of digital transformation, and IT must still play catch-up.

Fortunately, mature IDaaS vendors create easy-to-use connectors enabling organizations to plug these new SaaS applications into their IDaaS implementation as fast as the new applications appear. Leveraging a proven IDaaS solution enables new SaaS applications to be used securely with necessary GRC processes without slowing down users working to grow the business and seize new opportunities.

Consider End-to-End Solutions

One of the principles of Enterprise Architecture is building a road map describing your desired target state and how it supports your strategic objectives. Without a defined goal and plan to get there, organizations create a series of short-vision solutions that only solve individual challenges and completely fail to meet long-term enterprise objectives. Experience has shown this is a very expensive, inefficient, and wasteful way of doing business.

Rather than buying a series of disjointed, short-term IAM solutions, or creating application-specific custom IAM-like solutions, consider the value of a true enterprise level IDaaS to meet the needs of all your applications. One IDaaS solution will simplify your IT landscape, give you consistent GRC across your applications, and lower your infrastructure costs while preparing your organization for digital transformation.

Evaluate the Maturity and Capability of Your IDaaS Provider

Just as not all IT vendors and cloud service providers are the same, certainly not all IDaaS providers have the same capabilities or maturity. IAM and cloud computing are rapidly evolving technologies; expect continual change and evolution within this market space.

First, determine and document your IDaaS scope, requirements (needs and wants), and your risk tolerance; let that drive your vendor selection criteria. Next, leverage multiple objective resources to learn about the capabilities, strengths, and weaknesses of IDaaS vendors meeting your criteria. Many reputable research organizations publish structured market analysis on technology products. Finally, conduct your own market analysis and request vendor demonstrations to form your own opinions. These steps are time-consuming, but you and your management will have confidence that you made the best, most informed decision.

Validate the Security of Your Cloud Vendors

"Who is watching the watcher?" is a serious question for those in the security and audit compliance field, and it certainly rings true for cloud vendors in the IDaaS space. No vendor will volunteer that it doesn't run a tight ship for internal GRC and security, so how can you trust your organization's security to an off-site provider? How can you convince your management that the risk is worth the reward?

Obviously, as part of your research you need to measure vendors' maturity and linage — particularly for cloud hosting and the source of their IDaaS offering. Are they a new company on a shoe-string budget catering to lower-end clients with cost as the primary driver? Are they relatively new in either the cloud or IAM field where they gained those capabilities via recent acquisitions and are simply rebranding someone else's products and services? Or do they have legitimate experience and expertise in cloud and IAM services where offering IDaaS is a logical progression?

Study the documented (not verbal) compliance standards published by vendors. In particular, become educated on the various government compliance standards for cloud hosting providers. To do business with many government organizations and in highly regulated industries, vendors must be certified against those standards; this requires meeting stringent security and GRC rules. Regardless of your industry, select a vendor that meets or exceeds those standards and ensures your IDaaS and data is hosted with the same degree of compliance (not in a 2nd tier lower security data center).

Ensure Visibility via Audits, Metrics, and Dashboards

It is not enough that you are following security policies and GRC standards, but you must *prove* you are compliant. IDaaS offerings automate auditing and report metrics via easy to use dashboards. Stored without the risk of tampering, these tools generate audit trails that withstand the scrutiny of auditors.

High-quality IDaaS solutions leverage logic algorithms, Big Data, and analytics to trigger alerts when suspicious activity occurs. For instance, how can the same person access an application from the United States but moments later from overseas? Or is it normal for an employee to download very large amounts of data late at night? IDaaS systems should trigger alerts and/or take preventative action when these events occur.

Embrace Self-Service and Delegated Administration

Security and GRC should work *with* the users, not *against* them. Automated account processes, workflows, and password recovery mechanisms are both secure and necessary to support agile business practices in the age of digital transformation. Properly implemented self-service and delegated administration portals are secure and still maintain audit trails, but they don't slow down business in the process.

Discover how IDaaS benefits your organization

Many organizations struggle to keep up with Identity and Access Management (IAM) and seek a better solution. In this book, you find out how deploying IAM as a cloud-based IDaaS solution solves many challenges. IDaaS lowers TCO, simplifies architecture, improves security and compliance, and more. Via Cloud Identity, IBM's IDaaS offering, you gain robust governance, risk, and compliance (GRC), identity governance and administration (IGA), and security.

Inside...

- The identity management landscape
- IAM business drivers
- IDaaS architecture and components
- Technical and business advantages
- Cloud Identity use cases
- Ten IDaaS planning items

Mike Wessler, certified OCP, CISSP, and PMP, specializes in Oracle technology with a passion for Technical Architecture and has authored/co-authored eight books.

Sean Brown, Senior Product Manager at IBM, leads the overall market strategy, planning, and development for IBM's Cloud Identity portfolio.

ISBN: 978-1-119-47264-3
Part #: 71013371USEN-00
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.