Future-proofing Your Tactical IAM Projects

Make sure that addressing today's IAM challenges doesn't prevent you from solving tomorrow's

By Todd Peterson, IAM evangelist, Dell Software

Software

Introduction

The phrase “identity and access management” (IAM) is often reserved for large, strategic projects such as governance, enterprise provisioning and privileged account management. Without question, those things are very important and deserve the attention, budget and effort they get.

But there is another layer of IAM, one that falls more to the tactical, day-to-day tedium of simply enabling users to get to the systems and applications they need to do their jobs. Most organizations attack these IAM tasks as simply part of daily IT operations, without any conscious classification that what they are doing is fundamentally IAM. But it’s important to understand how these types of IAM activities can, and often do, stand in the way of success with their cooler big brothers.

I like to think of IAM as a specialized version of Maslow’s hierarchy of needs: if the basics are not taken care of, the more advanced activities can never get off the ground (see Figure 1).

That is, before any organization can get to the pinnacle of the hierarchy — governance — it must ensure that all the levels below are fully satisfied. And that’s where many IAM projects fail, or at least struggle mightily — requiring much more time, money, and effort than necessary.

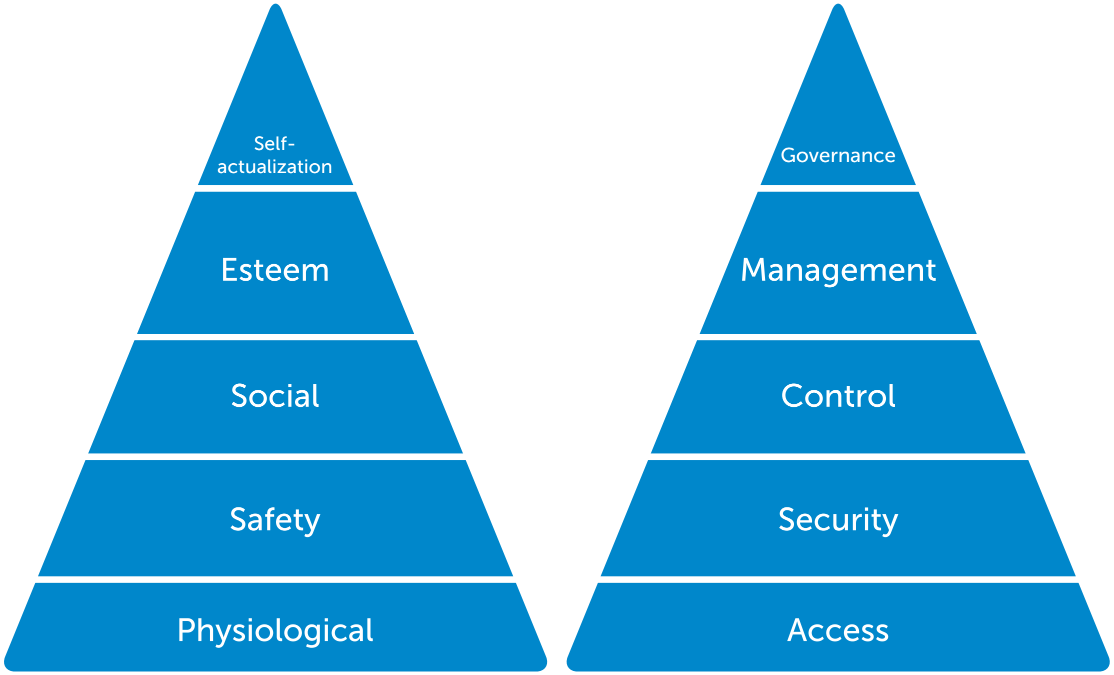


Figure 1: Maslow’s hierarchy and the hierarchy of IAM needs

The IAM challenge du jour

How the basic A's of IAM become barriers to IAM success

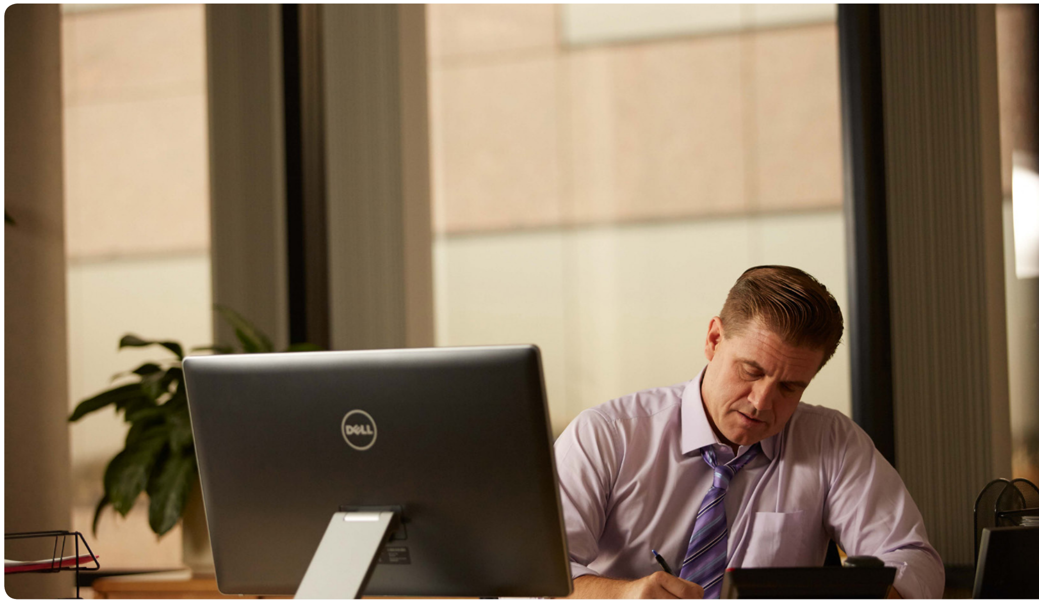
Every system, every application and every user population requires three of the four basic A's of IAM: authentication, authorization and administration. (Moving beyond control and into governance requires the fourth A: audit.) Every system or application needs a way for users to identify themselves as the right person to be logging on — authentication. Every system or application needs a way to control what that person can do once they are logged on — authorization. And every system or application needs some way for the organization to set up authentication and authorization correctly — administration.

And that's where the fun begins.

Because there is rarely a common authentication method across diverse systems and applications, organizations end up with many passwords, all using different complexity rules and expiring at different times — an administrative nightmare. And because there is no single concept of authorization that can be used across all systems and applications, organizations end up spending inordinate amounts of time simply defining who a user is and what that means for specific systems — and then repeating the process over and over again for every other system or application. Moreover, because all these systems and applications have come from different vendors, been developed in-house by different teams at different times, and/or been purchased with varying levels of attention to security, administration is a jumbled mess of manual processes, tedious tasks, and disjointed tools and interfaces.

Transforming barriers to IAM success into enablers of that success

It's no wonder that the vast majority of organizations find themselves mired in what I like to call the "challenge du jour" — they are stuck down in the security and control levels of the hierarchy, struggling to reach the upper echelons of control and governance. But take heart: you are not alone. Many, many organizations struggle with the same challenges, and there are strategies that can transform these day-to-day challenges from barriers to IAM success into enablers of that success.



IAM projects — if done right — can be a catalyst for IAM success on a larger scale.

In my years of helping customers at all levels of the hierarchy with a wide range of IAM needs, I've seen a few common project types that can either bog down IAM projects or — if done right — can actually be a catalyst for IAM success on a larger scale:

- Single sign-on (SSO)
- Password management
- Strong authentication
- Active Directory (AD) management and security

For the remainder of this ebook, I'll discuss each of these project types and provide some proven strategies that can move them from IAM barrier to enabler.

Superior single sign-on

For many people, particularly those outside of IT, single sign-on is the end-all, be-all of IAM. After all, if your end users, managers and executives have to remember only one password and can get to everything they need whenever they need it, IT is the hero and everybody is happy. But it's a lot easier said than done.

The challenges of single sign-on

The big challenge with single sign-on is the constantly evolving nature of the systems and applications that users must access. A home-grown application built five years ago will undoubtedly have different authentication requirements than a new software as a service (SaaS) application that just came online last year — so the ideal SSO approach for one will be woefully inadequate for the other. This challenge is evident even between two modern applications: for instance, a Windows-based SaaS offering, such as Office 365, uses different protocols and authentication than an equally modern SaaS application like Google Apps or Salesforce.com. This diversity of systems and applications expands further as the user's access point changes from a laptop or desktop computer to a mobile device. And we have yet to take into account the challenges of granting remote users the access they need.

> The big challenge with single sign-on is the constantly evolving nature of the systems and applications that users must access.

Consequently, most organizations approach authentication across diverse applications in a piecemeal manner that still requires multiple passwords and different solutions depending on whether the user is on premises or remote. The result is more IT involvement than is ideal, as well as continued user dissatisfaction that often expresses itself in practices that undermine security, such as writing passwords down.

Strategies for making your SSO project an enabler of IAM success

Some proven strategies that can ensure that your single sign-on project is an enabler of IAM success include:

- **Inclusion** — Many SSO solutions are great for some SaaS applications but not so good for other applications that use different standards. And many completely leave out older applications that don't use modern standards. Therefore, approach SSO from the mindset that you are going to implement a solution that includes the widest range of the systems in your environment. This list will typically include all modern standards, such as SAML, WS Federation, OAuth and OpenID Connect, plus some older authentication methods like HTTP headers, credential injection and standard Windows authentication.
- **Don't settle for the lowest common denominator** — The temptation to use a more primitive SSO solution, such as a credential injection solution, is strong, and this approach can, in fact, achieve the end of eliminating multiple passwords. However, the price of not being able to take advantage of the advanced security and ubiquity of newer standards is not worth the convenience, particularly since solutions exist that provide the best of both worlds.

> Look for SSO solutions that provide a seamless experience whether the user is on-premises, remote or switching between the two.

- **Don't make users' lives difficult** — Another knee-jerk reaction to the SSO challenge is to address mobility as a separate access issue from on-premises needs. This typically results in user dissatisfaction and inefficiency, which in turn leads to users attempting to make their lives easier by circumventing security. Accordingly, look for SSO solutions that provide a seamless experience whether the user is on-premises, remote or switching between the two. And don't forget the possibility that users may want and need access from devices not controlled by the organization. In particular, remember that a virtual private network (VPN) is great, but it isn't right in every situation. Look for a non-VPN SSO option for those situations where the VPN simply won't cut it.

Password management — "I can do it myself"

The most obvious symptom of a faulty "pain du jour" approach to IAM is a heavy reliance on IT for establishing, maintaining and evolving user access rights. And the top indicator that you may have a problem is the number of IT-assisted password resets in your organization. Analysts report that the average password reset costs about $25. But that amount hides additional, often larger, costs, including the lost productivity as the user jumps through the hoops necessary to receive assistance from IT, the work that IT is unable to do as they help the user, and the security risks of the practices users resort to in order to avoid calling IT.

> Choose a self-service password reset solution that enables users to help themselves when they've forgotten a password.

Several password management practices can move this obstacle out of the way:

- **Self-service** — Choose a self-service password reset solution that enables users to help themselves when they've forgotten a password. Make sure that it adequately supports the passwords used most often (typically Active Directory) that it is easy to use, that it is accessible in whatever way a user prefers to access it, and that it integrates with other IAM solutions.
- **Single sign-on** — Implementing single sign-on can dramatically reduce the number of IT-assisted password resets. And coupling a self-service solution with SSO can get you close to eliminating them entirely.
- **Unify** — Any efforts that remove the need for additional passwords will also reduce the incidents of IT-assisted resets. The most common example of this type of solution is the Active Directory bridge, which eliminates passwords on Unix, Linux and Mac systems entirely in favor of the universal Active Directory password. One large bank that I'm aware of was able to eliminate a $1 million/month password-reset expense simply by joining its Unix and Linux systems to AD. Combining this approach with a self-service solution turbocharges these benefits.

Strong authentication — when passwords aren't enough

Many regulations and some best-practices frameworks require strong authentication for certain access types, such as high-value transactions, riskier access scenarios or access to specific sensitive systems. But implementing multi-factor authentication can, and often does, add complexity that reduces productivity and keeps the organization from maturing to higher levels of the IAM hierarchy.

> Look for a multi-factor authentication solution that seamlessly plugs into what you already have, uses established standards, and can build on existing directories and authorizations.

Some suggestions to make a multi-factor authentication project as low-impact as possible, without sacrificing security, include:

- **Seek simplicity** — Many multi-factor authentication solutions require dedicated and proprietary technology that must be managed in addition to the established infrastructure that it secures. Look for a solution that seamlessly plugs into what you already have, uses established standards, and can build on existing directories and authorizations.
- **Shop around** — Proprietary solutions often make their money on the second-factor end of the equation. That is, the token used to generate a one-time password is expensive and will provide authentication only for the time specified in the license. There are, however, open standards for multi-factor authentication that will allow you to shop around for the most affordable option for your needs. You just have to be sure to implement a solution that supports those standards.
- **Integrate** — The value of a multi-factor authentication solution can be augmented when it is integrated with other IAM projects such as a single sign-on, remote access, password management or privileged account management solution.

Active Directory management and security

Active Directory holds such a prominent position in the enterprise that inadequate management and security of this universally accepted directory can be a major barrier to IAM success. For all its goodness, AD is woefully lacking in native management tools, privileged account management and natural integration with the rest of the heterogeneous enterprise. Consequently many enterprise IAM projects fail to get off the ground simply because IAM for AD is so difficult.

> Look for tools that allow you to delegate to administrators just as much of the AD Admin credential as they need to do their job. And if this tool also provides AD management, all the better.

But AD is not going anywhere, and there are strategies that can remove the challenges AD typically presents for successful enterprise IAM. To move AD management and security from a "pain du jour" to an IAM asset, a few technologies and strategies are key:

- **Don't go native** — AD includes management tools, but those tools are cumbersome to use, limited in their scope, and rarely include the full functionality required by organizations seeking to manage AD. The result is wasted time spent on tedious and error-prone manual tasks, plus the inevitable impact that inefficiency has on IT and ultimately the rest of the enterprise. However, tools exist that automate these tasks, provide workflows to ensure accuracy of actions, and provide nearly-instantaneous results that are correct every time. Look for a tool that will enable you to do everything you need for AD — and for that matter, everything you think you may someday need. If AD is a stumbling block of an enterprise IAM project, taking this "get AD right" approach can entirely remove the need to custom-build AD logic and IAM functionality in an IAM framework.
- **Secure AD** — Managing AD effectively is one very important thing, but securing AD is another. Natively, AD lacks the ability to granularly define what administrators can do with their AD Admin access, which causes compliance problems and security risk. Look for tools that allow you to delegate to administrators just as much of the AD Admin credential as they need to do their jobs. And if this tool also provides AD management, all the better.
- **Extend AD** — As mentioned earlier, an AD bridge is one extremely valuable solution to the password management issue. What's more, joining Unix, Linux and Mac systems to the trusted realm of AD means that any existing management of AD automatically extends to those systems as well. That is, if a tool is in place that includes workflows to set up, modify and retire AD accounts, that same tool will have a similar impact on Unix, Linux and Mac — eliminating the need to individually manage directories, identities and authentication/authorization on those systems. One government agency estimates a $45 million annual savings in IT workload simply by automating AD management and extending that management to its Unix and Linux systems.

Future-proof your IAM with Dell One Identity

The Dell One Identity family of IAM solutions includes everything you need to move your organization's IAM project up the hierarchy and into success. Whether that project is an enterprise provisioning project, a privileged account management project or a governance project, as discussed in earlier ebooks in this series, or a tactical "pain du jour" project as discussed in this ebook, the Dell One Identity solutions are designed to solve immediate problems while setting you up for future success — even when you don't know what the future holds.

> Dell One Identity solutions are designed to solve immediate problems while setting you up for future success — even when you don't know what the future holds.

Specifically for these access management needs, Dell One Identity offers:

- **Cloud Access Manager** — This web access management solution provides SSO across the widest range of applications and authentication types, from modern federation to legacy methods. It also offers just-in-time provisioning for the most popular SaaS applications, social authentication and secure remote access without a VPN. In addition, Cloud Access Manager includes Dell's Security Analytics Engine, which delivers a context-based, adaptive security model that takes into account the dynamic factors that affect security (such as time, location, device and history) to provide exactly the right access control every time.
- **Password Manager** — This self-service password reset solution eliminates the need for users to call the help desk every time they forget their passwords. Password Manager seamlessly integrates across the Dell One Identity family and is the ideal complement to any governance or access control project.
- **Defender** — Dell One Identity's multi-factor authentication solution is a standards-based one-time password (OTP) product that uses Active Directory and existing AD authorizations to drive multi-factor requirements. It supports any standards-based token, including those from Dell or other vendors, and integrates out-of-the-box with Dell One Identity Manager, Cloud Access Manager, ActiveRoles Server, Enterprise Single Sign-on and a range of privileged account management solutions.
- **Privileged Access Suite for Unix** — This Dell One Identity AD bridge solution extends Active Directory, and any AD-based IAM solution, to Unix, Linux and Mac systems. This includes single sign-on, provisioning and password management as well as privileged account management of those non-Windows systems.
- **ActiveRoles Server** — Dell's industry-leading AD management and security solution overcomes the shortcomings of native tools with automation, integration, and years of experience delivering superior management of the AD and extended AD environment. It supports not only the most complex AD topologies but also Exchange, Lync, Office 365 and anything joined to AD through Privileged Access Suite for Unix. In addition, ActiveRoles Server provides granular delegation of the AD Admin account to kick-start security and compliance.

For more information about how these and other Dell One Identity solutions can help you find success in your IAM project — whatever that project may be — please visit software.dell.com/IAM.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.Dell.com
Refer to our Web site for regional and international office information.