Identity and Access Management for the Real World: Access Management

By Todd Peterson
IAM evangelist, Dell Software

DELL Software

Introduction

In an ideal world, we'd have the budget and time we need to get things done. And tomorrow would be predictable. But that's simply not the case, especially in the IT universe.

As you well know, the world of identity and access management (IAM) is one of constant change, shrinking deadlines, minuscule budgets, overtaxed staff and unmerciful regulations. Unfortunately, this historical approach to IAM involves piecing together "half solutions" in hope that tomorrow's solutions will address real world needs.

This short e-book evaluates what IAM for the real world would, should and can look like. It delves into the most pressing IAM issues faced by virtually every organization and offers actionable, affordable and sustainable approaches to the challenges you face. Among the formidable IAM issues and challenges IT departments face today is access management. We'll explore why it's so hard, how it's evolving and what companies are doing to address it. Best of all, you'll discover some valuable insight into what you can do right now to simplify and streamline access management in your organization.

At Dell, we help you achieve your IAM objectives for your real world in a way that enables you and your business to achieve your goals. I hope you find value in "Identity and Access Management for the Real World: Access Management."

Conventions

Throughout this e-book, we've used a number of conventions to help highlight important points, provide supporting evidence, or advise you of our obvious bias. Look for the following conventions:

Real-world example – Stories of real organizations, facing real challenges, and really solving their problems (often the names have been changed to protect the innocent)

Facts & figures – Research-based information that supports principles discussed throughout the e-book

Techie alert – Definitions and terms used in the identity and access management industry that may not be familiar to you (Then again they might.)

Useful tip – Information that will help you easily achieve things discussed throughout the e-book

Blatant sales pitch – Where we get to why we actually wrote this e-book. It may be a little biased, but we suspect that the reason you’re reading this e-book is to find solutions to your challenges. This is where we give them to you.

Westley: "Give us the gate key."

Yellin: "I have no gate key."

Inigo Montoya: "Fezzik, tear his arms off."

Yellin: "Oh, you mean this gate key."

The Princess Bride – 1987

Access Management – After all, if you can't get to your stuff, what's the point?

It's all about access … isn't it? The only reason technology exists is to make people's lives easier. The only reason IT exists is to make people's use of technology easier. And the only reason everything is so difficult these days is that there are outside forces that demand that someone control who can do what with technology.

It could be the threat of a nefarious party from outside of your organization trying to steal data, break systems, or just prove a point. Or it could be insiders stumbling across information that you would rather they not see. Perhaps it's the threat of some pencil-pusher throwing the book at you for some rule you never knew existed. No matter what the scenario, the need to manage access is ubiquitous.

The foundation for everything is access. When access is broken, no amount of security, control, management or governance matters. This e-book will address the foundational concepts of access.

It's a simple equation… Authentication + Authorization = Access. Even though it may be simple, it's much easier said than done.

So why is it all so hard?

The vast majority of organizations spend most of their time on the day-to-day tasks associated with granting access. Their never-ending focus seems to be on making IAM processes as efficient as possible. But, once again, the challenge is complexity and diversity.

You know that with every system, a point of authentication and an account must be set up ("provisioned") for user access, including a password that must be maintained. These tasks usually fall on IT because they have the rights and tools to set up accounts and enforce password security rules, as well as reset passwords, when necessary.

This complexity is well illustrated by data from The Aberdeen Group, who surveyed thousands of companies with an average size of 21,000 employees on the current state of their IAM approach. Results show a tangled web of complexity that traps organizations in the lower tiers of the pyramid.

- **On average, surveyed companies supported 198 applications**. That's potentially 198 places where accounts must be set up and managed, 198 different passwords and password policies, and dozens of IT professionals just to support users on this wide range of applications.

- **On average the typical end user must access 27 different applications.** Even if only half of those require unique passwords, how many of your users can remember 13 different passwords? And who has to help them when they forget?

- **On average it takes 12 hours to provision a new user.** That's a full day and a half where users are being paid, but don't have the access they need to do their jobs. And who is responsible for setting up those accounts? How many IT teams must be involved to "fully" provision a user?

- **On average it takes 4.9 hours to de-provision a user.** That's more than half a day, giving a disgruntled former employee plenty of time to do damage.

For these reasons, IAM has often been considered the realm of "provisioning" and "single sign-on." After all, setting up an account and giving a user only one password should eliminate the need for IT-assisted password resets, at least in theory.

The evolving enterprise

Gone are the days of all users on premises. No longer do average users require access to only a handful of IT-controlled applications. And control over this business-enabling technology is rapidly moving beyond the direct control of the organization and into the realm of third parties, such as outsourced service providers and software-as-a-service (SaaS) vendors. Plus there's the trend of mission-critical data and applications owned and managed by partners or vendors.

Today users can be anywhere and everywhere, and the applications and data they must access can run the gamut from fully within your control to entirely outside of your influence. Simply granting someone appropriate access based on what they need and how they are logging in has now become an endlessly moving target.

But let's not forget what the purpose of technology is in the first place – helping your organization reach its goals. Ultimately IAM exists to help organizations achieve business agility. That means the ability to better achieve objectives such as generating revenue, serving constituents or changing the world through innovation. Agility is dependent on governance – the ability to enforce and know that activities being performed are done according to the rules. And governance cannot be achieved without security.

Access management exists to efficiently execute the tasks that enable users to do their jobs and ultimately enable the business. Unfortunately, every organization, even the most agile, has pockets of difficulty on the access and security fronts that are preventing them from reaching higher levels of control, security and governance.

> It was found that each individual IT-assisted access management activity cost more than $300. When applied to its 250,000 users, the annual expense was staggering

The wide world of access management

These "keeping the lights on" activities – also known as access management – cover the gamut of needs across the full range of systems. These activities must be performed on each and every system for each and every user before any additional value can be realized. This diversity and redundancy stands in the way of efficiency.

For example, why does it take a day and a half to fully provision a user? It's because provisioning is performed individually on each system by specialized IT resources that may be following their usual—yet potentially outmoded—practices. The same holds true for passwords.

A large government agency calculated the complete cost to manage user access across its Windows and Unix/Linux environments. Taking into account labor costs, physical resources, the cost of downtime and other factors, it was found that each individual IT-assisted access management activity cost more than $300. When applied to its 250,000 users, the annual expense was staggering.

Some of the most common access management principles include:

- Provisioning –setting up, lifecycle management, and retiring of the mandatory user accounts that enable access. To many, provisioning is considered the end-all be-all of IAM.
- Password management –processes for establishing and enforcing password policy, including expiration frequency and password complexity, as well as anything done to facilitate changing and resetting passwords. This is a constant headache for help desk techs.
- Single sign-on – creating a single login scenario for users to eliminate multiple passwords. Single sign-on is perhaps the most misunderstood aspect of identity administration.
- Strong authentication – those things done to ensure that user logins are as secure as possible. This may include stronger password policy, encryption technology to protect the password in transit, or adding additional "factors" to more advanced identity verification.

So when you step back and look at what impacts all these common access management principles, you find that each of them is impacted by the:

- Number of systems they must be executed on
- Diversity of those systems
- Amount of manual work typically required of IT
- Number of IT teams that must be involved
- Business importance of the system in question

In other words, as things get more complex and as systems become more incompatible, the more difficult they are to get right… and the more impossible it is to properly address security and achieve governance and business agility.

Provisioning

Account setup, changing, and retiring are significant challenges, particularly with user population growth and the diversity and increase of systems that must be accessed. Manual processes demand dedicated IT staff for each system. Workflows are often based on how they have done things in the past. Provisioned rights are rarely anything more secure than "give Joe the same access that Jane has," even though there is no guarantee that Jane even has the correct access in the first place. It's a burden for IT, a productivity killer for end users, and an auditor's compliance-violation poster child.

> Single sign-on is the next most visible area of identity and access management. But single sign-on (SSO) is many things and no one definition covers all use cases and all available technologies.

"Traditional" IAM frameworks aren't much better. While they are designed to automate provisioning enterprise-wide, by their very nature, they require everything custom-built. Account definitions, authorization roles, business logic, workflow, and approvals all must be customized for each and every system. Consequently if and when the framework is finally up-and-running, requirements have changed and the customization starts over.

A large investment firm recently chose to go the IAM framework route for provisioning. The customized solution required a team of nearly two-dozen Java developers working full time to build the required provisioning capabilities. After more than 18 months (imagine the cost of this team of highly paid full-time professionals) the company has succeeded in automating provisioning for only one system and has been unable to automate de-provisioning on that same system. The hundreds of other applications within the scope of the project remain untouched.

Obviously, a real-world approach to provisioning would navigate the complexity of even the largest and most diverse enterprise. It would be rapid to deploy and nimble enough to quickly adjust to changing requirements. And it would remove the shortcomings of relying on IT for everything by automated process and putting control in the right hands. Dell One Identity Manager solution delivers provisioning that satisfies all of those demands.

Single sign-on

Single sign-on is the next most visible area of identity and access management. But single sign-on (SSO) is many things and no one definition covers all use cases and all available technologies. Essentially, SSO means reducing the number of logins required to access multiple, diverse applications. There are many technologies and several common strategies that can all legitimately claim the title of SSO, namely:

- True SSO – authentication to multiple systems with a single login and a single credential shared by those systems and generated upon that login. True SSO is what Microsoft has created for Windows systems with Active Directory (AD) and is commonly offered by AD bridge technologies for non-Windows systems that leverage the AD credential.

- Enterprise SSO (or form-fill SSO) – technologies that store diverse passwords and automatically enter them when a login action is undertaken. These types of solutions typically cover the widest range of systems, however, they are inferior from a security standpoint to true SSO.

- Password synchronization (or same sign-on) – technologies that make sure that all passwords across multiple systems are the same. Password synchronization still requires individual logins for each system, however, it ensures that the user only has to remember one password, albeit entered each time access is required.

- Federated SSO – solutions for access that cross organizational boundaries. Federation solutions trust the user identity and rights that originate from outside of the requesting organization—such as between a vendor and supplier or between partnering companies. Federation scenarios require an identity provider

(IDP) or the party supplying the identity and a service provider (SP), or the party granting the access.

- Web SSO – single sign-on to web applications on the Internet or on premise, accessed via a browser either on premises or remotely.

Every environment is different, but it is safe to assume that no environment is adequately served by a single SSO solution type. In fact, even within specific types of SSO, different applications can have different requirements. For example some web applications use a standard called SAML to provide authentication, while others leverage Microsoft's WS Federation. Still others use proprietary means of authentication and can only be served with a form-fill SSO solution.

Consequently, a real-world approach to SSO will provide the best SSO option for each and every affected application. This may mean AD-based true SSO for Unix and Linux systems and SAP, password synchronization for a mainframe, a combined and broad web SSO and federation solution for web applications, and an enterprise SSO solution for the rest.

Password management

If we didn't have a need for secure and controlled authentication, none of the challenges of IAM would exist. But we need security and we need the assurance that the person logging on is the approved user. In other words, at a minimum, we need passwords. And someone has to manage those passwords.

Nothing kills productivity or needlessly diverts IT resources better than a forgotten password. Each password reset costs every organization a different amount, but odds are it isn't the best use of IT's time or talents. Conservative estimates place the cost of a single IT-assisted password reset in the neighborhood of $25. In a large organization with tens of thousands of users each with a dozen or more passwords, the tab can grow quickly.

Single sign-on is one approach to alleviate the password burden. Another, complimentary approach is to remove the resetting of passwords from IT and place it in the hands of the end users. IAM for the real world adds self-service password resets and granular password policy to provisioning and single sign-on, as well as to governance capabilities. Dell One Identity can help your organization do SSO the right way with a complete range of SSO options and adjacent technologies that offer benefits achieved through streamlined logons.

Strong authentication

The natural next step is to strengthen authentication beyond the native capabilities of individual systems or in excess of the typical username and password login. Many organizations choose to introduce additional levels of authentication assurance for specific users, such as contractors. They may also choose stronger authentication for highly sensitive needs, such as for privileged access or for regulated transactions. Access can also be requested in scenarios outside of IT's direct control, such as for remote and mobile users.

The agency reported a savings of more than $40 million in the first year of this unified and automated identity administration approach.

Strong authentication can take the form of extending a more secure authentication method, such as Active Directory's Kerberos authentication, to systems with less secure methods, such as Unix and Linux systems. It can also be adding a second factor to usernames and passwords. A real-world approach to IAM will make strengthening authentication simple, affordable and easy to manage without sacrificing security.

What if you could get to one identity?

The government agency discussed earlier faced the challenges of provisioning, single sign-on and password management that result from extreme complexity and diversity. Account management, password resets and group management were difficult for its Active Directory environment, which only required one identity per user. Those essential tasks were nearly impossible for its Unix and Linux systems, which required a distinct identity for each user on every server.

By placing a bet on Active Directory, the agency fully automated account and group management, dramatically relieving IT of a previously obtrusive workload. It also moved password resets away from IT by enabling end users to reset their own forgotten passwords. Finally, the agency removed the need for Unix and Linux systems to have their own identity stores, opting instead to link them to the single AD identity through an Active Directory bridge. That meant that the account management activities performed through automated tools on AD would automatically affect access to Unix and Linux systems. Active Directory groups could now be used to control that access, and a user self-service password reset performed on the AD identity would grant seamless access to Unix and Linux.

The agency reported a savings of more than $40 million in the first year of this unified and automated identity administration approach.

The benefits of this unified approach to access management are fairly obvious. The fewer identities there are to administer, and the better you are able to administer them, the higher your IT organization can move up the hierarchy pyramid. So how can you achieve this when complexity is the rule and you may already have tools, or even an IAM framework, in place?

I've seen many organizations similar to the example above that have faced those exact same challenges. Without fail, the key to successful access management has been to follow a few basic principles:

- **Automate what matters most**. In most organizations, the largest and most important identity store to administer efficiently is Active Directory. Typically, every user has an AD account. AD groups are used to control access to important Windows resources, such as Exchange. And the AD password is the one users remember because they use it every day. But managing AD can be difficult without help. Tools exist to help you manage AD users and groups efficiently and securely.

- **Enable users to help themselves.** Simply implementing an AD-based self-service password reset solution can dramatically improve operational efficiency. At an estimated $25 per IT-assisted reset, the return on investment of a self-service solution is rapid and significant.

- **Extend AD.** If AD has challenges, Unix, Linux and Mac OS X systems have them in spades. By their very nature, Unix-based systems do not share a common identity store like AD. Consequently every server has a distinct identity for every user. That means many passwords to remember and generally, only highly paid Unix IT staff are able to reset forgotten passwords. Active Directory bridge technologies remove the identity burden from Unix, Linux and Mac, and allow them to participate as a "full citizen" in AD, much like a Windows resource. So the administrative activity performed through an AD-optimized tool automatically takes care of account creation and termination, group enrollment, and identity lifecycle management needs required for Unix access. And a self-service password reset in AD automatically restores access to the Unix system.

- **Start with SSO where it will have the biggest impact.** Single sign-on can make a significant difference, particularly where user satisfaction and IT efficiency are concerned. However, universal SSO can be difficult to achieve. Choose the systems and access scenarios that are causing the most inefficiency and biggest security risk and implement SSO starting there. Often SSO for web applications, remote users, and federated scenarios will yield significant and immediate positive results.

- **When in doubt, use strong authentication.** For those users and access scenarios that concern you the most, consider adding a two-factor authentication solution. But be cautious and choose a solution that doesn't add to the IT workload and doesn't require additional complexity to increase security.

This approach firmly supports the modular and integrated strategy that is so critical to IAM success. An AD-optimized administration solution can be implemented stand-alone, as can a self-service password reset solution or an AD bridge. However when combined, the benefits are amplified. None rely on a proprietary "framework" for success. In fact, dozens of organizations with established IAM frameworks have seen an accelerated return on investment. They optimize access management for AD and extend it to many non-Windows systems, eliminating the need for cumbersome custom integration and inferior management of access to AD, Unix, Linux and Mac.

Dell One Identity

The Dell One Identity set of solutions is a comprehensive collection of modular and integrated tools to address your real-world access management needs, regardless of where you currently stand with IAM. Dell enjoys deep expertise in Active Directory, and we pioneered the Active Directory bridge space. Dell IAM solutions can help your organization move up the pyramid to security, control, management and, ultimately, governance – all with the endgame of enabling business agility.

> Dozens of organizations with established IAM frameworks have seen an accelerated return on investment. They optimize access management for AD and extend it to many non-Windows systems.

For access management, the Dell One Identity family includes:

- **Optimized Active Directory security and management** – Active Roles is the industry leader in AD administration that includes account management, group management, security and many other IT-enabling capabilities that overcome the native weaknesses of AD.

- **Active Directory bridge** – The Privileged Access Suite for Unix includes the most robust and long-standing AD bridge on the market. It removes the need to administer identity on a box-by-box basis for Unix, Linux and Mac OS X systems.

Plus, it enables advanced security and manageability features only available through AD.

- **Single sign-on** – Dell One Identity has the industry's most complete set of single sign-on options. This includes Cloud Access Manager, a unified SSO solution for access to web applications on premises and remotely, regardless of application or authentication needs, such as federations and SaaS. Dell One Identity also includes solutions for true SSO, password synchronization and enterprise SSO.

- **Multifactor authentication** – Dell One Identity includes Defender, a one-time password solution that builds on existing AD infrastructure for an easily implemented and managed alternative to passwords only.

- **Virtual directory services** – Dell One Identity overcomes the challenges of incompatibility and complexity presented by multiple disparate identity stores. This is done through a virtual directory server that removes the burden of integration from the directory itself, and facilitates rapid and thorough integration and migration.

Would you like more information on access management solutions within the Dell One Identity family? Try a free online demo, download a 30-day trial, or visit us at software.dell.com/solutions/identity-and-access-management/.

Identity and Access Management for the Real World

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

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.Dell.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.

iam.askanexpert@software.dell.com