WHITE PAPER

Securely Managing Your UNIX Environment

Written by Jason Fehrenbach,
One Identity senior product manager

Abstract

UNIX systems face special identity and access management (IAM) challenges. This white paper details those challenges and explains how they can be overcome with the right practices and the right tools, enabling you to enhance security, achieve compliance, and dramatically improve operational efficiency.

Introduction

UNIX, its rebellious brother Linux, and its hipster cousin Mac OS X, are all foundational technologies at the vast majority of medium-sized and larger organizations. I'll simply use the term "UNIX" from this point on to encompass the full range of UNIX-based systems (including Linux and Apple Macintosh). UNIX was here before Windows and will be around for the long haul. Due to its stability, cost-effectiveness, and openness, UNIX (in all its flavors) continues to grow, and its legion of fans steadfastly hold to its virtues.

But as with any technology, the real-world implications of its adoption present challenges to those organizations that choose to embrace UNIX. Twenty-first-century realities demand heightened security of technology beyond practices that were common only 20 years ago. Today's UNIX-based organization must account for a more stringent compliance environment, more sophisticated and varied threats, and the demand of interoperability with the full range of non-UNIX systems—with Microsoft Windows being at the front of the line.

ONE IDENTITY

This white paper discusses the common challenges facing UNIX-based organizations and some easily implemented practices and technologies that can help increase security, achieve compliance, and dramatically improve operational efficiency.

The Four A's

In order to be of use, a system—UNIX included—must be used. And in order for a system to be used, it must be accessed. Appropriate access to systems demands following the core tenets of identity and access management (IAM). These tenets can be summarized in four A's:

- Authentication—Verifying the identity of the person requesting access
- Authorization—Providing the appropriate level of access to the authenticated person
- Administration—The tasks and activities associated with maintaining the lifecycle of the user identity
- Audit—The activities performed to satisfy compliance demands that authentication, authorization, and administration all occur according to established rules and best practices

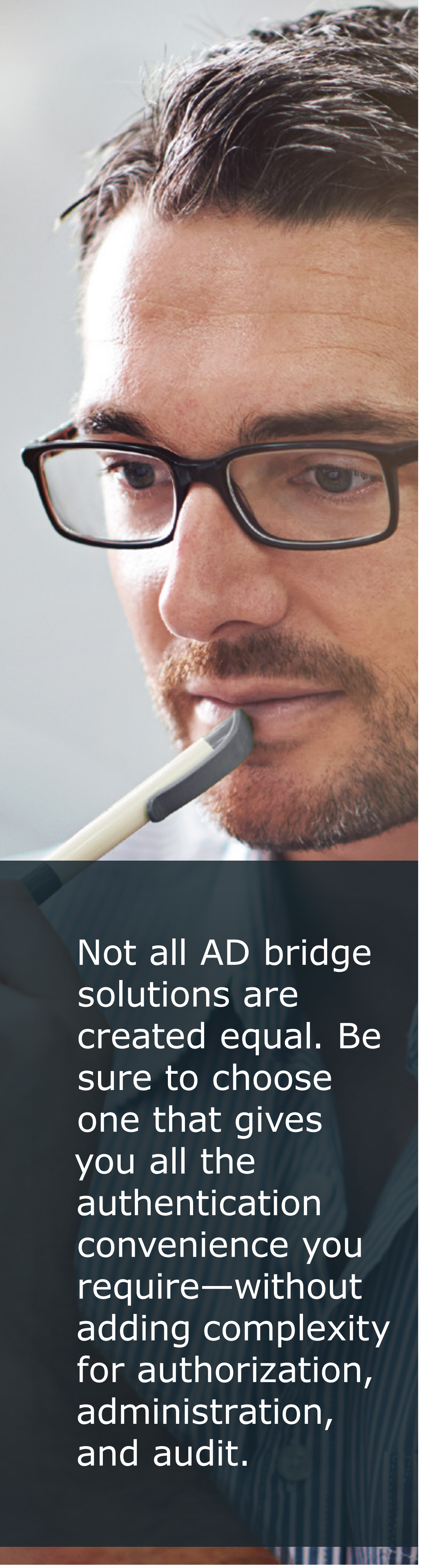
Each UNIX system includes a directory that houses a collection of user accounts (or identities) that are referenced when access requests are made. Consequently access is granted or denied based on the parameters of the identity in the directory and the rights associated with it. Among the administrative activities required to maintain this identity some of the most common are: provisioning (setting up the account), de-provisioning (terminating the account), and managing passwords (initial setup, periodic changes, and enforcement of security rules such as length and complexity requirements).

The trouble with UNIX

As is painfully obvious to anyone with a sizeable UNIX installation, IAM for UNIX systems is difficult with native capabilities. Normally, each UNIX system is an island unto itself, with its own directory and its own stand-alone authentication, authorization, and administration requirements. When an audit is required, the identical task must be performed individually on each and every UNIX box.

A government agency researched the hard costs associated with identity administration across its UNIX environment and the nearly 250,000 users that access those systems. The agency estimated that more than $45 million was spent annually on the provisioning and de-provisioning of UNIX accounts and on routine administrative tasks such as password resets. Similar results have been reported in UNIX-centric enterprises across the entire range of industries, from finance to technology, from

One government agency reports spending more than $45 million annually on the provisioning and de-provisioning of UNIX accounts and on routine administrative tasks such as password resets.



Not all AD bridge solutions are created equal. Be sure to choose one that gives you all the authentication convenience you require—without adding complexity for authorization, administration, and audit.

energy to education, and from manufacturing to retail.

The reason for the high costs? Simply put, it's expensive to perform the same action, again and again, across systems that are not sharing the same basic identity infrastructure. Managing identities and access for multiple UNIX systems is complex and inefficient because each system is unconnected and each is a disjointed island unto itself. Let's examine the specific issues with each of the four A's for UNIX.

Authentication in UNIX

No native single sign-on burdens users with multiple accounts and passwords

For organizations with multiple UNIX systems, authentication is a box-by- box process. Each user must have an account on each system he or she needs to access. There is no easy way to ensure that the accounts are the same. Due to the errors that creep in over time, inconsistency of the timing of deployment, and the fact that practices and support staff change over time, a single physical user may be represented by dozens (or even hundreds or thousands) of separate accounts that bear no connection with each other. The user names may be different, the user IDs (UIDs) may be different, and the passwords will most certainly be different, expiring at different times and possibly requiring different security policy.

In other words, natively UNIX does not provide any sort of single sign- on environment for users. Users who must access multiple UNIX systems are required to remember many passwords and must spend large amounts of time simply logging in and out of each system. Early efforts to consolidate logins and identities in UNIX (such as NIS), unfortunately, do not live up to modern security and compliance standards. For example, NIS sends passwords over the wire in clear text, an obvious violation of virtually every compliance regulation.

Administrators have to provision each account separately

UNIX accounts present issues for administrators as well as end users. Natively, it is not possible to provision all UNIX accounts for a user in one action. The account must be set up individually (even if it represents the same person) on each box. That's not much of a problem with one, two, or even 10 UNIX boxes and a handful of users. But what about when the UNIX install stretches into the hundreds or thousands and the number of users grows as well?

Active Directory bridge solutions extend authentication and administration to UNIX

Since the early part of the 21st century, technologies have existed that overcome the shortcomings of both native UNIX authentication and NIS. Active Directory (AD) bridge solutions extend the authentication security, manageability, and single sign-on capabilities of Microsoft Active Directory—and specifically its enterprise-class implementation of the Kerberos and LDAP protocols—to UNIX, Linux, and Mac OS X systems. With an AD bridge solution, a single logon to AD can authenticate and grant access to the entire range of UNIX systems that have "joined" the AD trusted realm. And a single account in AD is all that must be provisioned, managed, and terminated.

Be sure to choose your AD bridge solution carefully, so as not to complicate other A's

However not all AD bridge solutions are created equal. If authentication were the only concern, any solution would do. But the implications of joining a UNIX system to AD extend beyond simply authentication to authorization, administration, and audit. The right AD bridge solution for your environment would be the one that gives you all the authentication convenience you require, without adding complexity for authorization, administration, and audit. In other words, the more transparent your AD bridge is, the better off you are.

Authentication Services is the most mature, and most robust AD bridge on the market. It pioneered the AD bridge market and has been providing unified authentication for UNIX-based systems since 2004. Multiple deployments of Authentication Services exceed 100,000 users and tens of thousands of servers. In fact, the top 10 largest Active Directory bridge deployments all use Authentication Services (with one deployment nearing 100,000 servers). For a discussion of the important issues to consider when selecting an AD bridge solution see the One Identity white paper "Choosing the Right Active Directory Bridge Solution."

Authorization for UNIX

Similar to authentication, each UNIX system requires its own authorization. The challenges of box-by-box authorization can be overcome by using an AD bridge. Basing authorization rights on AD group membership overcomes the administrative, security, and compliance challenges of natively building and enforcing authorization individually on each UNIX-based server.

It's important to choose an AD bridge solution that enables AD-based authorization without introducing additional complexities and more layers of management or infrastructure. Authentication Services provides the most seamless integration between AD and UNIX and leverages familiar and established AD administrative practices and interfaces.

Identity administration for UNIX

Provisioning is time-consuming for administrators

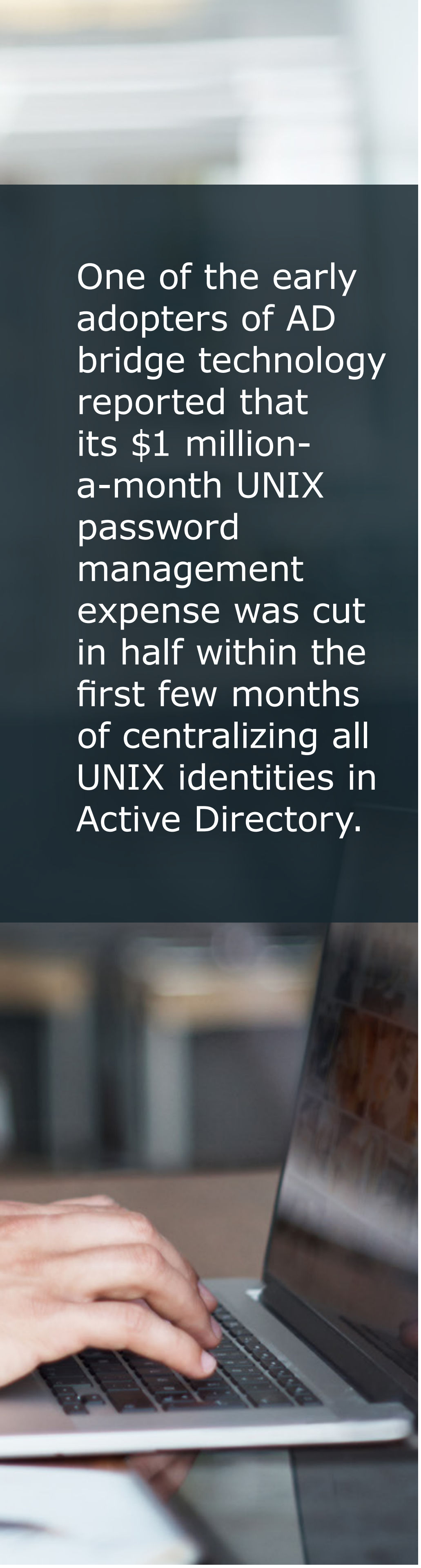
Neither authentication nor authorization for UNIX systems can adequately occur if identity administration is not under control. Again, the challenge with UNIX is the fact that identity must exist on every box. Therefore, provisioning user accounts for a new employee could involve manually setting up accounts on dozens, hundreds, or even thousands of UNIX servers. It is nearly impossible to maintain consistency of username and UID. And the negative impact on productivity can be crippling, as all the provisioning work on UNIX systems typically must be performed by administrators whose primary jobs are not user support.

Manual de-provisioning processes entail significant risks

As troublesome as provisioning is, de- provisioning is downright dangerous. Delays in terminating access to UNIX systems present compliance violations, at best, and an open door to malicious activity, at worst. The highly publicized breach at Fannie Mae was a direct result of delays in terminating access to UNIX systems. With the high number of servers involved, the manual nature of UNIX identity administration, and the lack of centralized oversight available natively in UNIX, it's a miracle that we haven't had more Fannie Mae's.

Password management is a drain on users and administrators alike

Finally, there's the issue of passwords. Every box requires an account, which means every box requires a password. Again, the administrative tasks associated with managing those passwords—enforcing complexity rules, requiring periodic changes, and resetting forgotten passwords—are an incredible drain on operational efficiency.



One of the early adopters of AD bridge technology reported that its $1 million-a-month UNIX password management expense was cut in half within the first few months of centralizing all UNIX identities in Active Directory.

Unifying identities across the enterprise with Authentication Services yields significant savings

The earlier example of the government agency spending more than $45 million annually on provisioning-related tasks, while quite impressive, is not uncommon. One of the early adopters of AD bridge technology reported that its $1 million- a-month UNIX password management expense was cut in half within the first few months of centralizing all UNIX identities in Active Directory.

Through Authentication Services, this major bank entirely eliminated user accounts across all of its UNIX systems (thousands of them) in favor of a single AD account that controlled all access. The result was one account to provision, one account to de-provision, and one password for each user to remember. These capabilities are only enhanced as additional identity administration tools—such as Active Roles for AD identity administration and Password Manager for self-service password resets, both from One Identity—are seamlessly integrated with Authentication Services to fully encompass the UNIX environment.

Authentication Services provides the most complete and flexible integration of UNIX with AD, which results in less administrative overhead, no negative impact on the performance of AD, and the most pristine UNIX identity environment available—which can then easily be extended into additional areas of identity and access management, such as automated provisioning, access governance, multifactor authentication, change tracking and audit, and privileged account management.

Audit for UNIX

Compliance and security demand increasing levels of visibility into the access rights of individuals and the activities they perform with those rights. The common theme of UNIX as disjointed islands applies to audit as well: natively, it is nearly impossible to adequately audit a large UNIX environment. But auditing Active Directory is simpler due to the preponderance of tools available. Simply pulling UNIX identity, authentication, authorization, and administration into AD means that an audit of AD will reveal much of what is needed—but not all. There are unique needs in UNIX (such as reports on access to root) that an AD audit simply doesn't cover.

AD bridge solutions include built-in reporting tools. Unfortunately most limit reporting to the AD bridge itself, and do not cover the entire AD-enabled UNIX environment. Authentication Services includes comprehensive audit that goes beyond the solution itself to also include all aspects of UNIX identity including audit, alerting, and change tracking of all UNIX-centric information managed via AD.

The special case of root

The power of the root account, and the challenges of managing that power

A unique challenge facing UNIX organizations is the question of how to manage privileged (or superuser) accounts. UNIX systems have a single, all-powerful administrative account called root. The root account is required for any administrative activity, from a simple password reset to the ability to install software (or malware), so the account's all-powerful password is often shared across multiple administrators. There is no individual accountability tied to anyone's use of root, no native ability to watch what people do with root, and no way to delegate only the appropriate root capabilities for the job at hand.

It's a fact: at most organizations, administrators share privileged accounts

In a recent survey of users of various IAM solutions, nearly half the respondents reported having more than 100 privileged accounts (including multiple root accounts) in their organization, and more than half of those respondents report that those accounts are used by more than 10 administrators. In addition, two thirds of the respondents report sharing the administrative password (including the root password) among more than three administrators.

Sudo helps with the challenges of privileged accounts, but it has limitations

The open source community has stepped up to address the challenges of root in UNIX environments with a project called sudo. Sudo stands for "superuser do" and provides the ability to delegate portions of root to specific administrators based on their role, mitigating the dangers of root's all-or-nothing legacy. Sudo ships with virtually every distribution of Linux and with most commercial UNIX installs. If you have UNIX, it's safe to assume that you have sudo and are probably using it to help with privileged account management.

However, sudo has some specific native constraints surrounding its use:

- Sudo must be installed and managed individually on each UNIX server.
- The policy file that controls the delegation of root permissions also exists independently on each UNIX server.
- Sudo does not provide the ability to generate reports on the rights it controls.
- Sudo does not provide the ability to audit activity performed though it.

In a survey of 100 users of sudo, only one-quarter report that sudo is good enough for all of their root

Privilege Manager for Sudo is an ideal alternative for the majority of servers at UNIX organizations, while providing unified management and a single pane of glass view for both AD bridge (Authentication Services) and high-requirement root delegation (Privilege Manager for UNIX).

account delegation needs. That leaves 75 percent with needs beyond what sudo can cover. When asked what challenges they face with sudo, 16 percent felt it was difficult to manage, 17 percent felt that maintaining consistency of sudo policy across all affected servers was troublesome, and 16 percent felt that sudo was lacking in its ability to satisfy the need for information required by compliance and security audits.

Root delegations tools that replace sudo

Because of sudo's limitation, Active Directory bridge vendors offer root delegation tools meant to replace sudo. However, a deeper dive into the data reveals that, at most organizations, sudo is good enough for a majority of UNIX servers, although they wish it was more convenient and offered greater visibility. Only a small portion of their servers require delegation capabilities more advanced than those available through sudo—the capabilities touted by AD bridge vendors as available add-ons to basic AD bridge functionality.

Yet most AD bridge vendors address only the needs of that small portion of servers, offering only a sudo replacement. Only One Identity addresses both needs, providing a replacement for sudo for those situations and servers where that is the preferred option, as well as enhancements to sudo that overcome each of the constraints discussed earlier. And unlike some other solution sets, the One Identity option does not require an AD bridge to achieve root account authorization.

One Identity offers a complete solution for UNIX IAM

One Identity solutions for UNIX IAM comprises three tools:

- **Authentication Services**—One Identity's AD bridge solution
- **Privilege Manager for UNIX**—A sudo replacement for high-requirement rootdelegation
- **Privilege Manager for Sudo**—A tool that empowers organizations to maintain their sudo installation while overcoming the native constraints of sudo

These tools share a powerful management interface and are tightly integrated. Specifically, Privilege Manager for Sudo provides a central policy server for sudo that creates a single point of management for sudo policy files across any number of UNIX servers. That "single source of the truth" for sudo can leverage the power of AD identity and groups (via Authentication Services) to influence and normalize the policy. In addition, with all policy centrally managed, the One Identity solution makes it easy to gather and report on the rights associated with administrators, sudo policy, and who is able to do what on which servers—a major boon to compliance and security efforts. Finally, Privilege Manager for Sudo delivers keystroke logging to provide an audit trail of precisely what individual administrators do with the rights they have been granted via sudo.

At a fraction of the cost of traditional sudo replacements from other vendors, Privilege Manager for Sudo is an ideal alternative for the majority of servers at UNIX organizations, while providing unified management and a single pane of glass view for both AD bridge (Authentication Services) and high- requirement root delegation (Privilege Manager for UNIX).

Conclusion

The many and varied challenges of identity and access management for UNIX systems are generally based on the disjointed nature of UNIX and the repetitive, inconsistent, and cumbersome requirements of managing authentication, authorization, and identity administration on a box-by-box basis. Active Directory bridge solutions overcome these challenges, but not all AD bridge solutions are created equally. Authentication Services from One Identity provides the most robust, flexible, powerful, and extensible alternative for those organizations looking to extend the IAM power of AD to UNIX, Linux, and Mac OS X systems.

For More Information

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software 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 Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE 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 QUEST SOFTWARE 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 QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software 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. Quest Software does not make any commitment to update the information contained in this document.

About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

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

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (**www.quest.com**) for regional and international office information.

ONE IDENTITY™