Managing Heterogenous Environments With Delinea's Enhanced Identity-Centric PAM Solution

Seema Kalwani

seemakalwani@gmail.com
Independent contributor, IL, USA

Abstract
This paper introduces delinea's Centrify product, the benefits it offers to bridge Microsoft Active directory (AD) with UNIX servers extending capabilities of AD to UNIX in simple and complex environments. Implementation and auditing aspects of the product are discussed.

Keywords: Centrify, Delinea, UNIX, AD Bridging, PAM

I. INTRODUCTION

Delinea is redefining the legacy approach to Privileged Access Management by delivering multi-cloud-architected Identity-Centric PAM to enable digital transformation at scale. Centrify Identity-Centric PAM establishes trust, and then grants least privilege access just-in-time based on verifying who is requesting access, the context of the request, and the risk of the access environment. Delinea centralizes and orchestrates fragmented identities, improves audit and compliance visibility, and reduces risk, complexity, and costs for the modern, hybrid enterprise. Over half of the Fortune 100, the world's largest financial institutions, intelligence agencies, and critical infrastructure companies, all trust Delinea to stop the leading cause of breaches – privileged credential abuse.

Over the past few years, it has become evident that privileged credentials are the enabling targets that cyber attackers are after, evidenced by Delinea research that shows nearly three-quarters of all data breaches involve access to a privileged account. Concurrently, digital transformation has significantly expanded the IT landscape and increased the number of potential vulnerabilities that can be exploited by threat actors. The increase in cyberattacks and the expanding attack surface that now includes cloud, DevOps, containers, microservices, and more has made securing access to the modern IT estate more challenging than ever.

1) *Centrify Identity Centric PAM Solutions help Organizations:*

- Secure privileged access to an increasingly decentralized modern attack surface
- Reduce risk, complexity, and costs
- Improve audit and compliance visibility
- Protect against compromised credentials, the leading point of attack used in data breaches
- Enable secure remote access for outsourced IT
- Secure data lakes
- Reduce cyber risk exposure from external threat actors
- Minimize exposure to ransomware attacks
- Limit exposure to insider threats

2) Microsoft's Enhanced Security Administrative Environment (ESAE)

Microsoft's Enhanced Security Administrative Environment (ESAE), aka "Red Forest," is a popular security model designed to help minimize the risk of a domain-level breach. It is ideal for companies with large populations of Windows servers but leaves potential holes in heterogeneous IT infrastructure environments. Administrator privileges configured in the Red Forest are not enforced on their Linux and UNIX servers, resulting in a decentralized and fragmented security posture.

To bridge this gap, Delinea has enhanced its Identity-Centric PAM solution to extend privilege elevation configurations in the Red Forest to Linux and Unix. Delinea is the first PAM vendor to support the most common Red Forest administrator use cases by providing identity consolidation and least privilege capabilities to *NIX platforms. For administrators logging into a Linux or UNIX system, Delinea ensures that the user's Red Forest security group memberships are honored, whether logging directly into the server or indirectly via Kerberos Single Sign-On (SSO) from another Windows system.

Many organizations have complex Active Directory infrastructures forged through rapid organic growth or mergers and acquisitions. They have long relied on Delinea's innovations, such as supporting complex one-way, cross-forest trusts. Those who have embraced a Red Forest model benefit from enhanced protection against domain-specific attacks. However, organizations that also have a Linux or Unix estate have not been able to take advantage of this, resulting in a patchwork security posture with access controls managed in multiple places. Delinea extends these benefits to heterogeneous environments, ensuring that Red Forest shadow group membership and related privileges are honored on Linux and Unix servers. With this, IT gains a true centralized PAM solution that reduces risk, improves operational efficiencies, and helps ensure compliance.

II. Core elements of Identity Centric PAM Solution

1) Delinea Authentication Service

- Joins Linux and Unix servers to Active Directory
- Navigates the one-way, cross-forest trust required in Red Forest architectures

2) Delinea Privilege Elevation Service

- Upon login to a domain-joined Windows server, Delinea interrogates the Kerberos login ticket to obtain Red Forest group membership
- Upon direct login to a *NIX server, Delinea honors the Red Forest security group membership and applies the privileges to the administrative session
- During Kerberos-based SSO from a domain-joined Windows server to a *NIX server, Delinea honors the Red Forest security group membership and applies the privileges to the administrative session

III. Active Directory Bridging

At a basic level, Active Directory (AD) bridging enables non-Windows systems to be joined to AD. Doing this allows Active Directory benefits to be extended consistently across Windows, Linux, and UNIX IT systems and network devices.

One key benefit is allowing administrators to log in to non-Windows systems using their dedicated AD login credentials instead of a local privileged account such as root, ec2-user, or ubuntu. As part of an identity consolidation best practice, this helps reduce the attack surface by avoiding the proliferation of multiple local accounts across IT systems and ensures full accountability of privileged activities by preventing the use of these anonymous shared, privileged accounts.

More advanced AD bridging capabilities include supporting complex multi-forest AD architectures and trust models, a hierarchical model for cross-platform role-based access control, deep AD service integrations (e.g., Kerberos, AD-DNS, and AD-CS), extending AD group policy to non-Windows platforms, and Windows smart card login configuration extended to Linux systems.

A. Advantages of Active Directory Bridging

- It's a Privileged Access Management (PAM) capability.
- It enables administrators to log in to Linux machines using their Active Directory account.
- It allows us to leverage Active Directory groups when defining PAM roles.

For an Active Directory shop with *NIX servers, administrators benefit from using their Active Directory credential to log in anywhere and leverage Active Directory Kerberos for single sign-on. With centralized management in Active Directory, you reduce operational overhead, avoid security gaps, and minimize access governance and control inconsistencies. You can also eliminate the many local privileged accounts admins use to log in to *NIX systems, relying instead on a single Active Directory account, thus reducing your attack surface.

AD Bridging helped eliminate the challenges of overlapping identity silos. It allowed non-Windows systems to “join” to AD. AD then saw the computers as part of the Windows domain, allowing them to become AD clients for services such as authentication, authorization, policy management, and directory services.

B. Active Directory Bridging, Authorization, and Accounting

Using authentication to identify the user is not enough. We must then use permissions to control what the user can do and keep tabs on that activity if we need to investigate or prove compliance. These are the Authorization and Accounting portions of the AAA framework; we'll explore these now.

C. Authorization

Managing what users can do on *NIX systems is a combination of native OS controls and "sudo" rights. Native OS controls are limited – read/write/execute permission for users and groups – no fine-grained control.

A regular *NIX user has limited rights, unable to run privileged system commands. The native sudo program enables controlled elevation of permissions, obtaining its instructions from a local /etc/sudoers file you must configure and manage on each system. This model doesn't scale when you have dozens or hundreds of systems (we have customers with thousands). It increases administrative overhead and introduces the risk of toxic combinations, security gaps, over-privileged users, and failed audits.

With AD Bridging, a local client allows you to join *NIX servers to Active Directory, like joining a Windows server to the domain. We eliminate dependence on the local /etc/sudoer files, enabling you to manage policies for privilege elevation ("Authorization") centrally in Active Directory. This centralized management also extends to policies for login ("Authentication") and multi-factor authentication (MFA)—with the client enforcing them locally on each system.

To avoid upsetting your organization's Windows team, you can isolate these *NIX policies from other Windows-centric Active Directory policies and configurations.

D. Accounting

Imagine the scene—there is a potential breach in progress. You must log in to several *NIX systems and trawl through their local log files in a hurry. Much noise contaminates the logs and sifting through thousands of unrelated events is laborious and error-prone. You see lots of privileged activity attributed to "root." But who was logged in as root? There's no accountability. Repeat this for each system, and by the time you find valuable intel, the cyber attacker has left the building—with your data.

AD Bridging supports restrictive, fine-grained policies to align permissions to the task better. Logged privileged activity is distinct, non-cryptic, and easy to analyze through a centralized interface. Enforcing the Principle of Least Privilege, AD Bridging ties activity to a unique Active Directory user for accountability. With session recordings, you can replay privileged activity for any user on any machine in any time range. You can also search across recordings for applications run or commands typed at the keyboard.

IV. ADVANCED ACTIVE DIRECTORY BRIDGING

A. Complex AD architectures

Basic AD Bridging solutions simply don’t possess the smarts to see and navigate all forests, trees, domains, and nested groups. Delinea solved this by building deeper awareness and insight — leveraging the AD Global Catalog, being multi-DC aware, and site topology aware. Support of AD Group nesting in case the user is not a member of a top-level group. For performance and availability, it can find the nearest DC that’s alive or alternatives if it’s not. No stone left unturned.

Basic AD Bridging solves the core authentication challenge but is constrained by simple AD constructs such as Org Units, Containers, and Security Groups when shaping their governance model. You may want to segregate roles and rights and their management along departmental boundaries such as HR, Finance, and Sales and delegate administration to specific admins within those departments. You may prefer geographical or functional segmentation such as North America, EMEA, and APAC or Mid, West, East, and South-Central sales regions. Perhaps you need to segment servers based on regulatory compliance, grouping them into PCI, HIPAA, or GDPR. Or perhaps a mix of models.

B. Separating the Windows from Unix using Zones

AD for Windows servers is hard enough but bringing Linux and UNIX into the fold becomes untenable. Patented Zones technology delivers this capability and more without AD schema modification or installation on DCs. You manage it the console (see image) that is an MMC snap-in just like AD Users and Computers (ADUC). It has the same look and feel and so we’re not changing the way you manage users and computers today. Wherever you place your users and computers in AD we work with that. Only requirement is an additional OU for our own data such as the Zone definitions.

C. Zero Trust

At a basic level, Zones overlay AD’s essentially flat container model with a hierarchical model allowing customers to organize assets how they like, define login roles and rights, specify time- boxes that only permit login during specific time periods, and delegate their management to specific admins. Delinea separates identity from permission. Just because you exist doesn’t mean you have rights. This is core to Zero Trust.

D. *Roles and Rights*

Roles and rights can be defined at the computer or Zone level and common roles can be defined (e.g.) at the root for inheritance to all child Zones.

Zones also provide the foundation for identity consolidation and AD-based login. For an administrator with multiple Linux and UNIX accounts, their UIDs and GIDs can be mapped to a single AD account and those local accounts removed (removing multiple points of attack and reducing administration overhead) allowing the user to log into any managed system with their AD credentials. Using an AD account to log into Linux means we're now deferring to AD for password policy. Auditors love this since it's now consistent, cross-platform, and centrally managed from AD.

E. *Group Policy*

Centralized Windows Group Policy management and automation of computer and user configurations gives IT huge returns. However, Linux and UNIX systems don't have a group policy concept and their computer and user policies require IT to manually configure and manage them per system. Yet another IT overhead that tends not to be prop erly managed and that can open you up to significant risk.

Basic AD Bridging doesn't help. Delinea's solution, however, extends Windows Group Policy to Linux and UNIX. Administrators can use their existing tools and processes to standardize configurations, cross platform. We have identified and defined a set of user and computer configurations specific to Linux and UNIX systems that, like their Windows counterparts, can be centrally managed from the Group Policy Management Console.

V. PROVISIONING ACCESS

A way to ease implementation of provisioning access to the users once the bridging is in place. Usually, organizations divide servers for use based on environment – development, test and production. There may be different teams that work on each environment and different people need access to different environments.

- Creating a computer group and have dev computer part of the computer group
- Creating a role group and have development team members part of the role group
- Mapping of the computer group and role group

This allows all user in the role group to access all computers in the computer group. There can be several applications in an organization, each application can have there our computer groups and role groups to provision access.

A. *Automation*

The process can be automated using ServiceNow or any other tool where user can request access. On the click of the button API can be used to provision user or computer in their groups making access provisioning simple and easy

VI. DECIDING WHETHER TO AUDIT USER ACTIVITY

Just as it is important to protect assets and resources from unauthorized access, it is equally important to track what users who have permission to access those resources are doing or have done in the past. For users who have privileged access to computers and applications with sensitive information, auditing their actions helps ensure accountability and improve regulatory compliance.

There are many reasons for organizations to establish auditing policies and enable auditing of user activity. For example, you might want to audit activity for any of the following reasons:

- To prove certain computers or applications are secure in order to comply with government or industry regulatory requirements.
- To report on actions taken by users with elevated privileges.
- To prevent the use of shared passwords when more than one person needs administrative access to a computer or an application.
- To improve accountability when users with elevated permissions have access to privileged resources.
- To detect suspicious activity and mitigate the threat posed by malicious insiders or third parties who have access to sensitive systems.
- To pinpoint actions that may have caused failures and simplify troubleshooting procedures.
- To capture information, such as the steps that resolved an open case, that can be used to help your organization improve its helpdesk operations or security procedures.

VII. Auditing Architecture and Dataflow

The following figure illustrates the basic architecture and flow of data with a minimum number of auditing components installed.

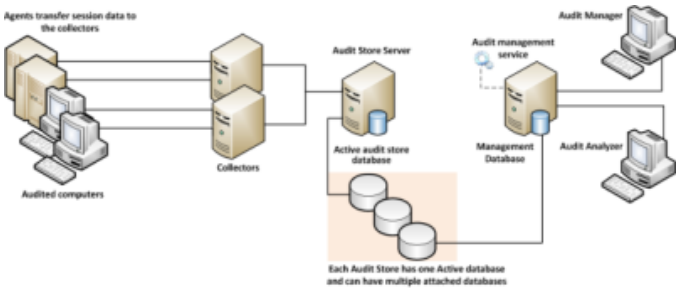

Fig. 1. Aduit infrasturcture taken from Delinea Audit guide

In the illustration, each agent connects to one collector. In a production environment, you can configure agents to allow connections to additional collectors for redundancy and load balancing or to prevent connections between specific agents and collectors. You can also add audit stores and configure which connections are allowed or restricted. The size and complexity of the auditing infrastructure depends on how you want to optimize your network topology, how many computers you are auditing, how much audit data you want to collect and store, and how long you plan to retain audit records.

The following diagram shows how the Linux Desktop auditing session data is collected.

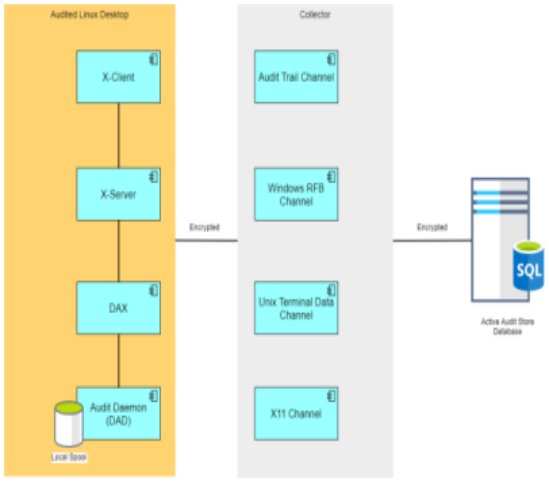

Fig. 2. Linux desktopauditing session date taken from Delinea Audit guide

Within the Linux Desktop, there's a component called DAX that generates the recorded session data and passes it to the audit daemon. The audit daemon encrypts and passes the recorded session data to the collector. The collector channels session data of different types together and passes that encrypted session data along to the active audit store database.

CONCLUSION

Centrify has great features for an organization using heterogenous systems to accomplish AD bridge for non-Microsoft UNIX systems. Allowing /etc/passwd and user file on Unix servers to be slim delegating the authentication services to Active directory. Making management easier from a single repository. Providing audit capabilities to comply with Government/industry regulatory requirements. Detecting suspicious activities and mitigating the threat at the same time making troubleshooting simple.

REFERENCES

[1] Cision PRWEB, https://www.prweb.com/releases/Delinea_Again_Named_a_Leader_in_2020_Gartner_Magic_Quadrant_for_Privileged_Access_Management/prweb17315198.htm, Aug. 10, 2020

[2] Delinea, https://delinea.com/news/Delineas-identity-centric-pam-extends-benefits-microsofts-red, Feb 2020

[3] Delinea, https://delinea.com/blog/ad-bridging (Accessed Dec 2024)

[4] Delinea,https://delinea.com/resources/advanced-ad-bridging-whitepaper, (Accessed Dec 2024)

[5] Delinea,https://docs.delinea.com/online-help/server-suite/install/deployment/provisioning/index.htm, (Accessed Dec 2024)