Privileged Access - Linux/Unix Privileged Access Management and Active Directory

Overview

Privileged Access to Linux servers is currently provisioned to GENPAM accounts, onboarded into CyberArk safes, by way of Delinea in Linux.

At present the Delinea configuration is manual, using the Delinea UI.

Although there is another story looking to leverage SABRE work to fix issues running Delinea PowerShell code via pipeline (works when run manually), the scope of this story (**ECSM-12848** - Getting issue details... STATUS) is to investigate if Delinea is the correct way forward from both an AD Bridging perspective and a PAM/Access provisioning perspective, and if a combination of OS native capabilities and Ansible automation capabilities can meet requirements in terms of controls/governance and speed of delivery.

What Is AD Bridging?

Active Directory bridging **connects non-Windows and cloud services to an AD network**

It serves as an identity consolidation service that permits clients to log in across a hybrid infrastructure of Windows, Linux, and Unix servers using their AD credentials.

It may also be referred to as AD joining.

What is Privileged Access Management?

Privileged access management (PAM) consists of the cybersecurity strategies and technologies for exerting control over the elevated ("privileged") access and permissions for users, accounts, processes, and systems across an IT environment. By right-sizing privileged access controls, PAM helps organizations condense their organization's attack surface, and prevent, or at least mitigate, the damage arising from external attacks, as well as from insider malfeasance or negligence.

While privilege management encompasses many strategies, a central goal is the enforcement of least privilege, defined as the restriction of access rights and permissions for users, accounts, applications, systems, devices (such as IoT) and computing processes to the absolute minimum necessary to perform routine, authorized activities.

Alternatively referred to as privileged account management, privileged identity management (PIM), or just privilege management, PAM is considered by analysts and technologists as one of the most important security projects for reducing cyber risk and achieving high security ROI.

The domain of privilege management falls within the broader scope of identity and access management (IAM) and identity security. Together, PAM and IAM help to provide fined-grained control, visibility, and auditability over all credentials, privileges, and access.

While IAM controls provide authentication of identities to ensure that the right user has the right access as the right time, PAM layers on more granular visibility, control, and auditing over privileged identities and session activities. PAM is at the core of identity security, which analysts and IT leaders consider central to protecting enterprise assets and users in an increasingly perimeter less, work-from-anywhere (WFA) world.

Source: What is Privileged Access Management (PAM)? | BeyondTrust

Current Status

1. Currently, domain join is being done via Delinea (vmbuild script initiates delinea adjoin command on the VM
2. Delinea is also used on some, but not all, Linux and Unix servers to control privileged access - with many also using sudoers file, suusers file and other Linux privileged access concepts.
3. Delinea may be reviewed and may no longer be considered strategic.
4. Red Hat Enterprise Linux (RHEL) now supports AD domain join natively from RHEL 8 onwards

Requirements

1. Use native and vendor supported tooling where possible
2. Use strategic tooling rather than bespoke code where possible
3. Reduce tooling footprint (and so complexity/cost) where possible including reduction in vendors in use.
4. Ensure that privileged access is managed in line with PAM controls:
    a. Use CyberArk where appropriate - session isolation, session recording
    b. Use PIM type functionality where CyberArk isn't possible/practical
    c. Adhere to least-privilege principles and don't over permission access
    d. Adhere to JIT/JEA principles where possible - avoid standing privilege if possible

What's possible?

Domain Join

RHEL Native Domain Join

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/integrating_rhel_systems_directly_with_windows_active_directory/connecting-rhel-systems-directly-to-ad-using-sssd_integrating-rhel-systems-directly-with-active-directory

Forest functional level range: Windows Server 2008 - Windows Server 2016
Domain functional level range: Windows Server 2008 - Windows Server 2016

Direct integration has been tested on the following supported operating systems:

Supported Domain Controller OS Versions:

Windows Server 2022 (RHEL 8.7 and above)
Windows Server 2019
Windows Server 2016
Windows Server 2012 R2

RHEL Pre 8.0 and other Linux/Unix Distributions

Older version of RHEL, and other versions of Linux and Unix based OSes may also have native domain join capability - likely to require modification of Kerberos configuration, SSSD, realmd and other components. Beyond the scope of this paper to explore every possible *nix distribution available.

Other AD Bridging Tools

Other AD bridging tools likely exist from other vendors, whether or not they also include Privileged Access Management capabilities.

However, they are likely to incur cos, plus the effort to learn and switch to it from Delinea - may reduce cost savings enough to make it no longer worthwhile pursuing.

Privileged Access Management

Retain Delinea

It is valid to consider retaining Delinea due to the capabilities it offers over and above AD Bridging.

However, if this were to be the agreed approach, there are opportunities to improve how this is managed and provisioned at present.

Currently, provisioning is being done manually in the Delinea Access Manager GUI app.

There are PowerShell cmdlets available to automate this configuration: Access Control with PowerShell (delinea.com)

This has already been heavily used in the AD Automation scripts developed as part of CTM in 2022: ADAutomation_JSON.ps1 - Repos (azure.com)

However, this currently only works if the script is run interactively as a normal user with the appropriate privileges - it is not currently able to work when that script is run via the AD Automation pipeline: processADAutomation.yml - Repos (azure.com)

This is expected to be addressed through either the rollout of SABRE or through work to use Certificate authentication and CredSSP - to bypass issues with impersonation and privilege elevation due to ADO Agent sandboxing controls.

Identify and migrate to alternative PAM tooling for Linux

Would require a separate research activity to identify competitors to Delinea and compare functionality/carry out a PoC

Use Ansible to provision and configure Linux access

Ansible has modules that can help with this:

FreeIPA - open source tooling for privileged access management - also has Ansible Modules to control it's configuration: Ansible Galaxy

Native OS modules in Ansible:

https://docs.ansible.com/ansible/latest/collections/community/general/keyring_module.html#ansible-collections-community-general-keyring-module

https://docs.ansible.com/ansible/latest/collections/community/general/keyring_info_module.html#ansible-collections-community-general-keyring-info-module

ldap_attrs module – Add or remove multiple LDAP attribute values

ldap_entry module – Add or remove LDAP entries

ldap_passwd module – Set passwords in LDAP

ldap_search module – Search for entries in a LDAP server

pam_limits module – Modify Linux PAM limits

pamd module – Manage PAM Modules

selinux_permissive module – Change permissive domain in SELinux policy

selogin module – Manages Linux user to SELinux user mapping

Coverage, Governance and Compliance

The RHEL solution only covers RHEL 8.0 and above, any strategic approach must work for all versions of *nix OSes to ensure that privileged access is configured, managed and audited in a consistent manner across our entire estate. Even just considering RHEL - most of our RHEL estate in the cloud is in the 7.x stream, and on-prem, may be even older and out of support in the case of some legacy systems.

Although Delinea is used in parts of our estate at present, a review is required to identify suspected gaps - e.g. can privileged access be configured outside of Delinea? It is suspected that the answer to that may be a resounding yes.

Would the SOC detect that and respond/remediate? This is an open question that has been asked of the SOC engineering and operational teams to identify the current *nix monitoring use cases, what events are being ingested into Sentinel etc.

Summary/Recommendation

Category	Description	Pros	Cons
AD Bridging	OS Native Domain Join	Native capability, no additional cost. Can be automated easily with Ansible or other automation tools	Isn't suitable for all versions of RHEL in our estate, far less all *nix OS versions
	Alternative AD Bridging software	Can potentially address coverage e.g. would work for all *nix OS that we use now or in the future	Likely to incur cost for licencing Opportunity cost to retool and migrate from Delinea May not include privileged access management features that Delinea has.

Privileged Access Management	Retain Delinea	Known solution, very effective for AD join and provisioning granular privileged access, following the privilege of Least Principle. Can be automated Effective auditing capabilities (may need to be tuned further)	Requires some further work to allow it to be able to be automated through ADO pipelines. Doesn't stop access being provisioned outside of Delinea using OS native capabilities
	Identify and migrate to alternative PAM tooling for Linux	May maintain feature parity from a PAM perspective but better integrate into ADO pipelines, Ansible etc (e.g. if there is an Ansible module for it) May be more attractively priced than Delinea	Requires funding, effort to undergo an RFP process and POCs plus migration effort, retraining (admins and users alike)

Based on the research conducted and the current state of our estate, the recommendation is to continue with use of Delinea for both AD Bridging and Privileged Access Management.

However, this should also include work to identify governance gaps and remediate - ensure there are adequate controls around OS config changes outside of Delinea (preferably preventative, but as a minimum there needs to be effective detective controls so that if a change is made out-of-band, that SOC/CSIRT will detect it and investigate/remediate).