Nellsoft GmbH, Sihleggstrasse 23, 8832 Wollerau – Switzerland
Tel. +41 44 500 16 50, Fax. +41 44 500 16 51
info@nellsoft.com, http://www.nellsoft.com

Checklist for a great PAM deployment

Author: Lionel Gresse
Date: 1st October 2019

I've been privileged to install and operate Privileged Access Management (PAM) systems for a couple of years. I had the chance to experiment with many types of deployment. With this document, my goal is to share my experience with you. I want you to benefit from these long hours of work and from the right choices but also the mistakes that I and many others made.

I've listed 29 points to consider when planning for a PAM deployment. Today they are all part of my methodology. Like any pilot before take-off, I go through all of them to ensure a safe and successful PAM deployment.

Nellsoft GmbH, Sihleggstrasse 23, 8832 Wollerau – Switzerland
Tel. +41 44 500 16 50, Fax. +41 44 500 16 51
info@nellsoft.com, http://www.nellsoft.com

Table of content

Nellsoft GmbH, Sihleggstrasse 23, 8832 Wollerau – Switzerland
Tel. +41 44 500 16 50, Fax. +41 44 500 16 51
info@nellsoft.com, http://www.nellsoft.com

1. PAM or PAM: Privileged Account Management vs. Privileged Access Management

When choosing a PAM product, be aware that many vendors mean a different thing with PAM. Some vendors say Privileged Account Management, and others mean Privileged Access Management. In the first case, you'll have a product with strong capabilities in credential management and storage features. In the second one, you'll get a product with more features on the connection side, like client connectivity filtering or session recording.
This difference is historical. 10 years ago, those two sets of products were different market segments. But as technology matured, new features were added, and the two market segments merged.

2. Different users require different access to the account data

At first sight, accessing an account is a black and white issue: someone can use it or not. However, it is subtler than this, and this is where a PAM can help.
An external consultant, for instance, needs to connect with a specific account but doesn't need to see the password or be able to connect his laptops' local drive to the server. A server manager needs to manage password rotation. Different populations have different needs on the same data they can access.
When deploying a PAM, you'll need to think about the various actions your IT population has on the credentials. Doing this analysis before choosing a product
is a best-practice because not every PAM product has the same features. You'll better understand your needs, and you will sort out the nice-to-haves from the musts.

3. Accessing unprotected privileged accounts' password is easy

There is a discrepancy between how PAM deployment is prioritized and how often intrusions target privileged accounts. It is surprisingly easy to get access to privileged accounts in a large organization. There are too many of them, and they remain active due to a lack of oversight and poor management. Sooner or later, they end up in a spreadsheet on a shared folder. Internal search engines such as SharePoint will index them and make them easy to find. At this point, it is game over. The intruder goes to the corporate SharePoint website, enters the right keyword such as "administrator" or "root", and he gets privileged access on critical IT resources.

4. How to define your access matrix

The access matrix describes who access which credentials and what they can do on them. You will need to answer those questions to create it:

- What are the systems whose privileged accounts are in scope? Network infrastructure? Operating Systems? Directory accounts? SaaS application accounts?
- Who is using them: external users that are visiting only a few days per year? External users that stay onsite for a significant period like 3 to 6 months? Business users? Internal system administrator?
- Is the privileged account generic by nature or should the generic privileged account be replaced by a personal one?

- Is password rotation needed, and how does it influence the accounts? Should new accounts be created to optimize password rotation?
- Who is going to create, revoke, and maintain account access?
- How should the account be organized to simplify the use of the PAM?
- Do you want to record the session of your administrators?
- Which account requires permission from its owner before being shared?

5. Pricing models are very different between vendors

Choosing a PAM product is not limited to selecting the best technical features. Any organization has a budget, and CISO and CIO must make the best of their limited resources. Unfortunately for them, vendors have different pricing models. Some vendors charge per feature, others charge per user, and some per server. Some have a traditional perpetual licensing model, others use a subscription model, and some offer both.
Depending on an organization structure, I've seen differences by a factor of 2 to 3 for the same product between 2 clients.
My advice is, therefore, to always ask for a quotation from all the vendors you are considering. The financial side of the equation might surprise you.

6. As the vault containing all keys, you must harden your PAM

Securing the PAM should not be overlooked. Over time, it will hold all the logical keys of an organization. Stealing its content or making it unavailable will be damageable, and I can already imagine the headlines in the press about an organization whose PAM has been compromised.
You should consider this platform as critical for your organization. If you look into a cloud offering as well, make sure that your cloud vendor is as good in system and cloud management than it is in software development. Read the fine print of your contract and ask for audit results to make sure that you won't have a bad surprise down the road.

7. Deploying a PAM means changing work habits in the IT department

Implementing a PAM is a change management challenge. No matter how user-friendly a PAM is, it will change the way your system administrators work forever. This aspect is sometimes the most challenging part of a PAM deployment, especially in global organizations.
My general advice here is to look for quick wins and productivity enhancements wherever it is possible.
Let me illustrate this with an example. Some PAM products offer discovery features to find service account across all systems. Building the inventory of all privileged accounts is often mandatory for compliance but is almost impossible to do manually. Using the discovery feature of a PAM solves the issue within a few hours and provides a quick win.

8. Business users should be using a PAM

System administrators are traditionally typical PAM users. However, the same needs related to critical accounts exist within other departments and with external business partners. They use vital applications for the organization: ERP, payroll management software, social networks

account, email management tools. They deal with many external providers: communication consultants, web designers, marketing partners. Shake both, and you have a sure disaster coming, for instance, if a Mailchimp account is misused.

9. Recording connections for accountability

Recording sessions adds accountability. It is often easier than implementing sound log management across all systems. Most recordings can be indexed for easy retrieval. You have only one system to configure, namely the PAM, instead of a dozen ones from various vendors and technology.

10. External users will use your PAM

Since a PAM is highly critical from a security point of view, it is tempting to install it deep into the LAN to protect it from the outside world. Unfortunately, external consultants and users are typical users of a PAM. So you'll need to think about Internet access to your PAM and how you secure it. This use case will come sooner or later.

11. Rotating password: only possible through automation

A security best practice is to change passwords regularly, including privileged ones. A manual process is realistic for user passwords because each user has only one password to rotate. Privileged accounts are very different. Many system administrators use dozens of accounts. Changing them manually every 30 days is not realistic.

The only way to solve this challenge is to implement an automatic process where the PAM rotate passwords and updates all items using them, such as services, scripts, or scheduled tasks. There are already many products that can do it, and the challenge is not technological. In my experience, the problem is to change the perception of password rotation and this technology.

12. Rotating all administrative passwords can be tricky

Let's face it: some administrative passwords are difficult to change. Some are used in scripts or by running services. Some are local accounts in a SaaS solution or an appliance with almost no API. But there are a couple of strategies to solve this.

One is to use centralized directories so that the PAM can rotate the password on a widely supported platform such as an Active Directory or an LDAP one, instead of on a proprietary appliance.

A second strategy is to link an account with all the resources using it so that the PAM can update them. For instance, some products are able to update scripts, database records, or Windows services when they rotate a password.

13. Managing the inventory of privileged accounts

Delegating the management of privileged accounts to the persons who are most knowledgeable about them is the best practice. In large organizations, it is typically team leaders who best know who should access what. They also know first-hand, which external users will need access.

In my experience, large scale deployments have decentralized privileged accounts management. The security team role is then limited to maintaining the PAM and setting up the automated processes for privileged accounts such as password rotation, or session recording.

14. PAM also applies to business users

I see more and more organizations using a PAM to solve the issue of privileged business accounts. Some business accounts have the same requirements as technical ones because they have identical security risks. For instance, someone can obtain substantial financial rewards by gaining access to an HR system. The same is possible with ERPs or accounting systems.
Using a PAM solution will provide the same benefits in this sphere:

- Secure storage of credentials
- Automated password rotations
- Session recording for accountability
- Workflow to provide access to a privileged account
- Inventory management of privileged accounts

15. Monitor access to privileged accounts

Monitoring access to privileged accounts provides accountability. Root accounts and generic domain accounts are untraceable. It is impossible to know who did what at a given time, even with the best log management system in place. Putting a PAM in place will help solve this issue since the PAM will trace who uses which account at a given time. Some products even have the concept of locked usage: during a specific period, only one user has access to the privileged account. All actions done with a generic account become traceable instantly.
However, monitoring access to privilege account has a second less known benefit. It is a deterrent against misuse. Human beings avoid mischief if they know that their actions will be audited and recorded, and if they know that they won't be able to deny it. There is an Italian saying that describes it best: L'occasione fa il ladro, which means the opportunity makes a thief. Remove the opportunity, and there is no thief.

16. Recording administrative sessions requires storage and resources

I often hear CISO and CIO saying that they want to record all sessions and keep it for at least one year. But a lack of resource planning usually makes it impossible. They are often surprised that recording hours and hours of videos needs storage and CPU time for compression.
If such an idea interests you, plan at least a few terabytes if you want to store video sessions for one year for a dozen system administrators.

17. Providing

on-demand access
On-demand access is, in my opinion, a crucial use case for PAM because it automates access management and ensures accountability. Yet, it is a simple use case to build in a PAM

compared to password rotation or session recording. If I compare this to building manual processes for on-demand access to privileged accounts, it is a no-brainer.

18. Encrypted password storage is a must, but do you manage it correctly?

Encrypting passwords during storage has been a common practice for more than 20 years. However, cryptographic best practices often lack. Most IT managers assume that cryptographic algorithms are robust and never challenge them. Master keys are not secured and never rotated. Very few IT managers even know what an HSM is.
If you implement a PAM, you need to make sure that your critical passwords are stored securely. I recommend rotating the encryption keys regularly. I also recommend using an HSM to store them.
What is an HSM? HSM means Hardware Security Module. This piece of hardware is either embedded within a PCI card or either runs as a dedicated hardware appliance. It generates and stores encryption keys and limits their access through an API or a set of remote commands. Traditionally, a program reads a key in a file and encrypt data. With an HSM, the same program will pass the unencrypted data to the HSM, which will return it encrypted.
I can only recommend using an HSM to secure the storage of credentials in a PAM.

19. Using a PAM to have two factors authentication on privilege accounts

Implementing two factors authentication (2FA) for privileged accounts is a best practice and is even mandatory for compliance with security standards such as PCI-DSS. It is, however, a challenge because it requires the 2FA solution to integrate with all the systems that system administrators work with. In the real world, there are always exceptions, incompatibilities, products requiring an upgrade or a costly additional module to purchase.
A PAM is an excellent way to add 2FA to privileged accounts authentication. It works by putting the 2FA authentication on the PAM. System administrators then connect transparently to the resources they have access to. Most PAM solutions provide it as a standard feature, and it requires no configuration change on target systems.

20. Should you place your PAM in the cloud?

In 2019, most vendors offer their applications in the cloud, and PAM solutions are no exception. Cloud-based PAMs create no maintenance work. They are faster to deploy, at least in the initial phase. They can be scaled up and down to follow business requirements. On the downside, cloud-based PAMs rely on network availability and bandwidth performance. They create a financial lock-in with the vendor because migrating to another solution is more complicated. The migration must be completed before the payment anniversary of the subscription. It is impossible to stop paying maintenance before the new solution is in place.
My recommendation is that the PAM architecture should match the infrastructure it protects. If the data center is already in the cloud, a cloud-based PAM makes sense. If your organization has issues maintaining and securing over time such a critical system, you should also consider a cloud-based PAM. But I would not recommend it for IT infrastructure where all the data

sources are on-premise, or for PAM that must be available even in a situation where no network is available for some time.
If your goal is to save money, let's be clear: cloud-based PAMs are not cheaper. Clients may change their PAMs more often than usually thought. Many advanced PAM features are resource-intensive: account discovery scans, password rotation, and above all session recording. Vendors are well aware that and have implemented exit barriers or aggressive amortization. Subscriptions often require a three years commitment. They amortized hardware resources over short periods, and licenses' costs are identical.

21. Where should you position your PAM?

You should place your PAM system where its users can access it best and as a gateway if it is used to enforce privileged access. You have two questions to ask yourself:

- Do you want to use your PAM to proxy your privileged access? If this is the case, the PAM must be in a DMZ. You will then allow only access from this DMZ to your systems. You may also choose to position it in your cloud if this is where you run your servers.
- Which users will use it? If you have external users, you'll need to put the PAM either in a DMZ or in a location accessible through your remote VPN solution. If you have only internal users, you may place it in your management LAN. You may also choose a private or public cloud if your internal users are globally scattered.

22. PAM and PCI certification

A PAM makes it easier to achieve PCI certification. In my experience, it is one of the best solutions to solve the following points:

- Chapter 2.1
- Chapter 7.1
- Chapter 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7

In a nutshell, a PAM will solve many issues related to default password removal, password rotation, 2FA, and password management. For PCI-DSS certification, my experience is that many products fulfill all the requirements in their basic offering and do not require the most expensive licenses.

23. You will need a high availability solution

This question bodes down to whether you can afford not to have the PAM up and running for a few days or not. PAMs are like all IT systems. They need maintenance, upgrade, and sometimes have issues. Even if they are usually very reliable, they may be down for a few hours or a few days.
What happens during that time? Can your system administrator sit idle during that time? Of course not. Therefore, you'll need a process to backup your credentials in clear text with secure physical storage and to provide this data when required. This process is similar to the management of backup tapes or critical business archives.
It is critical to plan and test this process early in the deployment of a PAM. It cannot be an after-thought.

24. Virtual or physical infrastructure?

Most of the PAM vendors propose both hardware and virtual appliances or offer software solutions that support virtual infrastructure. In my experience, virtual machines are cheaper, even free with some vendors.
PAMs can be resource-intensive. The workload they handle in some use cases can surprise most of the newcomers. Whether a virtual or physical infrastructure is the best approach is still an open discussion. Some of my clients have great performances with virtual appliances; some favored to stay with hardware ones.

25. Don’t forget the backup and recovery strategy

This advice is generic to any IT systems, but it also applies to PAM. Backups offer protection against configuration errors, hardware failure, and unexpected issues. Even if it is not a main corporate asset, the right practice is to regularly back up the PAM and apply best practices: review the back up once a year, keep them in a trustworthy location, and develop a straightforward recovery process.
All these pieces of advice are standard backup practices. However, not all IT departments apply it to their PAM. When trouble occurs, they have to reinstall the system from scratch, and the significant downtime they experience is avoidable.

26. Be aware of the time you'll spend on it

PAM solutions differ in their ease of use. Different architectures and designs create more or less ambiguous detection and manual clarification. The primary cause of manual troubleshooting with a PAM is an issue in the communication with the end server and the integration with the local client. They are 99% of all my support tickets. With the wrong setup and processes, they can keep the IT security team busy for hours and create frustrated users.

27. Don’t forget the out-of-band management of physical appliances

PAMs are sometimes in a remote datacenter or in a cloud environment. Out-of-band access is needed to have reliable access when network connectivity is lost. It should not be overlooked, especially in PAM deployment, which enforces remote access.

28. Don’t forget to give visibility to management

Management needs to understand why they invest in IT. They are accountable just like anyone in the organization. Though information needs can vary from one organization to another as the PAM use cases differ, your management typically needs the following monthly KPIs (Key Performance Indicator).

- Security
    - Number of privileged accounts per platform and total
    - Number of systems per shared privileged account
    - Time to deactivate terminated system administrators
    - Time to determine what IT systems a departed administrator accessed before leaving
    - Separation of duty violations

- Productivity
    - Number of password changes per month
    - Number of emergency admin access per month
    - Average number of distinct accounts per user
    - Number of new accounts provisioned per month
    - Average time it takes to provision or de-provision a user
    - Number of privileged accounts without an owner
- Cost savings
    - Person days to change passwords on all privileged accounts
    - Annual cost for production migrations because developers cannot be granted temporary access.

29. Monitor for performance and availability

PAMs, like all IT systems, have limited resources. Performance issues lead to erratic behaviors and even random blocking of a legitimate connection. Unfortunately, the monitoring of security systems is not a priority and not a widespread practice. Basic monitoring such as free memory, CPU usage, or disk activity is often not done, and the lack of resources is seldom detected.

I experienced it first hand with some of my clients. I, therefore, recommend implementing performance monitoring on a PAM solution.