cyberelements

Deploying PAM in compliance with AD tiering principles

Introduction

At almost 25 years old, Microsoft's Active Directory has become more mature and is still popular among the majority of IT departments. Its role is **crucial within an information system** because it is often the one that is responsible with all the identification and authentication services of an organization.

It is therefore essential to reinforce its protection, especially in the current context where cyber threats are constantly increasing. Taking control of an organization's Active Directory is like taking control of its data, and it is easy to imagine what a malicious person could do with it. A "Golden Ticket" attack, for example, would allow a cybercriminal equipped with a tool such as Mimikatz, to extract the password hash of an authenticated administration account in order to obtain access to all the objects in an Active Directory domain, and therefore to all the servers and domain controllers. In its guide “Secure system administration”, the NCSC (National Cyber Security Centre) presents the design principles for IT and OT systems to help you develop and implement your own system management strategy to protect your most sensitive data. In this guide, the NCSC explains that the directory or directories containing administration accounts must be protected in terms of confidentiality and integrity and must not be exposed on less trusted environments.

The NCSC also specifies that in case of a managed information system (IS) based on a Microsoft Active Directory, it is recommended to **first adopt a privileged account management model** (three-tier model) for this directory and to **secure its configuration**. This recommendation also states that additional technical measures restricting the use of administration accounts on workstations should be implemented.

It is therefore essential that all these measures and recommendations be applied during administration in critical environments.

Privileged account management (PAM) solutions will therefore have to interface with these Active Directory protection contexts, without reducing the expected level of security.

In this document, we describe the aspects of Active Directory tiering and we present how to easily implement a PAM solution such as Cleanroom to provide optimal coverage in terms of security.

1

Active Directory Tiering

The principle

Partitioning

Since Active Directory 2012 R2, Microsoft offers a **multi-level administration model that allows the partitioning of authentication secrets**.

In the three-tier model recommended by the NCSC, a tiering will allow to reference a set of resources according to their criticality and to assign to each tier, dedicated administration accounts to protect authentication secrets.

In fact, the different layers of the information system infrastructure are partitioned on three administration levels to ensure that, in the event of a cyber-attack, a corrupted workstation does not corrupt the infrastructure servers and the Active Directory domain controllers storing the authentication secrets. The goal is to limit the lateral movement of an attacker between the different third parties.

Description of the tiers:

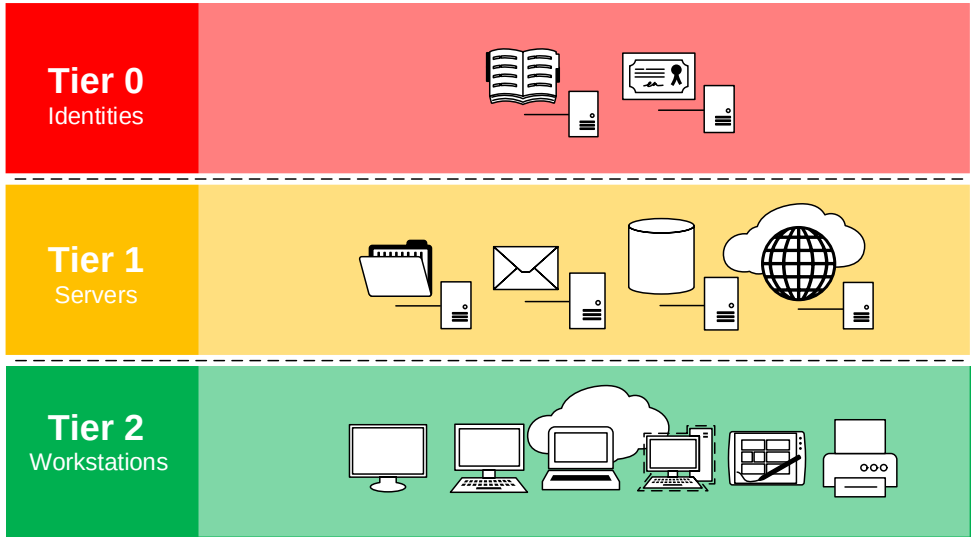
- **Tier 0** (Identities): it integrates the servers holding the identities and the authentication secrets of the organization.
- **Tier 1** (Servers): it integrates the servers that do not hold the identities.
- **Tier 2** (Workstations): it integrates the client workstations, office automation, etc...

Tier 0 is the most sensitive level of this model because compromising the directory, for example, would implicitly compromise the elements of the other tiers. If the Active Directory goes down, the whole organization goes down. Tier 1 is certainly the most important level because it generally contains all the organization's data. Tier 2 is the most vulnerable.

Partitioning

This multi-level model allows the separation of the administration roles of tier 2 "workstations", tier 1 "servers" and tier 0 "identities". **This implies the creation of one or more administration accounts in each tier. Since these accounts will be different in each tier, an administrator who needs to access the resources of all three tiers will need to have at least three different administration accounts.**

The NCSC recommends that administration accounts are exclusively reserved for administration actions.



The administrator of an organization will therefore have to use at least four accounts if he wants to access both his business applications and the resources of the three tiers:

- The account tiers0_adm to manage the resources of tier 0.
- The account tiers1_adm to manage the resources of tier 1.
- The account tiers2_adm to manage the resources of tier 2.
- His personal account to connect to his business applications.

Authentication protocols

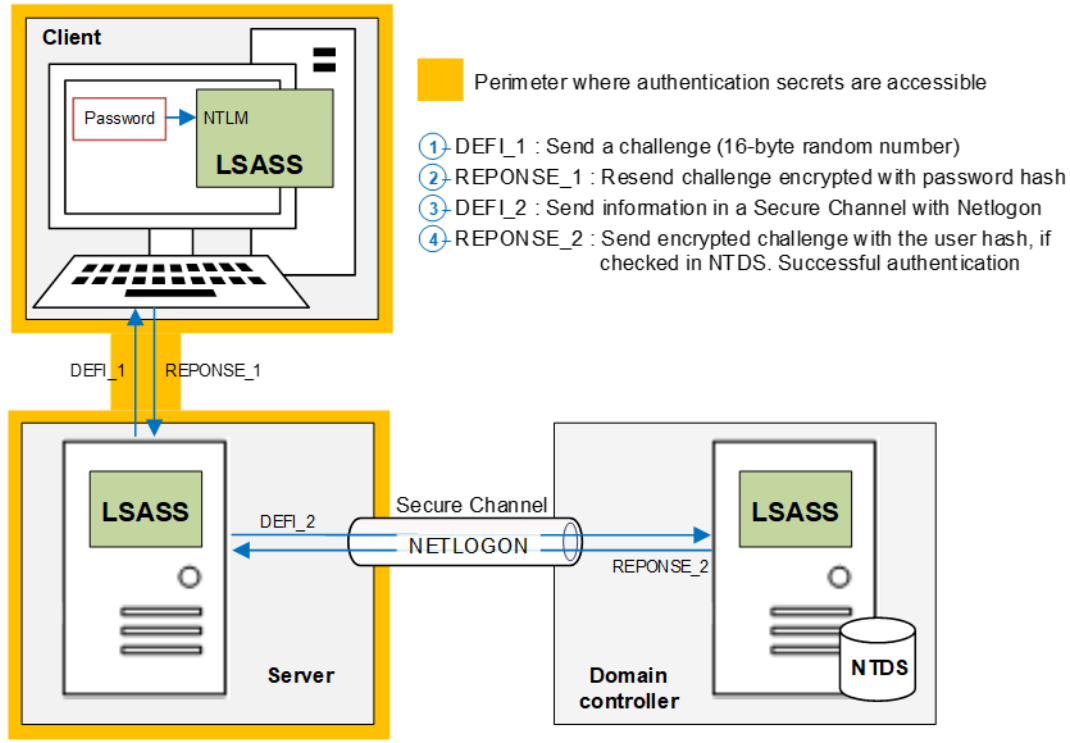
The protection of authentication secrets has therefore become one of the priorities for the security of administration accounts. In an Active Directory environment, they will circulate in different forms depending on the authentication protocol used. They can be in the form of passwords, Kerberos keys, NTLM fingerprints, encrypted blocks or challenge/response pairs.

The authentication protocols proposed by Microsoft in Windows are NTLM and Kerberos. The choice of the protocol model will therefore be crucial to maximize the protection of authentication secrets against corruption attempts by malicious persons.

The NTLM protocol

NTLM is the historical authentication protocol of Windows, and many applications still use it today. Even if the Kerberos protocol should be preferred in Active Directory domains, NTLM in its second version, coupled with a complex password policy, is still tolerated, but very limited for privileged accounts.

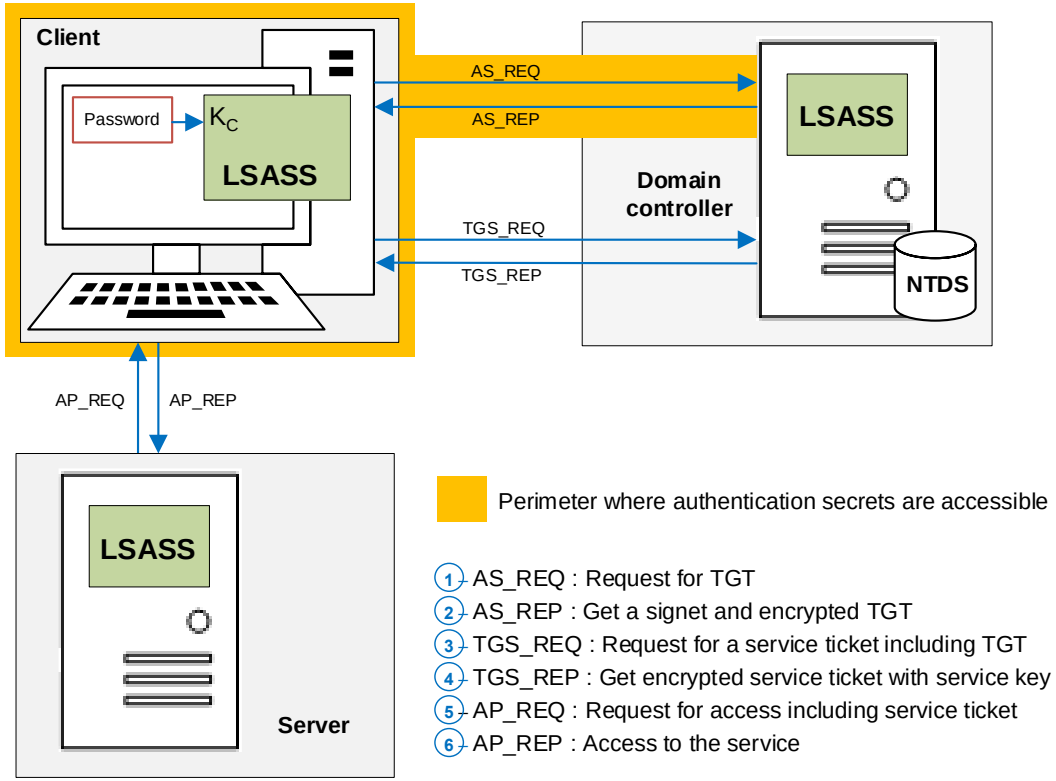
The figure below presents a synoptic of NTLM authentication. It highlights the perimeter where authentication secrets are accessible. It does not protect them very well because it impacts both the client computer, the remote resource server and the challenge/response exchanges between the computer and the remote server.



The Kerberos protocol

Kerberos is an authentication protocol based on a secret key mechanism (symmetric cryptography) and the use of tickets. It is the default authentication protocol used by Microsoft Windows because it radically improves the protection of authentication secrets compared to the NTLM protocol. In fact, the target resource server is not concerned by the authentication information.

The figure below shows a synopsis of Kerberos authentication. It highlights the perimeter where authentication secrets are accessible. We can see that it protects them better than the NTLM authentication because it only impacts the client workstation and the AS (Authentication Service) exchanges.



Securing authentication

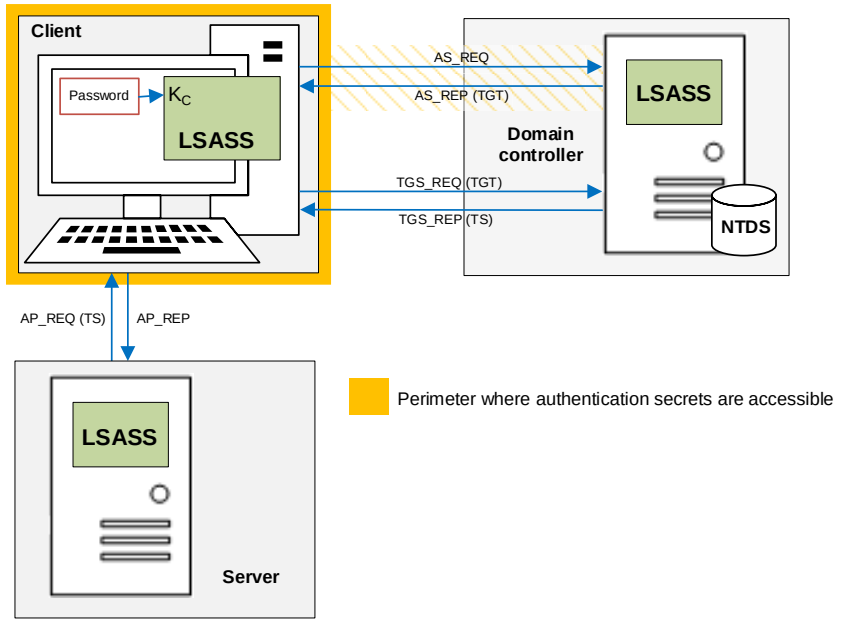
Authentication and the choice of protocol play a key role in protecting the information system. In Active Directory administration environments, Microsoft recommends strengthening authentication security as follows:

- ❑ NTLM side: Prohibit the use of NTLM.
- ❑ Kerberos side:
  - Harden AS exchange protection.
  - Forbid Kerberos delegation.
  - Dedicate Privileged Access Workstation (PAW) to administration accounts.

Kerberos shielding

The "AS-REQ" exchange between the workstation and the domain controller is certainly the Achilles heel of Kerberos. It is possible to secure it by adding to the user's authentication request the computer account information. Indeed, since Windows Server 2012, Microsoft has strengthened Kerberos authentication. This is relected in the integration of the FAST (Flexible Authentication via Secure Tunneling) protocol. It reinforces protection at the level of AS (Authentication Service) exchanges and uses the TGT of the workstation associated with the session key. This is known as Kerberos shielding.

The figure opposite shows a synoptic diagram of authentication with Kerberos shielding. The perimeter where authentication secrets are accessible is better protected than that of Kerberos authentication, since it impacts the client workstation and AS exchanges are more secure.



Securing authentication

The "Protected Users" security group

The "Protected Users" security group, which appeared with Windows Server 2012 R2, changes the way authentication is performed by, among other things, addressing the following two security requirements for authentication: Prohibit Kerberos delegation and prohibit the use of NTLM. All administrators assigned to this group benefit from these restrictions.

The authentication silo

The role of the authentication silo allows to dedicate the PAW workstation of a third-party (that we will see next) to the administration accounts of the same third-party. This assignment is done through an authentication policy. In this way, an administrator will only be able to connect to the resources of a third-party with the administration accounts and the PAW associated with this same third-party through an authentication policy.

Recommendations

It is therefore recommended to apply the protections listed below in the context of administration with AD tiering:

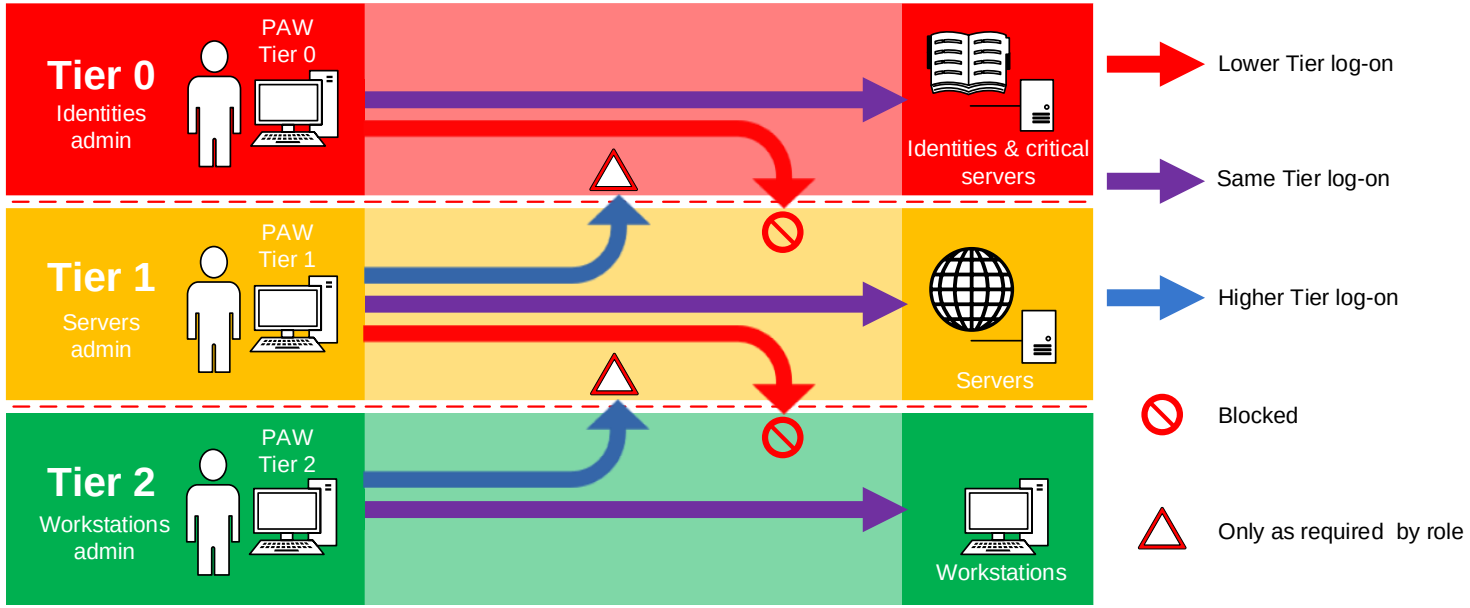
- ❑ NTLM: Prohibit the use of NTLM → Using the "Protected Users" group.
- ❑ Kerberos:
  - Harden the protection of AS exchanges → Using Kerberos shielding.
  - Prohibit Kerberos delegation → Using the "Protected Users" group.
  - Dedicate PAWs to administration accounts → Configuration of authentication silos.

The PAW workstation

To administer the resources of a tier in a multi-tiered Active Directory model, the administrator must log in with an admin account for the tier and from a workstation that is also in that same tier.

All workstations are in tier 2, which is a major problem if the administrator needs to access resources from tiers 0 and 1.

To remove this restriction, secure physical workstations dedicated to administration are implemented in each of the tiers. To limit their exposure, these workstations, called **PAW** (**P**rivileged **A**ccess **W**orkstation), cannot exchange with instances external to the tier where they are implemented. In any case, it will be necessary to manage incoming and outgoing network connections very carefully if the need arises. These PAW administration workstations must not have access to the Internet, must block USB device connections, etc...



cyberelements

The PAW workstation

The NCSC specifies that an essential security measure is to dedicate a physical workstation to administration actions. This administration workstation must be distinct from the workstation that allows access to conventional resources accessible on the organization's IS (business resources, internal messaging, document management, Internet, etc.).

Privileged Access Workstations (PAW) meet this recommendation because they are solely dedicated to administration purposes. Their security is reinforced, and they are used exclusively to access critical resources to perform administration tasks.

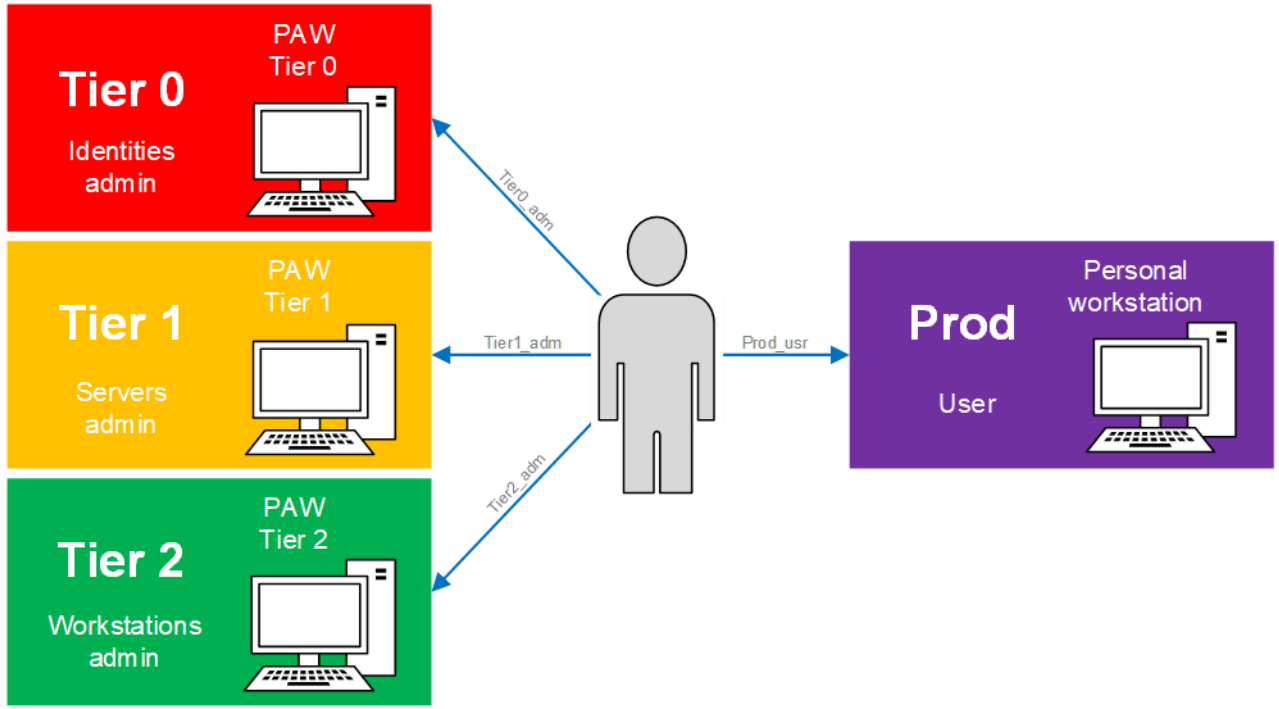
The security of the PAW administration accounts must also be strengthened. This can be done via free tools such as Microsoft LAPS, which manages the complexity and rotation of local administrator accounts on the PAW workstation. However, LAPS is limited on the number of accounts it can manage, so it will be necessary to use third-party solutions such as PAM, which will at a minimum manage the complexity and rotation of administrator accounts, but with an unlimited number of accounts.

The PAW workstation

The three-tier administration model requires a multiplication of accounts but especially of workstations to perform administration tasks.

As explained above, an administrator will potentially need:

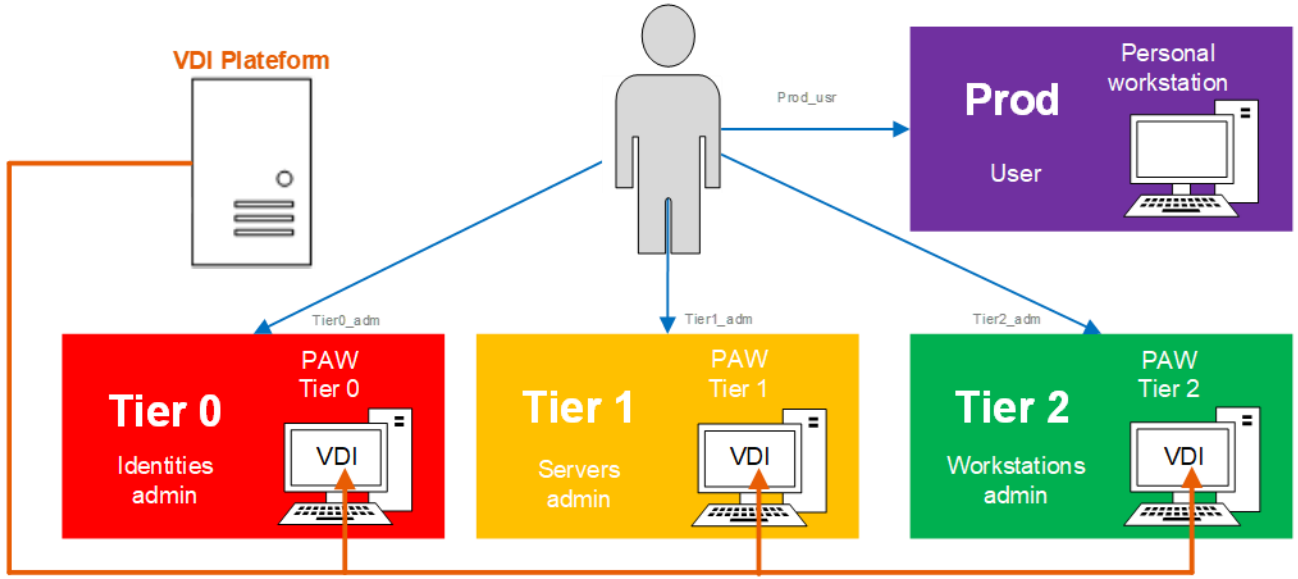
- Four physical workstations: 3 PAWs and 1 user workstation.
- Four Active Directory accounts: 3 administration workstations and 1 user workstation.



The PAW workstation

This three-tier administration model is rather restrictive from an operational point of view, but also from an economic point of view, as the hardware costs added to the operating costs of the PAW workstations are quite high. VDI technologies can be implemented to facilitate the deployment of PAW workstations and optimize their MCS (**M**aintain in **S**afe **C**onditions). Just like physical workstations, virtual PAW workstations provide key capabilities to satisfy certain recommendations made by the NCSC in its "Secure system administration" guide.

- The hardening of the administration workstation OS.
- The possibility to have automatic and regular updates.
- The security to prohibit incoming connections.
- Restriction of administration rights on the administration workstation.
- Management of administrator rights according to the rule of least privilege.
- Limitation of the software installed on the administration workstation.



cyberelements

2

cyberelements

cyberelements is the only SaaS Zero Trust platform that secures access of standard or privileged users to their business applications and critical resources. cyberelements combines, within a single, unified experience, all the elements that organizations need to secure employee access to their IT and OT systems: identity management (IAM), access management (AM), remote access (ZTNA) and privileged access (PAM).

Deployable in a few minutes, cyberelements is designed to meet the most stringent security requirements, thanks to its intrinsic Zero Trust features: double barrier, protocol break, random and volatile network ports, connection tunnel with your own key, connection to the resource only at the time of use, outgoing flow and no port opening.

3

Integration of cyberelements in a tiered context

The various elements that have just been discussed highlight the good practices to be applied in an administration context with an Active Directory environment.

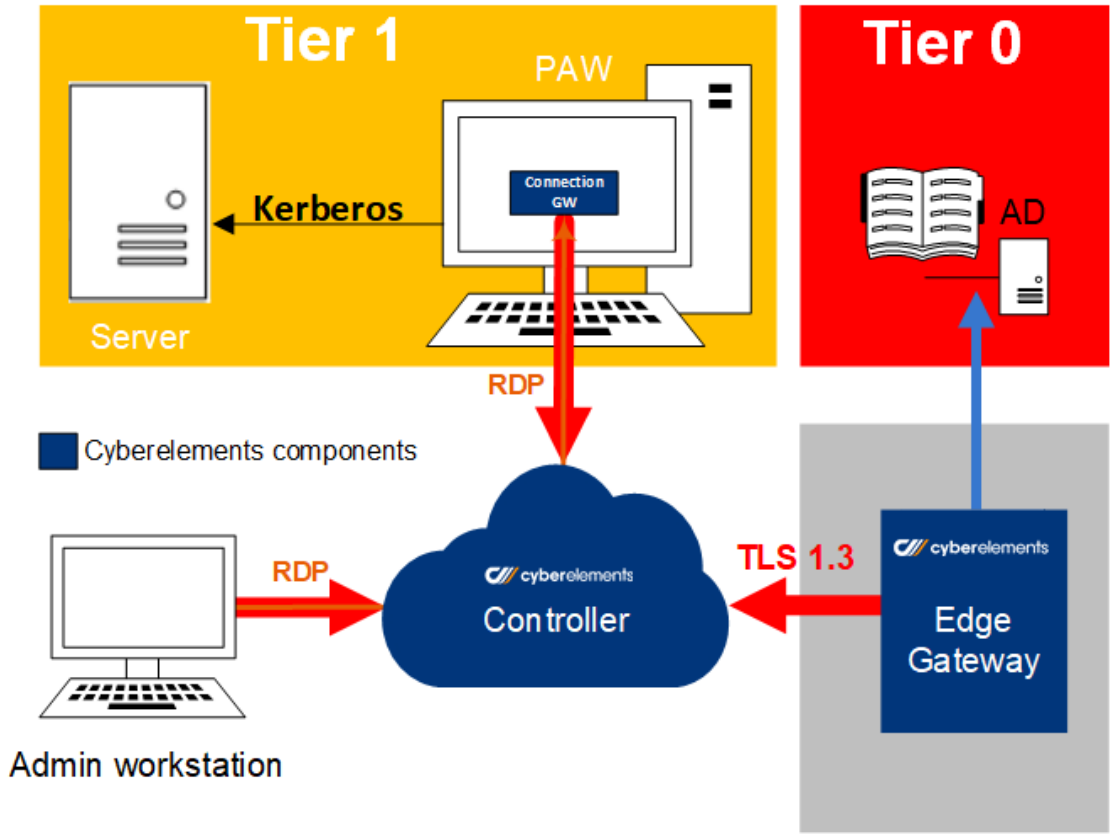
The administration operations must be performed in a three-tier model which allows to separate the resources according to their criticality. Each tier must have at least one administration account and a PAW workstation to administer the resources referenced in that tier. The network exchanges between the PAW station and the various infrastructure elements must be done with the Kerberos authentication protocol with shielding.

The principle

In order to meet all the prerequisites for AD tiering, cyberelements interfaces between the administrator's workstation and the PAW workstation.

A cyberelements component will be implemented on the PAW workstation:

- **Edge Gateway**: It is a software gateway that initiates a secure TLS1.3 tunnel in outgoing flow to cyberelements. No incoming flow is possible on the PAW workstation.



cyberelements

The principle

The administrator's connection to the PAW workstation is made via the RDP protocol. The connection flow is fully encapsulated in the TLS 1.3 tunnel from the Edge Gateway, and **no inbound flow is required to the PAW workstation** for maximum security.

Authentication on the PAW workstation is performed using the shielded Kerberos protocol. The authentication token is generated by cyberelements via an exchange between Edge Gateway and the Active Directory controller.

PAW workstations should not exchange with instances external to the third-party where they are implemented. But in the case of an access policy that requires remote administration, for example for third-party maintainers, the access will have to be configured to ensure that the PAW workstation only accesses a single endpoint and that it cannot browse the Internet.

Network accesses based on a Zero Trust approach, more commonly known as ZTNA (Zero Trust Network Access), meet this access policy and cyberelements uses this ZTNA technology natively.

This approach allows to keep the advantages of cyberelements, including:

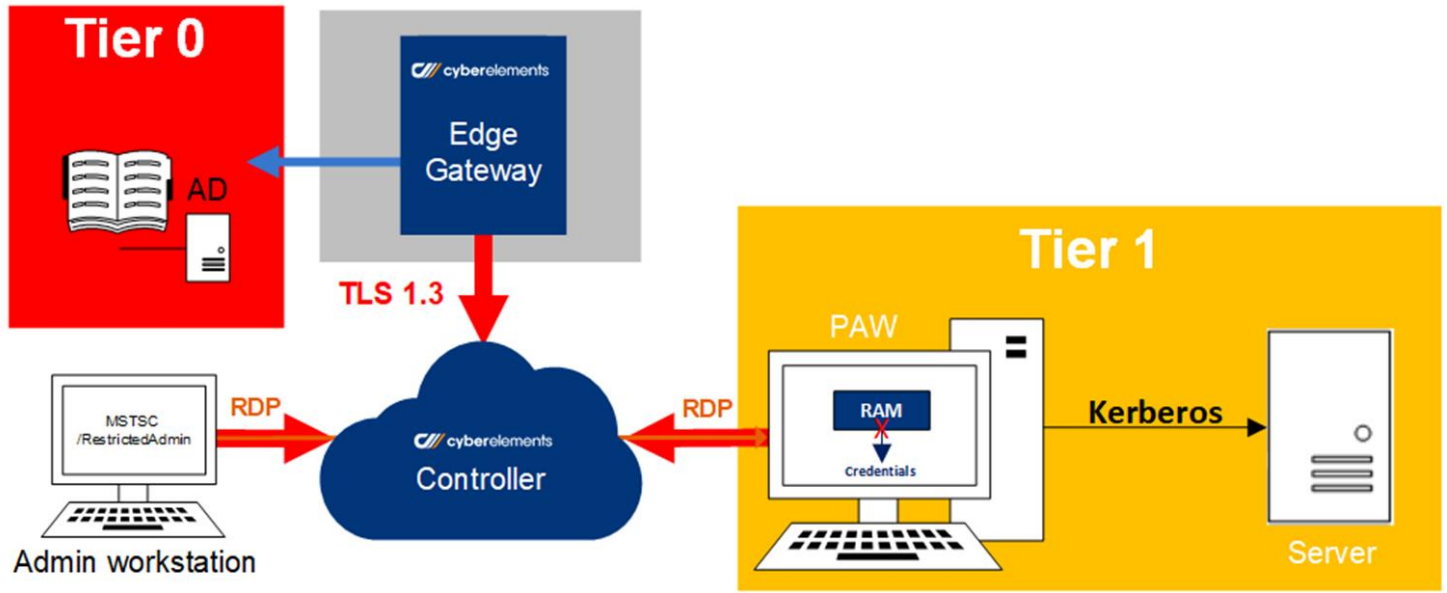
- Video traceability of access.
- Control of actions performed.
- Password vault.
- Etc.

"Restricted Admin" mode

cyberelements interfaces between the administrator's workstation and the PAW workstation. During the authentication process via the RDP protocol, the LSASS service, in charge of providing the SSO (Single Sign-On) mechanism, will load the hash of the administrator's password into the memory of the PAW workstation. If the latter were to be compromised, a "Pass-the-Hash" attack, which consists of using the password hash to authenticate to a resource, could compromise all the resources of the administered third-party.

By enabling the "**Restricted Admin**" mode, available since Windows Server 2012 R2, the credentials that are entered during the RDP connection, including the password hash, are not memorized and stored in the memory of the PAW workstation.

It is therefore required to enable the "Restricted Admin" mode to reinforce the protection of the third-party resources. The activation can be done by GPO or by registry key.



"Restricted Admin" mode

The table below shows that many authentication methods store authentication secrets in memory, especially in Active Directory environments where security is not enforced.

		KERB	HASHES		PLAINTEXT PASSWORDS				
		TGT	LM	NT	Tspkg	Wdigest	Kerb	LiveSSP	Third Party SSP
without security reinforcement	Microsoft account								~
	Local account								~
	Domain account								~
with security reinforcement	Microsoft account				*	**			~
	Local account				*	**			~
	Domain account				*	**			~
New features	Protected Users								~
	Restricted Admin RDP								

~ Only if installed

* Off by default

** Only by default on Windows 8.1 and Windows Server 2012 R2

Password data in memory

No password data in memory

cyberelements

Technical abbreviations and references

To facilitate the readability and understanding of this document, you will find in the table below the list of technical abbreviations (acronyms) used.

AS	Authentication Service
FAST	Flexible Authentication via Secure Tunneling
LAPS	Local Administrator Password Solution
LM	LAN Manager
LSASS	Local Security Authority Subsystem Service
MSC	Maintenance in Safe Conditions
NCSC	National Cyber Security Center
NT	New Technology
NTDS	NT Directory Services
NTLM	NT Lan Manager
PAM	Privileged Access Management
PAW	Privileged Access Workstation
IS	Information System
TGT	Ticket Granting Ticket
ZTNA	Zero Trust Network Access

References

The tiered administration - Aurélien Bordes:
https://www.sstic.org/2017/presentation/administration_en_silo/

Secure system administration guidance:
https://www.ncsc.gov.uk/collection/secure-system-administration/risk-manage-administration-using-tiers