

Modèle de document long

Sous-Titre : Dossier Projet

Classification Hardis Group : Crée un document.


Fatoumata Binta Diallo
GROUPE HARDIS [Company address]

VERSIONS


Version	Date	Auteur	Description
1.0	03/12/2024	F. BINTA DIALLO	Création

INTERLOCUTEURS


Votre Interlocuteur



Fatoumata Binta Diallo



Centre de Formation



SC-900

SOMMAIRE

1. Présentation de l'entreprise	3
2. <i>HARDIS GROUP</i>	3
3. <i>Nos Valeurs</i>	3
4. <i>LA Practice Cybersécurité</i>	3
5. <i>PROJET</i>	4
6. <i>Cahier des charges</i>	4
1. Administration et sécurisation des accès de l'infrastructure réseaux	4
2. hébergement web	5
3. SERVICES ACTIVE DIRECTORY	5
4. Audit de l'active directory (Pincastle)	5
5. ACCES DISTANT SECURISE	5
6. SAUVEGARDE	5
7. Contraintes	5
8. Livrables attendus	6
9. Planification et délais	6
7. <i>Déroulement du projet</i>	6
1. analyse des besoins et audit de l'infrastructure actuelle	6
2. Conception de la nouvelle infrastructure	6
3. Planification et stratégie de mise en œuvre	7
4. Acquisition et configuration des équipements	7
5. Déploiement de la nouvelle infrastructure	7
6. Tests et validation	7
7. Formation et transfert de compétences	7
8. Mise en production et suivi post-déploiement	8
8. <i>PROJET</i>	8
1. Infrastructure Actuel	8
2. Nouvelle Infrastructure	9
3. Adressage IP	Erreur ! Signet non défini.
4. Communication Réseau Interne	10
9. <i>CONFIGURATION</i>	11
1. Mise en place et configuration du firewall	11
2. Mise en place et configuration des switches	12
3. SERVEUR WEB	15
4. Mise en place d'un serveur Active directory primaire et secondaire	15
5. Audit de l'active directory avec Pincastle	17
6. Mise en place d'apache guacamole	22
10. <i>PROPOSITION D'AMELIORATION</i>	25
1. LA MISE EN PLACE D'UN PRA	25
2. MISE EN PLACE DE LA STRATEGIE DE SAUVEGARDE 3-2-1	25
26	
Annexes	27

PRESENTATION DE L'ENTREPRISE

1. HARDIS GROUP

Fondée en 1984, Hardis Group exerce le triple métier de société de conseil et de services IT, d'intégrateur Salesforce et d'éditeur de logiciels pour la logistique.

Hardis Group intervient dans plusieurs secteurs d'activité, notamment la logistique, la distribution, l'industrie et l'assurance. L'entreprise met également l'accent sur l'innovation, en intégrant des technologies avancées telles que l'intelligence artificielle, l'Internet des objets (IoT) et la robotique dans ses solutions.

Notre ambition est d'accélérer la transformation du commerce, de la supply Chain et des systèmes d'information de nos clients. Nous nous appuyons sur notre triple métier historique pour les accompagner dans leurs transformations stratégiques, organisationnelles et technologiques.

Nous avons la conviction que la transformation et le développement de nos clients passe par la création de toujours plus de valeur autour des technologies cloud (applications, plateformes et infrastructures), des données (intelligence artificielle, machine Learning, objets connectés, etc.) et de l'automatisation (robots, drones, RPA...).

2. NOS VALEURS

Chez Hardis group, notre culture est avant tout définie par des valeurs humaines que nous vivons et nous transmettons au quotidien.

Cet environnement où chacun travaille en confiance favorise les initiatives et l'innovation.

Avec plus de 70 métiers représentés, des profils et des personnalités variés, nous sommes tous différents mais nous avançons tous ensemble, et c'est bien là notre richesse !

3. LA PRACTICE CYBERSÉCURITÉ

La Practice Cybersécurité de HCO (Hardis Cloud Operations) vise à élever le niveau de sécurité global de ses clients. Pour ce faire, elle propose un accompagnement complet couvrant plusieurs axes d'évolution : gouvernance, formation, sensibilisation et technologies.

Notre mission est d'accroître la sécurité des entreprises et de leurs employés en exploitant nos compétences, nos connaissances et les technologies de pointe. Nous aidons les entreprises à renforcer leurs systèmes d'information en déployant des solutions de sécurité, en offrant des conseils avisés et en les accompagnant tout au long de leurs démarches.

4. PROJET

Déploiement d'une Infrastructure sécurisée, ce projet a été imaginé et réalisé en autonomie.

Dans le cadre de la croissance rapide de l'entreprise Aptsol, spécialisée dans le conseil en informatique et désormais active dans la vente de matériels informatiques, l'infrastructure actuelle ne répond plus de manière optimale aux besoins accrus en termes de performance, de sécurité et de scalabilité. Pour accompagner cette expansion, nous avons été mandatés pour repenser intégralement l'infrastructure informatique existante. Notre mission consiste à concevoir et déployer une infrastructure sécurisée, capable de répondre aux exigences actuelles de l'entreprise tout en optimisant l'efficacité opérationnelle et la protection des données.

Objectif du projet

L'objectif principal de ce projet est de déployer une infrastructure réseau moderne, robuste et hautement sécurisée, qui permettra à notre client de gérer efficacement sa croissance, d'assurer la continuité de ses activités et de protéger ses données. Nous visons à renforcer la sécurité de l'entreprise contre les menaces potentielles, tout en facilitant une maintenance simplifiée et une gestion évolutive.

5. CAHIER DES CHARGES

1. ADMINISTRATION ET SECURISATION DES ACCES DE L'INFRASTRUCTURE RESEAUX

- Configuration de deux switches Cisco sur Packet Tracer avec l'agrégation de liens (Link Aggregation) pour améliorer la bande passante et la tolérance aux pannes.
- Création des VLANs pour segmenter le réseau et pour une gestion optimale et sécurisée des flux selon les différents services pour mon projet nous avons (Vlan Administration, RH, Compta, IT).
- Implémentation des ACLs sur des switches de niveau 3 afin de renforcer la sécurité en restreignant l'accès aux données et aux systèmes sensibles, tout en contrôlant et limitant la communication au sein du réseau interne.
- Déploiement d'un pare-feu pfSense sur VMWare pour contrôler et monitorer les flux entrants et sortants.

2. HEBERGEMENT WEB

J'ai créé un site intranet afin de simplifier la communication interne, d'encourager la collaboration entre les équipes et de centraliser les applications métiers pour un accès optimisé.

3. SERVICES ACTIVE DIRECTORY

- Mise en place de deux serveurs Active Directory (AD) pour la gestion des identités machines et comptes utilisateurs, groupes, stratégies de groupe (GPO) et le contrôle d'accès.
- Mise en place d'un serveur AD secondaire en réplication pour garantir la haute disponibilité, la continuité de service en cas de panne, la répartition de charge et une maintenance sans interruption.

4. AUDIT DE L'ACTIVE DIRECTORY (PINCASTLE)

- J'ai mis en place PingCastle pour sécuriser l'Active Directory, qui est souvent une cible privilégiée lors de cyberattaques. Grâce à cet outil, j'ai pu détecter les vulnérabilités, notamment les faiblesses de configuration, et appliquer des solutions pratiques basées sur les recommandations d'organisations comme l'ANSSI. Il m'aide également à suivre l'évolution de la sécurité de l'infrastructure en générant des rapports clairs et un score de sécurité.

5. ACCES DISTANT SECURISE

- Installation d'Apache Guacamole sur Debian pour permettre un accès RDP sécurisé aux serveurs Active Directory.
- Configuration des paramètres d'authentification et des restrictions d'accès.

6. SAUVEGARDE

- Les sauvegardes d'Apsol sont entièrement externalisées et gérées via le cloud

7. CONTRAINTES

- Un budget restreint et limité
- Utilisation de matériel compatible avec les technologies open sources choisies (pfsense, packet tracer, apache guacamole).

8. LIVRABLES ATTENDUS

- Une Infrastructure réseau fonctionnelle avec switches et VLANs configurés.
- Un Pare-feu pfSense configuré et opérationnel.
- Deux serveurs Active Directory en haute disponibilité.
- Un Accès distant sécurisé via Apache Guacamole.
- Un Site web intranet
- Un Document d'architecture technique (DAT).

9. PLANIFICATION ET DELAIS

- Analyse des besoins et validation des spécifications : 1 semaine.
- Mise en place de l'infrastructure physique : 2 semaines.
- Installation des serveurs et services : 3 semaines.
- Tests, validation et mise en production : 1 semaine.
- Formation et remise de la documentation : 1 semaine.
- Durée totale estimée: 8 semaines.

6. DÉROULEMENT DU PROJET

1. ANALYSE DES BESOINS ET AUDIT DE L'INFRASTRUCTURE ACTUELLE

Recueil des exigences : Rencontrer les parties prenantes pour comprendre les besoins spécifiques de l'entreprise, les priorités, les attentes en termes de performance, de sécurité et de résilience.

Analyse de sécurité : Identifier les vulnérabilités potentielles et évaluer les niveaux de sécurité actuels.

2. CONCEPTION DE LA NOUVELLE INFRASTRUCTURE

Définition de l'architecture cible : Concevoir une architecture réseau adaptée aux besoins d'expansion et de sécurité, incluant les aspects de redondance, de fiabilité, et de scalabilité.

Choix des technologies : Sélectionner les technologies et solutions les plus adaptées (matériel réseau, logiciels de gestion, dispositifs de sécurité, etc.).

Plan de sécurité : Élaborer une stratégie de sécurité comprenant les protocoles de protection, les solutions de pare-feu, VPN, anti-intrusion, et autres mesures de cybersécurité.

Schéma et documentation : Créer une documentation complète et un schéma de la nouvelle architecture, facilitant la mise en place et la future maintenance. Planification et stratégie de mise en œuvre

3. PLANIFICATION ET STRATEGIE DE MISE EN ŒUVRE

Élaboration d'un planning détaillé : Prévoir les phases du projet avec des jalons pour le déploiement, la configuration, et les tests.

Plan de migration : Définir un plan pour migrer de l'ancienne à la nouvelle infrastructure en minimisant l'interruption des services.

4. ACQUISITION ET CONFIGURATION DES EQUIPEMENTS

Commande et réception des matériels : Acheter ou louer les nouveaux équipements réseau (switches, routeurs, serveurs, firewalls, etc.) et les logiciels nécessaires.

Préparation des configurations : Préconfigurer les équipements pour s'adapter à l'architecture cible.

Mise en conformité : Vérifier la compatibilité et la conformité des nouveaux équipements avec les normes et exigences de sécurité.

5. DEPLOIEMENT DE LA NOUVELLE INFRASTRUCTURE

Installation physique : Installer les nouveaux équipements dans les locaux ou data centers (câblage, positionnement, etc.).

Configuration et paramétrage : Configurer les équipements et les services réseau selon le plan défini.

Sécurisation : Mettre en place les dispositifs de sécurité (pare-feu, VPN, IDS/IPS) et s'assurer de leur bon fonctionnement.

6. TESTS ET VALIDATION

Tests de performance : Évaluer les performances du réseau (latence, bande passante, etc.) pour vérifier qu'elles répondent aux exigences.

Tests de sécurité : Réaliser des tests de pénétration pour valider la robustesse des dispositifs de sécurité.

Validation de la redondance : Tester les mécanismes de redondance et de sauvegarde pour garantir la résilience.

7. FORMATION ET TRANSFERT DE COMPETENCES

Formation du personnel : Former les équipes internes d'Aptsol sur l'utilisation et la maintenance de la nouvelle infrastructure.

Documentation et guides : Fournir une documentation complète et des guides de procédures pour les futures opérations de maintenance et de dépannage.

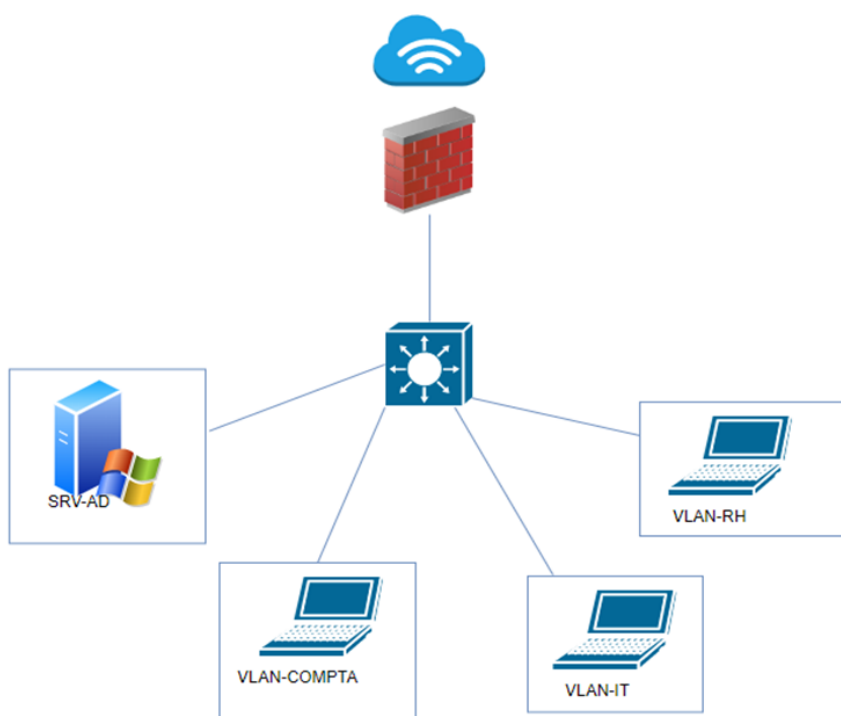
8. MISE EN PRODUCTION ET SUIVI POST-DEPLOIEMENT

Transition vers la production : Passer l'infrastructure en production en effectuant un suivi rapproché pour résoudre rapidement tout problème éventuel.

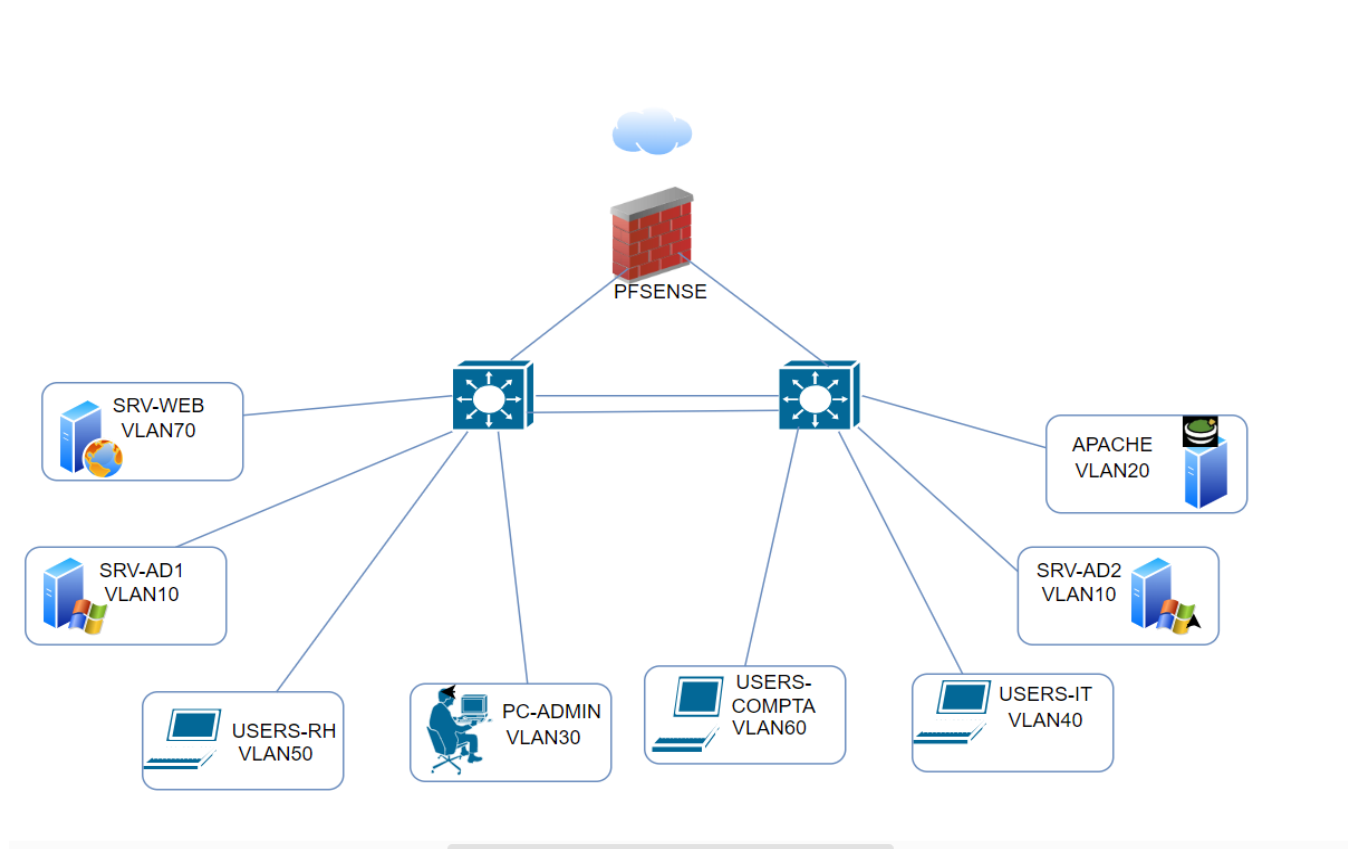
Support post-mise en œuvre : Offrir un support post-déploiement pour assister Aptsol dans les premiers mois d'utilisation et ajuster les configurations si nécessaire.

7. PROJET

1. INFRASTRUCTURE ACTUEL



2. NOUVELLE INFRASTRUCTURE



3. ADRESSAGE IP

J'ai mis en place un adressage IP basé sur le VLSM afin d'optimiser l'utilisation des adresses IP et de mieux répondre aux besoins variés des réseaux. Cette méthode me permet de créer des sous-réseaux de tailles différentes, adaptés aux besoins spécifiques de chaque segment. Elle réduit le gaspillage d'adresses IP et améliore la gestion globale du réseau.

MACHINES	VLAN	IP	CIDR	GATEWAY
Parefeu	5	192.168.5.1	30	192.168.5.1
AD1	10	192.168.10.2	29	192.168.10.1
AD2	10	192.168.10.3	29	192.168.10.1
APACHE	20	192.168.20.2	30	192.168.20.1
PCADMIN	30	192.168.30.2	30	192.168.30.1
IT	40	192.168.40.2	24	192.168.40.254
RH	50	192.168.50.2	24	192.168.50.254
COMPTA	60	192.168.60.2	24	192.168.60.254
SITE WEB	70	192.168.70.2	30	192.168.70.1

4. COMMUNICATION RESEAU INTERNE

SOURCES/DESTINATION	AD1	AD2	APACHE	PC-ADMIN	PC-IT	PC-RH	PC-COMPTA	SRV-WEB
AD1								
AD2								
APACHE								
PC-ADMIN								
PC-IT								
PC-RH								
PC-COMPTA								
SRV-WEB								
	COMMUNICATION				PAS DE COMMUNICATION			

8. CONFIGURATION

1. MISE EN PLACE ET CONFIGURATION DU FIREWALL

On met en place le firewall qui est la première ligne de défense contre les menaces externes telles que les attaques DDoS, les intrusions, et les logiciels malveillants.

Il filtre le trafic réseau en fonction de règles prédéfinies pour bloquer tout trafic non autorisé.

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 5ef2b94c899285556a8c

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

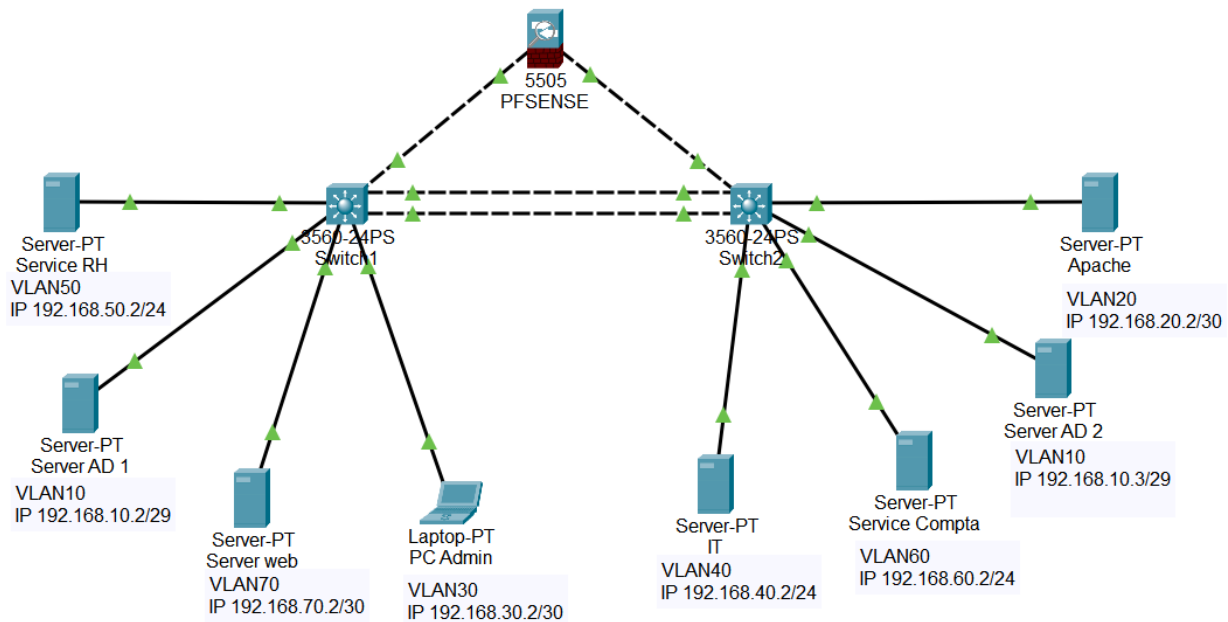
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.194/24
LAN (lan)      -> em1      -> v4: 192.168.5.1/30

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

2. MISE EN PLACE ET CONFIGURATION DES SWITCHES

J'ai mis en place la configuration réseau sur Cisco packet tracer



J'ai configuré l'agrégation de lien entre les deux switches afin d'assurer la redondance, permettant une redirection automatique du trafic en cas de panne et maintenir une continuité de service.

```
Switch#show interfaces etherchannel
FastEthernet0/1:
Port state      = 1
Channel group   = 1          Mode = Active          Gcchange = -
Port-channel    = Po1        GC      = -            Pseudo port-channel = Po1
Port index      = 0          Load = 0x00          Protocol   = LACP
```

Cette configuration a également été appliquée sur le deuxième switch.

J'ai mis en place des VLANs pour segmenter le réseau, renforcer la sécurité et optimiser la gestion globale de l'infrastructure.

VLAN	Name	Status
1	default	active
10	AD	active
20	APACHE	active
30	ADMIN	active
40	IT	active
50	RH	active
60	COMPTA	active
70	WEB	active

J'ai mis en place les ACLs pour sécuriser la communication du réseau interne en régulant l'accès aux ressources sensibles et en protégeant les données contre les accès non autorisés.

```
Switch>en
Switch#show access-lists
Extended IP access list AD1
 10 permit icmp 192.168.10.0 0.0.0.7 192.168.20.0 0.0.0.3 echo-reply
 20 deny icmp 192.168.10.0 0.0.0.7 192.168.20.0 0.0.0.3 echo
 30 permit udp 192.168.10.0 0.0.0.7 any eq domain
 40 deny ip any any
Extended IP access list APACHE
 10 permit tcp 192.168.20.0 0.0.0.3 192.168.10.0 0.0.0.7 eq 3389
 20 permit icmp 192.168.20.0 0.0.0.3 192.168.10.0 0.0.0.7
 30 permit icmp 192.168.20.0 0.0.0.3 192.168.40.0 0.0.0.255 echo-reply
 40 deny icmp 192.168.20.0 0.0.0.3 192.168.40.0 0.0.0.255 echo
 50 permit udp 192.168.20.0 0.0.0.3 192.168.10.0 0.0.0.7 eq domain
Extended IP access list PC-IT
 10 permit icmp 192.168.40.0 0.0.0.255 any
 20 permit udp 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.7 eq domain
 30 permit udp 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.7 eq 88
 40 deny ip any any
Extended IP access list SRV-WEB
 10 permit tcp any 192.168.70.0 0.0.0.3 eq 443
 20 deny ip any any
 30 permit tcp any 192.168.70.0 0.0.0.3 eq www
Extended IP access list PC-ADMIN
 10 permit icmp 192.168.20.0 0.0.0.3 192.168.70.0 0.0.0.3
 20 deny ip any any
Extended IP access list PC-COMPTA
 10 permit udp 192.168.60.0 0.0.0.255 192.168.10.0 0.0.0.7 eq 88
 20 permit udp 192.168.60.0 0.0.0.255 192.168.10.0 0.0.0.7 eq domain
 30 deny ip any any
Extended IP access list PC-RH
 10 permit udp 192.168.50.0 0.0.0.255 192.168.10.0 0.0.0.7 eq 88
 20 permit udp 192.168.50.0 0.0.0.255 192.168.10.0 0.0.0.7 eq domain
 30 deny ip any any
```

Par exemple sur cette règle j'autorise Apache à répondre quand le pc IT le ping et je bloque l'inverse

```
30 permit icmp 192.168.20.0 0.0.0.3 192.168.40.0 0.0.0.255 echo-reply
40 deny icmp 192.168.20.0 0.0.0.3 192.168.40.0 0.0.0.255 echo
```

Ping depuis le PC IT vers APACHE OK

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>|
```

Ping depuis APACHE vers le PC IT bloquer

```
C:\>ping 192.168.40.2

Pinging 192.168.40.2 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

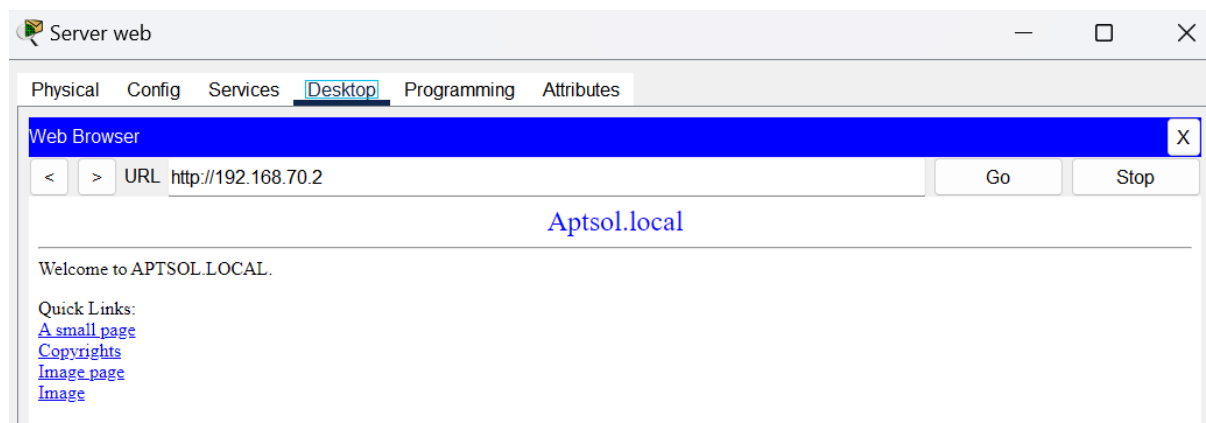
Ping statistics for 192.168.40.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>|
```

3. SERVEUR WEB

Configuration du serveur web intranet depuis Cisco packet tracer.

J'ai créé un site intranet pour améliorer la communication interne, favoriser la collaboration entre les équipes et centraliser les applications métiers, assurant ainsi un accès simplifié et efficace.

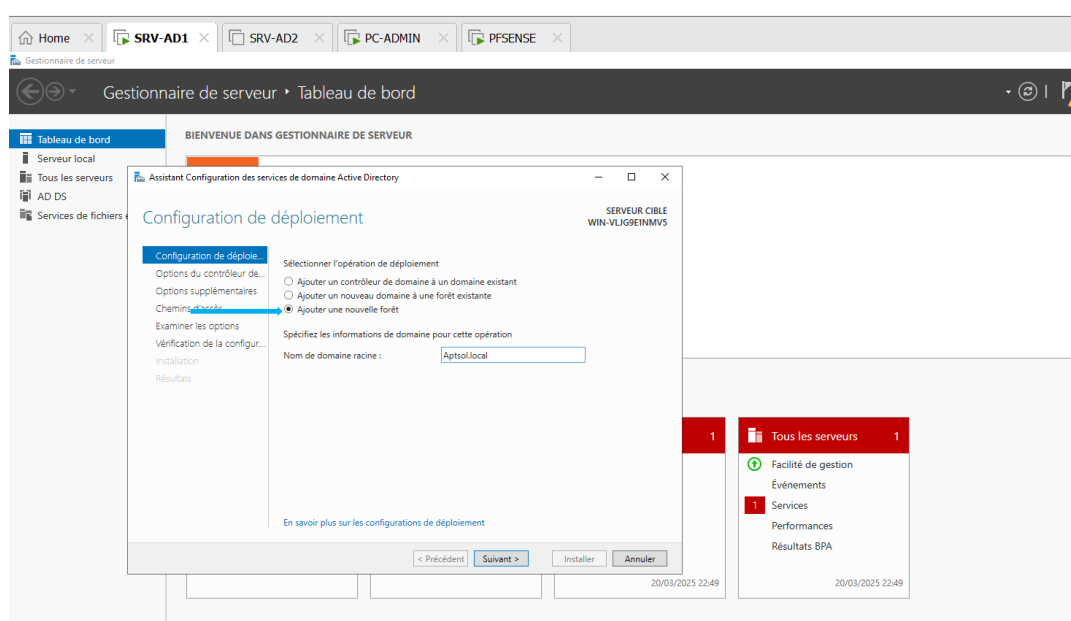


4. MISE EN PLACE D'UN SERVEUR ACTIVE DIRECTORY PRIMAIRE ET SECONDAIRE

J'ai mis en place un active directory pour centraliser la gestion des utilisateurs, des ordinateurs et des ressources du réseau. Il assure l'authentification et le contrôle des accès, garantissant une sécurité renforcée.

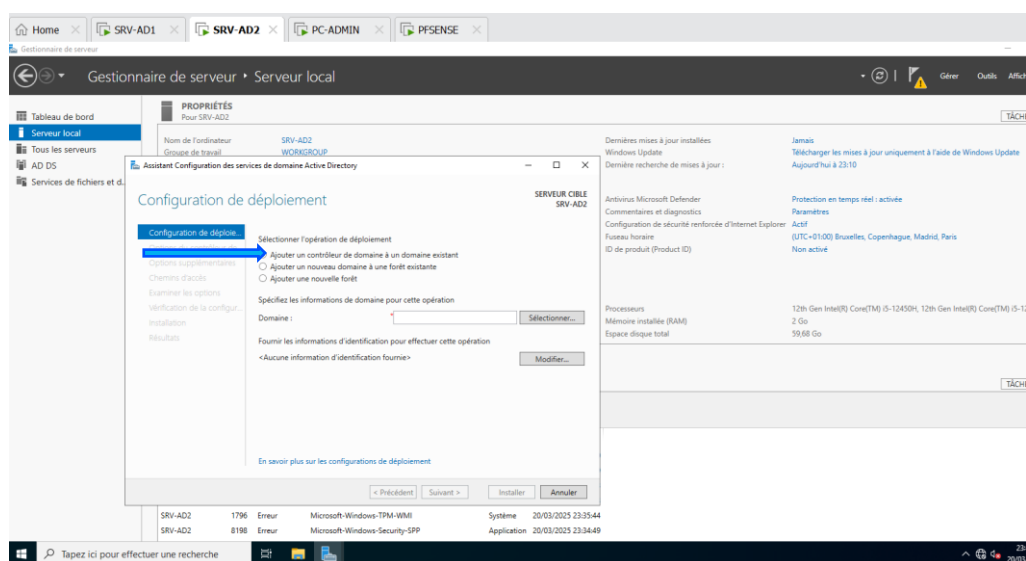
Il permet aussi l'intégration avec d'autres services tel que les serveurs de messagerie les bases de données et les applications métiers.

Pour la création de l'active directory primaire on ajoute une nouvelle forêt.



Dans un deuxième j'ai mis en place un active directory secondaire pour la haute disponibilité. En cas de défaillance du contrôleur principal, le secondaire prend le relais, assurant ainsi la continuité du service. Il permet aussi de faire la répartition des charges. De nombreuses normes de sécurité (ISO 27001, RGPD) recommandent la redondance des systèmes critiques comme l'active directory.

Pour la création de l'active directory secondaire on ajoute un contrôleur de domaine à un domaine existant



Les deux Active Directory sont correctement configurés

Utilisateurs et ordinateurs Active Directory					
Requêtes enregistrées					
Aptsol.local					
Builtin					
Computers					
Domain Controllers					
ForeignSecurityPrincipals					
Nom	Type	Type de contrôl...	Site	Description	
SRV-AD1	Ordinateur	GC	Default-First-Si...		
SRV-AD2	Ordinateur	GC	Default-First-Si...		

L'active directory fait office de serveur DNS

Exemple de ping avec le nom du serveur apache

```
C:\>ping apache

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

5. AUDIT DE L'ACTIVE DIRECTORY AVEC PINCASTLE

PingCastle est un outil spécialisé dans l'audit de sécurité des Active Directory.

J'ai mis en place PingCastle pour analyser la sécurité de l'Active Directory, identifier les vulnérabilités potentielles et évaluer les risques. Il me permet de recevoir des recommandations concrètes pour renforcer la protection et d'automatiser les audits afin de gagner en efficacité et d'avoir un environnement active directory sécurisé. Grâce à ses tableaux de bord intuitifs, il offre une vue claire et détaillée de l'état de votre système.

Exécution de pingcastle sur l'active directory

```
\==--0_ PingCastle (Version 3.3.0.1 25/09/2024 21:03:40)
 \ / \ ""> Get Active Directory Security at 80% in 20% of the time
  \ / \ '
 0"--0_ End of support: 2026-01-31
  \ , ' To find out more about PingCastle, visit https://www.pingcastle.com
   v For online documentation, visit https://helpcenter.netwrix.com/category/pingcastle
 For support and questions:
 - Open-source community, visit https://github.com/netwrix/pingcastle/issues
 - Customers, visit https://www.netwrix.com/support.html

What do you want to do?
=====
Using interactive mode.
Do not forget that there are other command line switches like --help that you can use

1-healthcheck-Score the risk of a domain
2-azuread -Score the risk of AzureAD
3-conso -Aggregate multiple reports into a single one
4-carto -Build a map of all interconnected domains
5-scanner -Perform specific security checks on workstations
6-export -Export users or computers
7-advanced -Open the advanced menu
0-Exit

=====
This is the main functionality of PingCastle. In a matter of minutes, it produces a report which will give you an overview of your Active Directory security. This report can be generated on other domains by using the existing trust links.
```

Remontée automatique du domaine Aptsol.local

```

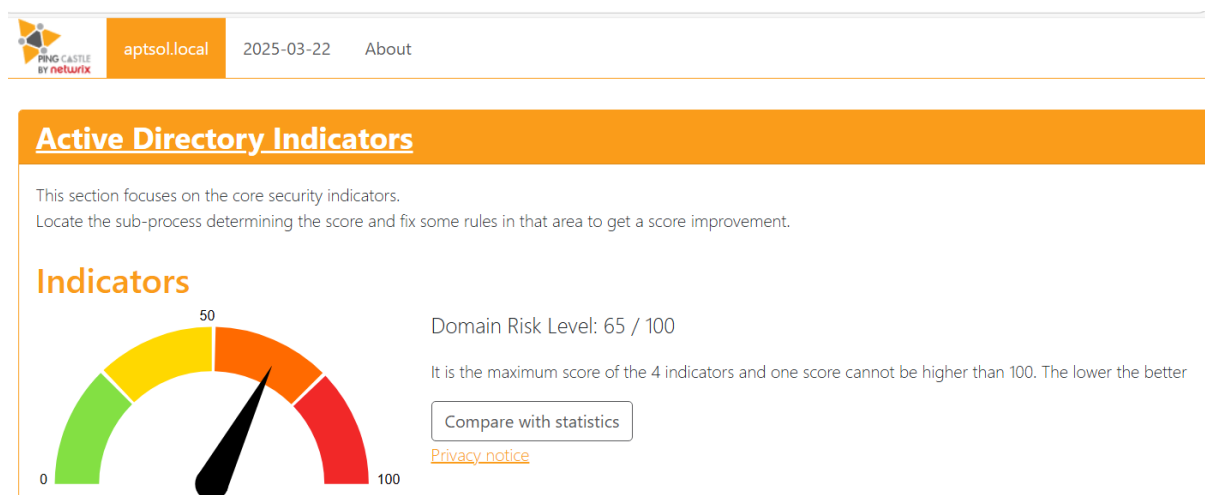
\==--0___ PingCastle (Version 3.3.0.1 25/09/2024 21:03:40)
\ / \ ""> Get Active Directory Security at 80% in 20% of the time
\ / \ , ' End of support: 2026-01-31
0"---0 To find out more about PingCastle, visit https://www.pingcastle.com
\ , ' For online documentation, visit https://helpcenter.netwrix.com/category/pingcastle
v For support and questions:
- Open-source community, visit https://github.com/netwrix/pingcastle/issues
- Customers, visit https://www.netwrix.com/support.html

Select a domain or server
=====
Please specify the domain or server to investigate (default:Aptsol.local)
  
```

Première Analyse

Le score est de 65/100

Les 65 représente le niveau de risque



Pour sécuriser L'Active Directory, j'utilise le tableau de bord de PingCastle, qui met en évidence les améliorations nécessaires afin de réduire le score de risque et renforcer la protection

Risk model ?

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Golden ticket
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Azure	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		Password retrieval
			Reconnaissance
			Temporary admins
			Weak password


Legend:

- score is 0 - no risk identified but some improvements detected
- score between 1 and 10 - a few actions have been identified
- score between 10 and 30 - rules should be looked with attention
- score higher than 30 - major risks identified

Pour réduire le score de risque, j'ai appliqué certaines remédiations recommandées par PingCastle dans le cadre des améliorations nécessaires.

J'ai par exemple ici une recommandation.

Par défaut, un utilisateur de base peut enregistrer jusqu'à 10 ordinateurs dans le domaine, ce qui représente un risque de sécurité. Pour éviter cela, il est recommandé de modifier l'attribut et de mettre le quota à 0



aptsolocal
2025-03-22
About

Check the process of registration of computers to the domain

Rule ID:
S-ADRegistration

Description:
The purpose is to ensure that basic users cannot register extra computers in the domain

Technical explanation:
By default, a basic user can register up to 10 computers within the domain. This default configuration represents a security issue as basic users shouldn't be able to create such accounts and this task should be handled by administrators.

If the value of the attribute ms-DS-MachineAccountQuota is not set (the program see this as "Infinite"), there is no limit to computer addition.

Note: this program checks also the GPO for SeMachineAccountPrivilege assignment. This assignment can be used to restrict the impact of the key ms-DS-MachineAccountQuota.

Advised solution:
To solve the issue, limit the number of extra computers that can be registered by a basic user. It can be reduced by modifying the value of *ms-DS-MachineAccountQuota* to zero (0). Another solution can be to remove the "Authenticated Users" group in the domain controllers policy altogether. Do note, that if you need to set delegation to an account, so it can add computers to the domain, it can be done through 2 methods: Delegation in the OU or by assigning the *SeMachineAccountPrivilege* to a special group

Rémédiation

Cette commande nous permet de récupérer la valeur de l'attribue qui est bien à 10

```
PS C:\Users\Administrateur> Get-ADObject -Identity "DC=Aptso1,DC=local" -Properties MS-DS-MachineAccountQuota

DistinguishedName      : DC=Aptso1,DC=local
MS-DS-MachineAccountQuota : 10
Name                   : Aptso1
ObjectClass             : domainDNS
ObjectGUID              : 5c8d87fd-5929-4022-b238-c0dcb235dcb1
```

Pour la rémédiation j'ai mis la valeur à 0 ce qui empêchera un utilisateur lamda d'ajouter des ordinateurs dans le domaine

Commande qui permet de remettre la valeur à 0

```
PS C:\Users\Administrateur> Set-ADDomain -Identity "DC=Aptso1,DC=local" -Replace @{"ms-DS-MachineAccountQuota"="0"}
```

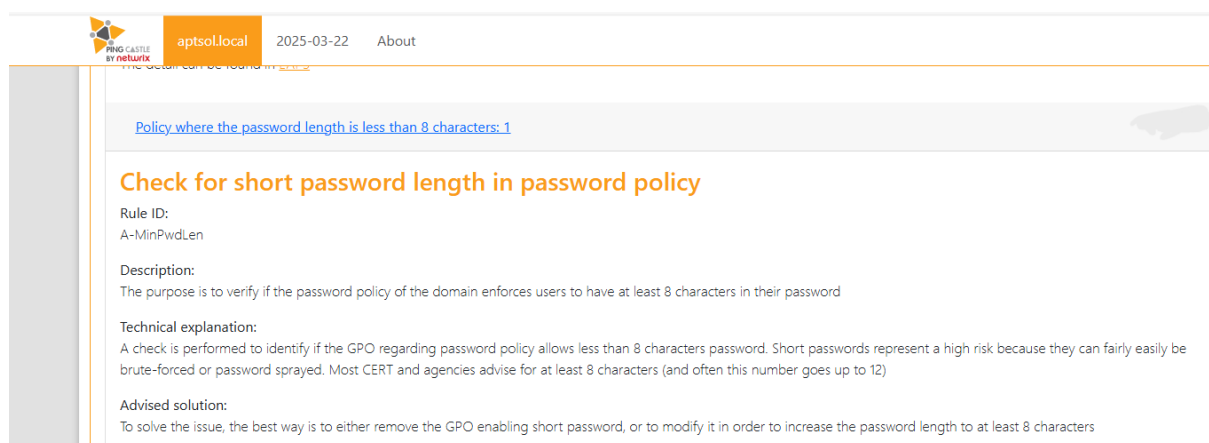
Résultat

```
PS C:\Users\Administrateur> Get-ADObject -Identity "DC=Aptso1,DC=local" -Properties MS-DS-MachineAccountQuota

DistinguishedName      : DC=Aptso1,DC=local
MS-DS-MachineAccountQuota : 0
Name                   : Aptso1
ObjectClass             : domainDNS
ObjectGUID              : 5c8d87fd-5929-4022-b238-c0dcb235dcb1
```

Deuxième exemple de recommandations

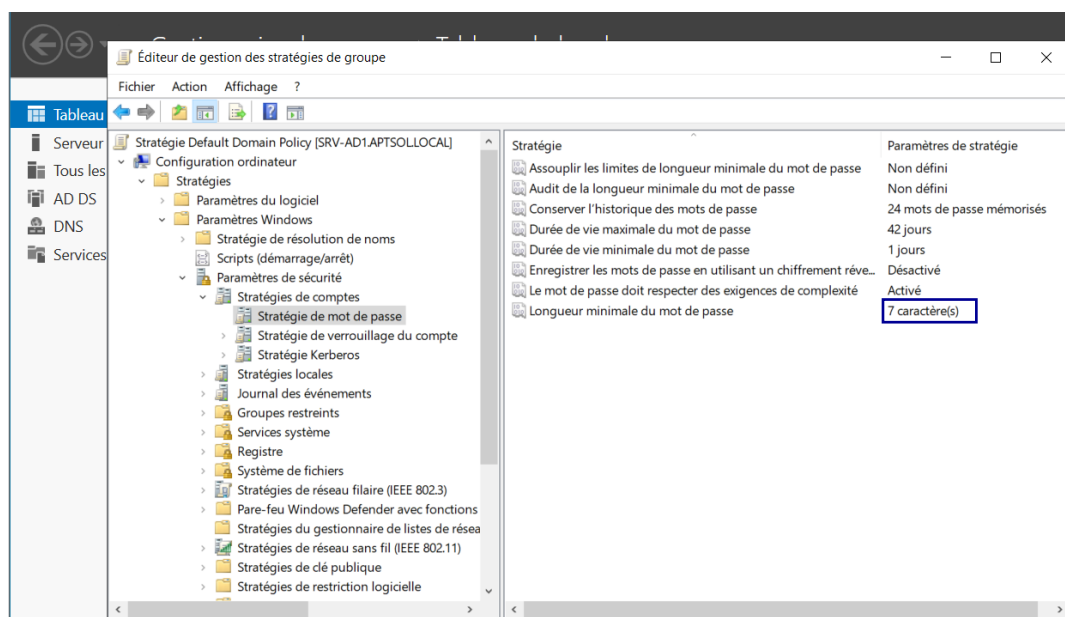
Dans cet exemple l'objectif est de vérifier si la politique de mot de passe impose une longueur minimale de 8 caractères pour les mots de passe. Si ce n'est pas le cas faire une GPO de rémédiation.



The screenshot shows a web-based interface for a security tool. At the top, there's a header with a logo, the text 'aptsol.local', the date '2025-03-22', and a link 'About'. Below the header, a message states 'The result can be found in [policy](#)'. A search bar contains the text 'Policy where the password length is less than 8 characters: 1'. The main content area is titled 'Check for short password length in password policy'. It lists the 'Rule ID' as 'A-MinPwdLen' and provides a 'Description' stating the purpose is to verify if the password policy of the domain enforces users to have at least 8 characters in their password. A 'Technical explanation' follows, stating that a check is performed to identify if the GPO regarding password policy allows less than 8 characters password, and that short passwords represent a high risk. An 'Advised solution' is provided at the bottom, suggesting to either remove the GPO enabling short password or to modify it to increase the password length to at least 8 characters.

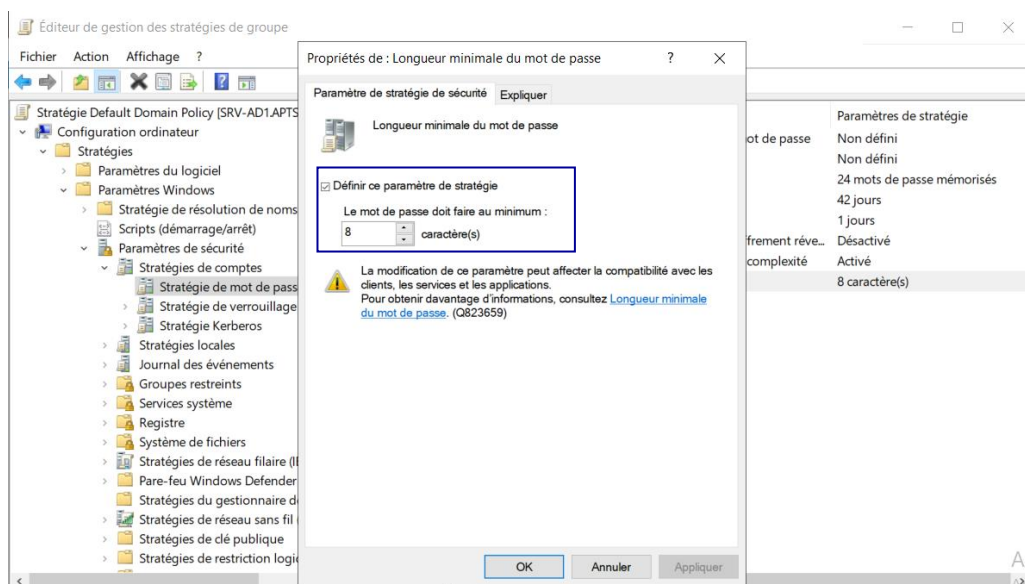
Vérification :

La longueur minimale est actuellement configuré à 7 caractères.

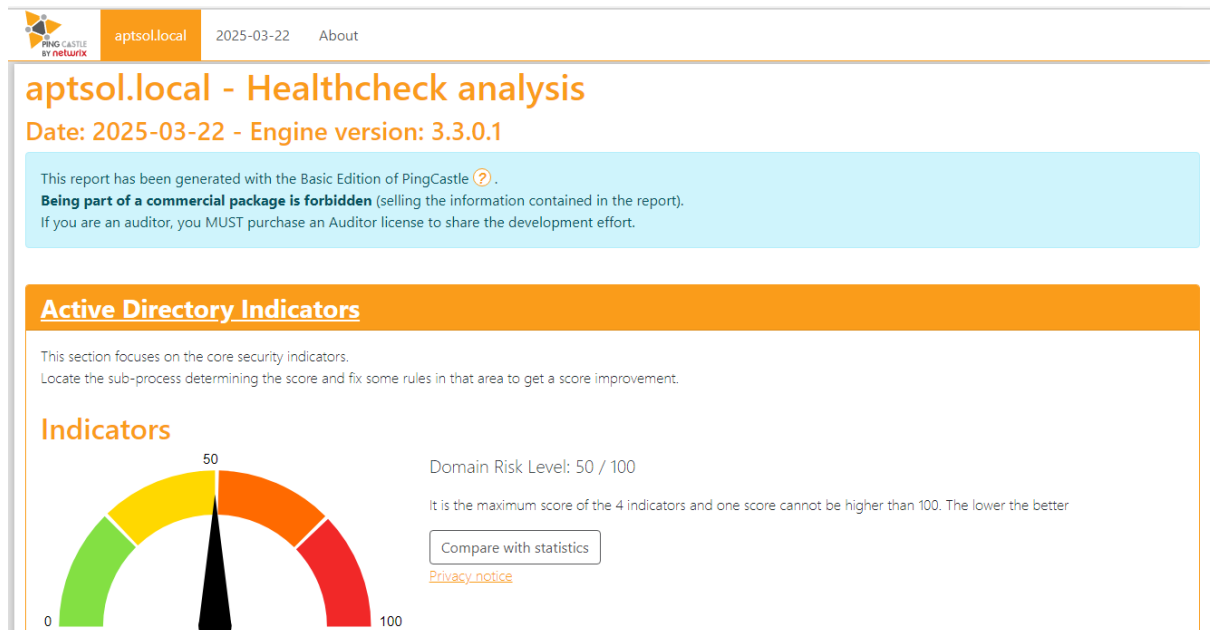


Rémédiation :

Je vais corriger cela en définissant la longueur minimale des mots de passe à 8 caractères, conformément aux recommandations de Pincastle.



Suite à ces remédiations, j'ai effectué une nouvelle analyse , ce qui a permis de réduire le score de risque à 50.



6. MISE EN PLACE D'APACHE GUACAMOLE

J'ai installé Apache Guacamole pour gérer à distance mes serveurs Active Directory. Cette solution centralise et simplifie l'accès à mes machines via une interface unique. Cette approche suit les recommandations de l'ANSSI, qui préconise un bastion d'administration pour sécuriser les accès et protéger les environnements Active Directory des risques liés aux comptes privilégiés.

J'ai installé apache guacamole sur une machine debian.

Vérification de l'installation de Apache Guacamole avec la commande

`sudo systemctl status guacd`

```

binta@debian: ~
● guacd.service - Guacamole Server
   Loaded: loaded (/etc/systemd/system/guacd.service; enabled; preset: enabled)
   Active: active (running) since Sat 2025-03-22 22:47:21 CET; 26s ago
     Docs: man:guacd(8)
    Main PID: 22543 (guacd)
      Tasks: 1 (limit: 2241)
    Memory: 10.6M
       CPU: 13ms
    CGroup: /system.slice/guacd.service
            └─22543 /usr/local/sbin/guacd -f

mars 22 22:47:21 debian systemd[1]: Started guacd.service - Guacamole Server.
mars 22 22:47:21 debian guacd[22543]: Guacamole proxy daemon (guacd) version 1.5.3 started
mars 22 22:47:21 debian guacd[22543]: guacd[22543]: INFO:      Guacamole proxy daemon (guacd) version 1.5.3 started
mars 22 22:47:21 debian guacd[22543]: guacd[22543]: INFO:      Listening on host ::1, port 4822
mars 22 22:47:21 debian guacd[22543]: Listening on host ::1, port 4822

```

Page de connexion Apache Guacamole

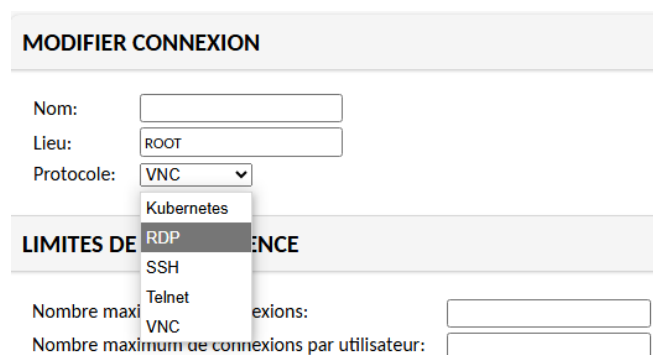
192.168.20.2:8080/guacamole/#/settings/mysql/history



The image shows the Apache Guacamole login interface. At the top is the Apache Guacamole logo, which consists of a stylized green and yellow bowl-like shape inside a black circle. Below the logo, the text "APACHE GUACAMOLE" is displayed in a bold, black, sans-serif font. Underneath the text are two input fields: the first is empty, and the second is labeled "Mot de passe" (Password). Below these fields is a dark grey button with the white text "Se connecter" (Log in).

Ajout des serveurs dans Apache Guacamole

Je dois renseigner plusieurs paramètres, comme le port utilisé pour la connexion à distance, le nom du serveur et l'adresse IP du serveur



The image shows the "MODIFIER CONNEXION" (Edit Connection) form in Apache Guacamole. The form has a light grey header with the title "MODIFIER CONNEXION". Below the header, there are several input fields and a dropdown menu. The "Nom:" field is empty. The "Lieu:" field contains the text "ROOT". The "Protocole:" dropdown menu is open, showing a list of protocols: "VNC", "Kubernetes", "RDP", "SSH", and "Telnet". Below the dropdown, there is a section titled "LIMITES DE CONNEXION" (Connection Limits). This section contains two rows of input fields. The first row is labeled "Nombre maximum de connexions:" and has an empty input field. The second row is labeled "Nombre maximum de connexions par utilisateur:" and also has an empty input field.



Ajout des serveurs active directory primaire et secondaire

Répéter mot de passe:

PROFIL

Nom:
 Adresse Mail:
 Organisation:
 Rôle:

RESTRICTIONS DE COMPTE

Connexion désactivée: ☐
 Mot de passe expiré: ☐
 Autoriser l'accès après:
 Ne pas autoriser l'accès après:
 Activer le compte après: 
 Désactiver le compte après: 
 Fuseau horaire utilisateur:

PERMISSIONS


Administration du système: ☐
 Créer de nouveaux utilisateurs: ☐
 Créer de nouveaux groupes d'utilisateurs: ☐
 Créer de nouvelles connexions: ☐
 Créer de nouveaux groupes de connexion: ☐
 Créer de nouveaux profils de partage: ☐






PARAMÈTRES

Sessions Actives Historique Utilisateurs Groupes **Connexions** Préférences

Cliquer ou appuyer sur une connexion en dessous pour la gérer. Selon vos permissions, les connexions peuvent être ajoutées, supprimées (protocole, nom d'hôte, port, etc) changées.

 Nouvelle Connexion

 Nouveau Groupe

  SRV-AD
 —   SRV-AD1
 —   SRV-AD2

9. PROPOSITION D'AMÉLIORATION

1. LA MISE EN PLACE D'UN PRA

Le PRA (Plan de Reprise d'Activité) est un ensemble de mesures et de procédures qu'une entreprise met en place pour pouvoir reprendre rapidement ses activités après un incident majeur (comme une panne, un incendie, une cyberattaque, ou toute autre catastrophe). L'objectif principal du PRA est de minimiser l'impact de cet incident sur l'entreprise, en permettant une reprise efficace de ses services et opérations essentielles.

2. MISE EN PLACE DE LA STRATEGIE DE SAUVEGARDE 3-2-1

La stratégie de sauvegarde 3-2-1 est une méthode de protection des données qui vise à garantir la sécurité et la disponibilité des informations critiques en cas de sinistre. Elle repose sur trois principes clés :

3 copies de données : Il faut avoir trois copies distinctes des données importantes.

Cela inclut la copie originale ainsi que deux sauvegardes supplémentaires. Cela permet de s'assurer que, même si une copie est endommagée, il en reste d'autres.

2 types de supports différents : Les deux copies de sauvegarde doivent être stockées sur des supports différents, par exemple, un disque dur externe et un stockage en ligne (cloud). L'idée est de diversifier les types de stockage pour éviter les risques liés à un même type de média (ex : un disque dur défectueux).

Une copie hors site : L'une des sauvegardes doit être stockée hors du site principal de l'entreprise, comme dans le cloud ou dans un autre lieu physique. Cela permet de protéger les données en cas de catastrophe qui pourrait affecter le site principal (incendie, inondation, vol, etc.).

La sauvegarde 3-2-1 garantit ainsi une meilleure résilience des données face aux pannes matérielles, aux attaques ou aux catastrophes naturelles.

CONCLUSION

La réussite de ce projet marque une étape significative dans la transformation numérique d'Aptsol. L'infrastructure mise en place est moderne et sécurisée.

Elle comprend un réseau configuré avec des switches, VLANs et ACLs, protégé par un pare-feu pfSense.

Deux serveurs Active Directory assurent la haute disponibilité. Un audit via Pincastle renforce la sécurité. Apache Guacamole garantit un accès distant fiable, et un site intranet simplifie la collaboration interne.

Ce projet m'a offert l'opportunité de mettre en pratique les connaissances acquises au cours de cette formation. Il a représenté un véritable défi, car j'ai dû concevoir et réaliser un projet de manière autonome. Bien que certaines étapes aient été complexes et exigeantes, j'ai réussi à mener ce projet à terme avec succès.

Annexes
DOSSIER PROJET