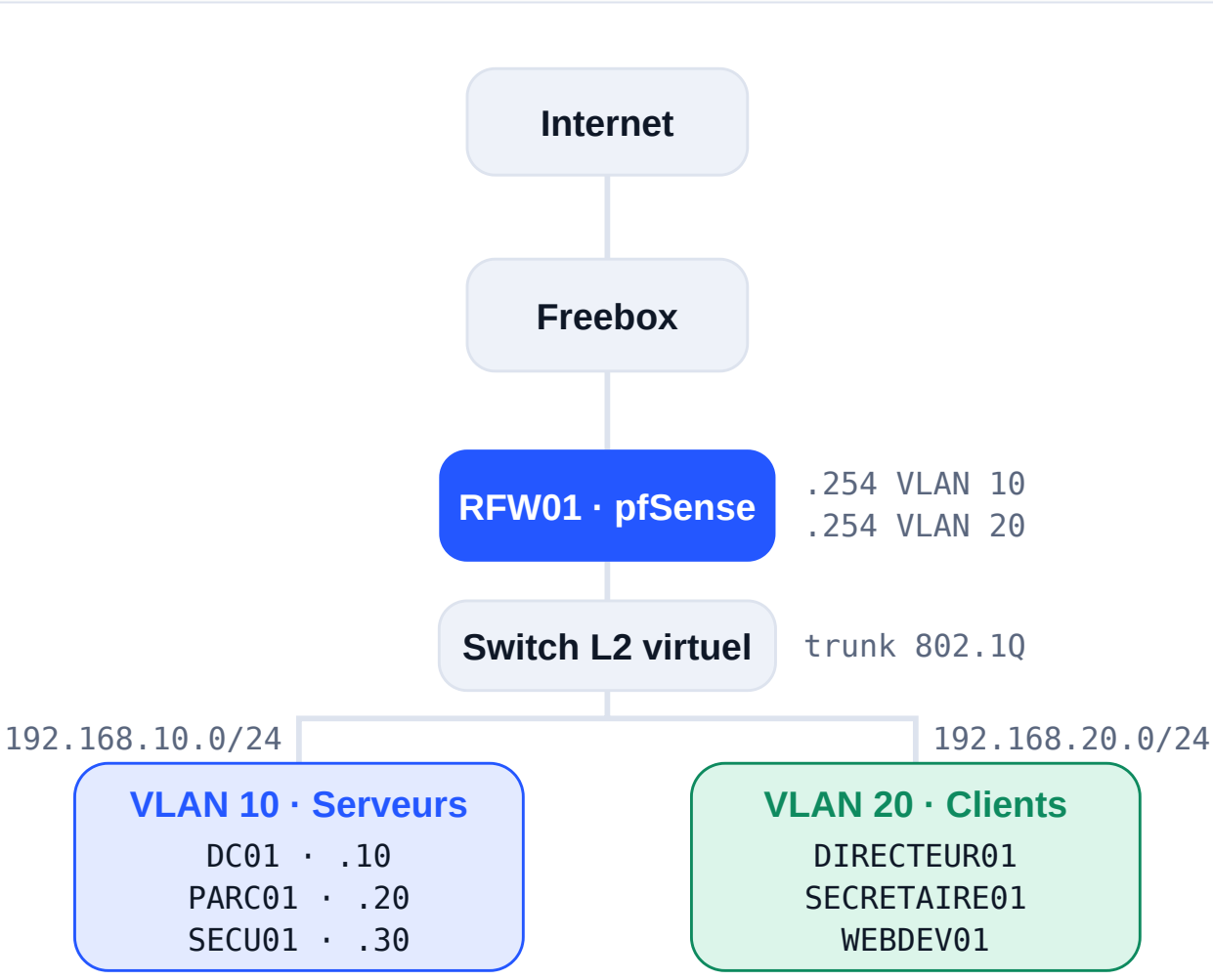
CAHIER DES CHARGES · MARTINS & CIE

Infrastructure informatique virtualisée de Martins & Cie.

Réseau segmenté en deux VLAN derrière le pare-feu pfSense RFW01, annuaire Active Directory sur DC01, gestion de parc et supervision sur PARC01 (GLPI, Zabbix) et poste d'audit SECU01 sous Kali Linux : besoins, architecture, droits, sécurité, déploiement et recette.

Domaine martinscie.lan Version 1.0 Date 19/11/2026 Statut à valider



192.168.10.0/24 pour les serveurs, 192.168.20.0/24 pour les postes. Tout passe par RFW01.

8	2	5	5
machines virtuelles	VLAN segmentés	utilisateurs	

répertoires partagés

31
besoins fonctionnels

29
tests de recette

15
chapitres

Le document

PRÉAMBULE

Fiche d'identité du document

RUBRIQUE	VALEUR
Projet	Infrastructure informatique virtualisée de l'entreprise Martins & Cie
Domaine Active Directory	martinscie.lan
Version / date	1.0 – 19 novembre 2026
Statut	Version initiale soumise à validation
Rédacteur	[à compléter]
Sources exploitées	Informations_VM.xlsx (machines virtuelles), utilisateurs.xlsx (comptes), Groupes.xlsx (groupes AD), Droits_dacces.xlsx (droits sur répertoires), schéma réseau SIO1_1SI_v1 (topologie, VLAN, adressage)
Confidentialité	Document interne. Il ne contient volontairement aucun mot de passe.

Historique des versions

VERSION	DATE	AUTEUR	MODIFICATION
0.1	19/11/2026	[à compléter]	Analyse des fichiers sources
1.0	19/11/2026	[à compléter]	Première rédaction complète du cahier des charges

Convention de lecture

- **[Source]** : exigence directement issue des fichiers fournis (tableurs ou schéma).

- **[Préco]** : préconisation complémentaire ajoutée par le rédacteur pour rendre la solution exploitable et sûre ; à valider.
- **Priorité** : **M** = Must (indispensable), **S** = Should (souhaitable), **C** = Could (optionnel).
- Lorsque deux sources se contredisent, le choix retenu est indiqué et la contradiction est listée au chapitre 15.

CHAPITRE 1

1 Présentation du projet

1.1 Contexte

Martins & Cie est une petite entreprise dirigée par son PDG, M. Serge Martins. Elle emploie cinq collaborateurs identifiés : un PDG, une secrétaire, un développeur web, une administratrice système et réseau, et un expert en cybersécurité. L'entreprise ne dispose pas aujourd'hui d'une infrastructure centralisée documentée : pas d'annuaire unique, pas de gestion des droits sur les données, pas de supervision ni de gestion de parc.

Le projet consiste à concevoir, déployer et documenter une infrastructure informatique complète, entièrement virtualisée, reproduisant le fonctionnement d'un système d'information de PME : réseau segmenté, annuaire Active Directory, services d'infrastructure, outil de gestion de parc et de support, supervision, pare-feu et poste dédié à la sécurité.

1.2 Objectifs

1. **Centraliser l'authentification** et la gestion des identités via un domaine Active Directory unique (martinscie.lan).
2. **Segmenter le réseau** en deux VLAN (serveurs et clients) derrière un pare-feu pfSense assurant routage, NAT et filtrage.
3. **Protéger les données** par des répertoires partagés dont l'accès est attribué selon le principe du moindre privilège.
4. **Maîtriser le parc** : inventaire automatique, gestion des tickets (GLPI) et supervision continue (Zabbix).
5. **Évaluer et améliorer la sécurité** grâce à un poste dédié (Kali Linux) opéré par l'expert cybersécurité.

6. **Documenter** l'ensemble pour permettre l'exploitation, la maintenance et la reproduction de l'environnement.

1.3 Périmètre

INCLUS DANS LE PROJET	EXCLUS DU PROJET
Réseau virtuel : 2 VLAN, switch L2 virtuel, trunk 802.1Q	Câblage physique et équipements réseau physiques
Pare-feu RFW01 (pfSense) : routage, NAT, règles, OpenVPN, proxy/filtrage	Configuration de la Freebox au-delà de la redirection de port VPN
Contrôleur de domaine DC01 : AD DS, DNS, DHCP	Messagerie, ERP, téléphonie
Serveur PARC01 : GLPI 10, Zabbix, Apache, MariaDB, PHP	Haute disponibilité et site de secours
Postes Windows 11 Pro et poste d'administration	Achat de matériel et de licences
Poste SECU01 (Kali Linux 2025)	Formation approfondie des utilisateurs
Comptes, groupes, droits d'accès, partages, GPO de base	Infogérance après la recette
Plan de tests, recette, documentation d'exploitation	

1.4 Parties prenantes et rôles

PERSONNE	IDENTIFIANT	RÔLE DANS L'ENTREPRISE	RÔLE DANS LE PROJET
Serge Martins	smartins	PDG et administrateur local de son poste	Commanditaire, valide la recette
Maria Bah	mbah	Administratrice système et réseau	Maître d'œuvre technique, administre DC01, PARC01 et RFW01
Léon Dasilva	ldasilva	Secrétaire	Utilisateur final (dossier Secrétariat)
Corentin Grimeau	cgrimeau	Développeur web	Utilisateur final (dossier Développement web)

PERSONNE	IDENTIFIANT	RÔLE DANS L'ENTREPRISE	RÔLE DANS LE PROJET
Hervé Nyame	hnyame	Expert cybersécurité	Audit et tests d'intrusion depuis SECU01

1.5 Hypothèses et contraintes

- Tout l'environnement tourne sur un hôte de virtualisation unique, relié à Internet par une Freebox (le fichier source n'impose pas de produit d'hyperviseur : il est à choisir, voir 3.6).
- Le plan d'adressage de référence est celui du schéma réseau : VLAN 10 = 192.168.10.0/24 (serveurs), VLAN 20 = 192.168.20.0/24 (clients).
- Les logiciels sont ceux listés dans le fichier des machines virtuelles : pfSense, Windows Server 2025, Debian 12, Windows 11 Pro 26H2, Kali Linux 2025, GLPI 10, Zabbix, Apache 2, MariaDB 10, PHP 8.1.
- Les licences Windows (serveur et postes) sont fournies par l'entreprise ou couvertes par un programme pédagogique ou d'évaluation.
- Environnement à usage de démonstration et de formation : aucune donnée réelle de production n'y est hébergée.

CHAPITRE 2

2 Expression des besoins

2.1 Besoins fonctionnels

Chaque besoin porte un identifiant unique, utilisé dans le plan de tests (chapitre 12) pour garantir la traçabilité.

TABLEAU 1 — BESOINS FONCTIONNELS

ID	BESOIN	PRIO.	ORIGINE
EF-R01	Segmenter le réseau en VLAN 10 (serveurs, 192.168.10.0/24) et VLAN 20 (clients, 192.168.20.0/24)	M	Source
EF-R02	RFW01 est la passerelle de chaque VLAN (.254) et assure le routage inter-VLAN	M	Source

ID	BESOIN	PRIO.	ORIGINE
EF-R03	Translation d'adresses (NAT) sortante vers la Freebox et Internet	M	Source
EF-R04	Règles de pare-feu par VLAN en refus par défaut (chapitre 8)	M	Source
EF-R05	Accès distant par VPN OpenVPN authentifié	S	Source
EF-R06	Proxy et filtrage web pour les postes clients	S	Source
EF-R07	Switch L2 virtuel en trunk 802.1Q portant les VLAN 10 et 20	M	Source
EF-R08	Relais DHCP sur l'interface VLAN 20 vers DC01 (sous-réseau distinct du serveur)	M	Préco
EF-A01	Domaine Active Directory martinscie.lan hébergé sur DC01	M	Source
EF-A02	DNS intégré à l'AD, redirecteurs 8.8.8.8 et 8.8.4.4	M	Source
EF-A03	DHCP sur DC01 : étendue VLAN 20 de 192.168.20.100 à 192.168.20.253	M	Source
EF-A04	Unités d'organisation Utilisateurs et Groupes à la racine du domaine	M	Source
EF-A05	Création des 5 comptes utilisateurs (mbah, smartins, ldasilva, cgrimeau, hnyame)	M	Source
EF-A06	Création des groupes : Administration, Direction, Secrétariat, Développement web, Sécurité, et rattachement aux groupes d'administration intégrés	M	Source
EF-A07	Changement obligatoire du mot de passe initial à la première connexion	M	Source
EF-A08	Jonction de tous les postes Windows au domaine	M	Préco
EF-A09	Stratégies de groupe (mots de passe, verrouillage, lecteurs réseau, administrateur local du poste direction)	S	Préco
EF-D01	Cinq répertoires partagés : Direction, Administration, Secrétariat, Sécurité, Développement web	M	Source

ID	BESOIN	PRIO.	ORIGINE
EF-D02	Droits d'accès par utilisateur conformes à la matrice du chapitre 6 (Pas d'accès / Lecture / Lecture-écriture)	M	Source
EF-D03	Application des droits via des groupes de sécurité (modèle AGDLP) plutôt que par compte nominatif	S	Préco
EF-D04	Montage automatique des lecteurs réseau selon l'appartenance aux groupes	S	Préco
EF-P01	GLPI 10 : inventaire du parc matériel et logiciel	M	Source
EF-P02	GLPI 10 : gestion des tickets d'assistance (helpdesk)	M	Source
EF-P03	Zabbix : supervision des serveurs et postes (disponibilité, CPU, RAM, disque, services)	M	Source
EF-P04	Alertes Zabbix vers l'administratrice (courriel ou ticket GLPI)	S	Préco
EF-P05	Accès SSH administratif sur PARC01	M	Source
EF-S01	Poste SECU01 sous Kali Linux 2025 dédié à l'audit de sécurité	M	Source
EF-S02	Audit de vulnérabilités et rapport périodiques sur le périmètre autorisé	S	Préco
EF-S03	Sauvegarde et restauration de DC01, PARC01 et RFW01	S	Préco
EF-C01	Postes DIRECTEUR01, SECRETAIRE01 et WEBDEV01 sous Windows 11 Pro, adressage DHCP en VLAN 20	M	Source
EF-C02	Poste d'administration de Maria Bah (Windows 11 Pro) disposant des outils RSAT	M	Source

2.2 Besoins non fonctionnels

TABLEAU 2 — BESOINS NON FONCTIONNELS

DOMAINE	EXIGENCE	CRITÈRE DE VALIDATION
Sécurité	Moindre privilège, refus par défaut sur le pare-feu, comptes nominatifs, mots de passe conformes à la politique du chapitre 10	Tests T-S01 à T-S06 réussis

DOMAINE	EXIGENCE	CRITÈRE DE VALIDATION
Disponibilité	Services d'infrastructure (DNS, DHCP, AD, pare-feu) disponibles pendant les heures de bureau ; pas de haute disponibilité requise	Redémarrage complet de l'environnement en moins de 15 minutes, services opérationnels
Performance	Ouverture de session de domaine en moins de 60 secondes ; interface GLPI et Zabbix réactive (< 3 s par page)	Mesure lors de la recette
Capacité	Ressources cumulées de l'environnement couvertes par l'hôte (voir 4.1)	Hôte disposant d'au moins 20 % de marge
Maintenabilité	Systèmes mis à jour mensuellement ; configuration documentée ; scripts de création réutilisables	Procédures d'exploitation livrées
Sauvegarde	Sauvegarde quotidienne des configurations et bases ; test de restauration trimestriel	Restauration d'un élément réussie
Traçabilité	Journalisation des connexions (AD), des événements du pare-feu et des actions d'audit	Journaux consultables et conservés 6 mois (à valider)
Conformité	Données personnelles des utilisateurs limitées au strict nécessaire (identité, rôle, identifiant) conformément au RGPD	Registre de traitement simple tenu à jour
Compatibilité	Postes clients compatibles Windows 11 (TPM virtuel et démarrage sécurisé activés sur les VM)	Installation de Windows 11 réussie

CHAPITRE 3

3 Architecture réseau

3.1 Schéma de principe

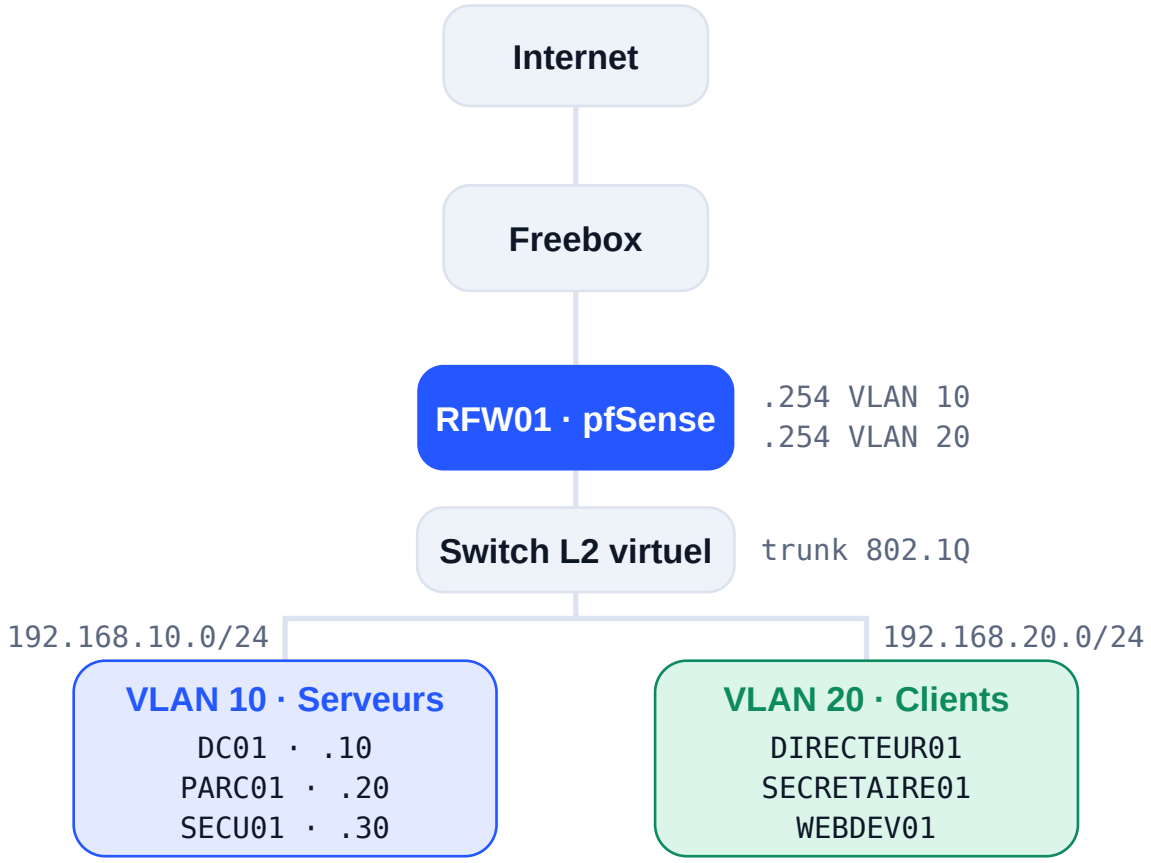


Figure 1 – Architecture réseau cible (schéma SIO1_1SI_v1)

Le trafic descendant suit la chaîne Internet → Freebox → RFW01 → switch L2 virtuel. Le switch distribue les deux VLAN : le VLAN 10 porte les serveurs (DC01, PARC01, SECU01) et le VLAN 20 porte les postes clients (DIRECTEUR01, SECRETAIRE01, WEBDEV01). Tout échange entre VLAN passe obligatoirement par RFW01, point unique de filtrage.

3.2 Plan d'adressage par VLAN

TABLEAU 3 – PARAMÈTRES DES VLAN

PARAMÈTRE	VLAN 10 – SERVEURS	VLAN 20 – CLIENTS
Identifiant 802.1Q	10	20
Réseau	192.168.10.0/24 (255.255.255.0)	192.168.20.0/24 (255.255.255.0)
Passerelle (RFW01)	192.168.10.254	192.168.20.254
Mode d'adressage	IP fixes de .1 à .99	DHCP de .100 à .253

PARAMÈTRE	VLAN 10 – SERVEURS	VLAN 20 – CLIENTS
Plage réservée	192.168.10.1 – .99 (serveurs)	192.168.20.1 – .99 (matériel réseau, réservations)
Serveur DNS fourni	192.168.10.10 (DC01) – saisie manuelle	192.168.20.x : option DHCP 192.168.10.10
Serveur DHCP	Aucun (IP statiques)	DC01 (192.168.10.10) via relais DHCP sur RFW01
Domaine DNS	martinscie.lan	martinscie.lan
Diffusion	192.168.10.255	192.168.20.255

3.3 Plan d'adressage détaillé

TABLEAU 4 – ADRESSAGE DES ÉQUIPEMENTS

ÉQUIPEMENT	VLAN	ADRESSE IP	MODE	RÔLE
Freebox	WAN	Adresse LAN de la box (à relever)	Fournie	Accès Internet. Vérifier que son réseau ne recouvre ni 192.168.10.0/24 ni 192.168.20.0/24
RFW01 – interface WAN	WAN	Attribuée par la Freebox (DHCP ou réservation)	DHCP	Sortie Internet, VPN
RFW01 – VLAN 10	10	192.168.10.254/24	Fixe	Passerelle serveurs
RFW01 – VLAN 20	20	192.168.20.254/24	Fixe	Passerelle clients
DC01	10	192.168.10.10/24	Fixe	AD, DNS, DHCP
PARC01	10	192.168.10.20/24	Fixe	GLPI, Zabbix
SECU01	10	192.168.10.30/24	Fixe	Audit Kali
DIRECTEUR01	20	192.168.20.100–.253	DHCP (réservation conseillée)	Poste du PDG

ÉQUIPEMENT	VLAN	ADRESSE IP	MODE	RÔLE
SECRETAIRE01	20	192.168.20.100–.253	DHCP (réservation conseillée)	Poste de la secrétaire
WEBDEV01	20	192.168.20.100–.253	DHCP (réservation conseillée)	Poste du développeur
Poste administrateur	20	192.168.20.100–.253	DHCP	Poste de Maria Bah

REMARQUE Le fichier des machines virtuelles indique des adresses de la forme « 192.16.x.254 / 192.168.x.1 / .2 / .3 ». Le schéma, plus précis, fixe x = 10 et attribue .10, .20 et .30. Le présent document retient les valeurs du schéma (voir chapitre 15).

3.4 Services réseau

TABLEAU 5 — SERVICES D'INFRASTRUCTURE

SERVICE	HÉBERGÉ SUR	DESCRIPTION ET PARAMÈTRES
Routage inter-VLAN	RFW01	Interfaces VLAN 10 et VLAN 20 sur le parent du trunk ; routage statique des réseaux connectés
NAT sortant	RFW01	NAT automatique ou hybride des deux sous-réseaux vers l'interface WAN
DNS	DC01	Zone martinscie.lan intégrée à l'AD ; redirecteurs 8.8.8.8 et 8.8.4.4 ; résolution inverse des deux sous-réseaux
DHCP	DC01	Étendue VLAN 20 (.100 à .253) ; options : routeur 192.168.20.254, DNS 192.168.10.10, domaine martinscie.lan ; bail 8 jours
Relais DHCP	RFW01	Service DHCP Relay sur l'interface VLAN 20 vers 192.168.10.10
VPN	RFW01	OpenVPN, authentification par certificat et compte AD (LDAP) ; réseau de tunnel dédié, par exemple 10.8.0.0/24
Proxy / filtrage	RFW01	Squid et module de filtrage d'URL pour le VLAN 20 ; catégories à bloquer définies avec la direction

SERVICE	HÉBERGÉ SUR	DESCRIPTION ET PARAMÈTRES
Synchronisation horaire	DC01 / RFW01	DC01 maître de temps du domaine (source NTP externe) ; RFW01 et PARC01 synchronisés sur DC01

3.5 Matrice de flux autorisés

Politique générale : **refus par défaut**, puis autorisation explicite des seuls flux nécessaires. Les règles sont évaluées de haut en bas sur l'interface d'entrée du trafic. Dans pfSense, la règle n° 4 (blocage) est donc placée **après** les règles n° 7 et 8, qui constituent des exceptions pour le poste d'administration et SECU01.

TABLEAU 6 — RÈGLES DE PARE-FEU CIBLES

N°	SOURCE	DESTINATION	SERVICES / PORTS	ACTION
1	VLAN 20	DC01	DNS 53 TCP/UDP, Kerberos 88, RPC 135, LDAP 389 TCP/UDP, SMB 445, kpasswd 464, LDAPS 636, catalogue global 3268/3269, RPC dynamiques 49152-65535	Autoriser
2	VLAN 20	PARC01	HTTP 80 et HTTPS 443 (GLPI) ; 10051/TCP (Zabbix, agents actifs)	Autoriser
3	VLAN 20	Internet	HTTP 80 / HTTPS 443 via proxy	Autoriser
4	VLAN 20	Autres hôtes du VLAN 10	Tous	Bloquer + journaliser
5	DC01, PARC01	Internet	80, 443 (mises à jour), 53, 123 (DNS, NTP)	Autoriser
6	PARC01	VLAN 20 et VLAN 10	Zabbix agent 10050/TCP, SNMP 161/UDP si besoin	Autoriser
7	Poste admin.	VLAN 10	RDP 3389, WinRM 5985/5986, SSH 22, HTTPS 443 (pfSense)	Autoriser (source restreinte)
8	SECU01	VLAN 10 et VLAN 20	Tous, pendant les fenêtres d'audit validées par la direction	Autoriser + journaliser
9	WAN	RFW01	OpenVPN UDP 1194 (redirection de port sur la Freebox)	Autoriser
10	Tout	Tout	Tout le reste	Bloquer

POINT D'ATTENTION RFW01 est placé derrière la Freebox (double NAT). Il faut donc (a) décocher « Block private networks » sur l'interface WAN de pfSense, puisque son adresse WAN est privée, et (b) rediriger UDP 1194 de la Freebox vers l'adresse WAN de RFW01 pour que le VPN soit joignable de l'extérieur.

3.6 Plateforme de virtualisation

Les fichiers sources ne désignent pas l'hyperviseur (le type d'invité « Debian 10 64 bits » mentionné pour Kali évoque une interface de type VirtualBox ou VMware Workstation). Le choix est laissé au maître d'œuvre, sous réserve de respecter les exigences suivantes :

- Prise en charge du marquage 802.1Q sur un port trunk vers RFW01, ou à défaut plusieurs cartes réseau virtuelles reliées à des réseaux internes distincts (une par VLAN) ;
- Prise en charge du TPM virtuel et du démarrage sécurisé pour Windows 11 ;
- Instantanés (snapshots) pour sécuriser les opérations de configuration ;
- Hôte physique d'au moins 8 cœurs, 32 Go de RAM et 500 Go de stockage SSD (voir 4.1).

CHAPITRE 4

4 Infrastructure virtuelle : fiches machines

4.1 Synthèse et dimensionnement

TABLEAU 7 — RESSOURCES PAR MACHINE VIRTUELLE

VM	SYSTÈME	RÔLE	VLAN	VCPU	RAM	DISQUE
RFW01	pfSense 2.x (FreeBSD)	Pare-feu / passerelle	10 et 20	1	1 Go	20 Go
DC01	Windows Server 2025	AD DS, DNS, DHCP	10	2	2 Go	60 Go
PARC01	Debian 12	GLPI, Zabbix	10	2	2 Go	30 Go
SECU01	Kali Linux 2025	Audit sécurité	10	2	2 Go	50 Go

VM	SYSTÈME	RÔLE	VLAN	VCPU	RAM	DISQUE
DIRECTEUR01	Windows 11 Pro 26H2	Poste direction	20	2	4 Go	60 Go
SECRETAIRE01	Windows 11 Pro 26H2	Poste secrétariat	20	2	4 Go	60 Go
WEBDEV01	Windows 11 Pro 26H2	Poste développement	20	2	4 Go	60 Go
Poste admin.	Windows 11 Pro 26H2	Poste administrateur	20	2	4 Go	60 Go
Total (7 VM)				**13**	**19 Go**	**340 Go**
Total (avec poste admin.)				**15**	**23 Go**	**400 Go**

Avec le poste d'administration, l'environnement réclame **15 vCPU, 23 Go de RAM et 400 Go de disque** (sans lui : 13 vCPU, 19 Go, 340 Go). Les disques peuvent être alloués dynamiquement ; il faut néanmoins prévoir la capacité maximale, ainsi que de la place pour les instantanés. D'où la recommandation d'un hôte de 8 cœurs, 32 Go de RAM et 500 Go de SSD, qui laisse une marge de 25 à 30 % pour l'hôte lui-même.

POINT D'ATTENTION Les 2 Go de RAM de DC01 correspondent à un minimum. Windows Server 2025 avec AD, DNS et DHCP fonctionnera, mais sera plus à l'aise à 4 Go. De même, 1 Go pour pfSense est juste si le proxy avec cache et le filtrage d'URL sont actifs : 2 Go sont conseillés.

4.2 RFW01 – Pare-feu pfSense

CARACTÉRISTIQUE	VALEUR
Système	pfSense 2.x sur FreeBSD (version exacte à préciser ; le fichier source indique « 2. »)
Ressources	1 vCPU, 1 Go de RAM, 20 Go de disque
Interfaces	WAN (vers Freebox) ; trunk 802.1Q portant VLAN 10 (192.168.10.254/24) et VLAN 20 (192.168.20.254/24)

CARACTÉRISTIQUE	VALEUR
DNS	192.168.10.10 (DC01), puis 8.8.8.8 et 8.8.4.4
Services	Passerelle LAN, NAT, règles de pare-feu, OpenVPN, proxy / filtrage
Comptes	admin (compte par défaut pfSense), administrateur, mbah

Exigences de configuration

- Assistant d'installation terminé, nom d'hôte RFW01, domaine martinscie.lan, fuseau Europe/Paris.
- Création des VLAN 10 et 20 sur l'interface parent du trunk ; affectation des interfaces et attribution des IP statiques.
- Désactivation du DHCP intégré de pfSense (le DHCP est porté par DC01) et activation du relais DHCP sur VLAN 20.
- Interface d'administration web en HTTPS uniquement, accessible depuis le poste d'administration seulement.
- Compte « admin » par défaut : mot de passe changé dès l'installation, puis désactivé au profit des comptes nominatifs si possible. Le compte « administrateur » est un compte générique : son usage est à justifier ou à supprimer (voir 10.2).
- Journalisation des règles de blocage ; export des journaux vers un stockage durable (syslog vers PARC01, à définir).

4.3 DC01 – Contrôleur de domaine

CARACTÉRISTIQUE	VALEUR
Système	Windows Server 2025
Ressources	2 vCPU, 2 Go de RAM, 60 Go de disque
Adresse	192.168.10.10/24, passerelle 192.168.10.254
DNS client	127.0.0.1 en préféré (DC01 se résout lui-même). 8.8.8.8 et 8.8.4.4 sont à placer en redirecteurs DNS, non comme DNS client
Rôles	Active Directory Domain Services, DNS, DHCP
Domaine	martinscie.lan (nouvelle forêt, niveau fonctionnel Windows Server 2025)

CARACTÉRISTIQUE	VALEUR
Étendue DHCP	VLAN 20 : 192.168.20.100 à 192.168.20.253, masque 255.255.255.0
Comptes	administrateur (compte intégré) et mbah

Exigences de configuration

- Nom NetBIOS MARTINSCIE ; chemin de la base AD, journaux et SYSVOL sur le disque système (60 Go suffisants pour ce volume).
- Zones DNS directe (martinscie.lan) et inverses (10.168.192 et 20.168.192) intégrées à l'annuaire, mises à jour dynamiques sécurisées.
- DHCP autorisé dans l'AD ; étendue VLAN 20 créée avec les options routeur (003), DNS (006) et nom de domaine (015).
- Sites et services AD : sous-réseaux 192.168.10.0/24 et 192.168.20.0/24 déclarés dans le site par défaut.
- Compte « administrateur » intégré renommé ou fortement protégé ; son usage courant est interdit.
- Sauvegarde de l'état du système planifiée (voir chapitre 10).

REMARQUE Le fichier source nomme une machine « DC01/DC02 » pour le poste de Maria Bah. Un seul contrôleur de domaine (DC01) figure dans le schéma ; ce document considère DC02 comme une mention de réserve et traite le poste de Maria Bah comme un poste d'administration (chapitre 15).

4.4 PARC01 – Serveur de gestion de parc et de supervision

CARACTÉRISTIQUE	VALEUR
Système	Linux Debian 12
Ressources	2 vCPU, 2 Go de RAM, 30 Go de disque
Adresse	192.168.10.20/24, passerelle 192.168.10.254, DNS 192.168.10.10
Services	GLPI 10, Zabbix Server 5, Apache 2, MariaDB Server 10, PHP 8.1, serveur SSH
Comptes	root, glpi, Admin (compte de l'interface Zabbix), mbah, administrateur

Exigences de configuration

- Deux bases MariaDB distinctes (glpidb et zabbix) avec un utilisateur applicatif dédié par base et des droits limités à sa base.
- Apache 2 en HTTPS avec un certificat (autosigné au minimum, idéalement émis par une autorité interne) ; deux hôtes virtuels ou deux chemins : /glpi et /zabbix.
- PHP 8.1 avec les extensions requises par GLPI 10 (curl, gd, intl, mysqli, mbstring, xml, zip, bcmath, opcache, ldap) et par Zabbix (gd, bcmath, mbstring, xml, ldap).
- GLPI : suppression des fichiers d'installation après déploiement, changement des mots de passe des comptes par défaut (glpi, tech, normal, post-only), authentification par l'AD (LDAP) activée.
- Zabbix : changement du mot de passe du compte Admin par défaut ; agents installés sur tous les hôtes supervisés.
- SSH : connexion directe de root interdite (PermitRootLogin no), connexion par clé pour les administrateurs, accès limité au poste d'administration.

POINT D'ATTENTION Zabbix 5.0 est une branche ancienne dont le support de l'éditeur est terminé, et dont les paquets ne sont pas fournis pour Debian 12. De même, Debian 12 embarque PHP 8.2 par défaut : PHP 8.1 nécessite un dépôt tiers. Il est donc recommandé de valider avec le commanditaire le choix d'une version LTS à jour (Zabbix 6.0 ou 7.0 LTS) ; la suite du document reste valable pour toutes ces versions.

4.5 SECU01 – Poste d'audit de sécurité

CARACTÉRISTIQUE	VALEUR
Système	Kali Linux 2025 (invité de type « Linux Debian 10 64 bits »)
Ressources	2 vCPU, 2 Go de RAM, 50 Go de disque
Adresse	192.168.10.30/24 (fixe, VLAN 10), passerelle 192.168.10.254
Services / outils	Distribution Kali : nmap, Wireshark, Metasploit Framework, Nikto, Hydra, OpenVAS / Greenbone, entre autres
Comptes	kali (compte par défaut), hnyame

Exigences de configuration et d'usage

- Compte « kali » par défaut : mot de passe changé, puis compte désactivé ou supprimé ; usage exclusif du compte hnyame.

- Aucun test hors du périmètre défini : seules les machines de l'environnement Martins & Cie sont ciblées, et jamais Internet.
- Chaque campagne d'audit fait l'objet d'une autorisation écrite de la direction (date, périmètre, nature des tests) et d'un rapport.
- Règle de pare-feu n° 8 limitée dans le temps ; les journaux de RFW01 conservent la trace des actions.
- Disque chiffré et instantané conservé avant chaque campagne pour revenir à un état sain.

4.6 Postes clients Windows 11

TABLEAU 8 — POSTES CLIENTS

POSTE	UTILISATEUR	RÔLE	RESSOURCES	PARTICULARITÉS
DIRECTEUR01	smartins	PDG	2 vCPU, 4 Go, 60 Go	Serge Martins est administrateur local de ce poste uniquement (GPO « Groupes restreints »)
SECRETAIRE01	ldasilva	Secrétaire	2 vCPU, 4 Go, 60 Go	Lecteur Secrétariat en lecture-écriture ; bureautique
WEBDEV01	cgrimeau	Développeur web	2 vCPU, 4 Go, 60 Go	Lecteur Développement web en lecture-écriture ; outils de développement (voir note ci-dessous)
Poste administrateur	mbah	Administratrice système et réseau	2 vCPU, 4 Go, 60 Go	RSAT (outils AD, DNS, DHCP, GPO), client SSH, navigateur pour pfSense, GLPI, Zabbix

REMARQUE Le schéma indique « WEBDEV01 – Linux · Développement » tandis que le fichier des machines décrit « DEVWEB01 – Windows 11 Pro 26H2 ». Ce document retient le nom du schéma (WEBDEV01) et le système du fichier de spécifications (Windows 11 Pro), indispensable à l'application des GPO. À confirmer (chapitre 15).

Socle commun des postes

- Windows 11 Pro 26H2, TPM virtuel et démarrage sécurisé activés, chiffrement BitLocker recommandé.
- Nom de machine conforme à la convention (voir 5.5), IP en DHCP, jonction au domaine martinscie.lan.
- Pare-feu Windows actif, Windows Update géré par GPO, Microsoft Defender actif.
- Agent Zabbix et agent GLPI (inventaire) installés et configurés pour contacter PARC01.
- Raccourci vers le portail de support GLPI sur le bureau.

CHAPITRE 5

5 Active Directory et gestion des identités

5.1 Domaine

PARAMÈTRE	VALEUR
Nom DNS du domaine	martinscie.lan
Nom NetBIOS	MARTINSCIE
Racine LDAP	DC=martinscie,DC=lan
Contrôleur de domaine	DC01 (192.168.10.10)
Nombre de forêts / domaines	1 / 1
Suffixe UPN	@martinscie.lan

5.2 Structure des unités d'organisation

```
DC=martinscie,DC=lan
├── OU=Utilisateurs comptes des 5 collaborateurs
├── OU=Groupes groupes de sécurité métier
└── OU=Ordinateurs [Préco] comptes machines des postes clients
```

Les deux premières unités d'organisation sont celles des fichiers sources (chemins « OU=Utilisateurs, DC=martinscie, DC=lan » et « OU=Groupes, DC=martinscie, DC=lan »). L'unité Ordinateurs est ajoutée afin d'y appliquer les GPO propres aux postes sans toucher

au conteneur Computers par défaut ; la commande redircmp permet d'y rediriger les nouvelles jonctions.

5.3 Comptes utilisateurs

TABLEAU 9 — COMPTES UTILISATEURS

IDENTIFIANT	PRÉNOM NOM	MACHINE	RÔLE	OU
mbah	Maria Bah	Poste admin. ; accès aux serveurs DC01 et PARC01	Administratrice système et réseau	OU=Utilisateurs
smartins	Serge Martins	DIRECTEUR01	PDG et administrateur local	OU=Utilisateurs
ldasilva	Léon Dasilva	SECRETAIRE01	Secrétaire	OU=Utilisateurs
cgrimeau	Corentin Grimeau	WEBDEV01	Développeur web	OU=Utilisateurs
hnyame	Hervé Nyame	SECU01	Expert cybersécurité	OU=Utilisateurs

Règles de création : identifiant = initiale du prénom + nom en minuscules ; UPN identifiant@martinscie.lan ; compte activé ; **changement de mot de passe obligatoire à la première connexion** (EF-A07). Les mots de passe initiaux et définitifs figurent dans le fichier utilisateurs.xlsx ; ils sont volontairement omis de ce document (voir 10.1).

5.4 Groupes de sécurité

TABLEAU 10 — GROUPES

GROUPE	MEMBRE	RÔLE DU GROUPE	EMPLACEMENT
Administration	mbah	Gestion du dossier Administration et administration métier	OU=Groupes
administrateurs	mbah	Administration locale des serveurs (voir remarque)	OU=Groupes selon la source
Admin de Domaine	mbah	Administration du domaine (voir remarque)	OU=Groupes selon la source
Direction	smartins	Dossier Direction	OU=Groupes

GROUPE	MEMBRE	RÔLE DU GROUPE	EMPLACEMENT
Secrétariat	ldasilva	Dossier Secrétariat	OU=Groupes
Développement web	cgrimeau	Dossier Développement web	OU=Groupes
Sécurité	hnyame	Dossier Sécurité	OU=Groupes

POINT D'ATTENTION « administrateurs » et « Admin de Domaine » correspondent aux groupes intégrés de Windows (Administrateurs et Admins du domaine). Un groupe de même nom ne peut pas être recréé dans OU=Groupes : le nom (sAMAccountName) est unique dans le domaine. La mise en œuvre consiste donc à ajouter mbah à ces groupes intégrés. Comme ils sont très privilégiés, il est préférable d'utiliser pour ces tâches un compte d'administration distinct (par exemple mbah-adm) et de laisser mbah comme compte courant (voir 10.2).

5.5 Conventions de nommage

OBJET	CONVENTION	EXEMPLES
Identifiant utilisateur	initiale du prénom + nom, minuscules, sans accent ni espace	mbah, smartins, hnyame
Poste client	FONCTION + numéro à deux chiffres, majuscules	DIRECTEUR01, SECRETAIRE01, WEBDEV01
Serveur	FONCTION courte + numéro	DC01, PARC01, SECU01, RFW01
Groupe métier	Nom du service	Direction, Secrétariat
Groupe d'accès [Préco]	GL_<Dossier>_<LE|L> (groupe local de domaine : lecture-écriture ou lecture)	GL_Direction_LE, GL_Securite_L

5.6 Stratégies de groupe (GPO) recommandées

TABLEAU 11 — GPO

GPO	CIBLE	PARAMÈTRES
GPO-Politique-MotDePasse	Domaine (politique par défaut)	Longueur minimale 12, complexité activée, historique 12, durée max 90 jours, verrouillage après 5 échecs pendant 15 minutes

GPO	CIBLE	PARAMÈTRES
GPO-Postes-Securite	OU Ordinateurs	Pare-feu Windows actif, Defender actif, écran de veille verrouillé après 10 min, Windows Update planifié
GPO-Lecteurs-Reseau	OU Utilisateurs (filtrage par groupe)	Montage des partages selon l'appartenance : lettre unique par dossier
GPO-Admin-Local-Direction	DIRECTEUR01	Groupes restreints : smartins membre des administrateurs locaux de ce poste uniquement
GPO-RSAT-Admin	Poste administrateur	Autorise RDP et WinRM depuis le VLAN 20 pour mbah uniquement
GPO-Audit	Domaine / serveurs	Audit des ouvertures de session, de la gestion des comptes et des accès aux objets sensibles

CHAPITRE 6

6 Gestion des droits d'accès aux répertoires

6.1 Principes

- Trois niveaux de droit : **Pas d'accès**, **Lecture**, **Lecture/écriture**.
- Chaque répertoire a un propriétaire fonctionnel qui seul y écrit ; les autres collaborateurs sont soit en lecture, soit sans accès, selon la sensibilité.
- Le PDG (smartins), l'administratrice (mbah) et l'expert cybersécurité (hnyame) disposent d'un droit de lecture sur tous les répertoires : pilotage pour le premier, administration et audit pour les deux autres.
- Le développeur (cgrimeau) n'a accès qu'à son propre répertoire ; la secrétaire (ldasilva) n'accède qu'à Secrétariat et à Direction en lecture.

6.2 Matrice des droits

TABLEAU 12 — MATRICE DES DROITS (AUCUN = PAS D'ACCÈS ; L = LECTURE ; L/E = LECTURE ET ÉCRITURE)

RÉPERTOIRE	CGRIMEAU	LDASILVA	SMARTINS	MBAH	HNYAME
Direction	Aucun	L	L/E	L	L

RÉPERTOIRE	CGRIMEAU	LDASILVA	SMARTINS	MBAH	HNYAME
Administration	Aucun	Aucun	L	L/E	L
Secrétariat	Aucun	L/E	L	L	L
Sécurité	Aucun	Aucun	L	L	L/E
Développement web	L/E	Aucun	L	L	L

Lecture de la matrice : chaque ligne est un répertoire et chaque colonne un utilisateur. Chaque dossier compte exactement un utilisateur en lecture/écriture, son propriétaire fonctionnel.

REMARQUE Dans la source, le droit de « Direction » pour la secrétaire est écrit « dasilva » (sans « l »), alors que le compte est ldasilva. Il est interprété comme ldasilva, qui reçoit donc un accès en lecture au dossier Direction. Ce choix est à confirmer par le PDG, car un accès d'une secrétaire au dossier de la direction est inhabituel (chapitre 15).

6.3 Synthèse par utilisateur

TABLEAU 13 — DROITS PAR UTILISATEUR

UTILISATEUR	LECTURE / ÉCRITURE	LECTURE SEULE	AUCUN ACCÈS
cgrimeau (développeur)	Développement web	–	Direction, Administration, Secrétariat, Sécurité
ldasilva (secrétaire)	Secrétariat	Direction	Administration, Sécurité, Développement web
smartins (PDG)	Direction	Administration, Secrétariat, Sécurité, Développement web	–
mbah (admin.)	Administration	Direction, Secrétariat, Sécurité, Développement web	–
hnyame (cybersécurité)	Sécurité	Direction, Administration, Secrétariat, Développement web	–

6.4 Mise en œuvre technique (modèle AGDLP)

Pour éviter d'attribuer des droits compte par compte, la matrice est traduite en groupes d'accès. Les comptes utilisateurs sont placés dans des groupes globaux (les groupes métier du chapitre 5), eux-mêmes membres de groupes locaux de domaine qui portent les permissions NTFS et de partage.

- **A** (Accounts) : les comptes sont membres des groupes globaux métier ;
- **G** (Global) : groupes Direction, Administration, Secrétariat, Sécurité, Développement web ;
- **DL** (Domain Local) : deux groupes par dossier, GL_<Dossier>_LE et GL_<Dossier>_L ;
- **P** (Permissions) : les groupes locaux de domaine reçoivent les droits NTFS Modification (LE) ou Lecture et exécution (L) sur le dossier.

TABLEAU 14 — GROUPES D'ACCÈS PAR DOSSIER

DOSSIER	GROUPE LE (LECTURE/ÉCRITURE)	GROUPE L (LECTURE)	AUCUN ACCÈS
Direction	GL_Direction_LE ← smartins	GL_Direction_L ← mbah, hnyame, ldasilva	cgrimeau
Administration	GL_Administration_LE ← mbah	GL_Administration_L ← smartins, hnyame	cgrimeau, ldasilva
Secrétariat	GL_Secretariat_LE ← ldasilva	GL_Secretariat_L ← mbah, smartins, hnyame	cgrimeau
Sécurité	GL_Securite_LE ← hnyame	GL_Securite_L ← mbah, smartins	cgrimeau, ldasilva
Développement web	GL_DevWeb_LE ← cgrimeau	GL_DevWeb_L ← mbah, smartins, hnyame	ldasilva

- Héritage désactivé à la racine de chaque dossier ; seuls les groupes ci-dessus, SYSTEM et Admins du domaine figurent dans les ACL.
- Le groupe « Utilisateurs authentifiés » et « Tout le monde » ne figurent dans aucune ACL ; le partage SMB accorde « Contrôle total » aux groupes et c'est la couche NTFS qui restreint.
- Énumération basée sur l'accès (Access-Based Enumeration) activée : un utilisateur ne voit que les dossiers auxquels il a accès.

- Hébergement : le fichier des machines n'indique pas de serveur de fichiers. Les partages sont prévus sur DC01 (volume de données dédié, ajouté au besoin) à l'emplacement D:\Partages, sauf décision contraire. L'hébergement des données sur un contrôleur de domaine est toléré dans ce contexte réduit mais déconseillé en production : un serveur de fichiers dédié (FS01) est alors à prévoir.

6.5 Exemple de script de mise en place

Copier

```
# À exécuter sur DC01 avec un compte administrateur du domaine
$racine = "D:\Partages"
$dossiers = @{
"Direction" = @{LE="GL_Direction_LE"; L="GL_Direction_L"}
"Administration" = @{LE="GL_Administration_LE"; L="GL_Administration_L"}
"Secrétariat" = @{LE="GL_Secretariat_LE"; L="GL_Secretariat_L"}
"Sécurité" = @{LE="GL_Securite_LE"; L="GL_Securite_L"}
"Développement web" = @{LE="GL_DevWeb_LE"; L="GL_DevWeb_L"}
}
foreach ($d in $dossiers.Keys) {
$chemin = Join-Path $racine $d
New-Item -ItemType Directory -Path $chemin -Force | Out-Null
$acl = Get-Acl $chemin
$acl.SetAccessRuleProtection($true, $false) # coupe l'héritage
foreach ($id in "NT AUTHORITY\SYSTEM", "MARTINSCIE\Admins du domaine") {
$acl.AddAccessRule((New-Object Security.AccessControl.FileSystemAccessRule($id,"FullCo
}
$acl.AddAccessRule((New-Object Security.AccessControl.FileSystemAccessRule("MARTINSCIE
$acl.AddAccessRule((New-Object Security.AccessControl.FileSystemAccessRule("MARTINSCIE
Set-Acl $chemin $acl
New-SmbShare -Name $d -Path $chemin -FullAccess "MARTINSCIE\Utilisateurs du domaine" -
}
```

CHAPITRE 7

7 Gestion de parc, support et supervision (PARC01)

7.1 GLPI 10

TABLEAU 15 — EXIGENCES GLPI

FONCTION	EXIGENCE DÉTAILLÉE
Inventaire	Agent GLPI sur chaque poste et serveur Windows ; inventaire matériel (CPU, RAM, disque), logiciels installés, utilisateur connecté, adresse IP

FONCTION	EXIGENCE DÉTAILLÉE
Entités et lieux	Une entité Martins & Cie ; lieux et services correspondant aux répertoires (Direction, Secrétariat, etc.)
Utilisateurs	Importation des comptes depuis l'AD (LDAP) ; profils : Super-Admin (mbah), Technicien (mbah), Self-Service (autres) ; hnyame en lecture des tickets de sécurité
Helpdesk	Création de tickets par les utilisateurs depuis le portail ; catégories Incident, Demande, Sécurité ; urgence, impact et priorité ; suivis et solutions
Niveaux de service	Prise en compte sous 4 h ouvrées et résolution cible sous 2 jours ouvrés pour une priorité normale (valeurs à valider)
Notifications	Courriel ou ticket pour les créations, assignations et clôtures ; nécessite un relais de messagerie (SMTP) à fournir
Base de connaissances	Articles de procédure (mot de passe, VPN, accès aux dossiers) accessibles aux utilisateurs
Sécurité GLPI	HTTPS, comptes par défaut changés, fichier install supprimé, droits restreints sur /files

7.2 Zabbix

TABLEAU 16 — EXIGENCES ZABBIX

FONCTION	EXIGENCE DÉTAILLÉE
Hôtes supervisés	RFW01, DC01, PARC01, SECU01 et les 4 postes Windows 11 (8 hôtes)
Éléments surveillés	Disponibilité (ping), CPU, mémoire, espace disque, trafic réseau, services critiques (AD DS, DNS, DHCP sur DC01 ; apache2 et mariadb sur PARC01)
Modèles	Windows by Zabbix agent, Linux by Zabbix agent, pfSense par SNMP, ICMP Ping
Déclencheurs	Hôte injoignable > 3 min ; disque > 85 % ; CPU > 90 % pendant 10 min ; service arrêté ; certificat proche d'expiration
Alertes	Notification par courriel à mbah ; sévérité Haute et Désastre en priorité
Tableaux de bord	Vue d'ensemble de l'infrastructure : état des VM, services, alertes en cours

FONCTION	EXIGENCE DÉTAILLÉE
Rétention	Historique 30 jours, tendances 1 an (à ajuster selon l'espace disque de 30 Go)

7.3 Socle applicatif

- Apache 2 sert GLPI et l'interface web de Zabbix ; modules rewrite, ssl et headers activés ; ServerTokens Prod.
- MariaDB 10 : mysql_secure_installation exécuté, accès réseau limité à localhost (bind-address = 127.0.0.1), jeu de caractères utf8mb4.
- PHP : paramètres de production (display_errors=Off, date.timezone=Europe/Paris, memory_limit ≥ 256M, max_execution_time ≥ 300 pour Zabbix).
- Mises à jour de sécurité Debian automatiques (unattended-upgrades).

CHAPITRE 8

8 Pare-feu et accès distant (RFW01)

8.1 Interfaces

TABLEAU 17 — INTERFACES PFSENSE

INTERFACE	TYPE	ADRESSE	REMARQUES
WAN	Ethernet	DHCP depuis la Freebox	Désactiver « Block private networks » (double NAT) ; garder « Block bogon networks »
VLAN10 (SRV)	VLAN 802.1Q, ID 10	192.168.10.254/24	Passerelle des serveurs
VLAN20 (CLI)	VLAN 802.1Q, ID 20	192.168.20.254/24	Passerelle des clients ; relais DHCP actif

8.2 NAT et règles

- NAT sortant : mode automatique ou hybride, pour 192.168.10.0/24 et 192.168.20.0/24 vers l'interface WAN.
- Règles par interface conformes à la matrice du tableau 6 ; règle finale « Bloquer tout » avec journalisation.

- Alias pfSense pour DC01, PARC01, SECU01, poste administrateur et ports AD, afin que les règles restent lisibles.
- Aucune règle « Tout autoriser » laissée active après les tests.

8.3 OpenVPN

PARAMÈTRE	VALEUR
Mode	Accès distant (utilisateurs), SSL/TLS avec authentification par certificat et par compte AD (LDAP)
Protocole / port	UDP 1194, redirigé depuis la Freebox vers RFW01
Réseau de tunnel	10.8.0.0/24 (exemple, hors des plages LAN)
Réseaux accessibles	VLAN 10 pour l'administration (mbah) ; accès limité par règle sur l'interface OpenVPN
DNS poussé	192.168.10.10, domaine martinscie.lan
Autorité de certification	CA interne pfSense ; certificats serveur et un certificat par utilisateur autorisé ; révocation prévue
Utilisateurs autorisés	mbah (obligatoire) ; autres sur décision de la direction
Durcissement	TLS ≥ 1.2, chiffrement AES-256-GCM, tls-auth ou tls-crypt activé, délai d'inactivité et expiration des certificats

8.4 Proxy et filtrage

- Squid en mode transparent ou explicite sur l'interface VLAN 20 ; cache modeste (quelques Go) pour tenir dans les 20 Go de disque.
- Filtrage d'URL par catégories (adulte, malware, hameçonnage, jeux d'argent, etc.) et liste d'exceptions gérée par mbah.
- Si le filtrage HTTPS est activé, la CA interne est déployée sur les postes par GPO ; sinon le filtrage se limite aux noms de domaine.
- Journaux d'accès consultables par mbah et hnyame.

8.5 Administration et sauvegarde

- Interface web accessible uniquement depuis le poste d'administration, en HTTPS, avec délai de session court.
- Export automatique de la configuration (config.xml) après chaque modification importante, stocké hors de RFW01.
- Mises à jour de pfSense planifiées après sauvegarde et instantané de la VM.

CHAPITRE 9

9 Mise en œuvre DNS et DHCP (DC01)

9.1 Étendue DHCP

TABLEAU 18 — ÉTENDUE DHCP

PARAMÈTRE	VALEUR
Nom de l'étendue	VLAN20-Clients
Plage	192.168.20.100 à 192.168.20.253
Masque	255.255.255.0
Routeur (option 003)	192.168.20.254
Serveur DNS (option 006)	192.168.10.10
Nom de domaine (option 015)	martinscie.lan
Durée du bail	8 jours
Exclusions	Aucune dans la plage ; les adresses .1 à .99 restent hors plage pour les réservations
Réservations [Préco]	DIRECTEUR01, SECRETAIRE01, WEBDEV01 et poste administrateur, par adresse MAC

REMARQUE Le fichier des machines mentionnait une étendue « de .50 à .200 », sans VLAN. Le schéma précise « .100 à .253 » pour le VLAN 20 ; cette dernière valeur est retenue (chapitre 15).

9.2 Exemple de commandes

```
# DHCP : étendue VLAN 20
Add-DhcpServerv4Scope -Name "VLAN20-Clients" -StartRange 192.168.20.100 -EndRange 192.
-SubnetMask 255.255.255.0 -LeaseDuration 8.00:00:00 -State Active
Set-DhcpServerv4OptionValue -ScopeId 192.168.20.0 -Router 192.168.20.254 `
-DnsServer 192.168.10.10 -DnsDomain martinscie.lan
Add-DhcpServerInDC -DnsName dc01.martinscie.lan -IPAddress 192.168.10.10
# DNS : redirecteurs et zones inverses
Set-DnsServerForwarder -IPAddress 8.8.8.8, 8.8.4.4
Add-DnsServerPrimaryZone -NetworkId "192.168.10.0/24" -ReplicationScope Domain
Add-DnsServerPrimaryZone -NetworkId "192.168.20.0/24" -ReplicationScope Domain
```

Copier

9.3 Création des OU, comptes et groupes

```
Import-Module ActiveDirectory
$base = "DC=martinscie,DC=lan"
"Utilisateurs","Groupes","Ordinateurs" | ForEach-Object { New-ADOrganizationalUnit -Na
$users = @(
@{Id="mbah"; Prenom="Maria"; Nom="Bah"},
@{Id="smartins"; Prenom="Serge"; Nom="Martins"},
@{Id="ldasilva"; Prenom="Léon"; Nom="Dasilva"},
@{Id="cgrimeau"; Prenom="Corentin"; Nom="Grimeau"},
@{Id="hnyame"; Prenom="Hervé"; Nom="Nyame"}
)
foreach ($u in $users) {
$mdp = Read-Host "Mot de passe initial pour $($u.Id)" -AsSecureString # jamais en clai
New-ADUser -Name "$($u.Prenom) $($u.Nom)" -GivenName $u.Prenom -Surname $u.Nom `
-SamAccountName $u.Id -UserPrincipalName "$($u.Id)@martinscie.lan" `
-Path "OU=Utilisateurs,$base" -AccountPassword $mdp -Enabled $true -ChangePasswordAtLo
}
# Groupes métier (globaux)
"Administration","Direction","Secrétariat","Développement web","Sécurité" | ForEach-Ob
New-ADGroup -Name $_ -GroupScope Global -GroupCategory Security -Path "OU=Groupes,$bas
Add-ADGroupMember "Administration" mbah
Add-ADGroupMember "Direction" smartins
Add-ADGroupMember "Secrétariat" ldasilva
Add-ADGroupMember "Développement web" cgrimeau
Add-ADGroupMember "Sécurité" hnyame
# Groupes intégrés d'administration (mbah)
Add-ADGroupMember "Admins du domaine" mbah
Add-ADGroupMember "Administrateurs" mbah
```

Copier

CHAPITRE 10

10 Sécurité

10.1 Gestion des mots de passe

Le fichier utilisateurs.xlsx contient, en clair, un mot de passe de première connexion commun à tous (identique pour les cinq comptes) et un mot de passe définitif construit sur le même modèle, prévisible. Cette pratique est contraire aux bonnes pratiques de sécurité : un mot de passe partagé, prévisible et stocké en clair compromet tous les comptes à la fois. Ce cahier des charges impose donc :

- **Aucun mot de passe en clair** dans un document, un script ou un fichier partagé ; le fichier utilisateurs.xlsx est retiré des supports partagés après la création des comptes.
- **Mots de passe initiaux uniques** par compte, générés aléatoirement et transmis par un canal distinct, avec changement obligatoire à la première connexion (EF-A07).
- Politique de domaine : 12 caractères minimum, complexité, historique de 12 mots de passe, expiration à 90 jours (ou phrase de passe longue sans expiration forcée), verrouillage après 5 échecs.
- Les mots de passe actuellement consignés dans utilisateurs.xlsx sont à considérer comme **compromis** et à remplacer avant toute mise en service.
- Un gestionnaire de mots de passe est recommandé pour les comptes de service et d'administration.

10.2 Comptes à privilèges

TABLEAU 19 — COMPTES À PRIVILÈGES

CONSTAT DANS LES SOURCES	RISQUE	EXIGENCE
Compte générique « administrateur » présent sur RFW01, DC01 et PARC01	Actions non attribuables à une personne	Désactiver ou renommer ; utiliser des comptes nominatifs ; si conservé, mot de passe fort, usage tracé
mbah utilisé pour toutes les tâches (courantes et d'administration) sur plusieurs systèmes	Compromission du poste = compromission du domaine	Séparer un compte courant (mbah) et un compte d'administration (par ex. mbah-adm)
root sur PARC01	Cible privilégiée des attaques SSH	Interdire la connexion SSH de root ; sudo pour mbah
Comptes par défaut : admin (pfSense), Admin (Zabbix), glpi (GLPI), kali (Kali)	Identifiants connus publiquement	Changer le mot de passe à l'installation, désactiver si inutilisé

CONSTAT DANS LES SOURCES	RISQUE	EXIGENCE
smartins administrateur local de DIRECTEUR01	Un poste de direction ciblé par l'hameçonnage devient critique	Limiter à ce poste ; privilégier une élévation à la demande ; protection renforcée du poste

10.3 Durcissement des systèmes

TABLEAU 20 — DURCISSEMENT

SYSTÈME	MESURES
RFW01	Administration web limitée au poste d'administration, mises à jour, journalisation, sauvegarde de config.xml
DC01	Mises à jour mensuelles, pare-feu Windows actif, signature SMB, désactivation de SMBv1 et de NTLMv1, protection du compte administrateur intégré, audit avancé
PARC01	SSH par clé, pare-feu local (ufw ou nftables) limitant les ports 22, 80, 443, 10051 aux sources autorisées, fail2ban, mises à jour automatiques de sécurité
Postes Windows	BitLocker, Defender, pare-feu actif, droits d'utilisateur standard (hors smartins sur son poste), exécution de macros limitée, Windows Update par GPO
SECU01	Isolé par règles de pare-feu hors audit, chiffrement du disque, instantané avant chaque campagne, aucun stockage de données client non chiffré

10.4 Sauvegarde et restauration

TABLEAU 21 — SAUVEGARDES

ÉLÉMENT	MÉTHODE	FRÉQUENCE	RÉTENTION
DC01 (AD, DNS, DHCP)	Sauvegarde de l'état du système (Windows Server Backup) + export de la configuration DHCP	Quotidienne	14 jours
Partages de fichiers	Sauvegarde des volumes de données avec conservation des ACL	Quotidienne	30 jours
PARC01	Dump mariadb des bases glpidb et zabbix, archive de /etc et des fichiers GLPI	Quotidienne	14 jours
RFW01	Export config.xml	À chaque changement	10 versions

ÉLÉMENT	MÉTHODE	FRÉQUENCE	RÉTENTION
Machines virtuelles	Instantané avant toute opération majeure ; export complet mensuel	Mensuelle	3 exports

Règle 3-2-1 recommandée : trois copies, sur deux supports différents, dont une hors de l'hôte. Un test de restauration est réalisé à chaque trimestre et consigné.

10.5 Journalisation et supervision de la sécurité

- Audit AD : ouvertures de session, verrouillages, modifications de groupes et d'utilisateurs, accès refusés aux partages.
- Journaux du pare-feu : blocages, VPN, activité du filtrage web ; envoi syslog vers PARC01.
- Revue mensuelle des événements critiques par mbah et hnyame.
- Durée de conservation à confirmer en fonction des obligations légales applicables (à valider avec le commanditaire).

10.6 Cadre d'utilisation du poste SECU01

- Utilisation strictement réservée à l'expert cybersécurité sur des cibles autorisées par écrit.
- Les résultats (vulnérabilités, preuves) sont confidentiels, stockés dans le dossier Sécurité (accès hnyame en écriture, mbah et smartins en lecture).
- Toute découverte critique est signalée sans délai à mbah et à la direction.

CHAPITRE 11

11 Plan de déploiement

11.1 Phases et livrables

TABLEAU 22 — PHASES DU DÉPLOIEMENT

PHASE	TRAVAUX	PRÉREQUIS	LIVRABLE	DURÉE EST.
0. Préparation	Validation du cahier des charges, choix de l'hyperviseur, vérification	–	CDC validé	1 jour

PHASE	TRAVAUX	PRÉREQUIS	LIVRABLE	DURÉE EST.
	des ressources et des licences, résolution des points du chapitre 15			
1. Socle virtuel	Réseaux virtuels, trunk 802.1Q, modèles de VM	Phase 0	Hyperviseur opérationnel	1 jour
2. Pare-feu	Installation de RFW01, VLAN, NAT, règles minimales, accès Internet	Phase 1	Sortie Internet des 2 VLAN	1 jour
3. Annuaire	DC01 : AD DS, DNS, DHCP, OU, comptes, groupes ; relais DHCP	Phase 2	Domaine fonctionnel	2 jours
4. Parc et supervision	PARC01 : Debian, Apache, MariaDB, PHP, GLPI, Zabbix	Phase 3	GLPI et Zabbix accessibles	2 jours
5. Postes	Installation des Windows 11, jonction au domaine, agents GLPI et Zabbix	Phases 3 et 4	4 postes intégrés	2 jours
6. Données et droits	Dossiers, groupes d'accès, ACL, GPO, lecteurs réseau	Phase 5	Droits conformes à la matrice	2 jours
7. Sécurité	SECU01, règles finales du pare-feu, OpenVPN, proxy, durcissement, sauvegardes	Phase 6	Sécurité en place	3 jours
8. Recette	Exécution du plan de tests, correction des écarts	Phase 7	PV de recette	2 jours
9. Documentation	Dossier d'exploitation, procédures, schéma à jour, passation	Phase 8	Dossier final	1 jour

La durée totale estimée est d'environ **17 jours ouvrés** pour une personne ; ces durées sont indicatives et à ajuster selon l'expérience de l'équipe. Les instantanés sont pris à la fin de chaque phase pour permettre un retour arrière.

11.2 Ordre de démarrage de l'environnement

1. Hôte de virtualisation et réseaux virtuels ;

2. RFW01 (routage, NAT) ;

3. DC01 (DNS, AD, DHCP) : attendre que les services soient démarrés ;

4. PARC01 ;

5. SECU01 (si une campagne est prévue) ;

6. Postes clients.

L'arrêt s'effectue dans l'ordre inverse.

CHAPITRE 12

12 Plan de tests et recette

La recette est prononcée par M. Martins sur la base de ce plan. Chaque test renvoie à un ou plusieurs besoins du chapitre 2.

TABLEAU 23 — PLAN DE TESTS

TEST	BESOIN(S)	PROCÉDURE	RÉSULTAT ATTENDU
T-R01	EF-R01, R07	Depuis DC01 puis un poste client, afficher la configuration IP	DC01 en 192.168.10.10, poste en 192.168.20.x, chacun dans son VLAN
T-R02	EF-R02	Depuis un poste client, ping de 192.168.20.254, puis de 192.168.10.254	Les deux passerelles répondent
T-R03	EF-R03	Depuis un poste client et depuis DC01, ouvrir un site Internet	Accès réussi
T-R04	EF-R04	Depuis un poste client, tenter une connexion RDP vers DC01 et SSH vers PARC01	Connexions refusées et journalisées
T-R05	EF-R05	Établir un VPN depuis l'extérieur avec le compte mbah	Tunnel établi, accès au VLAN 10 ; autre compte refusé
T-R06	EF-R06	Accéder à une URL d'une catégorie bloquée	Page de blocage affichée, événement journalisé
T-R07	EF-R08, A03	Démarrer un poste client en DHCP	Adresse entre .100 et .253, passerelle .254, DNS

TEST	BESOIN(S)	PROCÉDURE	RÉSULTAT ATTENDU
			192.168.10.10
T-A01	EF-A01, A02	nslookup dc01.martinscie.lan et d'un nom externe depuis un poste	Résolutions correctes
T-A02	EF-A04, A05	Lister les OU et comptes (Active Directory Users and Computers)	OU Utilisateurs et Groupes ; 5 comptes présents
T-A03	EF-A06	Lister l'appartenance des groupes	Conforme au tableau 10
T-A04	EF-A07	Première ouverture de session d'un compte	Changement de mot de passe exigé
T-A05	EF-A08	Vérifier la jonction de chaque poste	Poste visible dans OU Ordinateurs, ouverture de session de domaine réussie
T-A06	EF-A09	Tester un mot de passe non conforme et 5 échecs successifs	Refusé ; compte verrouillé 15 minutes
T-D01	EF-D01	Se connecter à \\DC01 en tant que mbah et lister les partages	5 partages présents
T-D02	EF-D02	Pour chaque utilisateur, tenter lecture et écriture sur chacun des 5 dossiers	Résultat identique à la matrice du tableau 12 (25 cas)
T-D03	EF-D03	Vérifier les ACL avec Get-Acl	Seuls les groupes prévus, SYSTEM et Admins du domaine
T-D04	EF-D04	Ouvrir une session avec chaque compte	Lecteurs réseau montés selon les droits
T-P01	EF-P01	Consulter l'inventaire dans GLPI	Les 8 machines inventoriées avec matériel et logiciels
T-P02	EF-P02	Créer un ticket en tant que ldasilva, l'assigner et le clore en tant que mbah	Cycle complet, notifications émises
T-P03	EF-P03	Consulter Zabbix	8 hôtes disponibles, données récentes

TEST	BESOIN(S)	PROCÉDURE	RÉSULTAT ATTENDU
T-P04	EF-P04	Arrêter le service DNS sur DC01	Alerte levée en moins de 5 minutes, notification reçue
T-P05	EF-P05	Se connecter en SSH à PARC01 avec mbah, puis tenter root	mbah accepté ; root refusé
T-C01	EF-C01, C02	Vérifier systèmes, ressources et agents des postes	Conformes au tableau 8
T-S01	EF-S01	Se connecter à SECU01 avec hnyame ; vérifier le compte kali	Accès réussi ; compte kali désactivé
T-S02	EF-S02	Lancer un scan nmap autorisé du VLAN 20 depuis SECU01	Scan réalisé, journalisé dans RFW01, rapport rédigé
T-S03	10.1	Rechercher des mots de passe en clair dans les documents livrés et scripts	Aucun
T-S04	10.2	Vérifier l'état des comptes par défaut (admin, Admin, glpi, kali, root SSH)	Mots de passe changés ou comptes désactivés
T-S05	EF-S03	Restaurer un fichier, un objet AD et une base GLPI depuis les sauvegardes	Restauration réussie
T-S06	10.3	Analyse de vulnérabilités de PARC01 et DC01	Aucune vulnérabilité critique ou élevée non traitée

Critères d'acceptation

- 100 % des tests de priorité Must réussis ; aucun défaut bloquant ou critique ouvert.
- Tests de priorité Should réussis, ou écart documenté et accepté par le commanditaire.
- Dossier d'exploitation livré et relu par l'administratrice.
- Procès-verbal de recette signé par le PDG et l'administratrice.

CHAPITRE 13

13 Livrables attendus

TABLEAU 24 — LIVRABLES

LIVRABLE	CONTENU	DESTINATAIRE
Environnement opérationnel	Les huit machines virtuelles conformes au présent document	Direction, mbah
Dossier d'architecture	Schéma réseau à jour, plan d'adressage, matrice de flux	mbah
Dossier d'exploitation	Procédures : démarrage, arrêt, sauvegarde, restauration, création et départ d'un utilisateur, ajout d'un poste, gestion des droits	mbah
Scripts	Scripts PowerShell et shell de déploiement, sans secret en clair	mbah
Registre des comptes et accès	Liste des comptes, groupes et droits (sans mot de passe)	Direction, mbah
Rapport d'audit initial	Résultat des premiers tests de sécurité depuis SECU01	Direction, hnyame
Procès-verbal de recette	Résultats du plan de tests, écarts, décision	Direction
Guide utilisateur	Connexion, accès aux dossiers, création d'un ticket, VPN (2 pages)	Utilisateurs

CHAPITRE 14

14

Risques et points de vigilance

TABLEAU 25 — RISQUES

RISQUE	PROBABILITÉ	IMPACT	PARADE
Hôte sous-dimensionné (RAM, stockage)	Moyenne	Élevé	Valider les ressources en phase 0 ; disques dynamiques ; démarrage échelonné
Mots de passe faibles ou partagés	Élevée	Élevé	Politique du 10.1, mots de passe uniques, changement forcé
Compromission d'un compte administrateur	Moyenne	Très élevé	Comptes d'administration séparés, audit, MFA pour le VPN si possible

RISQUE	PROBABILITÉ	IMPACT	PARADE
Perte de DC01 (point unique de défaillance)	Faible	Très élevé	Sauvegarde de l'état du système, instantanés, option d'un second contrôleur DC02
Mauvaise configuration du pare-feu (VLAN isolés, blocage involontaire)	Moyenne	Moyen	Mise en place par étapes, export de config, tests T-R01 à T-R07
Version obsolète (Zabbix 5, PHP 8.1)	Élevée	Moyen	Passer à une version supportée (4.4)
Double NAT (Freebox + pfSense) empêchant le VPN	Élevée	Moyen	Redirection de port sur la Freebox, test depuis l'extérieur
Usage détourné de SECU01	Faible	Élevé	Autorisations écrites, règle de pare-feu limitée, journalisation
Licences Windows non couvertes	Moyenne	Moyen	Vérifier en phase 0 ; versions d'évaluation sinon
Ambiguïtés des fichiers sources	Élevée	Moyen	Traiter les points du chapitre 15 avant la phase 1

15

CHAPITRE 15

Points à confirmer et incohérences relevées

L'analyse croisée des fichiers sources a fait apparaître des écarts. Le tableau indique la décision retenue dans ce document ; chaque ligne est à valider avant le début du déploiement.

TABLEAU 26 — ÉCARTS ET DÉCISIONS

N°	CONSTAT	DÉCISION RETENUE	À CONFIRMER PAR
1	Adresses du fichier VM de la forme « 192.16.x.254 » (faute de frappe probable), 192.168.x.1 / .2 / .3 pour DC01, PARC01, SECU01 ; schéma : 192.168.10.10 / .20 / .30	Adresses du schéma (x = 10 ; .10, .20, .30)	mbah
2	Étendue DHCP : .50 à .200 (fichier VM) contre .100 à .253 en VLAN 20 (schéma)	.100 à .253 en VLAN 20	mbah

N°	CONSTAT	DÉCISION RETENUE	À CONFIRMER PAR
3	Poste de développement : WEBDEV01 sous Linux (schéma) contre DEVWEB01 sous Windows 11 Pro (fichier VM)	Nom WEBDEV01, Windows 11 Pro	cgrimeau, mbah
4	« DC01/DC02 » désigne un poste Windows 11 de mbah ; seul DC01 apparaît dans le schéma. De même « PARC01/PARC02 » et « SECU01/SECU01 » dans utilisateurs.xlsx	Un seul DC01, un seul PARC01 ; poste administrateur distinct	mbah
5	Le poste administrateur n'apparaît pas dans le schéma	Ajouté au VLAN 20	mbah
6	Droit de « dasilva » sur Direction : compte inexistant (ldasilva ?) ; accès d'une secrétaire au dossier Direction inhabituel	Interprété comme ldasilva en lecture	smartins
7	Groupes « administrateurs » et « Admin de Domaine » listés dans OU=Groupes alors qu'ils existent déjà comme groupes intégrés	mbah ajouté aux groupes intégrés, non recréés	mbah
8	Aucun serveur de fichiers n'est prévu pour héberger les cinq répertoires partagés	Partages sur DC01 (volume dédié), FS01 conseillé à terme	mbah, smartins
9	Version de pfSense incomplète (« 2. »)	Version stable en vigueur à l'installation	mbah
10	Mots de passe en clair, partagés et prévisibles dans utilisateurs.xlsx	Exclus du document ; politique du 10.1	mbah, smartins
11	Zabbix 5 et PHP 8.1 sur Debian 12 : versions non supportées ou non natives	Recommandation Zabbix 6.0 / 7.0 LTS ; sinon conserver 5	mbah
12	Hyperviseur non précisé	Choix libre sous les contraintes de 3.6	mbah
13	Comptes sur les serveurs : « administrateur », « admin », «	Politique du 10.2	mbah, hnyame

N°	CONSTAT	DÉCISION RETENUE	À CONFIRMER PAR
	Admin », « root », « kali » sans responsable défini		
14	Relais de messagerie absent (notifications GLPI / Zabbix)	SMTP externe à fournir, ou alertes limitées aux interfaces	mbah

A

ANNEXE

Glossaire

TERME	DÉFINITION
802.1Q	Norme de marquage des trames Ethernet pour transporter plusieurs VLAN sur un même lien (trunk)
ACL	Liste de contrôle d'accès : permissions attachées à un dossier ou fichier
AD DS	Active Directory Domain Services : annuaire centralisant comptes, groupes et machines
AGDLP	Méthode : comptes (A) → groupes globaux (G) → groupes locaux de domaine (DL) → permissions (P)
DHCP	Protocole d'attribution automatique des adresses IP
DNS	Système de noms de domaine : traduit les noms en adresses IP
GLPI	Gestion libre de parc informatique : inventaire et gestion des tickets d'assistance
GPO	Stratégie de groupe : paramètres appliqués automatiquement aux utilisateurs et ordinateurs du domaine
LDAP	Protocole d'accès aux annuaires, utilisé par l'AD
NAT	Translation d'adresses : permet aux adresses privées d'accéder à Internet derrière une adresse publique
OU	Unité d'organisation : conteneur de l'AD pour structurer et déléguer
pfSense	Distribution FreeBSD de pare-feu et routeur open source
RSAT	Outils d'administration de serveur à distance pour Windows

TERME	DÉFINITION
UPN	Nom d'utilisateur principal (identifiant@domaine)
VLAN	Réseau local virtuel : segmentation logique d'un réseau physique ou virtuel
VPN	Réseau privé virtuel : tunnel chiffré vers le réseau de l'entreprise
Zabbix	Logiciel libre de supervision des systèmes et du réseau

B

ANNEXE

Fiche de suivi d'installation d'une machine

ÉTAPE	CONTRÔLE	FAIT
Création de la VM	Ressources conformes au tableau 7 ; carte réseau dans le bon VLAN	☐
Installation du système	Version conforme ; nom de machine respectant la convention	☐
Réseau	IP / DHCP conforme au tableau 4 ; DNS 192.168.10.10 ; ping de la passerelle	☐
Domaine	Jonction réalisée, compte machine dans la bonne OU	☐
Sécurité	Mises à jour, pare-feu, antivirus, comptes par défaut traités	☐
Agents	GLPI et Zabbix installés et remontant des données	☐
Sauvegarde	Instantané initial pris ; machine ajoutée au plan de sauvegarde	☐
Documentation	Fiche machine et schéma mis à jour	☐

© 2026 Portail SISR · Martins & Cie · SIO2 – 1SI Document interne, ne contient aucun mot de passe.