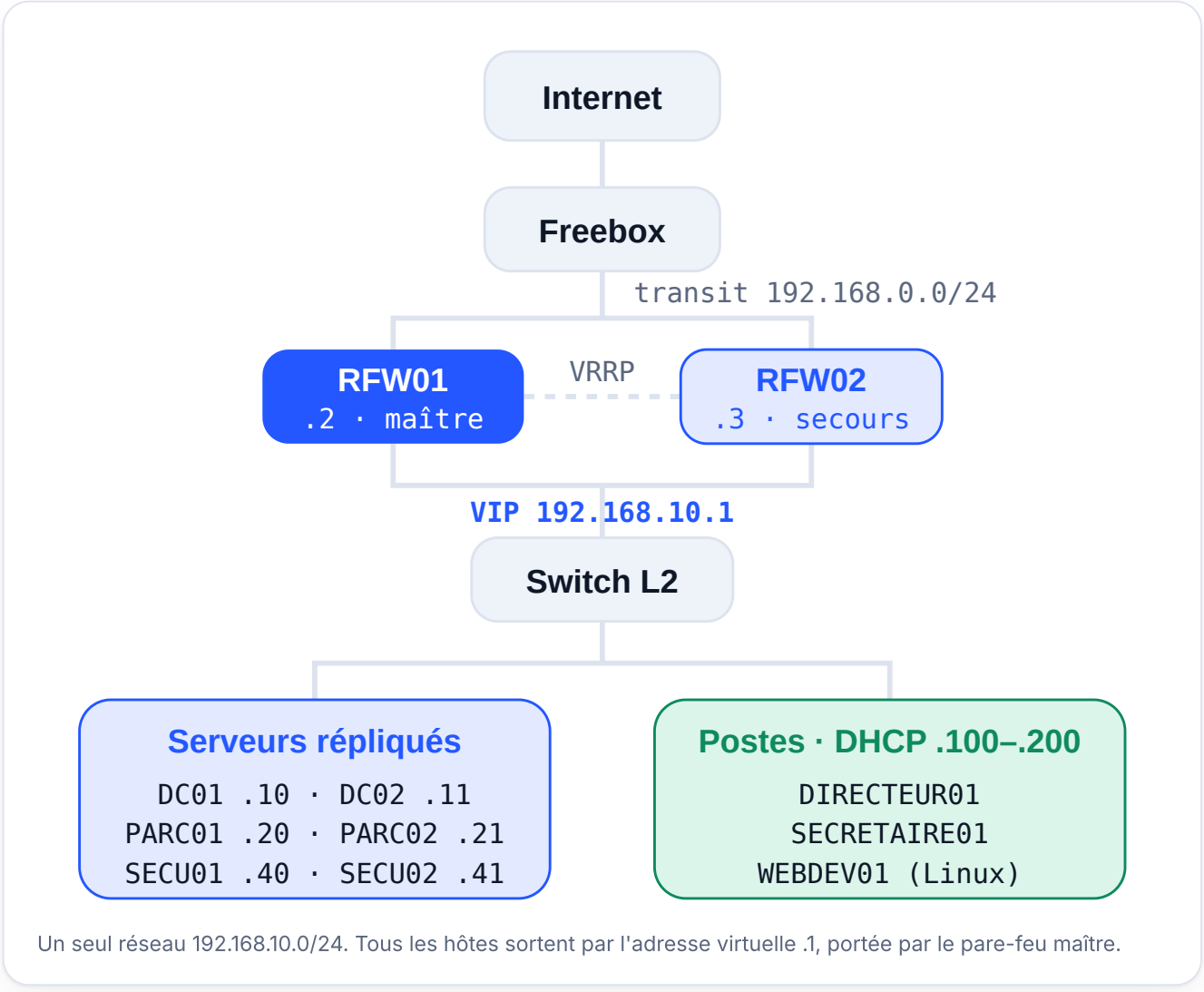
CAHIER DES CHARGES · SIO2 — 1SI

Un système d'information redondé et sécurisé.

Un réseau 192.168.10.0/24 derrière deux pare-feux en VRRP (VIP 192.168.10.1), un annuaire Active Directory sur DC01 et DC02, DHCP et DNS en basculement, des serveurs répliqués (PARC, SECU), un serveur de fichiers par service, intranet, helpdesk, supervision et VPN.

Domaine martinscie.lan Passerelle 192.168.10.1 (VIP) Schéma SIO2_1SI v2 Date 16/11/2026

Statut à valider



Un seul réseau 192.168.10.0/24. Tous les hôtes sortent par l'adresse virtuelle .1, portée par le pare-feu maître.

13	4	5	5	109
		utilisateurs		

éléments d'infrastructure

paires redondées

répertoires partagés

exigences référencées

14
tests de recette

10
chapitres

Le document

1 CHAPITRE 1

Contexte et objectifs

Ce cahier des charges définit la construction d'un système d'information complet, redondé et sécurisé pour le domaine Active Directory **martinscie.lan**, destiné à 5 utilisateurs, 3 postes de travail et 10 équipements d'infrastructure (accès opérateur, réseau et serveurs).

1.1 Contexte

L'entreprise dispose d'un réseau local unique en 192.168.10.0/24, raccordé à Internet par une Freebox. Elle emploie cinq personnes : un PDG, une secrétaire, un développeur web, un administrateur système et réseau, et un expert en cybersécurité. Le PDG, la secrétaire et le développeur disposent chacun d'un poste dédié ; l'administrateur et l'expert cybersécurité travaillent sur les serveurs. Chaque service dispose d'un répertoire propre sur le serveur de fichiers. Le projet porte la référence SIO2 – 1SI (schéma d'architecture v2).

1.2 Objectifs

- Centraliser l'authentification et la gestion des comptes dans un annuaire Active Directory redondé (DC01 / DC02).
- Fournir DHCP et DNS hautement disponibles, avec basculement automatique.
- Garantir la continuité de la connexion Internet et de la passerelle par une paire de pare-feux en VRRP (VIP 192.168.10.1).
- Mettre à disposition les services métier : serveur de fichiers par service, intranet, helpdesk, inventaire, supervision et VPN.
- Appliquer le principe du moindre privilège : chaque utilisateur n'accède qu'aux répertoires nécessaires, selon la matrice du chapitre 8.
- Répliquer les serveurs critiques (DC01→DC02, PARC01→PARC02, SECU01→SECU02) pour limiter les arrêts de service.

- Disposer d'une plateforme de test d'intrusion (Kali Linux 2025) dédiée à l'expert cybersécurité.

1.3 Documents sources

DOCUMENT	CONTENU EXPLOITÉ	REMARQUE
Schéma SIO2_1SI_v2 (image)	Topologie, adressage, rôles des machines, services, paramètres communs	Référence pour les chapitres 3 à 5
utilisateurs.xlsx	5 comptes : identifiant, nom, machine, rôle, OU	Référence pour le chapitre 6
Groupes.xlsx	7 appartenances de groupes dans l'OU Groupes	Référence pour le chapitre 7
Droits_dacces.xlsx	25 droits (5 répertoires × 5 utilisateurs)	Référence pour le chapitre 8

Les écarts et ambiguïtés relevés entre ces documents sont regroupés au chapitre 10 (points à valider).

CHAPITRE 2

2 Périmètre et inventaire

Le périmètre couvre 13 éléments installés dans un seul site : 1 routeur opérateur, 2 pare-feux, 1 commutateur, 6 serveurs et 3 postes de travail.

2.1 Inclus dans le projet

- Installation et configuration des 2 pare-feux en haute disponibilité (VRRP) et du commutateur L2 d'administration.
- Déploiement de l'annuaire Active Directory avec DNS et DHCP sur DC01, réplication sur DC02.
- Déploiement des serveurs d'applications PARC01 (helpdesk, supervision) et PARC02 (réplique).
- Déploiement des serveurs de sécurité SECU01 (Kali Linux 2025) et SECU02 (réplique).
- Préparation des 3 postes de travail (DIRECTEUR01, SECRETAIRE01, WEBDEV01) et jonction au domaine.

- Création des 5 comptes utilisateurs, 7 appartenances de groupes et 25 droits d'accès sur répertoires.
- Services transverses listés sur le schéma : helpdesk, inventaire, supervision, VPN, serveur de fichiers, intranet, réplication des serveurs, redondance réseau.

2.2 Hors périmètre

- Configuration côté opérateur de la Freebox (hors accès à ses réglages de redirection de ports et de mode routeur).
- Services non mentionnés dans les documents sources : messagerie, téléphonie, impression, Wi-Fi.
- Rachat de licences et fourniture matérielle (le dimensionnement est donné à titre indicatif au chapitre 10).

2.3 Inventaire des équipements

NOM	TYPE	ADRESSE IP	RÔLE	MACHINE LIÉE
Freebox	Routeur opérateur	Réseau de transit 192.168.0.0/24	Accès Internet	–
RFW01	Pare-feu	192.168.10.2	Pare-feu principal (maître VRRP)	RFW02
RFW02	Pare-feu	192.168.10.3	Pare-feu secondaire (esclave VRRP)	RFW01
Switch L2	Commutateur	192.168.10.4	Administration du réseau local	–
DC01	Serveur Windows	192.168.10.10	Active Directory, DNS, DHCP	DC02
DC02	Serveur Windows	192.168.10.11	Réplique de DC01 (AD, DNS, DHCP failover)	DC01
PARC01	Serveur	192.168.10.20	Helpdesk, supervision	PARC02
PARC02	Serveur	192.168.10.21	Réplique de PARC01	PARC01
SECU01	Serveur Linux	192.168.10.40	Kali Linux 2025	SECU02
SECU02	Serveur Linux	192.168.10.41	Réplique de SECU01	SECU01

NOM	TYPE	ADRESSE IP	RÔLE	MACHINE LIÉE
DIRECTEUR01	Poste Windows	DHCP (.100 à .200)	Poste de la direction	–
SECRETAIRE01	Poste Windows	DHCP (.100 à .200)	Poste du secrétariat	–
WEBDEV01	Poste Linux	DHCP (.100 à .200)	Poste de développement	–

Le schéma n'indique ni le système d'exploitation des serveurs PARC, ni le serveur hébergeant le serveur de fichiers, l'intranet, le VPN et l'inventaire : ces choix sont proposés au chapitre 5 et listés au chapitre 10 pour validation.

CHAPITRE 3

3 Architecture réseau

Le réseau est un LAN unique 192.168.10.0/24 protégé par deux pare-feux en VRRP, dont la passerelle virtuelle 192.168.10.1 est le seul point de sortie vers la Freebox et Internet.

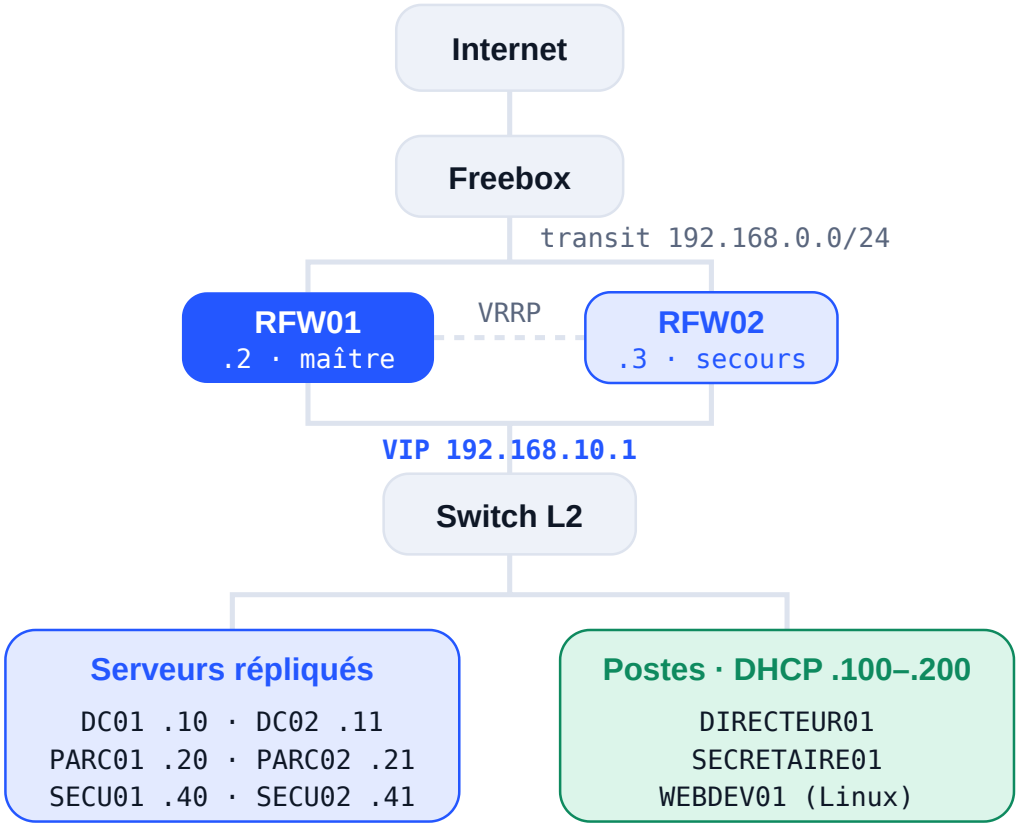


Figure 1 – Schéma d'architecture SIO2_1SI v2 : un seul réseau 192.168.10.0/24 derrière la paire de pare-feux VRRP.

3.1 Chaîne de connexion

1. **Internet** : réseau public.
2. **Freebox** : routeur opérateur, relié aux pare-feux par un réseau de transit 192.168.0.0/24.
3. **RFW01 (192.168.10.2) et RFW02 (192.168.10.3)** : pare-feux en haute disponibilité VRRP, partageant la VIP 192.168.10.1.
4. **Switch L2 (192.168.10.4)** : commutateur d'administration, cœur du LAN.
5. **Postes et serveurs** : DIRECTEUR01, SECRETAIRE01, WEBDEV01, PARC01/02, SECU01/02, DC01/02.

3.2 Exigences réseau

RÉF.	EXIGENCE	NIVEAU
RES-01	Un seul réseau local 192.168.10.0/24, masque 255.255.255.0	Obligatoire
RES-02	La passerelle par défaut de tous les hôtes est la VIP 192.168.10.1, jamais l'adresse physique d'un pare-feu	Obligatoire
RES-03	RFW01 est maître VRRP, RFW02 prend le relais automatiquement en cas de panne ; temps de bascule cible inférieur à 5 secondes (valeur proposée)	Obligatoire
RES-04	Un lien de synchronisation HA relie les deux pare-feux (lien en pointillé du schéma) ; la configuration et l'état des sessions sont synchronisés	Obligatoire
RES-05	Le trafic sortant est traduit (NAT) vers le réseau de transit 192.168.0.0/24	Obligatoire
RES-06	Politique de filtrage par défaut : tout est refusé, seuls les flux du §3.3 sont ouverts	Obligatoire
RES-07	Le switch est administrable uniquement depuis les postes d'administration (SSH ou HTTPS, pas de Telnet ni HTTP)	Obligatoire
RES-08	Les clients utilisent DNS 192.168.10.10 puis 192.168.10.11	Obligatoire
RES-09	Les journaux des pare-feux et du switch sont envoyés à la supervision (PARC01)	Souhaitable
RES-10	Segmentation en VLAN (postes, serveurs, administration) à prévoir en évolution ; le schéma actuel n'en définit pas	Souhaitable

3.3 Flux principaux à autoriser

SOURCE	DESTINATION	SERVICE	USAGE
Postes	DC01, DC02	DNS 53, Kerberos 88, LDAP 389 / LDAPS 636, SMB 445, RPC 135	Authentification, GPO, fichiers
Postes	DC01, DC02	DHCP UDP 67/68	Attribution d'adresses
DC01	DC02	Réplication AD (RPC, LDAP, Kerberos, SMB), DHCP failover TCP 647	Redondance AD et DHCP
Postes	PARC01	HTTPS 443	Helpdesk, supervision, intranet
PARC01	Tous les équipements	SNMP 161, ICMP, agents	Supervision
PARC01	PARC02	Réplication applicative	Redondance
SECU01	SECU02	Réplication	Redondance
Poste d'administration (mbah)	Pare-feux, switch, serveurs	SSH 22, RDP 3389, HTTPS 443	Administration
Postes et serveurs	Internet (via VIP)	HTTP 80, HTTPS 443, DNS 53	Navigation, mises à jour
Internet	Pare-feux	Port du protocole VPN retenu	Accès distant (VPN)
SECU01	LAN	Scans et tests d'intrusion	Autorisé uniquement pour hnyame, sur fenêtre convenue

3.4 Redondance

ÉLÉMENT	REDONDÉ	MÉCANISME	POINT DE VIGILANCE
Accès Internet (Freebox)	Non	–	Point de défaillance unique
Pare-feux	Oui	VRRP, VIP 192.168.10.1	Synchroniser règles et sessions
Switch L2	Non	–	Point de défaillance unique : à corriger par un second switch (matériel et câblage)

ÉLÉMENT	REDONDÉ	MÉCANISME	POINT DE VIGILANCE
Contrôleurs de domaine	Oui	Réplication AD DC01→DC02	Vérifier la réplication régulièrement
DHCP	Oui	Failover entre DC01 et DC02	Plage commune .100 à .200
DNS	Oui	Deux serveurs, zone intégrée AD	Les clients reçoivent les deux adresses
Serveurs PARC	Oui	Réplique PARC02	Bascule à documenter
Serveurs SECU	Oui	Réplique SECU02	Bascule à documenter

CHAPITRE 4

4 Plan d'adressage, DHCP et DNS

Le réseau 192.168.10.0/24 est découpé en trois zones : adresses fixes de .1 à .99, adresses dynamiques de .100 à .200 et réserve de .201 à .254.

4.1 Paramètres communs

PARAMÈTRE	VALEUR
Réseau	192.168.10.0/24
Masque	255.255.255.0
Passerelle	192.168.10.1 (VIP VRRP)
DNS	192.168.10.10 puis 192.168.10.11
Domaine	martinscie.lan
Plage DHCP	192.168.10.100 à 192.168.10.200 (failover)
Adresses fixes	192.168.10.1 à 192.168.10.99
Réserve	192.168.10.201 à 192.168.10.254
Diffusion	192.168.10.255

4.2 Adresses fixes attribuées

ADRESSE	ÉQUIPEMENT	FAMILLE
192.168.10.1	VIP VRRP (passerelle)	Réseau
192.168.10.2	RFW01	Réseau
192.168.10.3	RFW02	Réseau
192.168.10.4	Switch L2	Réseau
192.168.10.10	DC01	Serveur
192.168.10.11	DC02	Serveur
192.168.10.20	PARC01	Serveur
192.168.10.21	PARC02	Serveur
192.168.10.40	SECU01	Serveur
192.168.10.41	SECU02	Serveur

Les familles d'adresses suivent une logique par dizaine : .1 à .9 réseau, .10 à .19 annuaire, .20 à .39 parc applicatif, .40 à .49 sécurité. Les adresses restantes de .5 à .99 sont libres pour les extensions.

4.3 Service DHCP

RÉF.	EXIGENCE	NIVEAU
DHCP-01	Le rôle DHCP est installé sur DC01 et DC02, autorisé dans l'Active Directory	Obligatoire
DHCP-02	Une étendue unique 192.168.10.100 à .200, en mode failover entre DC01 et DC02	Obligatoire
DHCP-03	Mode de failover proposé : répartition de charge 50/50, délai de basculement automatique	À valider
DHCP-04	Options distribuées : routeur 192.168.10.1, DNS 192.168.10.10 et .11, suffixe martinscie.lan	Obligatoire
DHCP-05	Durée de bail proposée : 8 jours	À valider
DHCP-06	Les adresses .1 à .99 et .201 à .254 sont exclues de l'étendue	Obligatoire
DHCP-07	Aucun serveur n'utilise le DHCP : les serveurs et pare-feux ont une adresse fixe	Obligatoire

4.4 Service DNS

RÉF.	EXIGENCE	NIVEAU
DNS-01	Le rôle DNS est installé sur DC01 (principal, .10) et DC02 (secondaire, .11)	Obligatoire
DNS-02	Zone directe martinscie.lan intégrée à l'Active Directory et répliquée sur les deux contrôleurs	Obligatoire
DNS-03	Zone inverse 10.168.192.in-addr.arpa avec enregistrements PTR pour toutes les adresses fixes	Obligatoire
DNS-04	Enregistrements A pour tous les hôtes de l'inventaire (chapitre 2.3)	Obligatoire
DNS-05	Alias proposés : intranet, helpdesk, supervision, fichiers, tous pointant vers l'hôte retenu au chapitre 5	À valider
DNS-06	Redirecteur DNS vers un serveur public ou la Freebox pour les noms externes	À valider
DNS-07	Mise à jour dynamique sécurisée uniquement	Obligatoire

CHAPITRE 5

5 Serveurs et services

Douze services sont listés sur le schéma ; six ont un hôte explicite (AD, DNS, DHCP, helpdesk, supervision, Kali), les autres sont placés ici par proposition et signalés « Proposé ».

5.1 Répartition des services

SERVICE	HÔTE	RÉPLIQUE	ORIGINE
Active Directory (AD DS)	DC01	DC02	Schéma
DNS	DC01	DC02	Schéma
DHCP	DC01	DC02 (failover)	Schéma
Helpdesk	PARC01	PARC02	Schéma
Supervision	PARC01	PARC02	Schéma
Inventaire	PARC01	PARC02	Proposé (couplable au helpdesk)

SERVICE	HÔTE	RÉPLIQUE	ORIGINE
Serveur de fichiers	PARC01	PARC02 (DFS-R)	Proposé
Intranet	PARC01	PARC02	Proposé
VPN	RFW01 / RFW02	Bascule VRRP	Proposé
Kali Linux 2025	SECU01	SECU02	Schéma
Réplication serveurs	DC01→DC02, PARC01→PARC02, SECU01→SECU02	–	Schéma
Redondance réseau	RFW01 / RFW02	VRRP	Schéma

5.2 Active Directory (DC01, DC02)

RÉF.	EXIGENCE	NIVEAU
AD-01	Forêt et domaine uniques : martinscie.lan (NetBIOS MARTINSCIE)	Obligatoire
AD-02	DC01 et DC02 sont tous deux contrôleurs de domaine et catalogues globaux ; DC01 porte les cinq rôles FSMO	Obligatoire
AD-03	Arborescence d'unités d'organisation : OU=Utilisateurs et OU=Groupes sous DC=martinscie,DC=lan, plus OU=Ordinateurs et OU=Serveurs proposées	Obligatoire
AD-04	Les 5 comptes du chapitre 6 sont créés dans OU=Utilisateurs ; les 7 appartenances du chapitre 7 dans OU=Groupes	Obligatoire
AD-05	Tous les postes Windows rejoignent le domaine ; le poste Linux WEBDEV01 s'authentifie sur l'AD (SSSD ou Kerberos)	Obligatoire
AD-06	Sites et services : un seul site, réplication intra-site automatique	Obligatoire
AD-07	Contrôle hebdomadaire de la réplication (outils repadmin, dcdiag)	Obligatoire
AD-08	Corbeille Active Directory activée	Souhaitable

5.3 Serveur de fichiers

RÉF.	EXIGENCE	NIVEAU
FIC-01	Un partage par répertoire : Direction, Administration, Secrétariat, Sécurité, Développement web	Obligatoire

RÉF.	EXIGENCE	NIVEAU
FIC-02	Les droits suivent la matrice du chapitre 8, appliqués par groupes de sécurité et non par utilisateur	Obligatoire
FIC-03	Les droits de partage sont ouverts à « Utilisateurs authentifiés », les droits réels sont portés par les permissions NTFS	Obligatoire
FIC-04	Énumération basée sur les accès : un utilisateur ne voit pas les dossiers auxquels il n'a pas accès	Obligatoire
FIC-05	Réplication DFS-R vers PARC02 ; espace de noms DFS unique \martinscie.lan\partages	Obligatoire
FIC-06	Versions précédentes (clichés instantanés) activées, deux fois par jour	Souhaitable
FIC-07	Audit des accès refusés et des suppressions sur les répertoires Direction et Administration	Obligatoire
FIC-08	Quota par répertoire proposé : 50 Go, alerte à 85 %	À valider

5.4 Helpdesk, inventaire et supervision (PARC01, PARC02)

RÉF.	EXIGENCE	NIVEAU
HLP-01	Outil de tickets accessible en HTTPS pour les 5 utilisateurs, avec authentification AD	Obligatoire
HLP-02	Catégories de tickets : réseau, serveur, poste, compte et droits, sécurité	Obligatoire
HLP-03	Les tickets sont traités par mbah ; les incidents de sécurité sont assignés à hnyame	Obligatoire
INV-01	Inventaire automatique des 13 éléments (matériel, système, logiciels, adresse IP) et rapprochement avec le helpdesk	Obligatoire
SUP-01	Supervision des 13 éléments : disponibilité (ping), CPU, mémoire, disque, services critiques	Obligatoire
SUP-02	Contrôles spécifiques : état VRRP, réplication AD, étendue DHCP, résolution DNS, réplication PARC et SECU	Obligatoire
SUP-03	Seuils d'alerte proposés : CPU supérieur à 85 % pendant 10 minutes, disque supérieur à 85 %, service arrêté	À valider
SUP-04	Alertes envoyées à mbah (tous niveaux) et hnyame (niveau sécurité)	Obligatoire

5.5 Intranet et VPN

RÉF.	EXIGENCE	NIVEAU
INT-01	Portail interne en HTTPS avec certificat émis par une autorité interne, accessible depuis le LAN et le VPN	Obligatoire
INT-02	Contenu minimal : annuaire, liens vers helpdesk et partages, procédures	Souhaitable
VPN-01	VPN d'accès distant terminé sur la VIP des pare-feux, avec bascule VRRP	Obligatoire
VPN-02	Authentification par compte Active Directory, double facteur souhaité	Obligatoire
VPN-03	Accès limité par groupe de sécurité ; aucun accès direct aux serveurs SECU	Obligatoire
VPN-04	Protocole à choisir (OpenVPN, WireGuard ou IPsec) et plage d'adresses VPN à définir hors de .1 à .254	À valider

5.6 Plateforme de sécurité (SECU01, SECU02)

RÉF.	EXIGENCE	NIVEAU
SEC-01	SECU01 exécute Kali Linux 2025 avec les outils de test d'intrusion à jour	Obligatoire
SEC-02	SECU02 est une réplique de SECU01 (instantané ou copie de la machine virtuelle)	Obligatoire
SEC-03	Seul hnyame utilise ces serveurs ; mbah les administre au niveau système	Obligatoire
SEC-04	Toute campagne de test fait l'objet d'une autorisation écrite du PDG et d'une fenêtre horaire	Obligatoire
SEC-05	Les rapports de test sont stockés dans le répertoire Sécurité uniquement	Obligatoire

CHAPITRE 6

6 Utilisateurs

Cinq comptes sont à créer dans l'unité d'organisation OU=Utilisateurs du domaine martinscie.lan, un par collaborateur, nommés selon la règle « initiale du prénom + nom ».

6.1 Liste des comptes

IDENTIFIANT	PRÉNOM NOM	RÔLE	MACHINE(S)	SERVICE (GROUPE)
mbah	Maria Bah	Administrateur système et réseau	DC01, DC02, PARC01, PARC02	Administration

IDENTIFIANT	PRÉNOM NOM	RÔLE	MACHINE(S)	SERVICE (GROUPE)
smartins	Serge Martins	PDG et administrateur local	DIRECTEUR01	Direction
ldasilva	Léon Dasilva	Secrétaire	SECRETAIRE01	Secrétariat
cgrimeau	Corentin Grimeau	Développeur web	WEBDEV01	Développement web
hnyame	Hervé Nyame	Expert cybersécurité	SECU01, SECU02	Sécurité

Toutes les entrées sont rangées dans OU=Utilisateurs, DC=martinscie, DC=lan.

6.2 Exigences sur les comptes

RÉF.	EXIGENCE	NIVEAU
USR-01	Identifiant = première lettre du prénom + nom, en minuscules, sans accent ni espace	Obligatoire
USR-02	Chaque compte porte prénom, nom, rôle (description) et poste de rattachement	Obligatoire
USR-03	Un mot de passe provisoire est délivré à la première connexion ; le changement est imposé à l'ouverture de session	Obligatoire
USR-04	Le mot de passe provisoire est unique par compte et transmis hors du réseau (en main propre) ; il n'est consigné dans aucun fichier	Obligatoire
USR-05	Restriction de connexion : chaque utilisateur ne peut ouvrir une session que sur les machines listées ci-dessus	Obligatoire
USR-06	smartins est administrateur local de DIRECTEUR01 uniquement ; il n'est pas administrateur du domaine	Obligatoire
USR-07	mbah est membre de Admins du domaine ; elle dispose en plus d'un compte non privilégié pour la messagerie et la navigation	Souhaitable
USR-08	Aucun compte ne partage un mot de passe avec un autre ; aucun compte générique	Obligatoire
USR-09	Procédures d'arrivée, de départ et de changement de poste documentées dans le helpdesk	Souhaitable

6.3 Point d'attention sur les fichiers fournis

Le fichier utilisateurs.xlsx contient en clair, pour les 5 comptes, un mot de passe de première connexion et un mot de passe définitif, identiques d'un compte à l'autre et construits selon un

modèle prévisible. Ils ne sont pas reproduits dans ce document. Le cahier des charges exige leur remplacement (USR-03, USR-04 et la politique du chapitre 9) avant toute mise en production.

CHAPITRE 7

7 Groupes de sécurité et organisation AD

Sept groupes sont créés dans OU=Groupes : quatre groupes de service à un membre chacun, et trois groupes d'administration où mbah est la seule membre.

7.1 Groupes fournis

GROUPE	MEMBRE	TYPE	CHEMIN
Administration	mbah	Service	OU=Groupes, DC=martinscie, DC=lan
administrateurs	mbah	Privilégié	OU=Groupes, DC=martinscie, DC=lan
Admin de Domaine	mbah	Privilégié	OU=Groupes, DC=martinscie, DC=lan
Direction	smartins	Service	OU=Groupes, DC=martinscie, DC=lan
Secrétariat	ldasilva	Service	OU=Groupes, DC=martinscie, DC=lan
Développement web	cgrimeau	Service	OU=Groupes, DC=martinscie, DC=lan
Sécurité	hnyame	Service	OU=Groupes, DC=martinscie, DC=lan

7.2 Modèle de gestion des droits

Les droits de la matrice (chapitre 8) sont portés par des groupes et non par des comptes individuels, selon le principe AGDLP : les comptes entrent dans les groupes globaux de service, ceux-ci entrent dans des groupes locaux de domaine, qui reçoivent les permissions sur les répertoires. Dix groupes locaux de domaine sont proposés, créés dans OU=Groupes.

GROUPE LOCAL DE DOMAINE	PERMISSION	MEMBRES (GROUPES DE SERVICE)
DL_Direction_RW	Lecture/écriture	Direction
DL_Direction_RO	Lecture	Administration, Secrétariat, Sécurité
DL_Administration_RW	Lecture/écriture	Administration
DL_Administration_RO	Lecture	Direction, Sécurité
DL_Secretariat_RW	Lecture/écriture	Secrétariat

GROUPE LOCAL DE DOMAINE	PERMISSION	MEMBRES (GROUPES DE SERVICE)
DL_Secretariat_RO	Lecture	Administration, Direction, Sécurité
DL_Securite_RW	Lecture/écriture	Sécurité
DL_Securite_RO	Lecture	Administration, Direction
DL_DevWeb_RW	Lecture/écriture	Développement web
DL_DevWeb_RO	Lecture	Administration, Direction, Sécurité

Un service absent d'une ligne pour un répertoire n'a aucun accès : c'est le cas de Développement web sur 4 répertoires, de Secrétariat sur 3.

7.3 Exigences

RÉF.	EXIGENCE	NIVEAU
GRP-01	Les sept groupes du tableau 7.1 existent, avec les membres indiqués	Obligatoire
GRP-02	Les groupes de service sont de portée globale, les groupes de permissions de portée locale de domaine	Obligatoire
GRP-03	Les permissions NTFS ne sont jamais attribuées à un compte individuel	Obligatoire
GRP-04	L'ajout ou le retrait d'un membre se fait par une demande tracée dans le helpdesk	Obligatoire
GRP-05	Les groupes « administrateurs » et « Admin de Domaine » ne comptent que mbah ; toute modification génère une alerte	Obligatoire
GRP-06	Revue semestrielle des membres de tous les groupes par le PDG et l'administrateur	Souhaitable

7.4 Remarque sur les groupes privilégiés

Dans un annuaire Windows standard, les groupes Administrateurs et Admins du domaine sont des groupes intégrés, situés hors de l'OU Groupes. Le fichier les place dans OU=Groupes : il faut confirmer s'il s'agit de groupes personnalisés homonymes ou des groupes intégrés (point à valider, chapitre 10).

CHAPITRE 8

8 Matrice des droits d'accès

Les 25 droits définis (5 utilisateurs × 5 répertoires) se répartissent en 5 accès en lecture/écriture, 13 en lecture seule et 7 sans accès ; chaque service n'écrit que dans son propre répertoire.

8.1 Matrice

Légende : **LE** = lecture/écriture, **L** = lecture seule, **–** = pas d'accès.

UTILISATEUR	DIRECTION	ADMINISTRATION	SECRÉTARIAT	SÉCURITÉ	DÉVELOPPEMENT WEB
smartins (PDG)	LE	L	L	L	L
mbah (administrateur)	L	LE	L	L	L
ldasilva (secrétaire)	L	–	LE	–	–
cgrimeau (développeur)	–	–	–	–	LE
hnyame (cybersécurité)	L	L	L	LE	L

8.2 Lecture de la matrice

- **Direction** et **Administration** : le PDG et l'administrateur lisent les cinq répertoires mais n'écrivent que dans le leur.
- **Expert cybersécurité** : lecture sur les quatre autres répertoires, écriture sur Sécurité uniquement ; son rôle est un rôle d'audit.
- **Secrétaire** : accès limité à son répertoire et lecture du répertoire Direction ; aucun accès Administration, Sécurité ni Développement web.
- **Développeur web** : accès à son seul répertoire ; il est le profil le plus restreint.

8.3 Exigences

RÉF.	EXIGENCE	NIVEAU
DRT-01	La matrice 8.1 est appliquée telle quelle via les groupes du §7.2	Obligatoire
DRT-02	Un utilisateur sans droit ne voit pas le répertoire (énumération basée sur les accès)	Obligatoire
DRT-03	L'héritage est désactivé à la racine de chaque répertoire ; les droits « Système » et « Administrateurs » restent nécessaires pour la sauvegarde	Obligatoire

RÉF.	EXIGENCE	NIVEAU
DRT-04	Les 25 cas de la matrice font l'objet d'un test d'accès documenté (chapitre 10, recette)	Obligatoire
DRT-05	Tout refus d'accès sur Direction, Administration et Sécurité est journalisé	Obligatoire
DRT-06	Toute modification de la matrice passe par un ticket validé par le PDG	Obligatoire
DRT-07	mbah n'a que la lecture sur les répertoires des autres services ; comme administrateur du domaine elle peut techniquement les modifier, et cette possibilité est tracée par audit	Souhaitable

CHAPITRE 9

9 Sécurité, sauvegarde et continuité

La réplication des serveurs protège contre la panne d'une machine mais pas contre l'erreur, le chiffrement malveillant ou la suppression : une sauvegarde indépendante, absente du schéma, est donc exigée.

9.1 Politique de mots de passe

RÉF.	PARAMÈTRE	VALEUR PROPOSÉE
MDP-01	Longueur minimale	12 caractères
MDP-02	Complexité	Activée (3 familles de caractères sur 4)
MDP-03	Historique	12 derniers mots de passe interdits
MDP-04	Verrouillage	5 échecs, déverrouillage après 15 minutes
MDP-05	Changement à la première connexion	Obligatoire
MDP-06	Comptes d'administration	16 caractères minimum, politique distincte (PSO) pour mbah et hnyame
MDP-07	Stockage	Aucun mot de passe en clair dans un fichier, un ticket ou un message

9.2 Stratégies de groupe (GPO)

RÉF.	STRATÉGIE	PORTÉE
GPO-01	Verrouillage automatique de session après 10 minutes	Tous les postes

RÉF.	STRATÉGIE	PORTÉE
GPO-02	Mappage automatique des lecteurs réseau selon le groupe de service	Utilisateurs
GPO-03	Pare-feu Windows activé sur tous les profils	Postes et serveurs Windows
GPO-04	Mises à jour automatiques (WSUS ou Windows Update) avec fenêtre de maintenance	Postes et serveurs Windows
GPO-05	Désactivation des supports amovibles sauf pour hnyame	Postes
GPO-06	Restriction d'ouverture de session par machine (voir USR-05)	Utilisateurs
GPO-07	Audit des connexions, des modifications de groupes et d'accès aux fichiers	Contrôleurs de domaine, serveur de fichiers

9.3 Durcissement et sécurité réseau

- Seul le trafic listé au §3.3 est autorisé ; les pare-feux journalisent les refus.
- Les protocoles obsolètes (SMBv1, NTLMv1, Telnet, FTP en clair) sont désactivés.
- Les comptes d'administration ne servent pas pour la navigation ; l'administration se fait depuis des postes ou serveurs désignés.
- Les services web internes (intranet, helpdesk, supervision) sont exposés uniquement en HTTPS.
- Kali Linux (SECU01 et SECU02) n'est jamais accessible depuis le VPN ni depuis Internet.
- Les mises à jour de sécurité des pare-feux, du switch et des serveurs sont appliquées au plus tard 30 jours après leur publication, sous 7 jours pour les failles critiques.

9.4 Sauvegarde

RÉF.	DONNÉE	FRÉQUENCE	RÉTENTION PROPOSÉE	SUPPORT
SAV-01	État système AD (DC01, DC02)	Quotidienne	30 jours	Disque externe ou NAS
SAV-02	Partages de fichiers (5 répertoires)	Quotidienne, complète hebdomadaire	30 jours, 12 mois en mensuelle	NAS + copie hors site

RÉF.	DONNÉE	FRÉQUENCE	RÉTENTION PROPOSÉE	SUPPORT
SAV-03	Configurations des pare-feux et du switch	À chaque modification, et hebdomadaire	12 versions	Dépôt sécurisé
SAV-04	Serveurs PARC (helpdesk, supervision, intranet)	Quotidienne	14 jours	NAS
SAV-05	Machines virtuelles ou images SECU01, SECU02	Hebdomadaire	4 versions	NAS
SAV-06	Projets du poste WEBDEV01	Quotidienne + dépôt de code	30 jours	Serveur de fichiers et dépôt Git

- Règle 3-2-1 : 3 copies, 2 supports différents, 1 copie hors site ou hors ligne.
- Un test de restauration est réalisé chaque trimestre et consigné dans le helpdesk.
- Les sauvegardes sont chiffrées ; la clé est conservée par le PDG et l'administrateur.

9.5 Continuité : objectifs de reprise

Les valeurs ci-dessous sont des cibles proposées à faire valider par la direction.

SERVICE	PERTE DE DONNÉES MAXIMALE (RPO)	DÉLAI DE REPRISE (RTO)	MODÈLE DE REPRISE
Accès Internet et passerelle	0	5 secondes (VRRP)	Automatique
AD, DNS, DHCP	0 (réplication)	Immédiat	Automatique, deux contrôleurs actifs
Serveur de fichiers	15 minutes	1 heure	Bascule DFS-R vers PARC02
Helpdesk, supervision, intranet	24 heures	4 heures	Bascule manuelle vers PARC02
Plateforme de sécurité	1 semaine	1 jour	Remise en ligne de SECU02
Poste de travail	24 heures	1 jour ouvré	Réinstallation depuis image

CHAPITRE 10

10 Exigences non fonctionnelles, planning, recette et points à valider

Le projet est réalisable en environ 29 jours ouvrés en 12 phases, et 14 points des documents sources doivent être validés avant le démarrage.

10.1 Exigences non fonctionnelles

RÉF.	CATÉGORIE	EXIGENCE	NIVEAU
NF-01	Disponibilité	Aucun service critique (passerelle, AD, DNS, DHCP) n'est interrompu par la panne d'un seul équipement, hors switch et Freebox	Obligatoire
NF-02	Capacité	Réseau dimensionné pour 101 clients DHCP au maximum (.100 à .200) et 5 utilisateurs actifs	Obligatoire
NF-03	Performance	Authentification AD et ouverture de session en moins de 30 secondes ; résolution DNS en moins de 100 ms	Obligatoire
NF-04	Évolutivité	Réserve .201 à .254 et adresses fixes .5 à .99 disponibles ; ajout d'un second switch et de VLAN sans refonte	Souhaitable
NF-05	Maintenabilité	Documentation à jour de chaque équipement : adresse, version, configuration, procédure de bascule	Obligatoire
NF-06	Conformité	Données personnelles des 5 utilisateurs traitées selon le RGPD : minimisation, droit d'accès, durée de conservation des journaux limitée à 12 mois	Obligatoire
NF-07	Temps	Les horloges de tous les équipements sont synchronisées sur DC01 (NTP), écart maximal 5 minutes pour Kerberos	Obligatoire
NF-08	Nommage	Noms d'hôtes en majuscules, sans accent, au format utilisé sur le schéma	Obligatoire

10.2 Dimensionnement indicatif

Valeurs de départ proposées, à ajuster selon l'hyperviseur ou le matériel retenu.

MACHINE	VCPU	MÉMOIRE	DISQUE	REMARQUE
DC01, DC02	2	4 Go	80 Go	Windows Server

MACHINE	VCPU	MÉMOIRE	DISQUE	REMARQUE
PARC01, PARC02	4	8 Go	500 Go	Fichiers, helpdesk, supervision, intranet
SECU01, SECU02	4	8 Go	100 Go	Kali Linux 2025
DIRECTEUR01, SECRETAIRE01	2	8 Go	256 Go	Windows professionnel
WEBDEV01	4	16 Go	512 Go	Linux, environnement de développement

10.3 Planning prévisionnel

Durées en jours ouvrés, phases enchainées ; les phases 6 à 8 peuvent se recouvrir si deux personnes interviennent.

1. Cadrage et validation du cahier des charges : 2 jours.
2. Réseau : pare-feux, VRRP, switch, liaison Freebox : 3 jours.
3. Contrôleurs de domaine : AD, DNS, DHCP, réplication : 3 jours.
4. Unités d'organisation, comptes et groupes : 1 jour.
5. Serveur de fichiers, permissions et DFS-R : 3 jours.
6. Serveurs PARC : helpdesk, inventaire, supervision, intranet : 4 jours.
7. Serveurs SECU : Kali Linux et réplique : 2 jours.
8. VPN : 2 jours.
9. Postes de travail : jonction au domaine et GPO : 2 jours.
10. Sauvegarde et tests de restauration : 2 jours.
11. Recette et corrections : 3 jours.
12. Documentation et remise à l'équipe : 2 jours.

10.4 Plan de recette

RÉF.	TEST	RÉSULTAT ATTENDU
REC-01	Arrêt de RFW01 pendant un téléchargement	RFW02 reprend la VIP, la connexion Internet reprend en moins de 5 s

RÉF.	TEST	RÉSULTAT ATTENDU
REC-02	Retour de RFW01	Pas de coupure, rôle maître rétabli ou conservé selon la politique choisie
REC-03	Arrêt de DC01	Les ouvertures de session, le DNS et le DHCP continuent via DC02
REC-04	Création d'un objet sur DC01	L'objet apparaît sur DC02 en moins de 15 minutes
REC-05	Démarrage d'un poste en DHCP	Adresse comprise entre .100 et .200, passerelle .1, DNS .10 et .11
REC-06	Ouverture de session des 5 comptes sur leur machine	Succès, changement de mot de passe imposé
REC-07	Ouverture de session d'un compte sur une machine non autorisée	Refus
REC-08	Test des 25 droits de la matrice 8.1	Chaque résultat est identique à la matrice
REC-09	Accès à un répertoire interdit (cgrimeau sur Direction)	Dossier invisible ou accès refusé, événement journalisé
REC-10	Arrêt de PARC01	Bascule vers PARC02 dans le délai du §9.5
REC-11	Connexion VPN d'un utilisateur autorisé	Accès au LAN selon son groupe, aucun accès à SECU
REC-12	Panne simulée d'un service (DHCP)	Alerte reçue par mbah en moins de 5 minutes
REC-13	Restauration d'un fichier supprimé dans Secrétariat	Fichier restauré depuis les versions précédentes ou la sauvegarde
REC-14	Scan de vulnérabilités depuis SECU01 par hnyame	Rapport produit et stocké dans le répertoire Sécurité

10.5 Livrables

- Dossier d'architecture : schéma réseau, plan d'adressage, inventaire.
- Dossier d'exploitation : procédures de sauvegarde, de restauration et de bascule.
- Export de la structure Active Directory : OU, comptes, groupes, droits.
- Configurations sauvegardées des pare-feux et du switch.
- Procès-verbal de recette signé par le PDG et l'administrateur.

- Guide utilisateur d'une page : connexion, partages, helpdesk, VPN.

10.6 Points à valider

N°	CONSTAT DANS LES DOCUMENTS	PROPOSITION RETENUE DANS CE CAHIER
1	Le fichier utilisateurs.xlsx est fourni en deux exemplaires strictement identiques	Un seul fichier de référence
2	Dans Droits_dacces.xlsx, le répertoire Direction cite « dasilva » alors que le compte est ldasilva	Lire ldasilva (droit : lecture)
3	La machine de hnyame est « SECU01/SECU01 »	Lire SECU01/SECU02
4	Le poste du développeur est DEVWEB01 dans le fichier et WEBDEV01 sur le schéma	Retenir WEBDEV01
5	Mots de passe en clair, identiques et prévisibles dans utilisateurs.xlsx	Remplacement obligatoire (§6.3, §9.1)
6	Les groupes administrateurs et Admin de Domaine sont placés dans OU=Groupes	Confirmer groupes intégrés ou personnalisés (§7.4)
7	Sur le schéma, WEBDEV01 est relié graphiquement à DIRECTEUR01 et non au switch	Tous les postes sont raccordés au switch L2
8	Hôte du serveur de fichiers, de l'intranet, de l'inventaire et du VPN non indiqué	PARC01/PARC02 pour les trois premiers, pare-feux pour le VPN
9	Système d'exploitation de DC et PARC non indiqué	Windows Server pour DC et fichiers ; à confirmer pour le reste de PARC
10	Un seul switch et une seule Freebox	Point de défaillance accepté ou second switch ajouté
11	Aucune solution de sauvegarde sur le schéma	Ajout d'un NAS ou disque externe (§9.4)
12	Adresses de la Freebox et côté externe des pare-feux dans 192.168.0.0/24 non indiquées	À fournir pour le plan d'adressage
13	Mode de failover DHCP, protocole VPN et groupe autorisé au VPN non définis	Répartition 50/50 ; protocole à choisir ; groupe à définir

N°	CONSTAT DANS LES DOCUMENTS	PROPOSITION RETENUE DANS CE CAHIER
14	mbah administre DC et PARC mais pas SECU01/SECU02	Accès système à SECU accordé à mbah (SEC-03)

© 2026 Portail SISR · Martins & Cie · SIO2 – 1SI

Document interne, ne contient aucun mot de passe.