DEVOIR N° 1 · 1 MOIS · MARTINS & CIE

Socle réseau et annuaire : RFW01 et DC01.

Premier mois du projet Martins & Cie : segmenter le réseau derrière pfSense, monter le domaine martinscie.lan, puis traduire la matrice des droits en groupes AGDLP, partages et GPO. Quatre semaines, quatre jalons, un dossier technique.

Binôme **oui** Durée **4 semaines** Rendu **fin S4** Suite **devoir n° 2**

1

Semaine 1

Analyse et pare-feu RFW01

CDC, hyperviseur, VLAN 10/20, NAT

2

Semaine 2

Contrôleur de domaine DC01

AD DS, DNS, DHCP, relais DHCP

3

Semaine 3

Identités et droits d'accès

OU, comptes, AGDLP, partages, GPO

4

Semaine 4

Filtrage, tests et rendu

Matrice de flux, recette partielle

Chaque semaine se termine par un point d'étape et un instantané des VM.

4	13	15	2	2+
semaines	missions	tests de recette	VM serveurs	postes joints

/20
notation

L'énoncé

i

PRÉAMBULE

Fiche du devoir et consignes

RUBRIQUE	VALEUR
Intitulé	Devoir n° 1 – Socle réseau et annuaire de Martins & Cie
Classe	BTS SIO 1re année, option SISR
Durée	1 mois (4 semaines), travail en séance et en autonomie
Modalité	Binôme (trinôme accepté si effectif impair)
Document de référence	Cahier des charges Martins & Cie v1.0 – chapitres 1 à 6, 8, 9, 11, 12 et 15
Périmètre	Phases 0 à 3 et 6 du plan de déploiement (tableau 22 du CDC) : RFW01 et DC01, postes clients de test
Rendu	Dossier technique PDF + scripts + export de configuration, fin de semaine 4
Notation	/20, grille au chapitre 9 ; points d'étape hebdomadaires notés en continu

Consignes générales

- **Aucun mot de passe en clair** dans le dossier, les captures ou les scripts (test T-S03 du CDC appliqué au rendu). Les captures montrant un champ de mot de passe sont floutées.
- Un **instantané (snapshot)** est pris à la fin de chaque semaine et nommé `S1-fin`, `S2-fin`, etc.
- Chaque preuve (capture, sortie de commande) est **horodatée** et rattachée à l'identifiant du test qu'elle valide (T-R01, T-A02…).
- Le **journal de bord** (annexe A) est rempli à chaque séance ; il est relevé en fin de semaine.
- Toute décision qui s'écarte du CDC est justifiée par écrit dans le dossier.

1

CHAPITRE 1

Contexte et objectifs

1.1 Mise en situation

Vous intégrez l'équipe de **Maria Bah**, administratrice système et réseau de Martins & Cie. Le PDG, M. Serge Martins, vient de valider la version 1.0 du cahier des charges. Votre mission pour ce premier mois : livrer le **socle de l'infrastructure**, c'est-à-dire le réseau segmenté, le pare-feu et l'annuaire Active Directory avec les droits d'accès aux répertoires partagés. Le second devoir s'appuiera directement sur ce que vous aurez construit.

1.2 Objectifs pédagogiques

1. Analyser un cahier des charges et arbitrer les incohérences relevées au chapitre 15.
2. Configurer un pare-feu pfSense avec VLAN 802.1Q, NAT, relais DHCP et règles en refus par défaut.
3. Installer et configurer un contrôleur de domaine Windows Server 2025 (AD DS, DNS, DHCP).
4. Mettre en œuvre une gestion des droits selon le modèle AGDLP et le principe du moindre privilège.
5. Déployer des stratégies de groupe et prouver leur application.
6. Tester, documenter et rendre compte d'une mise en service.

1.3 Ce qui est attendu à la fin du mois

ÉLÉMENT	ÉTAT ATTENDU
RFW01	VLAN 10 et 20 opérationnels, NAT sortant, relais DHCP, règles 1, 3, 4, 5, 7 et 10 du tableau 6
DC01	Domaine martinscie.lan, zones DNS directe et inverses, étendue DHCP VLAN 20, sous-réseaux déclarés
Annuaire	3 OU, 5 comptes, 5 groupes métier, 10 groupes d'accès GL_, mbah dans les groupes intégrés
Données	5 partages sur D:\Partages, ACL conformes à la matrice du tableau 12, ABE activée
GPO	Mots de passe et verrouillage, lecteurs réseau, administrateur local de DIRECTEUR01, sécurité des postes
Postes	Au minimum 2 postes Windows 11 joints au domaine (DIRECTEUR01 et SECRETAIRE01)

CHAPITRE 2

2 Organisation du travail

2.1 Répartition des rôles

Dans chaque binôme, un étudiant tient le rôle de **responsable réseau** (RFW01) et l'autre celui de **responsable annuaire** (DC01). Les rôles s'inversent en semaine 3 pour que chacun manipule les deux briques. Les deux membres sont interrogés indifféremment lors des points d'étape.

2.2 Rythme de travail

MOMENT	CONTENU	DURÉE INDICATIVE
Début de semaine	Lecture des missions, répartition des tâches, mise à jour du journal de bord	15 min
Séances	Réalisation technique, prise des preuves	selon emploi du temps
Fin de semaine	**Point d'étape** : démonstration de 5 minutes des jalons de la semaine devant l'enseignant	5 à 10 min / binôme
Hors séance	Rédaction du dossier, recherches, préparation de la semaine suivante	2 h / semaine environ

2.3 Ressources fournies

- Le cahier des charges complet (portail inframcie.fr).
- Les ISO : pfSense CE, Windows Server 2025 (évaluation), Windows 11 Pro.
- Les fichiers sources Informations_VM.xlsx, Groupes.xlsx et Droits_dacces.xlsx (utilisateurs.xlsx n'est **pas** distribué : ses mots de passe sont considérés comme compromis, voir 10.1 du CDC).
- Un hôte de virtualisation par binôme : vérifier qu'il couvre les ressources des VM du devoir (RFW01, DC01, 2 postes au minimum).

ATTENTION Les scripts PowerShell du CDC (chapitres 6.5 et 9) sont des **exemples**. Vous devez les relire, les comprendre, les adapter et les commenter. Un script copié sans adaptation ni explication n'est pas noté.

CHAPITRE 3

3 Calendrier sur quatre semaines

TABLEAU 1 — CALENDRIER DU DEVOIR N° 1

SEMAINE	THÈME	PHASES CDC	JALONS DU POINT D'ÉTAPE
S1	Analyse et pare-feu RFW01	0, 1, 2	Note d'arbitrage du ch. 15 ; T-R01 (partiel), T-R02, T-R03

SEMAINE	THÈME	PHASES CDC	JALONS DU POINT D'ÉTAPE
S2	Contrôleur de domaine DC01	3	T-R07, T-A01, T-A05 sur un premier poste
S3	Identités et droits	3, 5, 6	T-A02, T-A03, T-A04, T-A06, T-D01, T-D03
S4	Filtrage, recette partielle, rendu	6, 8 (partielle)	T-R04, T-D02 (25 cas), T-D04 ; dépôt du dossier

CONSEIL Une semaine non terminée bloque la suivante : DC01 a besoin de RFW01 pour sortir sur Internet, et les postes ont besoin du relais DHCP. Signalez tout retard dès le point d'étape, une aide ciblée sera apportée.

S1

SEMAINE 1

Analyse et pare-feu RFW01

Objectif : comprendre le besoin, arbitrer les incohérences et livrer un pare-feu qui route et sort sur Internet.

M1.1 Analyser le cahier des charges

- Lire les chapitres 1 à 4 et 15 du CDC ; relever pour chaque VM du périmètre : système, ressources, VLAN, adresse.
- Rédiger une **note d'arbitrage** (1 page) : pour les points 1 à 8 du tableau 26, indiquer si vous retenez la décision proposée et pourquoi.
- Calculer les ressources nécessaires sur votre hôte pour le devoir 1, puis pour l'ensemble du projet ; conclure sur la faisabilité.

M1.2 Préparer le socle virtuel

- Choisir l'hyperviseur et justifier ce choix au regard des exigences de 3.6 (802.1Q ou réseaux internes, TPM virtuel, instantanés).
- Créer les réseaux virtuels : un lien WAN vers la Freebox (ou le réseau de la salle) et un lien trunk, ou à défaut un réseau interne par VLAN.

M1.3 Installer et configurer RFW01

- Installer pfSense : nom d'hôte RFW01, domaine martinscie.lan, fuseau Europe/Paris.
- Créer les VLAN 10 et 20 sur l'interface parent, affecter les interfaces SRV (192.168.10.254/24) et CLI (192.168.20.254/24).

- WAN en DHCP ; décocher « Block private networks » ; laisser « Block bogon networks ».
- Vérifier le NAT sortant automatique pour les deux sous-réseaux.
- Désactiver le serveur DHCP intégré sur les interfaces VLAN (le DHCP sera porté par DC01).
- Règles provisoires « autoriser tout » sur SRV et CLI **clairement nommées « TEMPORAIRE – S1 »** : elles seront supprimées en semaine 4.
- Changer le mot de passe du compte admin ; exporter config.xml.

Jalons du point d'étape

PREUVE ATTENDUE	TEST CDC	VALIDÉ
Note d'arbitrage des points 1 à 8 du chapitre 15	–	☐
Interfaces de RFW01 et leurs adresses (capture Status > Interfaces)	T-R01	☐
Ping des deux passerelles depuis une VM de test dans chaque VLAN	T-R02	☐
Accès à un site Internet depuis le VLAN 10 et le VLAN 20	T-R03	☐
Export config.xml daté et instantané `S1-fin`	–	☐

PIÈGE CLASSIQUE Si la Freebox (ou le réseau de la salle) utilise déjà 192.168.10.0/24 ou 192.168.20.0/24, le routage échoue de façon silencieuse. Vérifiez le plan d'adressage de l'amont **avant** de configurer les VLAN (tableau 4 du CDC).

S2 SEMAINE 2

Contrôleur de domaine DC01

Objectif : disposer d'un domaine fonctionnel qui distribue les adresses du VLAN 20 à travers le pare-feu.

M2.1 Installer DC01

- Windows Server 2025, nom DC01, IP 192.168.10.10/24, passerelle 192.168.10.254, DNS préféré 127.0.0.1 (et non 8.8.8.8, voir 4.3 du CDC).
- Ajouter un second disque virtuel pour le volume D: qui accueillera les partages en semaine 3.

M2.2 Créer le domaine et le DNS

- Promouvoir DC01 : nouvelle forêt martinscie.lan, NetBIOS MARTINSCIE.

- Configurer les redirecteurs 8.8.8.8 et 8.8.4.4, créer les zones inverses 10.168.192 et 20.168.192, mises à jour dynamiques sécurisées.
- Déclarer les sous-réseaux 192.168.10.0/24 et 192.168.20.0/24 dans Sites et services AD.

M2.3 Mettre en place le DHCP

- Installer et autoriser le rôle DHCP dans l'AD ; créer l'étendue VLAN20-Clients (.100 à .253), options 003, 006, 015, bail 8 jours.
- Sur RFW01, activer le **relais DHCP** sur l'interface CLI vers 192.168.10.10 ; ajuster la règle provisoire si besoin.
- Expliquer dans le dossier, avec un schéma, pourquoi un relais est indispensable ici (diffusion DHCPDISCOVER non routée).

M2.4 Intégrer un premier poste

- Installer DIRECTEUR01 (Windows 11 Pro, TPM virtuel, démarrage sécurisé) dans le VLAN 20.
- Vérifier l'obtention d'une adresse, puis joindre le poste au domaine.

Jalons du point d'étape

PREUVE ATTENDUE	TEST CDC	VALIDÉ
ipconfig /all de DIRECTEUR01 : adresse entre .100 et .253, passerelle .254, DNS 192.168.10.10	T-R07	☐
nslookup de dc01.martinscie.lan et d'un nom externe depuis le poste	T-A01	☐
Bail visible dans la console DHCP de DC01	T-R07	☐
Ouverture de session de domaine sur DIRECTEUR01	T-A05	☐
Instantané `S2-fin`	–	☐

S3 SEMAINE 3 — Identités, droits et GPO

Objectif : traduire les tableaux 9 à 14 du CDC en objets AD, en partages et en stratégies de groupe. Les rôles du binôme s'inversent.

M3.1 Structurer l'annuaire

- Créer les OU Utilisateurs, Groupes et Ordinateurs ; rediriger les nouveaux comptes machines vers OU=Ordinateurs (redircmp) et y déplacer DIRECTEUR01.
- Créer les 5 comptes par un **script PowerShell commenté** : mot de passe initial saisi avec Read-Host -AsSecureString, unique par compte, changement obligatoire à la première connexion.
- Créer les 5 groupes globaux métier et y placer les comptes ; ajouter mbah aux groupes intégrés Administrateurs et Admins du domaine (point 7 du ch. 15).

M3.2 Mettre en place les droits (AGDLP)

- Créer les 10 groupes locaux de domaine GL_<Dossier>_LE et GL_<Dossier>_L et les remplir à partir des **groupes globaux** (et non des comptes) conformément au tableau 14.
- Créer les 5 dossiers sous D:\Partages, couper l'héritage, appliquer les ACL NTFS, partager avec ABE.
- Produire la commande Get-Acl de chaque dossier et la comparer au tableau 12.

M3.3 Déployer les GPO

- Politique de mots de passe et de verrouillage du domaine (tableau 11).
- GPO-Lecteurs-Reseau : une lettre par dossier, ciblage par groupe (préférences de GPO).
- GPO-Admin-Local-Direction : smartins administrateur local de DIRECTEUR01 uniquement.
- GPO-Postes-Securite sur OU=Ordinateurs.
- Installer et joindre SECRETAIRE01 ; vérifier l'application avec gpresult /r.

Jalons du point d'étape

PREUVE ATTENDUE	TEST CDC	VALIDÉ
Arborescence ADUC : 3 OU, 5 comptes, groupes	T-A02	☐
Appartenance des groupes (Get-ADGroupMember) conforme au tableau 10	T-A03	☐
Changement de mot de passe exigé à la première connexion	T-A04	☐
Mot de passe non conforme refusé ; compte verrouillé après 5 échecs	T-A06	☐
Liste des 5 partages de \\DC01	T-D01	☐
ACL des 5 dossiers : seuls les groupes prévus, SYSTEM et Admins du domaine	T-D03	☐
gpresult /r sur SECRETAIRE01 ; instantané `S3-fin`	–	☐

À JUSTIFIER Le CDC attribue à ldasilva un accès en lecture au dossier Direction (point 6 du ch. 15). Indiquez dans le dossier comment vous retireriez ce droit si le PDG le refusait, et quel(s) objet(s) AD seraient modifiés.

S4 SEMAINE 4

Filtrage, recette et rendu

Objectif : refermer le pare-feu, prouver que les droits sont exacts, et rendre un dossier exploitable.

M4.1 Appliquer la matrice de flux

- Créer les alias pfSense : DC01, PARC01, SECU01, POSTE_ADMIN, PORTS_AD.
- Supprimer les règles « TEMPORAIRE – S1 » ; mettre en place les règles 1, 3, 4, 5, 7 et 10 du tableau 6 dans le bon ordre (exceptions avant le blocage n° 4).
- Activer la journalisation des règles de blocage ; exporter config.xml.
- Vérifier que les ouvertures de session, le DHCP et les lecteurs réseau fonctionnent toujours après filtrage.

M4.2 Recette des droits

- Remplir la **matrice des 25 cas** (5 utilisateurs × 5 dossiers) en testant réellement lecture et écriture ; comparer au tableau 12.
- Tester le montage des lecteurs réseau pour chaque compte.
- Tenter un RDP vers DC01 depuis un poste client et relever la ligne correspondante dans les journaux de RFW01.

M4.3 Finaliser le dossier

- Compléter le dossier technique (plan au chapitre 8) et relire l'ensemble à deux.
- Vérifier qu'aucun mot de passe n'apparaît dans les fichiers rendus.
- Préparer la démonstration finale de 10 minutes.

Jalons du point d'étape

PREUVE ATTENDUE	TEST CDC	VALIDÉ
Capture des règles des interfaces CLI et SRV (avec alias)	EF-R04	☐
RDP / SSH refusés depuis le VLAN 20 et visibles dans les journaux	T-R04	☐

PREUVE ATTENDUE	TEST CDC	VALIDÉ
Matrice des 25 cas remplie et conforme	T-D02	☐
Lecteurs montés pour chaque compte	T-D04	☐
Instantané `S4-fin` = état de départ du devoir n° 2	–	☐

IMPORTANT L'instantané `S4-fin` doit être conservé intact : c'est le point de départ du devoir n° 2.

CHAPITRE 8

8 Livrables

TABLEAU 2 — LIVRABLES DU DEVOIR N° 1

LIVRABLE	CONTENU	FORMAT
Dossier technique	Plan ci-dessous, 15 à 25 pages hors annexes	PDF
Note d'arbitrage	Décisions sur les points 1 à 8 du chapitre 15 (rendue en S1, intégrée en annexe)	PDF
Scripts	Création des OU, comptes, groupes, ACL et partages ; commentés, sans secret	.ps1
Configuration	Dernier export config.xml de RFW01 (mots de passe hachés uniquement)	.xml
Matrice de recette	25 cas de droits + tests du tableau 1 avec résultat et preuve	Tableur ou PDF
Journal de bord	Annexe A complétée pour les 4 semaines	PDF

Plan imposé du dossier technique

1. Page de garde, sommaire, historique des versions.
2. Contexte et périmètre du devoir.
3. Schéma réseau réalisé (outil au choix) et plan d'adressage effectif.
4. RFW01 : interfaces, NAT, relais DHCP, règles et alias (avec justification de l'ordre).
5. DC01 : AD DS, DNS, DHCP.
6. Annuaire : OU, comptes, groupes, schéma AGDLP.
7. Droits et partages : ACL, ABE, GPO.

8. Recette : tableau des tests, résultats, écarts et corrections.

9. Bilan : difficultés rencontrées, points restant à traiter pour le devoir n° 2.

CHAPITRE 9

9 Évaluation

TABLEAU 3 — GRILLE D'ÉVALUATION

CRITÈRE	ATTENDUS	POINTS
Analyse du besoin	Note d'arbitrage pertinente, calcul de ressources juste	2
Pare-feu RFW01	VLAN, NAT, relais DHCP, règles ordonnées et journalisées, alias	4
Contrôleur de domaine	AD DS, DNS (zones, redirecteurs), DHCP et options	3
Identités et droits	Comptes par script, AGDLP respecté, ACL exactes sur les 25 cas, ABE	5
Stratégies de groupe	4 GPO fonctionnelles et prouvées (gpresult)	2
Documentation et preuves	Dossier structuré, preuves rattachées aux tests, aucun secret	2
Points d'étape et oral	Jalons tenus, démonstration, réponses individuelles	2
Total		**20**

PÉNALITÉS Mot de passe en clair dans un livrable : **−2 points**. Règle « autoriser tout » encore active au rendu : **−2 points**. Retard de rendu : −1 point par jour ouvré.

9.1 Compétences du référentiel mobilisées

BLOC	COMPÉTENCE	OÙ
Bloc 1	Gérer le patrimoine informatique	Semaine 1 (inventaire des VM, ressources)
Bloc 1	Travailler en mode projet	Planification, journal de bord, points d'étape
Bloc 1	Mettre à disposition des utilisateurs un service informatique	Comptes, lecteurs réseau, recette
Bloc 2 SISR	Concevoir une solution d'infrastructure réseau	Arbitrages, adressage, matrice de flux

BLOC	COMPÉTENCE	OÙ
Bloc 2 SISR	Installer, tester et déployer une solution d'infrastructure réseau	RFW01, DC01, postes
Bloc 3	Sécuriser les équipements et les usages des utilisateurs	Filtrage, GPO, politique de mots de passe

A

ANNEXE

Journal de bord

À recopier dans le dossier et compléter à chaque séance.

MODÈLE DE JOURNAL DE BORD

DATE	ÉTUDIANT	TÂCHES RÉALISÉES	PROBLÈME RENCONTRÉ	SOLUTION / PISTE	TEST VALIDÉ

PORTAIL SISR1
← Rubrique Devoirs

MOIS SUIVANT
Devoir n° 2 – Services, supervision et sécurité →

© 2026 Portail SISR · Martins & Cie · SIO1 – SISR