DEVOIR N° 1 · 1 MOIS · SIO2 – SISR

Réseau haute disponibilité et annuaire redondé.

Premier mois du projet SIO2 – SISR : deux pare-feux pfSense en CARP derrière la passerelle virtuelle 192.168.10.1, deux contrôleurs de domaine, un DHCP en basculement, puis les droits AGDLP et des partages répliqués par DFS. Chaque semaine se conclut par une panne provoquée et mesurée.

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

1. Semaine 1
   Analyse et pare-feu RFW01
   Écarts, réseaux virtuels, transit, LAN, SYNC
2. Semaine 2
   Haute disponibilité RFW01 / RFW02
   CARP, pfsync, XMLRPC, NAT sur VIP
3. Semaine 3
   Annuaire redondé DC01 / DC02
   AD DS, DNS, basculement DHCP, FSMO
4. Semaine 4
   Droits, DFS et GPO, rendu
   AGDLP, DFS-N / DFS-R, GPO-01 à 07

Une panne provoquée et mesurée à chaque point d'étape à partir de la semaine 2.

4	12	10	2	25
semaines	missions	tests REC	paires redondées	droits vérifiés

/20
notation

L'énoncé

i

PRÉAMBULE

Fiche du devoir et consignes

RUBRIQUE	VALEUR
Intitulé	Devoir n° 1 – Réseau haute disponibilité et annuaire redondé de Martins & Cie
Classe	BTS SIO 2e 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 SIO2 – SISR v1.0 du 16 novembre 2026 et dossier du projet (rubrique Projet du portail)
Périmètre	RFW01, RFW02, DC01, DC02, DIRECTEUR01 et SECRETAIRE01 ; réseau 192.168.10.0/24, transit 192.168.0.0/24, lien SYNC 172.16.0.0/30
Rendu	Dossier d'architecture PDF + scripts + exports 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. Les mots de passe de utilisateurs.xlsx sont considérés comme compromis (écart n° 5) et ne sont jamais réutilisés.
- On ne modifie **jamais RFW02 directement** : toute règle est saisie sur RFW01 et recopiée par XMLRPC.
- Un **instantané** de chaque VM est pris en fin de semaine (`S1-fin` à `S4-fin`). Les répliques peuvent rester éteintes hors des tests de bascule pour économiser la mémoire de l'hôte.
- Chaque preuve (capture, sortie de commande) est **horodatée** et rattachée à une exigence (RES-, AD-, FIC-) ou à un test de recette (REC-).
- Le **journal de bord** (annexe A) est rempli à chaque séance.

1

CHAPITRE 1

Contexte et objectifs

1.1 Mise en situation

Martins & Cie ne veut plus qu'une seule panne arrête l'entreprise. Le cahier des charges SIO2 – SISR impose un réseau unique 192.168.10.0/24 derrière **deux pare-feux pfSense** partageant la passerelle virtuelle 192.168.10.1, et un annuaire porté par **deux contrôleurs de domaine**. Pour ce premier mois, vous construisez cette fondation redondée, puis vous y installez les comptes, les droits et les partages répliqués. Le devoir n° 2 ajoutera les services applicatifs, la supervision et la sécurité.

1.2 Objectifs pédagogiques

1. Analyser un cahier des charges et arbitrer les écarts entre schéma, CDC et fichiers sources.
2. Mettre en œuvre la redondance du premier saut (CARP, équivalent libre de VRRP) avec synchronisation des états et de la configuration.
3. Installer un annuaire Active Directory sur deux contrôleurs et en contrôler la réplication.
4. Partager une étendue DHCP entre deux serveurs en basculement.
5. Appliquer le modèle AGDLP et publier les partages dans un espace de noms DFS répliqué.
6. Prouver la tenue des exigences par des tests de bascule mesurés.

1.3 Ce qui est attendu à la fin du mois

ÉLÉMENT	ÉTAT ATTENDU
RFW01 / RFW02	CARP sur LAN (VIP .1) et WAN (VIP transit .1), pfsync et XMLRPC sur SYNC, NAT sortant sur la VIP WAN, refus par défaut
DC01 / DC02	Domaine martinscie.lan, deux catalogues globaux, FSMO sur DC01, DNS intégré avec zone inverse, corbeille AD
DHCP	Étendue .100 à .200 en basculement 50/50, options routeur .1, DNS .10 et .11
Annuaire	OU Utilisateurs, Groupes, Ordinateurs, Serveurs ; 5 comptes ; groupes de service ; 10 groupes DL_ ; PSO pour mbah et hnyame
Fichiers	5 partages publiés sous \\martinscie.lan\partages, répliqués par DFS-R, ABE, clichés instantanés
GPO	GPO-01 à GPO-07 du cahier des charges
Recette	REC-01 à REC-09 et REC-13 réussis et prouvés

CHAPITRE 2

2 Organisation du travail

2.1 Répartition des rôles

Un étudiant est **responsable réseau et haute disponibilité** (RFW01, RFW02), l'autre **responsable annuaire** (DC01, DC02). Les rôles s'inversent en semaine 3. Lors des tests de bascule, l'un provoque la panne et l'autre mesure et consigne.

2.2 Rythme de travail

MOMENT	CONTENU	DURÉE INDICATIVE
Début de semaine	Lecture des missions, répartition, journal de bord	15 min
Séances	Réalisation technique, prise des preuves	selon emploi du temps
Fin de semaine	**Point d'étape** : démonstration des jalons, dont une bascule en direct à partir de la semaine 2	5 à 10 min / binôme
Hors séance	Rédaction, recherches, préparation	2 h / semaine environ

2.3 Ressources fournies

- Le cahier des charges et le dossier du projet (rubrique Projet), dont l'inventaire des 13 éléments et le tableau des 21 points à confirmer.
- Les guides de la rubrique Tutos (pare-feux en haute disponibilité, DC01 et DC02, partages répliqués) : ils guident, ils ne remplacent pas votre compréhension.
- Les ISO pfSense CE, Windows Server 2025 (évaluation), Windows 11 Pro.
- Un hôte par binôme : en maquette, le périmètre du devoir demande environ 10 vCPU et 16 Go de RAM.

PIÈGE CLASSIQUE Deux pare-feux qui affichent MASTER en même temps (« double maître ») : les annonces CARP ne passent pas. Sous VirtualBox, le mode promiscuité des cartes WAN et LAN doit être réglé sur « Allouer les VM ». Vérifiez-le dès la semaine 1.

CHAPITRE 3

3 Calendrier sur quatre semaines

TABLEAU 1 — CALENDRIER DU DEVOIR N° 1

SEMAINE	THÈME	EXIGENCES	JALONS DU POINT D'ÉTAPE
S1	Analyse et pare-feu RFW01	RES-01, 05, 06	Note d'arbitrage ; RFW01 route et sort sur Internet
S2	Haute disponibilité des pare-feux	RES-02 à 04	REC-01, REC-02 ; XMLRPC prouvé
S3	Annuaire redondé	AD-01 à 08, RES-08	REC-03, REC-04, REC-05

SEMAINE	THÈME	EXIGENCES	JALONS DU POINT D'ÉTAPE
S4	Droits, DFS, GPO et rendu	FIC-01 à 08, GPO-01 à 07	REC-06 à REC-09, REC-13 ; dépôt du dossier

CONSEIL Une semaine non terminée bloque la suivante : sans la VIP .1, les contrôleurs n'ont pas Internet ; sans DC02, le basculement DHCP et DFS-R sont impossibles. Signalez tout retard dès le point d'étape.

S1

SEMAINE 1

Analyse et pare-feu RFW01

Objectif : comprendre le besoin de continuité, trancher les écarts et livrer un premier pare-feu opérationnel.

M1.1 Analyser le cahier des charges

- Lire l'architecture, l'adressage, les exigences et les risques du dossier du projet.
- Rédiger une **note d'arbitrage** (1 à 2 pages) sur les écarts 4, 6, 9, 12, 13, 15, 16, 17 et 20 : retenez-vous le choix proposé, et pourquoi ?
- Expliquer en une demi-page la différence entre VRRP et CARP, et pourquoi le schéma cite l'un et pfSense met en œuvre l'autre.
- Calculer les ressources nécessaires (maquette) pour le devoir 1, puis pour les 12 VM ; conclure sur la faisabilité.

M1.2 Préparer les réseaux virtuels

- Créer trois réseaux : **transit** (192.168.0.0/24, vers la Freebox ou le réseau de la salle), **LAN** (192.168.10.0/24) et **SYNC** (172.16.0.0/30, lien direct entre les deux pare-feux).
- Activer le mode promiscuité nécessaire à CARP sur les cartes transit et LAN des pare-feux.
- Produire le schéma réseau réalisé (outil au choix) avec toutes les adresses.

M1.3 Installer RFW01

- pfSense CE : nom RFW01, domaine martinscie.lan, fuseau Europe/Paris ; WAN 192.168.0.2/24, LAN 192.168.10.2/24, SYNC 172.16.0.1/30.
- Décocher « Block private networks » sur le WAN (double NAT) ; serveur DHCP de pfSense désactivé (le DHCP sera porté par DC01 et DC02).
- Alias ADMINS, DC, PARC ; règles minimales : LAN vers Internet en 80/443, DNS vers les DC ; interface d'administration réservée à l'alias ADMINS.

- Changer le mot de passe du compte admin ; exporter config.xml.

Jalons du point d'étape

PREUVE ATTENDUE	RÉFÉRENCE	VALIDÉ
Note d'arbitrage et explication VRRP / CARP	–	☐
Schéma réseau réalisé avec les trois réseaux	RES-01	☐
Une VM de test du LAN, passerelle 192.168.10.2 provisoire, accède à Internet	RES-05	☐
Règles de RFW01 avec alias, blocage par défaut journalisé	RES-06	☐
Export config.xml et instantané `S1-fin`	–	☐

PROVISOIRE Cette semaine, la VM de test utilise .2 comme passerelle. Dès la semaine 2, plus aucun hôte ne doit pointer vers .2 ou .3 : la seule passerelle autorisée est la VIP .1 (RES-02).

S2 SEMAINE 2

Haute disponibilité RFW01 / RFW02

Objectif : une passerelle qui survit à la panne d'un pare-feu en moins de 5 secondes, sans couper les sessions.

M2.1 Installer RFW02

- Même version de pfSense que RFW01 ; WAN 192.168.0.3/24, LAN 192.168.10.3/24, SYNC 172.16.0.2/30 ; mêmes noms d'interfaces dans le même ordre.
- Règle sur SYNC autorisant tout entre 172.16.0.1 et 172.16.0.2 uniquement.

M2.2 Mettre en haute disponibilité

- Sur RFW01 : synchronisation des états (pfsync) via SYNC, pair 172.16.0.2 ; synchronisation de la configuration (XMLRPC) vers 172.16.0.2 avec un compte dédié.
- Créer les adresses virtuelles CARP : 192.168.10.1/24 sur LAN et 192.168.0.1/24 sur WAN, même VHID et même mot de passe ; skew 0 sur RFW01, 100 recopié en secondaire sur RFW02.
- NAT sortant en mode hybride ou manuel : traduction des sources du LAN vers la **VIP WAN** 192.168.0.1.
- Autoriser CARP (protocole IP 112) entre les deux pare-feux ; vérifier qu'aucun « double maître » n'apparaît.

M2.3 Tester les bascules

- Passer la VM de test en passerelle .1 ; lancer un téléchargement long ou un ping continu vers Internet.
- Couper brutalement RFW01, mesurer la durée de coupure (REC-01), observer le statut CARP sur RFW02.
- Redémarrer RFW01 : constater le retour en maître et l'absence de coupure (REC-02). Indiquer la politique de préemption retenue.
- Ajouter une règle sur RFW01 et constater sa présence sur RFW02 ; tester le mode maintenance CARP.

Jalons du point d'étape

PREUVE ATTENDUE	RÉFÉRENCE	VALIDÉ
Status > CARP : RFW01 MASTER, RFW02 BACKUP pour les deux VIP	RES-03	☐
Ping continu pendant l'arrêt de RFW01 : coupure mesurée inférieure à 5 s	REC-01	☐
Retour de RFW01 sans coupure, rôle maître conforme à la politique choisie	REC-02	☐
Règle créée sur RFW01 visible sur RFW02 ; états pfsync visibles sur RFW02	RES-04	☐
Export config.xml des deux pare-feux ; instantané `S2-fin`	–	☐

POUR ALLER PLUS LOIN Comparez la coupure observée avec et sans pfsync (désactivé le temps du test) pendant une session SSH ouverte vers Internet. Expliquez le résultat.

S3

SEMAINE 3

Annuaire redondé DC01 / DC02

Objectif : un annuaire, un DNS et un DHCP qui continuent de répondre quand DC01 s'arrête. Les rôles du binôme s'inversent.

M3.1 Installer DC01

- Windows Server 2025, nom DC01, 192.168.10.10/24, passerelle **.1**, DNS 192.168.10.11 puis 127.0.0.1 (après promotion de DC02).
- Nouvelle forêt martinscie.lan, NetBIOS MARTINSCIE ; corbeille AD activée ; DC01 source de temps du domaine (NTP externe).
- DNS : redirecteurs, zone inverse 10.168.192.in-addr.arpa avec PTR des adresses fixes, mises à jour dynamiques sécurisées uniquement.

M3.2 Installer DC02 et vérifier la réplication

- Windows Server 2025, 192.168.10.11/24, DNS 192.168.10.10 puis 127.0.0.1 ; promotion en contrôleur supplémentaire, catalogue global et DNS.
- Ajouter un second disque à chaque DC pour les partages de la semaine 4.
- Contrôler avec `repadmin /replsummary`, `repadmin /showrepl` et `dcdiag /q` ; vérifier que DC01 porte les 5 rôles FSMO (`netdom query fsmo`).

M3.3 Mettre en place le DHCP redondé

- Rôle DHCP sur DC01 et DC02, autorisés dans l'AD.
- Étendue 192.168.10.100 à .200 sur DC01, options 003 = .1, 006 = .10 et .11, 015 = martinscie.lan, bail 8 jours.
- Configurer le basculement vers DC02 en répartition de charge 50/50 ; expliquer le MCLT dans le dossier.
- Installer DIRECTEUR01 (Windows 11 Pro, TPM virtuel) et le joindre au domaine.

Jalons du point d'étape

PREUVE ATTENDUE	RÉFÉRENCE	VALIDÉ
repadmin /replsummary sans erreur ; dcdiag /q vide	AD-01 à 03	☐
Arrêt de DC01 : ouverture de session, résolution DNS et renouvellement DHCP réussis via DC02	REC-03	☐
Utilisateur de test créé sur DC01, visible sur DC02 (heure de création et de constat)	REC-04	☐
ipconfig /all de DIRECTEUR01 : adresse .100 à .200, passerelle .1, DNS .10 et .11	REC-05	☐
État du basculement DHCP « Normal » sur les deux serveurs ; instantané `S3-fin`	–	☐

À NE PAS FAIRE Ne clonez jamais un contrôleur de domaine pour créer DC02 : installez-le, puis promouvez-le. Ne restaurez pas non plus un vieil instantané d'un seul DC sans comprendre les conséquences sur la réplication (USN).

S4 SEMAINE 4

Droits, DFS, GPO et rendu

Objectif : traduire la matrice des droits en groupes, publier des partages répliqués et appliquer les stratégies du cahier des charges.

M4.1 Comptes et groupes

- Créer les OU Utilisateurs, Groupes, Ordinateurs et Serveurs ; rediriger les comptes machines (redircmp).
- Créer les 5 comptes par un **script PowerShell commenté** (Read-Host -AsSecureString, mot de passe initial unique, changement à la première connexion) ; créer le compte d'administration mbah-adm.
- Groupes de service (globaux) ; mbah-adm dans les groupes intégrés Admins du domaine et Administrateurs (écart n° 6) ; PSO 16 caractères pour mbah, mbah-adm et hnyame.
- Créer les 10 groupes DL_<Dossier>_RW et DL_<Dossier>_RO et y placer les **groupes de service** conformément au dossier du projet.

M4.2 Partages répliqués

- Créer les 5 dossiers sur le volume de données de DC01 et de DC02, couper l'héritage, appliquer les ACL NTFS par les groupes DL_, partager avec ABE.
- Créer l'espace de noms de domaine `\\martinscie.lan\partages` avec deux cibles par dossier ; créer le groupe de réplication DFS-R entre DC01 et DC02.
- Activer les clichés instantanés sur le volume de données ; activer l'audit des accès refusés.

M4.3 Stratégies de groupe et recette

- Déployer GPO-01 à GPO-07 (verrouillage de session, lecteurs par groupe pointant vers l'espace de noms, pare-feu Windows, mises à jour, supports amovibles, ouverture de session limitée, audit).
- Installer et joindre SECRETAIRE01 ; vérifier avec gpresult /r.
- Remplir la **matrice des 25 droits** en testant réellement lecture et écriture ; tester cgrimeau sur Direction.
- Supprimer un fichier de Secrétariat et le restaurer depuis les versions précédentes.
- Compléter et rendre le dossier d'architecture.

Jalons du point d'étape

PREUVE ATTENDUE	RÉFÉRENCE	VALIDÉ
Première ouverture de session des 5 comptes : changement de mot de passe imposé	REC-06	☐
Session refusée sur une machine non autorisée (GPO-06)	REC-07	☐
Matrice des 25 droits remplie et conforme	REC-08	☐
cgrimeau : dossier Direction invisible ou refusé, événement 4656 / 5145 journalisé	REC-09	☐
Fichier de Secrétariat restauré depuis les versions précédentes	REC-13	☐
Fichier créé via DC01 présent sur DC02 (DFS-R) ; accès maintenu DC01 arrêté	FIC-04	☐

PREUVE ATTENDUE	RÉFÉRENCE	VALIDÉ
Instantané `S4-fin` = état de départ du devoir n° 2	–	☐

IMPORTANT Une réplication n'est pas une sauvegarde : une suppression sur DC01 est répliquée aussitôt sur DC02. Mentionnez-le dans le dossier et gardez les clichés instantanés actifs ; la sauvegarde indépendante sera mise en place au devoir n° 2.

CHAPITRE 8

8 Livrables

TABLEAU 2 — LIVRABLES DU DEVOIR N° 1

LIVRABLE	CONTENU	FORMAT
Dossier d'architecture	Plan ci-dessous, 20 à 30 pages hors annexes	PDF
Note d'arbitrage	Décisions sur les écarts étudiés et explication VRRP / CARP (rendue en S1)	PDF
Scripts	Création des OU, comptes, groupes, ACL, partages et DFS ; commentés, sans secret	.ps1
Configurations	config.xml de RFW01 et RFW02 ; export de la structure AD (OU, comptes, groupes)	.xml, .csv
Fiche de bascule	Mesures de REC-01 à REC-04 : heure, durée, observation	PDF ou tableur
Matrice de recette	25 droits + tests REC-01 à REC-09 et REC-13 avec preuve	Tableur ou PDF
Journal de bord	Annexe A complétée pour les 4 semaines	PDF

Plan imposé du dossier d'architecture

1. Page de garde, sommaire, historique des versions.
2. Contexte, périmètre et arbitrages retenus.
3. Schéma réseau réalisé, plan d'adressage et inventaire.
4. Pare-feux : interfaces, CARP, pfsync, XMLRPC, NAT, règles et alias.
5. Annuaire : DC01, DC02, FSMO, DNS, réplication, DHCP en basculement.
6. Identités et droits : OU, comptes, groupes, schéma AGDLP, PSO.
7. Fichiers : partages, DFS-N, DFS-R, ABE, clichés instantanés ; GPO.
8. Recette : tests, mesures de bascule, écarts et corrections.

9. Bilan : limites de la redondance (switch, Freebox), points pour le devoir n° 2.

CHAPITRE 9

9 Évaluation

TABLEAU 3 — GRILLE D'ÉVALUATION

CRITÈRE	ATTENDUS	POINTS
Analyse du besoin	Arbitrages argumentés, VRRP / CARP compris, calcul de ressources juste	2
Pare-feux en haute disponibilité	CARP sur 2 VIP, pfsync, XMLRPC, NAT sur VIP, règles et refus par défaut	5
Annuaire redondé	DC01 et DC02, réplication saine, DNS, FSMO, DHCP en basculement	4
Droits et fichiers	AGDLP respecté, 25 droits exacts, DFS-N et DFS-R, ABE, clichés	4
Stratégies de groupe	GPO-01 à 07 fonctionnelles et prouvées	1
Documentation et preuves	Dossier structuré, bascules mesurées, aucun secret	2
Points d'étape et oral	Jalons tenus, bascule en direct, réponses individuelles	2
Total		**20**

PÉNALITÉS Mot de passe en clair dans un livrable : **−2 points**. Hôte dont la passerelle est .2 ou .3 au rendu : **−1 point**. Modification faite directement sur RFW02 et perdue à la synchronisation : **−1 point**. Retard : −1 point par jour ouvré.

9.1 Compétences du référentiel mobilisées

BLOC	COMPÉTENCE	OÙ
Bloc 1	Gérer le patrimoine informatique	Inventaire, ressources, arbitrages
Bloc 1	Travailler en mode projet	Planification, journal de bord, points d'étape
Bloc 2 SISR	Concevoir une solution d'infrastructure réseau	Haute disponibilité, adressage, flux
Bloc 2 SISR	Installer, tester et déployer une solution d'infrastructure réseau	Pare-feux, contrôleurs, DFS, tests de bascule
Bloc 3	Garantir la disponibilité, l'intégrité et la confidentialité des services	CARP, réplication AD, DFS-R, clichés

BLOC	COMPÉTENCE	OÙ
Bloc 3	Sécuriser les équipements et les usages des utilisateurs	Refus par défaut, PSO, GPO

A

ANNEXE

Journal de bord et fiche de bascule

À recopier dans le dossier et compléter à chaque séance.

MODÈLE DE JOURNAL DE BORD

DATE	ÉTUDIANT	TÂCHES RÉALISÉES	PROBLÈME RENCONTRÉ	SOLUTION / PISTE	RÉFÉRENCE VALIDÉE

FICHE DE MESURE DES BASCULES

TEST	PANNE PROVOQUÉE	HEURE	DURÉE DE COUPURE	OBSERVATION
REC-01	Arrêt de RFW01			
REC-02	Retour de RFW01			
REC-03	Arrêt de DC01			
REC-04	Objet créé sur DC01			

PORTAIL SISR2
← Rubrique Devoirs

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

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