DEVOIR N° 2 · 1 MOIS · SIO2 – SISR

Services répliqués, supervision et sécurité.

Second mois du projet SIO2 – SISR : GLPI et intranet sur PARC01 avec leur réplique PARC02, un helpdesk utilisé pour de vrais tickets, Zabbix qui surveille chaque paire redondée, un VPN sur l'adresse virtuelle, un audit depuis SECU01, des sauvegardes 3-2-1 et la recette des 14 tests.

Binôme **identique** Durée **4 semaines** Départ **S4-fin du devoir 1** Rendu **PV de recette**

1

Semaine 1

PARC01 : GLPI et intranet

Debian 12, HTTPS par CA interne, LDAP

2

Semaine 2

Support, parc et réplique PARC02

Tickets, inventaire, MariaDB, rsync

3

Semaine 3

Supervision Zabbix 7.0 LTS

13 éléments, CARP, réplications, alertes

4

Semaine 4

VPN, audit, sauvegarde, recette

OpenVPN, SECU01/02, 3-2-1, PV

Le mois se conclut par la recette complète : REC-01 à REC-14.

4	12	6	13	14
semaines	missions	tickets à traiter	éléments supervisés	tests REC

/20
notation

L'énoncé

i

PRÉAMBULE

Fiche du devoir et consignes

RUBRIQUE	VALEUR
Intitulé	Devoir n° 2 – Services répliqués, supervision et sécurité de Martins & Cie
Classe	BTS SIO 2e année, option SISR
Durée	1 mois (4 semaines), travail en séance et en autonomie
Modalité	Même binôme que le devoir n° 1
Document de référence	Cahier des charges SIO2 – SISR v1.0 et dossier du projet (rubrique Projet du portail)
Point de départ	Instantané `S4-fin` du devoir n° 1 : pare-feux en CARP, DC01 et DC02, comptes, droits, DFS
Périmètre	PARC01, PARC02, SECU01, SECU02, WEBDEV01 ; VPN sur les pare-feux ; sauvegarde ; recette complète
Rendu	PV de recette, dossier d'exploitation, rapport d'audit, fin de semaine 4
Notation	/20, grille au chapitre 9 ; points d'étape hebdomadaires notés en continu

Consignes générales

- Les consignes du devoir n° 1 restent valables : aucun mot de passe en clair, aucune modification directe sur RFW02, instantané en fin de semaine, preuves rattachées à une exigence ou à un test REC-.
- Les comptes par défaut (glpi, tech, normal, post-only, Admin Zabbix, kali, root SSH) sont traités **le jour même** de l'installation (écart n° 21).
- SECU01 et SECU02 ne sont utilisés que sur le périmètre Martins & Cie et pendant la fenêtre autorisée par écrit (annexe B). Aucun accès VPN vers SECU (VPN-04).

RATTRAPAGE Un binôme dont le socle du devoir n° 1 n'est pas opérationnel reçoit en début de semaine 1 un environnement de référence. Le devoir n° 2 reste noté intégralement ; l'usage de cet environnement est mentionné dans le dossier.

CHAPITRE 1

1 Contexte et objectifs

1.1 Mise en situation

La fondation redondée est en service. M. Martins veut maintenant un **helpdesk** et un **inventaire** fiables, une **supervision** qui prévient avant les utilisateurs, un **accès distant** sécurisé et une première **campagne d'audit** menée par Hervé Nyame. Comme pour le réseau et l'annuaire, aucun service critique ne doit dépendre d'une seule machine : PARC01 a sa réplique PARC02, SECU01 sa réplique SECU02. Le mois se termine par la recette des 14 tests du cahier des charges.

1.2 Objectifs pédagogiques

1. Installer un serveur applicatif Debian 12 sécurisé (Apache, MariaDB, PHP 8.2) avec un certificat d'une autorité interne.
2. Déployer GLPI 10 : authentification AD, inventaire des 13 éléments, helpdesk avec catégories et niveaux de service.
3. Répliquer une base de données et des fichiers vers un serveur de secours, puis basculer manuellement dans un délai fixé.
4. Superviser une infrastructure redondée avec Zabbix 7.0 LTS : état CARP, réplication AD, DHCP, réplications applicatives.
5. Mettre en place un VPN redondé avec contrôle d'accès par groupe.
6. Conduire un audit encadré, sauvegarder selon la règle 3-2-1 et prononcer la recette.

1.3 Ce qui est attendu à la fin du mois

ÉLÉMENT	ÉTAT ATTENDU
PARC01	GLPI, Zabbix et intranet en HTTPS (helpdesk, supervision, intranet.martinscie.lan), MariaDB locale, SSH par clé
PARC02	Réplique MariaDB et fichiers synchronisés ; procédure de bascule testée en moins de 4 h (RTO)
GLPI	13 éléments inventoriés, comptes AD, catégories du CDC, 6 tickets du scénario traités, base de connaissances
Zabbix	13 éléments supervisés, déclencheurs CARP, réplication AD, DHCP, PARC et SECU ; alertes à mbah et hnyame
VPN	OpenVPN sur la VIP WAN, authentification AD, groupe GG_VPN, aucun accès à SECU
SECU01 / SECU02	Kali opérationnel, compte kali désactivé, réplique hebdomadaire, audit autorisé et rapport
Continuité	Sauvegardes du tableau du CDC, restauration testée, dossier d'exploitation, PV de recette

CHAPITRE 2

2 Organisation du travail

2.1 Répartition des rôles

Un étudiant est **technicien applicatif et support** (PARC01, PARC02, GLPI), l'autre **technicien supervision et sécurité** (Zabbix, VPN, SECU01, SECU02). Les rôles s'inversent en semaine 3. En semaine 2, chacun joue aussi l'utilisateur qui ouvre les tickets de l'autre.

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	5 à 10 min / binôme
Hors séance	Rédaction, procédures, préparation	2 h / semaine environ

2.3 Ressources fournies

- Le dossier du projet et votre dossier d'architecture du devoir n° 1.
- Les guides de la rubrique Tutos (GLPI, Zabbix, PARC02, SECU01 et SECU02, VPN, sauvegardes, recette).
- Les ISO Debian 12 (netinst) et Kali Linux 2025 ; l'archive GLPI 10 ; les agents GLPI et Zabbix.
- Un relais SMTP de test pour les notifications ; à défaut, alertes consultées dans les interfaces.
- Un partage ou disque externe jouant le rôle du NAS de sauvegarde absent du schéma (écart n° 11).

VERSIONS IMPOSÉES Le fichier Informations_VM cite Zabbix 5 et PHP 8.1. Le dossier du projet retient **Zabbix 7.0 LTS et PHP 8.2** (écart n° 18). Vérifiez sur les sites des éditeurs la compatibilité avec GLPI 10 et justifiez-la en une demi-page.

CHAPITRE 3

3 Calendrier sur quatre semaines

TABLEAU 1 — CALENDRIER DU DEVOIR N° 2

SEMAINE	THÈME	EXIGENCES	JALONS DU POINT D'ÉTAPE
S1	PARC01 : GLPI et intranet	HLP-01, INT-01, INT-02	GLPI et intranet en HTTPS, LDAP, comptes par défaut traités
S2	Support, parc et PARC02	HLP-02, 03, INV-01	6 tickets traités, 13 éléments inventoriés, REC-10

SEMAINE	THÈME	EXIGENCES	JALONS DU POINT D'ÉTAPE
S3	Supervision Zabbix	SUP-01 à 04, RES-09	13 éléments verts, REC-12
S4	VPN, audit, sauvegarde, recette	VPN-01 à 04, SEC-01 à 05, NF-01	REC-11, REC-14, restauration, PV signé

S1

SEMAINE 1

PARC01 : GLPI et intranet

Objectif : un serveur applicatif propre et sécurisé, joignable par des noms de service, avec un certificat reconnu par tous les postes.

M1.1 Installer et durcir PARC01

- Debian 12 sans bureau, nom PARC01, 192.168.10.20/24, passerelle .1, DNS .10 et .11, NTP sur DC01.
- SSH : PermitRootLogin no, clé pour mbah-adm, sudo ; pare-feu local nftables (les flux internes ne traversent pas pfSense) ; fail2ban ; unattended-upgrades.
- Enregistrements DNS : A et PTR de parc01, alias helpdesk, supervision et intranet.

M1.2 Monter le socle web

- Apache 2 (ssl, rewrite, headers, ServerTokens Prod), MariaDB liée à 127.0.0.1 en utf8mb4, PHP 8.2 et ses extensions.
- Autorité de certification interne (AD CS sur un DC ou CA dédiée, à justifier) ; certificat pour helpdesk, supervision et intranet ; CA déployée sur les postes par GPO (INT-02).
- Trois hôtes virtuels HTTPS ; redirection HTTP vers HTTPS.

M1.3 Installer GLPI 10 et l'intranet

- Base glpidb et utilisateur dédié ; installation, suppression de install.php, protection du dossier files.
- Comptes par défaut changés ou désactivés ; annuaire LDAP vers DC01 **et** DC02 (serveur de réplique) avec un compte de service non privilégié.
- Intranet : page d'accueil simple (ou ce portail) servie par intranet.martinscie.lan.
- Rédiger la note de versions.

Jalons du point d'étape

PREUVE ATTENDUE	RÉFÉRENCE	VALIDÉ
https://helpdesk.martinscie.lan sans avertissement de certificat depuis DIRECTEUR01	INT-02	☐

PREUVE ATTENDUE	RÉFÉRENCE	VALIDÉ
Connexion à GLPI avec un compte AD ; DC01 arrêté, connexion toujours possible	HLP-01	☐
Plus aucun avertissement de sécurité sur l'accueil de GLPI	écart 21	☐
SSH de mbah-adm par clé accepté, root refusé ; règles nftables affichées	–	☐
Note de versions ; instantané `S1-fin`	écart 18	☐

PIÈGE CLASSIQUE Si GLPI ne connaît que DC01 comme serveur LDAP, plus personne ne se connecte au helpdesk quand DC01 tombe : la redondance de l'annuaire ne sert à rien. Déclarez DC02 comme réplique LDAP et testez-le.

S2

SEMAINE 2

Support, parc et réplique PARC02

Objectif : un helpdesk réellement utilisé, un inventaire complet et une réplique de PARC01 prête à prendre le relais.

M2.1 Configurer GLPI

- Entité Martins & Cie ; groupes GLPI par service ; profils : mbah Super-Admin et Technicien, hnyame Technicien des tickets Sécurité, autres Self-Service.
- Catégories du CDC : réseau, serveur, poste, compte et droits, sécurité ; règle d'attribution automatique des tickets Sécurité à hnyame (HLP-03).
- Niveaux de service : prise en compte 4 h ouvrées, résolution 2 jours ouvrés (à valider) ; notifications par courriel.

M2.2 Inventorier les 13 éléments

- Agent GLPI sur DC01, DC02, DIRECTEUR01, SECRETAIRE01, WEBDEV01, PARC01, PARC02 et SECU01 / SECU02.
- RFW01, RFW02 et le switch par découverte réseau SNMP (ou saisie justifiée) ; Freebox en saisie manuelle.
- Bonus : déploiement de l'agent Windows par GPO.

M2.3 Construire PARC02

- Debian 12, 192.168.10.21, même socle que PARC01.
- Réplication MariaDB primaire → réplique (journal binaire, utilisateur de réplication limité à 192.168.10.21) ; contrôle par `SHOW REPLICA STATUS`.

- rsync nocturne par SSH (clé dédiée) des fichiers GLPI, de la configuration Apache, des certificats et de l'intranet.
- Rédiger puis tester la **procédure de bascule** : arrêt de PARC01, promotion de la réplique, bascule des alias DNS, contrôle ; chronométrer.

M2.4 Scénario de tickets à traiter

Chaque ticket est ouvert par l'utilisateur concerné avec son compte AD, catégorisé, pris en charge, suivi et résolu. La solution doit pouvoir devenir un article de la base de connaissances.

TABLEAU 2 — TICKETS DU SCÉNARIO

N°	DEMANDEUR	CATÉGORIE	DESCRIPTION	PRIORITÉ ATTENDUE
1	ldasilva	Compte et droits	« Le lecteur Secrétariat a disparu. » (l'enseignant aura retiré Secrétariat de DL_Secretariat_RW)	Haute
2	smartins	Réseau	« Internet a coupé quelques secondes ce matin. » Analyser les journaux CARP et expliquer	Moyenne
3	cgrimeau	Poste	WEBDEV01 (Debian) doit être joint au domaine par SSSD pour ouvrir sa session avec son compte AD (écart n° 17)	Moyenne
4	hnyame	Sécurité	Une connexion SSH root a été tentée sur PARC02 : vérification et durcissement	Haute
5	smartins	Compte et droits	Arrivée d'une comptable : compte, groupe, lecture sur Administration, accès VPN	Moyenne
6	mbah	Serveur	Le basculement DHCP affiche « Communication interrompue » sur DC02	Haute

À RÉDIGER Le ticket n° 5 donne lieu à la **procédure d'arrivée d'un utilisateur**, et le ticket n° 6 à une fiche de diagnostic. Les deux sont reprises dans le dossier d'exploitation.

Jalons du point d'étape

PREUVE ATTENDUE	RÉFÉRENCE	VALIDÉ
Les 13 éléments dans l'inventaire GLPI	INV-01	☐
6 tickets du scénario résolus, catégorisés, avec suivis ; ticket Sécurité attribué à hnyame	HLP-02, 03	☐
Réplication MariaDB sans retard (Seconds_Behind_Master à 0)	–	☐
Arrêt de PARC01 : helpdesk rendu par PARC02 dans le délai, durée mesurée	REC-10	☐
Instantané `S2-fin`	–	☐

S3 SEMAINE 3

Supervision Zabbix 7.0 LTS

Objectif : voir l'état de toute l'infrastructure redondée sur un écran et être prévenu avant les utilisateurs. Les rôles du binôme s'inversent.

M3.1 Installer Zabbix 7.0 LTS

- Serveur et interface web sur PARC01 (supervision.martinscie.lan en HTTPS), base zabbix dédiée, répliquée avec glpidb vers PARC02.
- Compte Admin changé, comptes nominatifs pour mbah et hnyame, authentification LDAP.

M3.2 Superviser les 13 éléments

- Agents sur Windows (DC01, DC02, postes) et Linux (PARC, SECU, WEBDEV01) ; mode actif pour les postes en DHCP.
- RFW01, RFW02 et switch en SNMP (v3 de préférence) ; Freebox en ICMP.
- Éléments spécifiques au CDC (SUP-02) : état CARP de chaque pare-feu, résultat de `repadmin` ou compteurs de réplication AD, état du basculement DHCP et taux d'occupation de l'étendue, résolution DNS, retard de la réplique MariaDB, date du dernier rsync et de la dernière copie SECU.

M3.3 Alerter et centraliser

- Déclencheurs : double maître CARP ou aucun maître, réplication AD en échec, étendue DHCP > 80 %, service DHCP arrêté, réplique MariaDB en retard > 5 min, hôte injoignable > 3 min.
- Actions : courriel à mbah pour Haute et Désastre ; à hnyame pour les déclencheurs de sécurité ; bonus : création de ticket GLPI.
- Syslog des pare-feux et du switch vers PARC01 (RES-09) ; conservation 12 mois au plus (NF-06).
- Tableau de bord « Continuité » : paires redondées, rôle de chacune, problèmes en cours.

Jalons du point d'étape

PREUVE ATTENDUE	RÉFÉRENCE	VALIDÉ
13 éléments disponibles, données récentes	SUP-01	☐
Arrêt de RFW01 : changement de rôle CARP visible dans Zabbix	SUP-02	☐
Arrêt du service DHCP sur DC01 : alerte reçue par mbah en moins de 5 minutes	REC-12	☐
Journaux des pare-feux reçus sur PARC01	RES-09	☐
Tableau de bord « Continuité » ; instantané `S3-fin`	SUP-04	☐

POUR ALLER PLUS LOIN Simulez une rupture de réplication AD (carte réseau de DC02 déconnectée pendant 30 minutes) : quand Zabbix le détecte-t-il ? Que montre `repadmin /replsummary` au retour ?

S4

SEMAINE 4

VPN, audit, sauvegarde et recette

Objectif : ouvrir un accès distant maîtrisé, auditer, sauvegarder indépendamment de la réplication, puis faire signer la recette.

M4.1 VPN redondé

- OpenVPN sur RFW01, à l'écoute de la **VIP WAN** (VPN-01) : CA du pare-feu, certificat serveur et utilisateurs, UDP 1194, tunnel 10.8.0.0/24, AES-256-GCM, tls-crypt.
- Authentification LDAP vers DC01 et DC02 limitée au groupe GG_VPN (écart n° 13) ; règles sur l'interface OpenVPN par groupe ; **aucun accès à SECU01 et SECU02** (VPN-04).
- Configuration recopiée sur RFW02 par XMLRPC ; redirection UDP 1194 sur la box vers la VIP WAN ; test de connexion pendant une bascule CARP.

M4.2 Plateforme d'audit

- SECU01 : Kali 2025, 192.168.10.40, compte hnyame, compte kali désactivé, accès système pour mbah-adm (écart n° 14), disque chiffré.
- SECU02 : copie hebdomadaire de SECU01 (clone complet, nom, adresse .41 et MAC modifiés) ; démarrage testé.
- Faire signer l'autorisation (annexe B) ; découverte nmap puis analyse OpenVAS / Greenbone des serveurs ; rapport déposé dans le dossier Sécurité (SEC-05).

M4.3 Sauvegarde, exploitation et recette

- Sauvegardes du CDC sur le support externe : état système AD, partages, config.xml des pare-feux, dumps et fichiers de PARC01, SECU ; chiffrement, rotation, règle 3-2-1.
- Restaurer un objet AD supprimé (corbeille), un fichier d'un partage et la base GLPI sur une VM de test.
- Dérouler **les 14 tests REC-01 à REC-14** sur l'environnement complet et remplir le procès-verbal.
- Rédiger le dossier d'exploitation (planning du tableau « Organisation de l'exploitation » du CDC) et le guide utilisateur d'une page.

Jalons du point d'étape

PREUVE ATTENDUE	RÉFÉRENCE	VALIDÉ
VPN établi avec un membre de GG_VPN, refusé hors groupe ; SECU injoignable dans le tunnel	REC-11	☐
Tunnel rétabli après arrêt de RFW01	VPN-01	☐
Compte kali désactivé ; SECU02 démarre et est à jour	SEC-01, 02	☐
Rapport d'audit stocké dans le répertoire Sécurité	REC-14	☐
Restaurations réussies : objet AD, fichier, base GLPI	REC-13	☐
14 tests REC passés sur l'environnement complet ; PV signé	NF-01	☐
Instantané `S4-fin`	–	☐

CADRE LÉGAL Un scan sans autorisation écrite, ou hors du périmètre Martins & Cie, entraîne la note de 0 au critère « Audit ». Accéder ou tenter d'accéder frauduleusement à un système est pénalement sanctionné (articles 323-1 et suivants du Code pénal).

CHAPITRE 8

8 Livrables

TABLEAU 3 — LIVRABLES DU DEVOIR N° 2

LIVRABLE	CONTENU	FORMAT
Dossier technique (suite)	PARC01, PARC02, GLPI, Zabbix, VPN, SECU, sauvegardes ; 20 à 30 pages hors annexes	PDF
Note de versions	Choix argumenté de PHP 8.2 et Zabbix 7.0 LTS (rendue en S1)	PDF
Export GLPI	Les 6 tickets du scénario avec suivis et solutions ; articles de la base de connaissances	PDF
Procédure de bascule PARC	Étapes, contrôles et durée mesurée (REC-10)	PDF
Rapport d'audit	Autorisation signée, méthode, constats par criticité, recommandations, corrections	PDF
Dossier d'exploitation	Sauvegarde, restauration, bascules, arrivée et départ d'un utilisateur, planning d'exploitation	PDF
Guide utilisateur	Connexion, partages, helpdesk, VPN (1 page)	PDF
PV de recette	REC-01 à REC-14 et contrôles techniques, avec résultat, preuve, écarts ; signatures	PDF

CHAPITRE 9

9 Évaluation

TABLEAU 4 — GRILLE D'ÉVALUATION

CRITÈRE	ATTENDUS	POINTS
Serveur applicatif	PARC01 durci, HTTPS par CA interne, alias DNS, versions justifiées	3
GLPI et support	Inventaire des 13 éléments, LDAP redondé, catégories, 6 tickets traités avec qualité	3
Réplique PARC02	Réplication MariaDB et fichiers, bascule documentée et mesurée	3
Supervision Zabbix	13 éléments, contrôles de redondance, alerte démontrée, tableau de bord	3
VPN et audit	VPN sur VIP par groupe sans accès SECU, SECU02, audit encadré et rapport	3
Sauvegarde et recette	3-2-1, restaurations réussies, 14 REC, PV honnête sur les écarts	3
Points d'étape et oral	Jalons tenus, démonstration, réponses individuelles	2
Total		**20**

PÉNALITÉS Mot de passe en clair dans un livrable : **−2 points**. Compte par défaut non traité : **−1 point** par compte. Scan hors autorisation : 0 au critère VPN et audit. Retard : −1 point par jour ouvré.

9.1 Compétences du référentiel mobilisées

BLOC	COMPÉTENCE	OÙ
Bloc 1	Gérer le patrimoine informatique	Inventaire GLPI des 13 éléments, versions
Bloc 1	Répondre aux incidents et aux demandes d'assistance et d'évolution	Scénario de tickets, niveaux de service
Bloc 1	Mettre à disposition des utilisateurs un service informatique	Intranet, helpdesk, guide utilisateur, recette
Bloc 2 SISR	Exploiter, dépanner et superviser une solution d'infrastructure réseau	Zabbix, bascules, dossier d'exploitation
Bloc 3	Garantir la disponibilité, l'intégrité et la confidentialité des services	PARC02, sauvegardes 3-2-1, VPN
Bloc 3	Sécuriser les équipements et les usages des utilisateurs	Durcissement, CA interne, audit SECU01

ANNEXE

A

Journal de bord

Même modèle que pour le devoir n° 1.

MODÈLE DE JOURNAL DE BORD

DATE	ÉTUDIANT	TÂCHES RÉALISÉES	PROBLÈME RENCONTRÉ	SOLUTION / PISTE	RÉFÉRENCE VALIDÉE

B

ANNEXE

Autorisation d'audit SECU01 / SECU02

À imprimer, compléter et faire signer **avant** toute action depuis SECU01 ou SECU02.

AUTORISATION DE CAMPAGNE D'AUDIT

RUBRIQUE	À COMPLÉTER
Demandeur	Hervé Nyame (hnyame) – binôme : .....
Autorisé par	Serge Martins, PDG (rôle tenu par l'enseignant)
Fenêtre d'audit	Du ...../...../..... à .....h..... au ...../...../..... à .....h.....
Périmètre autorisé	192.168.10.0/24, à l'exclusion de la Freebox, du réseau de transit et de toute autre adresse
Actions autorisées	Découverte réseau (nmap), analyse de vulnérabilités (OpenVAS / Greenbone), tests d'authentification sur comptes de test uniquement
Actions interdites	Exploitation destructive, déni de service, bascule volontaire d'un équipement, accès aux données des partages, tout trafic vers Internet
Engagements	Instantané avant campagne, journalisation, rapport déposé dans le dossier Sécurité sous 48 h, signalement immédiat de toute découverte critique
Signatures	Demandeur : ..... Direction : .....

MOIS PRÉCÉDENT
← Devoir n° 1 – Réseau haute disponibilité et annuaire redondé

PORTAIL SISR2
Rubrique Devoirs →